



Cadena de suministro, el peligro acecha



“Solo una cultura de ciberseguridad puede ser la mayor vacuna”
(Rosa Díaz, INCIBE)



“Cada vez que inviertes en educación el nivel de fraude baja”
(Iker Osorio, Cetelem)



#ITWebinars. Transacciones electrónicas europeas: cumpliendo con eIDAS



Revista IT Trends. En busca de la conectividad inteligente

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



it Digital Security



Directora Rosalía Arroyo
rosalia.arroyo@itdmgroup.es

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

Diseño revistas digitales Contracorriente

Producción audiovisual Favorit Comunicación, Alberto Varet

Fotografía Ania Lewandowska

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

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

Cadena de suministro, el peligro acecha



Las empresas, todas, se basan en proveedores, en terceras partes para la entrega de productos o servicios a sus clientes. Esa cadena de suministro es indispensable; costaría encontrar una empresa que no interactúe con proveedores o vendedores externos. Pero al mismo tiempo, también representan un enorme riesgo de seguridad porque suelen acceder a los sistemas o recursos de las empresas, y se termina compartiendo con ellos datos confidenciales y rutas de acceso. Esa capacidad de acceder a información confidencial es lo que lleva a estos terceros, a estos proveedores, a esta cadena de suministro a convertirse en un objetivo muy tentador para los ciberdelincuentes como punto de entrada de un objetivo concreto. ¿Por qué? Porque al final se busca el camino de menor resistencia y los ciberatacantes ya saben que desde hace años las empresas están reforzando sus defensas; de forma que en lugar de lanzar ataques directos, comprometen la cadena de suministro o un proveedor clave para conseguir acceso.

De todo ello hablamos en el tema de portada de este #ITDSJulio, que viene cargado de entrevistas. Rosa Díaz, Directora general de INCIBE; Iker Osorio, CISO de Cetelem; Emilio Román, que vuelve al mercado de seguridad como vicepresidente para la región de EMEA de Bitdefender; Laia Salas, responsable de Secura by Factum y Roberto Beitia, fundador y presidente de Sarennet, son los cinco protagonistas que nos dejan una imagen de lo que está pasando en el mercado de ciberseguridad.

Analizamos el impacto que COVID-19 ha tenido en el mercado, la nueva oleada de innovación de SonicWall y Bitdefender; y, de la mano de nCipher, la importancia de eIDAS, el Reglamento Europeo para el Reconocimiento de Identidades Electrónicas que se creó con el objetivo de garantizar las interacciones electrónicas entre ciudadanos, empresas y autoridades públicas dentro de la Unión Europea.

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



itds

Sumario

Actualidad



SonicWall se adentra en el mercado de Switches

Reportaje



Impacto de COVID-19 en la seguridad empresarial

#ITWebinars



Transacciones electrónicas europeas: cumpliendo con eIDAS

Revistas Digitales



IT Trends. En busca de la conectividad inteligente



Bitdefender. El factor humano llega a GravityZone

No solo IT



Seguridad Cloud: La capacidad de extender la empresa más allá de los límites



Contexto geoestratégico de la guerra tecnológica entre EE.UU. y China

Índice de anunciantes

Netskope	IT Whipepapers
Diario de un vendedor	Encuesta IT Trends
Alsid	Thales
Cytomic	Doc Teletrabajo
Secure&IT	IT User
Sophos	IT Reseller
Bitdefender	CDR Tecnología para tu empresa
IT Webinars	

Entrevista



“Solo una cultura de ciberseguridad puede ser la mayor vacuna”

Rosa Díaz, INCIBE



“Cada vez que inviertes en educación el nivel de fraude baja”

Iker Osorio, Cetelem



“Creemos que la mayor diferencia de Bitdefender está en la tecnología”

Emilio Román



“Ahora se están prestando muchos más servicios”

Laia Salas, Secura by Factum



“La ciberseguridad siempre ha formado parte de nuestra actividad”

Roberto Beitia, Sarenet

Julio 2020



Protección para trabajadores remotos

Cloud Native, fácil despliegue y sin Hardware

Utiliza la nube para habilitar acceso remoto con seguridad para cualquier usuario



Ahora más que nunca, los empleados deben trabajar desde lugares que están fuera del perímetro de la red corporativa tradicional.

La opción tradicional de VPN supone un acceso a las aplicaciones y a la red, pero no permite establecer un control sobre movimientos laterales y accesos indebidos.

Es por ello que nació Zero Trust Network Access, una solución de seguridad diseñada para dar acceso remoto a

cualquier aplicación, reduciendo la complejidad de despliegue, gestión y administración de appliances VPN tradicionales.

Netskope Private Access (NPA) es un servicio de acceso a la red basado en la nube y bajo un modelo de Confianza Cero el cual proporciona acceso rápido y seguro a las aplicaciones privadas que están alojadas en las nubes públicas o en los centros de datos de las empresas con segmentación y de forma transparente para el usuario.

Solicita una demostración: spain@netskope.com
www.netskope.com/es



“Solo una cultura de ciberseguridad puede ser la mayor vacuna”

(Rosa Díaz, INCIBE)

Mediaba el mes de noviembre de 2019 cuando INCIBE, el Instituto Nacional de Ciberseguridad, anunciaba el nombramiento de Rosa Díaz Moles como su nueva directora general. Los más de tres años pasados como directora general de Panda Security despertaron en esta licenciada en Ciencias Exactas pasión por la ciberseguridad y un propósito: “ayudar a las personas a estar más seguras en un mundo digital”.

Rosalía Arroyo

Los más de siete meses a cargo del Instituto, donde comenzó hace un año como subdirectora de Apoyo a Empresas e I+D+i de INCIBE, arrojan un balance positivo, dice la directiva en una entrevista online. “Esta situación no ha sido fácil para nadie, pero tenemos que quedarnos con el aprendizaje y de lo que puede cambiar todo un día para otro”, asegura Rosa Díaz destacando la importancia que durante la pandemia ha cobrado la seguridad y lo “gratificante” de establecer un nivel de concienciación de ciberseguridad en ciudadanos y empresas.

Esta concienciación no sólo pasa por la multitud de charlas y eventos que organiza INCIBE, sino que ha quedado patente con el 017, un teléfono de ayuda en ciberseguridad gratuito, confidencial y disponible desde el pasado mes de febrero tanto para empresas como ciudadanos, padres, menores y educadores.

El 017 centraliza los servicios de atención telefónica que ofrece INCIBE relativos a dudas o consultas sobre ciberseguridad, privacidad, confianza digital, uso seguro y responsable de Internet y de la tecnología.

Rosa Díaz e INCIBE

¿Qué quiere aportar Rosa Díaz Moles a INCIBE? “Toda esa parte de sensibilidad en cuanto a lo que es necesario para llegar a impactar en millones de empresas y ciudadanos”, responde, asegurando que desde que conoció el Instituto sintió ganas de participar en el proyecto. Quiere aportar toda la experiencia acumulada en empresas privadas, no sólo en Panda Security sino en los más de once años pasados en Sage, “porque la diversidad, como siempre decimos, influye a la hora de contribuir y aportar a los proyectos, y de hacer también cosas diferentes”.



El de la ciberseguridad "es un sector apasionante que podría atraer mucho talento"

A día de hoy se continúa con el actual plan estratégico, que arrancó en 2017 y finaliza este 2020, "y ahora en lo que estamos enfocados es en diseñar la estrategia de cara a los próximos cinco años; y en esa estrategia se incluirá todo aquello que tiene que ver con realizar acciones de gran impacto hacia empresas, ciudadanos, apoyo la industria, etc."

Reconociendo el trabajo de sus predecesores, el objetivo de Rosa Díaz es dar un paso más hacia la visibilidad "y que España sepa la importancia que tiene la ciberseguridad". Quiere hacer de la seguridad algo 'friendly' porque "para los que no estamos en el sector el tema es más difícil". Se trata de un ámbito en el que hay que tener mucho cuidado, asegura, "pero también un sector apasionante que podría atraer mucho talento".

También bajo el mandato de Rosa Díaz, y antes de crearse el número 017, INCIBE asumía la competencia en la designación y divulgación de vulnerabilidades a nivel internacional. Explica la directiva que el Instituto se convierte así en una Autoridad de Numeración de Vulnerabilidades (CVE Numbering Authorities), en el punto de contacto en España para la recepción de vulnerabilidades descubiertas en el ámbito de la Tecnología de la Información, los sistemas industriales y los dispositivos de Internet de las Cosas (IoT).

Además de identificar los CVE, "se trabaja conjuntamente con las organizaciones responsables de los productos afectados para que se mitigue la vulnerabilidad y el problema de seguridad detectado", explica Rosa Díaz.

Centro Europeo de Ciberseguridad

La sede de INCIBE está en León, ciudad que opta a ser la sede del Centro Europeo de Competencia Industrial, Tecnológica y de Investigación en Seguridad, o Centro Europeo de Ciberseguridad, que viene a ser el principal instrumento de la Unión Europea para poner en común las investigaciones en materia de ciberseguridad. La candidatura se hizo oficial el pasado 2 de junio y para Rosa Díaz "es una excelente noticia". Dice que, entre otras cosas, este Centro Europeo de Ciberseguridad reforzaría a León, a la comunidad autónoma de Castilla y León, y a España como un hub de innovación en ciberseguridad a nivel europeo; "León ya es un importante nodo en materia de ciberseguridad y también de tecnologías de información, por lo cual sería un refuerzo y una manera de fijar población en otras zonas, no solamente en las grandes urbes de Espa-





"Este es un sector en crecimiento, con una empleabilidad muy alta, y además con salarios y empleos muy cualificados"

ña. Es una excelente noticia para todos y vamos a ver en los próximos meses cómo se desarrolla esta candidatura".

Aclara la directora que nada tiene que ver esta candidatura con el hecho de que León, al ser la sede de INCIBE ya es un Centro Espejo de la Agencia Europea de Seguridad de las redes y la información (ENISA). Explica Rosa Díaz que habrá un Centro Espejo en cada uno de los estados miembros de la Unión Europea y que su objetivo es mantener a salvo una copia de seguridad de los datos almacenados en la agencia europea.

INCIBE y COVID-19

“Reorientamos nuestros objetivos y nos adaptamos a la nueva situación”, dice le responsable de INCI-

BE cuando le preguntamos cómo se ha afrontado desde el Instituto la pandemia sanitaria de COVID-19, “una situación excepcional que ha provocado un crecimiento notable de la dependencia del acceso a internet para trabajar, para estudiar, para cualquier cosa, incluso para hablar con nuestros amigos”.

La pandemia, además “ha supuesto una mayor exposición de ciudadanos, en especial menores y trabajadores, a estos riesgos cibernéticos porque la única forma de comunicación estaba siendo la tecnología”. Durante la crisis de COVID-19 se ha visto cómo los ciberdelincuentes han diseñado ataques y utilizado técnicas de ingeniería social para adaptar sus mensajes en un momento en el que la población estaba ávida de información; en todo caso, asegura

Rosa Díaz “el propósito realmente sigue siendo el mismo con el COVID o sin él, que es engañar al mayor número posible de usuarios y empresas”. Desde INCIBE “hemos sido muy conscientes de las dificultades, y junto con otros organismos, en especial el CCN-CERT, lanzamos la campaña con el hashtag #cybercovid19 para ofrecer consejos y soluciones a ciudadanos y empresas”.

Desde las redes sociales se lanzaban mensajes enfocados en tres temáticas: protección de datos, entretenimiento seguro y teletrabajo seguro, “y hemos ido adaptando toda la comunicación que hemos ido realizando”. El resultado es una serie de boletines, infografías e información que pueden encontrarse en la página web de INCIBE, y que van desde un “Teletrabaja de forma cibersegura durante la crisis del coronavirus”, a un “Cómo detectar y prevenirse ante los fraudes y bulos que circulan en relación al COVID-19”, o un “Identificación de páginas fraudulentas de venta de mascarillas y otros materiales sanitarios”.

“La verdad es que estamos muy satisfechos de cuál ha sido el trabajo”, dice la directora general de INCIBE, que destaca también cómo la nueva forma



"El propósito del ciberdelincuente realmente sigue siendo el mismo con el COVID o sin él, que es engañar al mayor número posible de usuarios y empresas"

de trabajar "nos ha dado la oportunidad de estar en el mismo día en tres eventos diferentes", lo que ha hecho que se haya incrementado "el número de impactos que hemos realizado junto con todo tipo de asociaciones, Cámaras de Comercio y terceros que nos han pedido que estuviéramos y que pudiéramos hablar adaptando el mensaje tanto a su sector como a su problemática. La verdad es que estoy muy satisfecha de toda la llegada que hemos tenido, que INCIBE haya podido estar en medio de una situación tan especial y excepcional".

Cultura de ciberseguridad

¿Lograremos llevar la ciberseguridad a las escuelas, tener cultura de ciberseguridad? "Esos son nuestros planes también", dice Rosa Díaz. Añade que éste es un sector relativamente novedoso y que todavía hay mucha gente que no lo conoce aunque la situación de pandemia ha puesto de manifiesto su importancia; "tenemos que empezar desde el público más pequeño, desde educación primaria, para que, por un lado conozcan el sector y sepan los riesgos a los que se enfrentan, pero también para que nos demos cuenta de que este es un

sector en crecimiento, con una empleabilidad muy alta, y además con salarios y empleos muy cualificados, de forma que también se conozca como opción profesional".

Sobre la asignatura pendiente de la empresa española, dice la directora general de INCIBE que hay que tener en cuenta que se habla de pequeñas y medianas empresas. "Estamos dando pasos en cuanto a inversión, pero todavía nos queda mucho por hacer", reconoce, añadiendo que aún hoy se oye a muchas micropymes y autónomos preguntar '¿quién me va a atacar a mí?' cuando se habla de los peligros y de los riesgos que hay en Internet.

"Muchas veces no se dan cuenta de que, aunque seamos una empresa pequeña, siempre va a haber alguien que esté interesado en conseguir la informa-



"Es una excelente noticia para todos y vamos a ver en los próximos meses cómo se desarrolla esta candidatura de León como sede del Centro Europeo de Ciberseguridad"

ción, o en convertirles en punto de acceso a empresas de mayor envergadura. Y en ese punto asegura Rosa Díaz que la labor de conciencia y formación deberían de ser una prioridad, no sólo porque es la que menos inversión económica requiere dada la cantidad de material que hay, sino porque "ya sabemos que el eslabón más débil de la cadena sigue siendo el humano, y también el más vulnerable".

Añade la directiva que las personas son, o bien la mayor debilidad, o la mayor fortaleza de una estrategia de ciberseguridad. "Por muy robustos que sean los sistemas, por mucho esfuerzo en identificación y respuesta a los incidentes, por muchos recursos de los que se disponga, si realmente luego se sigue utilizando una contraseña débil, el sistema se quiebra y sólo una cultura de ciberseguridad puede ser la mayor vacuna". Como contraseña débil, una de las más populares: 123456, la misma que ha permitido hackear más de 23 millones de



cuentas en todo el mundo, según un estudio sobre vulnerabilidades publicado en Reino Unido.

En todo esto de la concienciación no sólo se menciona una adecuada elección de las contraseñas sino estar atentos a una ingeniería social "que está mucho más profesionalizada". Dice Rosa Díaz que se habla siempre del sentido común, "pero también de informar, informar, e informar para que de esta manera todos nuestros empleados, colaboradores y ciudadanos sepan hacer frente a las ciberamenazas".

Actividades

Sobre si habrá un ENISE 2020 en León... "se están reorientando todas las actividades", dice la responsable de INCIBE. Antes que ENISE le toca el turno

al [Cybersecurity Summer BootCamp](#), que este año es online. El año pasado el evento, que tiene como objetivo formar y adiestrar en las últimas técnicas para la lucha contra los ciberdelitos, la gestión de incidentes de ciberseguridad y la legislación a tener en cuenta en todos ellos, atrajo a más de 350 personas que vinieron de 53 países.

El formato online servirá este año no sólo para ofrecer seminarios y keynotes de alto nivel, sino sesiones abiertas para que todos los profesionales de la ciberseguridad puedan participar de esta iniciativa conjunta de OEA e INCIBE.

Las sesiones abiertas, dice Rosa Díaz, "nos permiten trasladar esa importancia de la seguridad y conseguir atraer a cada vez más público". El even-



Enlaces de interés...

- [INCIBE](#)
- [León optará a ser la sede del Centro Europeo de Ciberseguridad](#)
- [Incibe impulsa el emprendimiento en ciberseguridad mediante jornadas online](#)

to, añade la directiva, no trata sólo de dar a conocer los riesgos de la ciberseguridad, “sino de poder atraer talento; poder atraer público que quieran reorientar su carrera, desempleados que puedan ver en el sector de la ciberseguridad una opción para conseguir empleabilidad y desarrollar sus siguientes años profesionales”.

Compartir en RRSS



Otros eventos que organiza INCIBE para formar y atraer talento son las jornadas “Espacios de ciberseguridad” dirigidas a estudiantes. Se trata de unas jornadas técnicas y gratuitas en las que se enseña, de forma práctica y con ejercicios reales, cómo funcionan determinados aspectos de ciberseguridad. Dirigidas principalmente a alumnos de Bachillerato Tecnológico, Formación Profesional relacionada con las Nuevas Tecnologías y Carrera Universitaria relacionada con las Nuevas Tecnologías (Informática, Telecomunicaciones o similar). Asegura Rosa

Díaz que son unas jornadas “muy bien valoradas que fomentan las vocaciones en torno a la ciberseguridad”.

El plan estratégico en el que se trabaja no sólo busca llegar a millones de ciudadanos y empresas, “para nosotros es muy importante el apoyo a la industria de la ciberseguridad porque estamos convencidos de que es una oportunidad real para generar puestos de trabajo y para conseguir la independencia en ciberseguridad que necesita tanto España como Europa”. 

¿Quieres tener éxito como vendedor de TI?

Lee “Diario de un vendedor de tecnología”

DESCARGAR



Con el apoyo de
GRENKE
FAST // FORWARD // FINANCE

Editado por
it Digital
MEDIA GROUP


IT Sales
INSTITUTE

Nueva oleada de innovación en SonicWall

SonicWall se adentra en el mercado de Switches

SonicWall sigue avanzando en el desarrollo y actualización de su oferta. El camino que inició hace cuatro años, tras la escisión de Dell, le lleva ahora a adentrarse en el mercado de los switches, del que se prevé un crecimiento medio anual del 4,91% hasta los 40.467 millones de dólares para 2026, datos pre-COVID-19.

El lanzamiento de la nueva familia de switches se enmarca en la estrategia SD-Branch de la compañía, una estrategia “que busca poner orden en las LANs de las delegaciones, de las oficinas remotas”, explica Sergio García, director general de SonicWall, a IT Digital Security. Hasta la llegada de la nueva familia de switches, SonicWall ha confiado en los de Dell, pero la escisión puso en marcha un produc-

to propio, una línea completa de nuevos switches multi-gigabit, para escalar y administrar de manera rentable ubicaciones remotas o sucursales.

Explica la compañía que las capacidades complementarias de Implementación Zero-Touch ayudan a abordar la escasez de expertos en ciberseguridad al permitir un despliegue rápido de dispositivos y servicios. Las funciones SD-WAN incorporadas permiten a las organizaciones aprove-



"La tecnología SD-WAN es el futuro, claramente"

char enlaces de Internet menos costosos. Además, las organizaciones también pueden elegir modelos de licencia de suscripción rentables para controlar los costos y reducir los gastos operativos.

El momento acompaña, porque si algo ha generado la pandemia sanitaria es un aumento de los ciberataques, si algo ha provocado COVID-19 es la pérdida definitiva de perímetro y una nueva forma de trabajar en remoto. El teletrabajo ha impulsado la venta de los SonicWall Secure Mobile Access (SMA), los módulos de acceso remoto de la compañía fruto de la adquisición de Aventail en 2007, que se han convertido, según Sergio Martínez, "en la joya de la corona".

La estrategia SD-Branch, los nuevos switches es sólo la punta del iceberg. Llegamos a una nueva oleada de innovación en SonicWall en torno a sus firewalls; la plataforma Single pane of glass (SPOG) y nuevo motor de sandboxing "con un algoritmo

Boundless Cybersecurity

Esta nueva oleada de innovación, que busca dar respuesta a una realidad de TI distribuida se enmarca en la nueva estrategia que la compañía anunció en febrero y que la pandemia sanitaria ha relegado a un segundo plano. Boundless Cybersecurity, nos cuenta Sergio Martínez, se basa en el siguiente concepto: la superficie de exposición crece exponencialmente, por lo que las necesidades de ciberseguridad de las empresas también crecen, sin embargo, su presupuesto y su personal de seguridad no, por lo cual se produce un gap que crece a medida que va pasando el tiempo. La situación lleva a SonicWall a postular su estrategia Boundless Cybersecurity y establecer tres pilares.

Conocer lo desconocido. Ya que mucho de lo que corre por ahí fuera es desconocido, lo primero que tenemos que hacer es conocerlo, de forma que cuando se diseñan los productos se integran "capacidades avanzadas para detectar lo que otros no han detectado, para hacerlo en tiempo real y de forma automática, para que no necesites más personal".

Visibilidad y control. El segundo pilar va enfocado a tener control de todo lo que pasa en la infraestructura. "Por ejemplo el

lanzamiento de switches es precisamente para eso, para que no haya un silo en las delegaciones, sino que puedas controlar todo el tráfico".

Escalabilidad. El tercer pilar es que todo escale, que con la misma plataforma se pueda controlar todo, "que te permita tener inteligencia avanzada de lo que sucede, que puedas tener personal avanzado y un ecosistema de gente que te pueda ayudar". Se trata además de que la continuidad de negocio sea mucho más sencilla, que no se paguen por licencias que no se van a utilizar... "todo lo que te ayude a que lo que inviertas en esto tenga un retorno muy elevado".

Esos son los tres pilares, esta es la Boundless Cyber Security.





"Pasada la necesidad inmediata, llega el momento de dejar que el firewall asuma su tarea mientras se colocan módulos de acceso remoto ya sean físicos, virtuales o en la nube para racionalizar el acceso a la red".

muy potente de detección de malware que detecta cosas que los demás no detectan", y que está pendiente de patente; y otros temas relacionados con los accesos o el cloud de los que por ahora no se puede comentar demasiado.

Teletrabajo

Sobre el teletrabajo, explica Sergio Martínez que la premura con la que se tuvo que hacer frente a la

situación llevó a muchos a establecer accesos remotos a través de los firewalls, "pero los firewalls no están preparados para eso, porque a medida que vas metiendo cada vez más usuarios concurrentes, y el firewall va asumiendo cada vez más líneas de comunicación seguras con los empleados distribuidos, el rendimiento del firewall cae y se ve comprometido".

Pasada la necesidad inmediata, llega el momento de estudiar las cosas con calma, llega el momento de "dejar que el firewall asuma su tarea mientras se colocan módulos de acceso remoto, ya sean físicos, virtuales o en la nube, para racionalizar el acceso a la red".

Ya sea un firewall, un switch o un módulo de acceso remoto, clave en su funcionamiento es Capture Security Center, la consola de gestión de la compañía "desde la que analizamos, detectamos y damos respuesta a los incidentes de seguridad". Añade el director general de SonicWall en España que un partner puede gestionar desde ahí todo su parque de máquinas instaladas, gestionar servicios, etc., "en general desde lo más básico a lo más complejo".

Por cierto, que en esta oleada de innovación llega Networks Security Manager (NSM), una actualización de Capture Security Center desarrollado con tecnologías de código abierto "que mejora la escalabilidad, la conectividad con otros módulos, tiene APIS más avanzadas. Este upgrade nos va a permitir hacer cosas muy potentes".

Lo que parece claro, en opinión de Sergio Martínez, es que las oficinas dejarán de ser lo que eran.

Enlaces de interés...

- | [SonicWall añade funcionalidades SD-WAN a su nueva oferta de switches](#)
- | ["SASE es un nuevo modelo de seguridad" \(Luis Fisas, SonicWall\)](#)
- | [SonicWall asegura el trabajo remoto con el modelo Boundless Cybersecurity](#)

Entre otras cosas, la conectividad es mucho más fácil y asequible gracias a la tecnología SD-WAN, "que la empresa española está empezando a incorporar", quizá no tan rápido como parecía, pero es el futuro claramente.

La nueva realidad pasa por Boundless Cybersecurity o Ciberseguridad sin Límites, sin Perímetro de SonicWall que controla las amenazas más evasivas y de vanguardia para proteger una fuerza laboral ilimitada en la que conviven usuarios remotos, móviles y habilitados para la nube. El objetivo es proteger a las organizaciones en una variedad de vectores de ataque, que incluyen redes, correo electrónico, acceso móvil y remoto, nube, aplicaciones SaaS, endpoints, dispositivos IoT y Wi-Fi. 

Compartir en RRSS



ALSID FOR **ACTIVE DIRECTORY**



Fix weaknesses before hackers exploit them
Detect & respond to attacks in real-time



“Está demostrado que cada vez que inviertes en educación el nivel de fraude baja”

(Iker Osorio, Cetelem)

Cetelem tiene motivos más que suficientes para ser una de las financieras más exitosas del mercado. Marca comercial de BNP Paribas Personal Finance, Cetelem está especializado en crédito al consumo, está establecida en más de 30 países y suma más de 27 millones de clientes en el mundo. En España Iker Osorio es la persona encargada de garantizar la ciberseguridad de una empresa que pertenece a uno de los sectores más regulados, la banca, y más atractivos para los ciberdelicuentes.

Rosalía Arroyo

Fotografía: Ania Lewandowska

El sector se enfrenta, además, a una serie de retos, empezando por una transformación digital meteórica que ha llevado al sector a pasar, en pocos años, de una banca tradicional a una banca online; “y ahora estamos yendo directamente a la banca móvil”. Para Iker Osorio esta evolución es uno de los grandes desafíos a los que se ha enfrentado el sector; “no se trata de una transformación digital, sino de una transformación digital móvil”, dice el

CISO de Cetelem, añadiendo que tan importante como el agregar nuevos servicios y la securización de los mismos es mantener la experiencia del usuario; “para mí, desde el punto de vista del cliente, es uno de los grandes retos”.

Habla también Osorio de los desafíos ocasionados por la regulación, y no sólo menciona la famosa GDPR sino PSD2, por la que “nos vemos obligados a liberar información que tenemos de nuestros clientes hacia terceros, para que la competencia



sea más sana, más abierta". Dice el CISO de Ce-
telem que, junto con el sector telco, la banca es el
que más volumen de datos tiene de los clientes,
información que hay que asegurar adecuadamente.
Añade que es importante proteger la información
relacionada con los hábitos de consumo del cliente
y que una de las cosas que traerá el futuro, desde
el punto de vista del negocio, "es hacer valor de esa
información de los datos".

Planteamos en este punto de la entrevista el pa-
pel que podrían desempeñar las redes sociales con
la información que manejan. Y es que desde hace
años se menciona la posibilidad de que una de las
redes sociales más populares pudiera colaborar
con las entidades financieras en temas de rating y
scoring de los usuarios y clientes comunes. "Noso-
tros no lo estamos utilizando ni estamos cerca de
utilizarlo", dice Iker Osorio, explicando que hacerlo
tiene implicaciones en protección de datos bastante
grandes; "parece una tecnología interesante, no te
voy a decir que no, pero creo que todavía queda
algún tiempo para que eso lo veamos, al menos de
manera generalizada".

El CISO y el código penal

¿Cuál es el futuro del CISO? No cabe duda de que
la evolución del CISO en los últimos años ha sido
importante; la figura ha ido cogiendo cada vez más
peso y una de las palancas para que esto ocurrie-
ra ha sido la regulación; "la regulación ha hecho
no sólo que nosotros tengamos que estar ahí, sino
que tengamos unas funciones, unas obligaciones

"Se empieza a oír el que los CISO puedan tener
una responsabilidad penal en caso de que no hagan
su trabajo como deben"

y unas responsabilidades". Espera Osorio que la
regulación siga evolucionando y apunta a que "se
empieza a oír el que los CISO puedan tener una
responsabilidad penal en caso de que no hagan su
trabajo como deben. No me gustaría que se avan-
zara por ahí, pero creo que puede ocurrir y, según
en qué sector, sería razonable pensarlo".

No parece justo que esto ocurriera, que se le pue-
da exigir ese nivel de responsabilidad a un CISO
mientras que admite y protege a los clientes incluso

cuando utilizan los servicios sin garantías, en dis-
positivos sin ningún tipo de solución de seguridad o
incluso rooteados, en redes inalámbricas gratuitas
que pueden ser espiadas... Ante esto explica Iker
Osorio que se están trabajando en algunas accio-
nes; "PSD2, por ejemplo, ya requiere que hagamos
algún tipo de actividad relacionada con el aware-
ness externo, es decir, educar a nuestros clientes
para que sean conscientes de las medidas de se-
guridad que tienen que tener con sus dispositivos".



◀ "Parece una obviedad que un equipo tenga antivirus, que un equipo esté actualizado..., pero hay muchas dificultades detrás de eso"

Los clientes, dice, ya no sólo utilizan una contraseña, sino un segundo factor de autenticación, "y eso ayuda a proteger la actividad del propio cliente".

Si un cliente no es consciente, o no usa sus credenciales con la debida diligencia, puede ser víctima de un fraude y de momento el sector financiero lo asume entendiendo que no existe negligencia, dice Osorio; "creo que ningún cliente quiere que le roben información o que le roben su dinero", y añade que educar a los clientes impacta directamente en las cuentas de la compañía porque "está demostrado que cada vez que inviertes en educación este nivel de fraude baja". De forma que más allá de la tecnología, de poner un segundo factor de autenticación o de poner todos los controles técnicos a nivel de ciberseguridad que se puedan, la concienciación del cliente es vital.

La concienciación al cliente pasará por explicarle por qué se ha vulnerado su credencial de acceso cuando se detecte que esto haya pasado, cómo puede evitarlo y pedirle incluso que reinicie su dispositivo o que acuda a su informático de confianza para que formateen su ordenador porque se ha detectado que tiene algún tipo de malware, "y llegará un punto en que evolucionaremos más todavía, poniéndonos del lado del cliente todo lo que se pueda. Creo sinceramente que esto llegará y que además será beneficioso, tanto para el cliente como para las entidades".

Es más, añade Iker Osorio que "no es descabellado pensar que un cliente tenga un rating mejor porque tenga una certificación en seguridad". Es decir, si un cliente tiene un equipo que tiene una

"Nosotros últimamente estamos encontrando muy interesante lo relacionado con el control de accesos privilegiados y control de accesos técnicos"

solución de seguridad, tiene además un firewall local... tendrá un rating mejor y un nivel de riesgo a fraude menor, "y esto no afecta sólo a la banca, afecta a las telco y otros muchos servicios a través de los cuales puede haber pérdida financiera".

Soluciones

Decíamos al comienzo que Cetelem es parte del grupo BNP Paribas; "somos un eslabón pequeño de un grupo muy grande y estamos muy dirigidos por la casa", dice Osorio explicando que a la hora de escoger tecnologías lo que hay es un catálogo muy cerrado establecido desde una central que tiene como objetivo consolidar. De forma que "el 80% de mi tecnología ya viene prefijada", porque "si yo quiero desplegar un SIEM y BNP Paribas tiene un SIEM preferido, muy probablemente nos vamos a ir al SIEM que utiliza BNP Paribas".

Con respecto a la adopción del cloud, es también la central quien toma las decisiones. Los recursos con lo que se cuentan han permitido crear una cloud privada que es utilizada por el grupo, por todas las entidades de BNP Paribas en todo el mundo. De esta forma, "la directriz es evitar, en la medida de lo posible, utilizar servicios en la nube

pública y utilizar los servicios en la nube privada de BNP Paribas".

Cuando no se decide desde la central, ¿cómo se escoge entre decenas de opciones? Aquí entra

en juego "el conocimiento de la comunidad". ¿Y la comunidad es...? "Los equipos de ciberseguridad de las empresas, de las consultoras, de las empresas de servicios, de todo. Hablo de todos. No hablo solo de los CISO, hay una comunidad de ciberseguridad que es muy importante y tiene el un tamaño razonable como para tener mucha experiencia, pero para que a su vez sea muy utilizable. No estamos hablando de que lancemos preguntas a millones de usuarios sino que son grupos todavía muy gestionables y que son lo suficientemente amplios



como para que preguntes: Oye, necesito un servicio, una solución, ¿qué usáis cada uno? ¿Qué os parece que es lo mejor? ¿Qué es lo peor? Funciona mucho. Nosotros no vamos a ser los que empezemos a utilizar un servicio súper novedoso; muy probablemente antes de que nosotros nos metamos como referencia inicial de un producto en España habrá otros X que lo estén utilizando. Utilizamos tecnología que está sobradamente contrastada”.

Seguimos hablando de soluciones... y servicios, que se consolidan también desde la central “para que sean comunes y homogéneos”. La buena noticia, explica Iker Osorio es que “se ha montado un servicio de operaciones de seguridad compartido para todas las filiales de BNP Paribas, y se ha elegido Madrid como el sitio en el que va a estar ubicado, con lo cual, evidentemente, para nosotros va a ser más sencillo”. La parte más operativa se realizará por tanto en ese centro de servicios compartidos, y los servicios más especializados, o de más nivel “lo llevaremos de manera interna o con proveedores que tengan más experiencia o nivel de conocimiento”.

Nivel de seguridad

¿Cómo valoras el grado de sensibilidad que la empresa española tiene en todo lo relativo a la seguridad de la información? Responde Iker Osorio que si uno de los elementos que ha impactado en la evolución del CISO ha sido la regulación, el otro han sido las incidencias. Mucha gente se sigue acordando de Wannacry y todo el impacto que



"En términos generales, las amenazas internas se tratan dentro de una estrategia de operaciones de riesgo"

tuvo; “quizá pensábamos que Wannacry iba a ser un evento especial y único, pero unos meses más tarde fue NotPetya y durante el año pasado hubo montón de empresas, entre septiembre y diciembre, que también tuvieron incidencias de ransomware. Ya no te voy a hablar de las fugas de información masivas durante el año 2018- 2019, que también han sido importantes”.

Si al comienzo se mencionaba la regulación como un potenciador del papel del CISO, se añaden ahora las incidencias como otro gran impulsor que ha colocado a los responsables de seguridad de la información de las empresas en los comités de dirección son las incidencias. Las incidencias son “lo que al final va a dotar de recursos al CISO”.

Para el CISO de Cetelem, la evolución de la relación de la empresa española ha sido grande, tanto como las incidencias, “porque van de la mano”. Las inversiones, asegura, también han aumentado, “pero queda mucho por hacer. Todo lleva un tiempo”.

Menciona a la pyme donde los medios son más limitados; “yo creo que hace falta quizá concienciar un poco a ese nivel y luego generar fórmulas alternativas a la figura del CISO en el nivel de pequeña y mediana empresa. Se están viendo ya fórmulas muy interesantes de CISOs virtuales, de CISOs como servicio, y creo que es un negocio que debería potenciarse muchísimo”.

Insider Threats

Un reciente informe de Ponemon Institute, 2020 Cost of Insider Threats: Global Report, indica que



"Se están viendo ya fórmulas muy interesantes de CISOs virtuales, de CISOs como servicio, y creo que es un negocio que debería potenciarse muchísimo"

las amenazas internas han crecido un 47% en los dos últimos años. Estas amenazas internas son el germen de muchos incidentes de seguridad y para muchos responsables de seguridad son una de las principales preocupaciones. ¿Quién puede ser una amenaza interna? No sólo hablamos de empleados, hablamos también de clientes, usuarios, proveedores... Hay, como dice Iker Osorio, "diferentes escenarios de riesgo por cada casuística". Frente a los empleados se despliegan controles que monitorizan su actividad o los accesos. En todo caso, dice también el directivo que no se trata de estar vigilando a la gente, "sino de hacer un poco de Threat Intelligence. Buscamos estar en ese nivel de madurez", un nivel que establezca que frente a una serie de

patrones de actividad se pueda establecer que dicha actividad es sospechosa. Es decir, "no se trata de vigilar a la gente, pero sí se trata de ver dónde puedes tener el riesgo o no".

En cuanto a los clientes... "existen controles, pero más enfocados a áreas de fraude con herramientas de scoring o de rating". En este caso explica Iker Osorio que no se trata tanto del cliente, sino del riesgo, "y en función del riesgo de transacción eres capaz de desplegar una serie de controles u otros".

En términos generales, las amenazas internas se tratan dentro de una estrategia de operaciones de riesgo. De esta forma la gente que tiene acceso a datos, que administra las bases de datos o sistemas, siempre va a tener el mayor nivel de control

posible, "no sólo con controles de acceso técnicos, sino que además tendrá su segundo factor de autenticación, monitorización de actividad, etc. Luego a nivel de clientes, las actividades más sospechosas tendrá otro tipo de controles, como puede ser una autenticación facial, una prueba de vida, etc."

Tecnologías imprescindibles

"Todas las que se pueda, aunque también va en función del negocio y recursos que tengas", responde Iker Osorio cuando le preguntamos qué tecnologías de seguridad son imprescindibles tener en una empresa.

Para el CISO de Cetelem son básicas las herramientas de protección de la infraestructura, como puede ser un firewall, o IPS, un WAF... Además, "nosotros últimamente estamos encontrando muy interesante lo relacionado con el control de accesos privilegiados y control de accesos técnicos".

Habla Osorio del Pack de CISO 1.0, un pack básico en el que tienes que tener, "sí o sí, protección de red a nivel de sistemas, antivirus, parcheos, hardenizado y gestión de vulnerabilidades. Y luego, que quizá no se le da tanta importancia como debería, pero para mí es tanto o más importante que todo lo que te he comentado, es saber qué tenemos en la casa, porque muchas veces tenemos unos procesos de control magníficos, pero que no están aplicados a todos los activos. De forma que herramientas de gestión de inventario y de descubrimiento son tanto o más importantes para un nivel de seguridad confiable". A continuación, añade Osorio



"Quizá pensábamos que Wannacry iba a ser un evento especial y único, pero unos meses más tarde llegaba NotPetya"

"ya podemos meter en temas de threat Intelligence interno/externo. Y Threat Hunting para mí ya es para nota, no es algo tan básico".

Lo del Pack del CISO me ha hecho gracia... "Sí, es que nos parece una obviedad que un equipo

tenga antivirus, que un equipo esté actualizado..., pero hay muchas dificultades detrás de eso. Una cosa es que tengas una empresa pequeña y sea gestionable, y otra cosa es que empieces a tener cierto tamaño, empresas en los que los activos TI

Enlaces de interés...

- ["Un servicio gestionado puede ser tan bueno como estés dispuesto a hacerlo" \(Iván Sánchez, Sanitas\)](#)
- ["La figura del CISO ha evolucionado bastante, y más que tiene que evolucionar" \(Mónica de la Huerga, Sopra Steria\)](#)

se cuentan por decenas de miles, tienes que tener unas herramientas automáticas muy avanzadas y tienes que tener los ambientes de IT muy peinados para conseguir ese básico, pero creo que es necesario".

Dice también el CISO de Cetelem que debe partirse de un básico para seguir creciendo y que a veces es un error ir a la estrategia más avanzada; "los proveedores siempre van a ofrecernos la solución mágica que, sin ningún tipo de esfuerzo va a ser capaz de no sólo detectar, sino de alertar y detener el ataque más sofisticado, y de repente nos damos cuenta de que tenemos la casa sin barrer en cosas como prevención más que detección". 

Compartir en RRSS



De la — hipótesis a la — caza

Threat Hunting: Zero Trust y Analítica de comportamiento

Nuestros servicios de **Threat Hunting e investigación** estudiarán y clasificarán todos los comportamientos de aplicaciones, máquinas y usuarios para erradicar las ciberamenazas avanzadas en tu entorno corporativo.



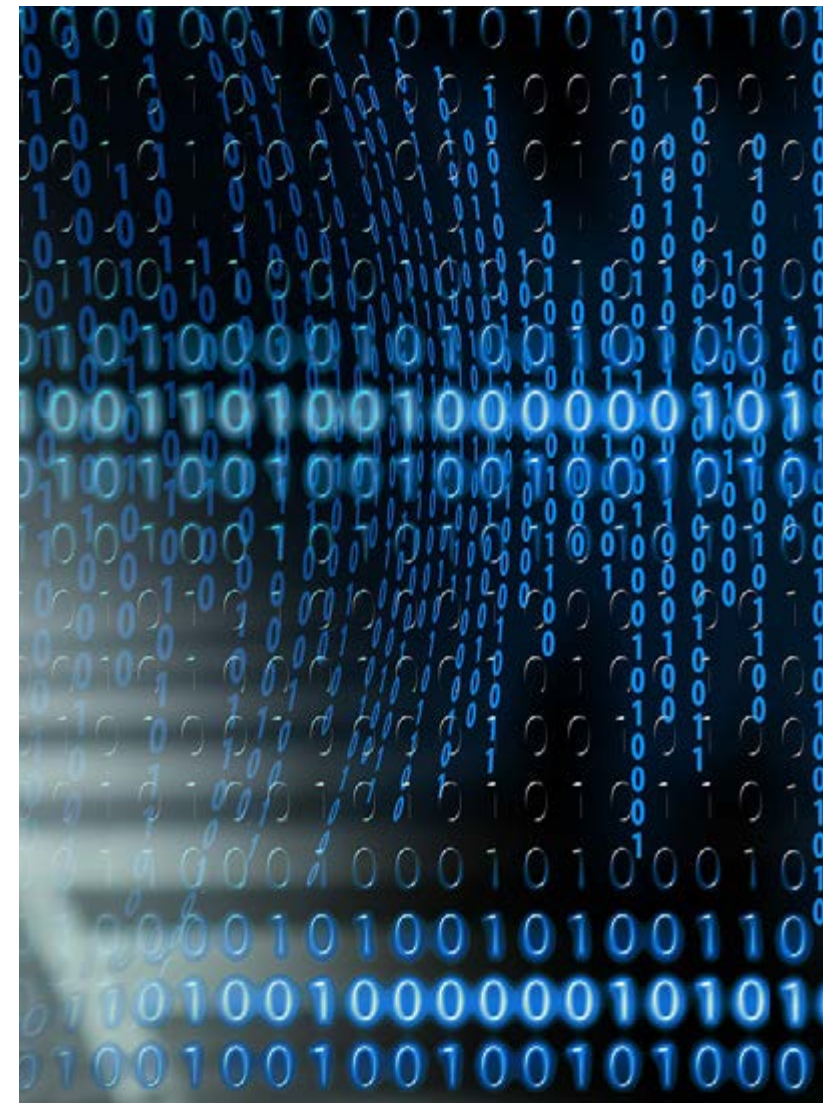
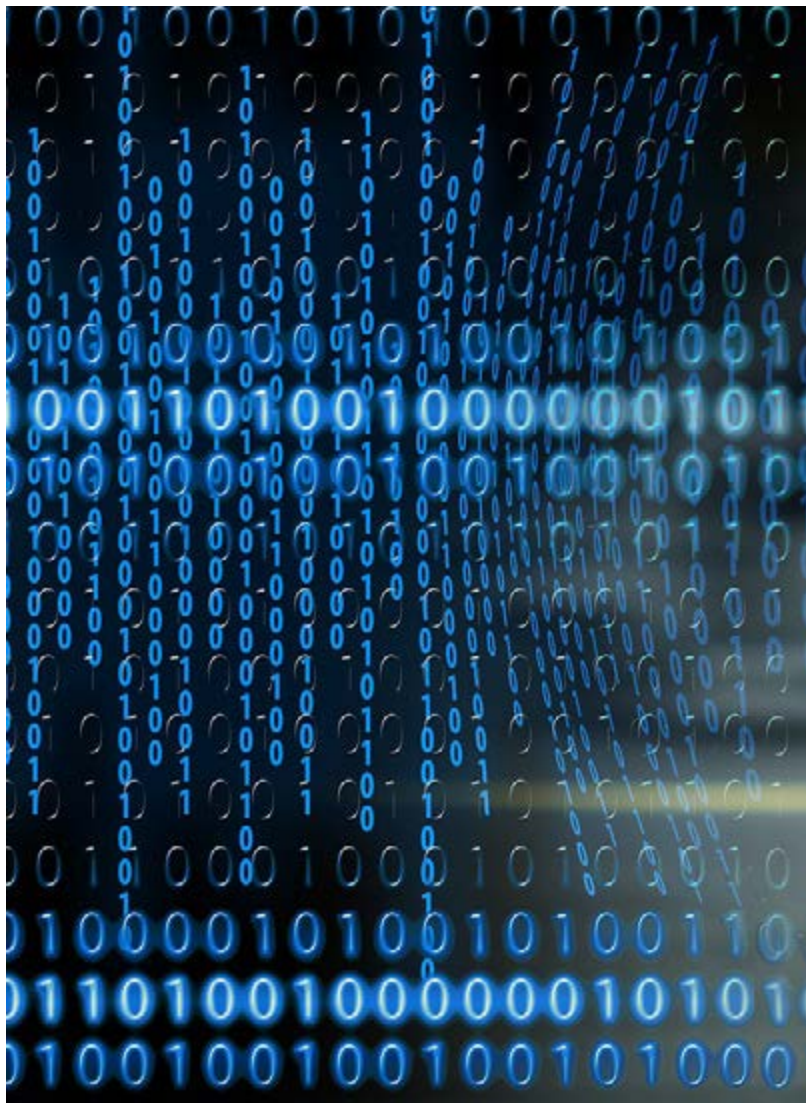
“Creemos que la mayor diferencia de Bitdefender está en la tecnología”

(Emilio Román)



Tras casi once años en Fortinet, donde acabó como vicepresidente de ventas de EMEA y APAC, y cinco años en Scality, un proveedor de almacenamiento cloud, Emilio Román vuelve al mundo de la seguridad y lo hace como vicepresidente de EMEA de Bitdefender.

Dice que en realidad nunca ha estado muy desligado del mundo de la seguridad, que lo encuentra “igual que lo dejé” en cuanto a empresas e individuos, no así en cuanto a tecnología “que ha cambiado radicalmente en los últimos años”, cuando se ha roto el perímetro de seguridad, la migración al cloud ha avanzado y temas como el IoT, los contenedores o el 5G se han convertido en el próximo campo de batalla para la ciberseguridad.



En los últimos años Bitdefender, fundada en 2001 en Bucarest, ha comprado tres empresas: Profil Technology, en 2017, y SMS eTech y RedSocks Security en 2018. En los últimos años el mundo del endpoint mira hacia los fabricantes de EDR y ha dado la bienvenida a nuevos entrantes en un mercado ya saturado con multitud de empresas.

Trabajo en equipo, independientemente de que se trabaje desde casa, en la oficina, o incluso en otro país, y una gran experiencia con el canal de distribución son dos de las cosas que Emilio Román quiere aportar a Bitdefender; “no solo en España, sino en toda Europa, tengo una larga experiencia y trayectoria de trabajo con partners, con un canal de

distribución a distintos niveles. Yo creo que, modestamente, es lo que puedo aportar”.

En 2011 Bitdefender lanza su oferta para empresas, un negocio que actualmente se reparte al 50% con el negocio de consumo. El nivel de crecimiento de ambos negocios es muy dice, asegura Emilio Román, asegurando que “disponemos de una tecnología y de un producto para securizar las mayores y más complejas infraestructuras”, un producto que, además, es muy fácil de usar y fácil de gestionar, con lo que no es un requerimiento el que las empresas dispongan de un equipo muy experto “sino que la misma tecnología, con la misma protección ante todo tipo de ataques, puede ser

utilizada por organizaciones y empresas de menor tamaño”.

El crecimiento del negocio empresarial y el de consumo es muy similar, “pero desde luego hay una grandísima apuesta por parte de Bitdefender en el sector empresarial”.

Sobre el peso que tienen los servicios gestionados dice el vicepresidente de EMEA que una de las tendencias que va a acelerar la pandemia sanitaria es la adopción de los servicios gestionados. Más de un 20% de los productos y soluciones de Bitdefender se entregan a través de proveedores de servicios de seguridad gestionados, “y es una parte del negocio que crece más que el resto”. Lo que todos

Impacto de la pandemia

“La pandemia no cambia el panorama, pero probablemente acelere las tendencias que ya vienen desde hace tiempo”, responde Román cuando le preguntamos si la crisis de COVID-19 cambiará los hábitos de compra de seguridad de las empresas.

No sólo habla de tendencias en cuanto a la utilización de la tecnología, sino en la manera de adquirirla. Reflexiona en que muchos de los decisores de compra en las empresas son milenials, con los que no solamente la facilidad de utilización, la facilidad de gestión, sino la



sencillez de adquisición de la tecnología es vital.

Asegura Román que “la facilidad de adquisición y de pago es absolutamente clave. Es nuestra parte del negocio de seguridad gestionada; trabajamos con nuestros partners y con plataformas digitales que permiten la adquisición fácil, la adquisición por uso, y el trabajo con suscripciones y no con licencias. Creemos que es una de las tendencias que está siendo acelerada y que va a ser acelerada por la situación actual de la pandemia”.

por uso mensual. Ahí es donde estamos, sin lugar a dudas”.

Guerra en el endpoint

“Nosotros no somos un nuevo fabricante que apuesta por una posible oportunidad de negocio, sino que venimos invirtiendo ahí desde hace muchísimos años”. Esta es la respuesta de Emilio Román cuando planteamos qué opina de la entrada de nuevos actores en el mercado de la seguridad endpoint. No sólo hablamos de un grupo de nuevas empresas (CrowdStrike, SentinelOne, Carbon Black...) que dieron un paso más allá de las soluciones antivirus/antimalware tradicionales hacia el nuevo concepto de EDR que empresas más asen-

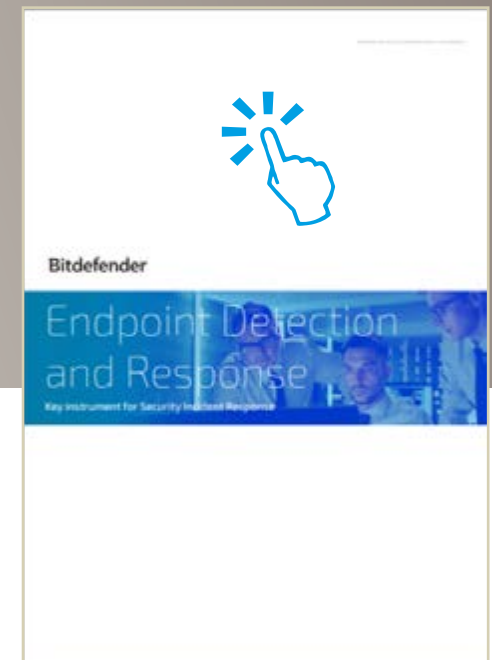


buscan, tanto las organizaciones como los partners, “es la facilidad de utilización de nuestros productos, así como la facilidad de adquirirlo, la posibilidad de comprarlo como un servicio, con una facturación



BITDEFENDER EDR

Para ayudar a los equipos de seguridad en el proceso de respuesta a incidentes Bitdefender desarrolló GravityZone Ultra, una plataforma de EDR y protección de endpoints de última generación integrada y fácil de usar, diseñada para proteger a las empresas contra las amenazas más sofisticadas.





"La innovación tecnológica en Bitdefender es clave no sólo en la realidad de hoy, sino de lo que esperamos que venga en el futuro"

tadas en el mercado de seguridad endpoint tardaron en adoptar, sino otros jugadores que amplían su alcance más allá de la seguridad de red para proteger el puesto de trabajo o los dispositivos móviles (Fortinet, Check Point, Palo Alto), etc.

Reconoce el directivo que "hay una clara tendencia del paso de protección del puesto de trabajo, de soluciones antivirus más tradicional a EDR e incluso a MDR"; insiste en que "la apuesta por la tecnología por nuestra parte no viene en los últimos años,

viene de hace muchísimos años"; y asegura que la compañía dispone de una base de clientes enorme en los que "el salto a EDR, a MDR, es sólo un upgrade de las soluciones existentes con la mejor de las tecnologías y sin tener que empezar desde cero".

El mercado de seguridad endpoint, que ha recuperado gran protagonismo ante la pérdida de un perímetro tras el que se escondieron durante años los puntos finales de las amenazas es una gran oportunidad de negocio, "pero creemos que solo se puede triunfar con la mejor de las tecnologías y creemos estar en posesión de ellas".

Innovación

"Nos consideramos como uno de los mayores innovadores a nivel global en ciberseguridad", dice Emilio Román, recordando que la compañía ya securizaba el IoT en 2015, con un producto llamado Bitdefender Box; y hacía malabares con la inteligencia artificial y el machine learning aplicado a la seguridad desde 2008. "Creemos que la mayor diferencia de Bitdefender está en la tecnología", asegura. De los más de 1.600 empleados, la mitad están dedicados a la investigación y desarrollo y, según Román, un tercio de las empresas de ciberseguridad en el mundo utilizan tecnología Bitdefender.

La innovación tecnológica en Bitdefender es clave "no sólo en la realidad de hoy, sino de lo que esperamos que venga en el futuro, es decir, 5G con aplicaciones de mucha más alta velocidad y, por tanto, con muchos más dispositivos conectados;

Enlaces de interés...

- I [Bitdefender anuncia soluciones de ciberseguridad gratuitas para las organizaciones sanitarias](#)
- I [Bitdefender ofrecerá Inteligencia de Amenazas a través de ThreatConnect](#)
- I [Nueva vulnerabilidad, irreparable, en procesadores Intel](#)
- W [Bitdefender EDR](#)

Quantum computing, que probablemente, junto con inteligencia artificial, va a implicar un cambio muy grande tanto para proveedores de servicios como para cibercriminales. Creemos que estamos ante una gran disposición de proveer de seguridad hoy, mañana y en los próximos cinco y diez años".

En todo caso, finaliza Emilio Román asegurando que la estrategia de la compañía es extraordinariamente clara: seguir ofreciendo una solución tecnológicamente a la cabeza, con una organización y un grupo de partners que directamente miran al canal de distribución con el que trabajamos. 

Compartir en RRSS



CIBERSEGURIDAD EN LA DESESCALADA DE LA COVID-19

& Promoción especial
Auditorías y seguridad gestionada

& Privacidad vs. COVID-19
¿Qué medidas de contención pueden implementar las empresas?

& Adecuación a la normativa e-commerce
¿Cómo adaptar una web para vender de forma online?

+ INFO



El impacto de COVID-19

en la seguridad
de las empresas

Bárbara Bécares

Julio 2020

El cambio en las rutinas a la hora de trabajar, de comunicarse con otras personas y de usar dispositivos personales para tareas empresariales que, en muchos casos, se están haciendo en remoto, tiene en riesgo las informaciones de las empresas. La incertidumbre por COVID-19, un virus contagioso que puede ser letal, lleva a las personas a estar más ansiosas por conseguir información y a fiarse de cualquier app o web para ello. Los ciberdelincuentes no pierden el tiempo y aprovechan la circunstancia.



El coronavirus nos ha llegado de la mano de una serie de cambios en las rutinas y en las formas de relacionarse y trabajar que afectan enormemente a la seguridad informática. El distanciamiento social que las personas de muchos países del mundo se han visto obligadas a acatar para frenar la expansión de este nuevo virus COVID-19 ha impulsado el uso de las tecnologías aún más que antes. Las videollamadas son una de las formas de comunicación más usadas, tanto para momentos de ocio como en entornos laborales. Muchas personas mantienen el teletrabajo, a pesar de que la vida va volviendo a eso que han llamado la nueva normalidad.

El pasado mes de marzo, la [Europol publicaba un estudio](#) en el que analizaba cómo los criminales van sacando partido de estas nuevas dinámicas por la situación vivida debido a COVID-19. Según señala, el número de ciberataques ha aumentado de forma exponencial, a medida que los ciberdelincuentes han adaptado sus ataques a la situación y además han “capitalizado las ansiedades y temores de la población”, con la propagación de campañas de ransomware y phishing escondida, en muchas



OCHO ACCIONES PARA SOBREVIVIR A COVID-19



CLICAR PARA
VER EL VÍDEO

ocasiones, de información y consejos para hacer frente a la pandemia.

El informe de la Europol también afirmaba que estos [ataques](#) tienen la posibilidad de crecer mientras las personas utilizan servicios online mucho más que nunca antes y con equipos que tienen en casa y que, en muchas ocasiones, carecen de protección.

Ante este panorama, encontramos que la ciberseguridad es una herramienta esencial. Las empresas tecnológicas tienen la oportunidad de mejorar sus

servicios y llevarlos a más clientes. En las siguientes líneas encontrarás un resumen a las principales amenazas actuales y unas ideas que empresas de ciberseguridad y CIO y CISO encargados de estrategias de protección deben adoptar frente al mundo de la “Nueva Normalidad”.

Para arrancar, hace falta recordar que un estudio realizado por BitDefender en España, afirma que los ataques relacionados con Social Media/Chatbots se han incrementado en un 38% y los relacionados con IoT, ciberguerra y phishing/whaling en

casi un 34%. A nivel global sobresale el incremento de los ciberataques dirigidos a la cadena de suministro, con un 38% por encima de lo habitual.

La desinformación como caballo de Troya

En marzo de 2020, el [CIBER Elcano](#) se hizo eco de avisos emitidos por la Organización Mundial de la Salud (OMS) que avisaban de que la pandemia vendría acompañada de acciones de desinformación y cibercriminalidad. Según los expertos, la bautizada como infodemia, ayudaría a COVID-19 a desplegar amenazas a través de la desinformación. Una sociedad sedienta de acceder a fuentes que respondan dudas en plena situación de incertidumbre, se ha mostrado más vulnerable a abrir enlaces dudosos que llegan acompañados de ataques.

El Centro Criptológico Nacional de España también presentó en el mes de marzo, viendo la situación que estaba llegando, un documento en el que aborda unas recomendaciones básicas ante las campañas de malware y de desinformación que



TECNOLOGÍA SD-WAN PARA POTENCIAR EL ESPACIO DE TRABAJO DIGITAL

La tecnología SD-WAN ayuda a las empresas a aprovechar al máximo su inversión, independientemente de que las personas trabajen desde una sucursal o desde una ubicación remota lejos del centro de datos. Permite utilizar todo el ancho de banda disponible, optimizar el rendimiento para aplicaciones virtuales, Web y SaaS como Office 365, además de otras aplicaciones de uso intensivo de ancho de banda como VoIP y garantizar conexiones siempre listas con la mejor calidad posible.



se están aprovechando de la pandemia del coronavirus. Como consejos para el usuario común, se recomienda nunca descargar aplicaciones que no sean oficiales ni abrir enlaces de los que no se está seguro del origen. Es algo común que cualquier cibernauta debería aplicar a la hora de acceder a Internet en cualquier momento, pero ahora ha tomado mayor relevancia por la gran cantidad de contenidos dañinos rulando por la Red y las redes sociales.

Todo esto, además de difundir información totalmente falsa que puede incluso ser perjudicial (por ejemplo, esas ideas de que COVID-19 pueden curarse con productos que, en realidad son perjudiciales para el organismo humano), consigue meter en millones de ordenadores virus capaces de robar información o secuestrar datos.

Durante las últimas dos semanas de marzo, la actividad maliciosa en la Red aumentó drásticamente, con una media diaria de unos 2.600 ciberataques,

de los cuales el 84% se trataba de phishing o suplantación de páginas web, según los expertos de Check Point Software Technologies.

Además, un estudio de ESET ha alertado de un ataque de phishing en el que se suplanta la identidad del Ministerio de Trabajo amenazando con una inspección a la empresa ante una supuesta denuncia. El resultado termina siendo la descarga e instalación de un malware en el sistema.

El Teletrabajo en tiempos de COVID-19: un alivio y un riesgo cibernético

Gracias a las herramientas tecnológicas, muchas empresas y muchos trabajadores y trabajadoras au-

tónomos han podido mantener su actividad y no se han visto en la necesidad de parar su producción. Eso es un lujo que algunos sectores se han podido permitir para reducir el impacto de esta gran crisis sanitaria y, a la par, económica, durante tiempos de confinamiento y distanciamiento social.

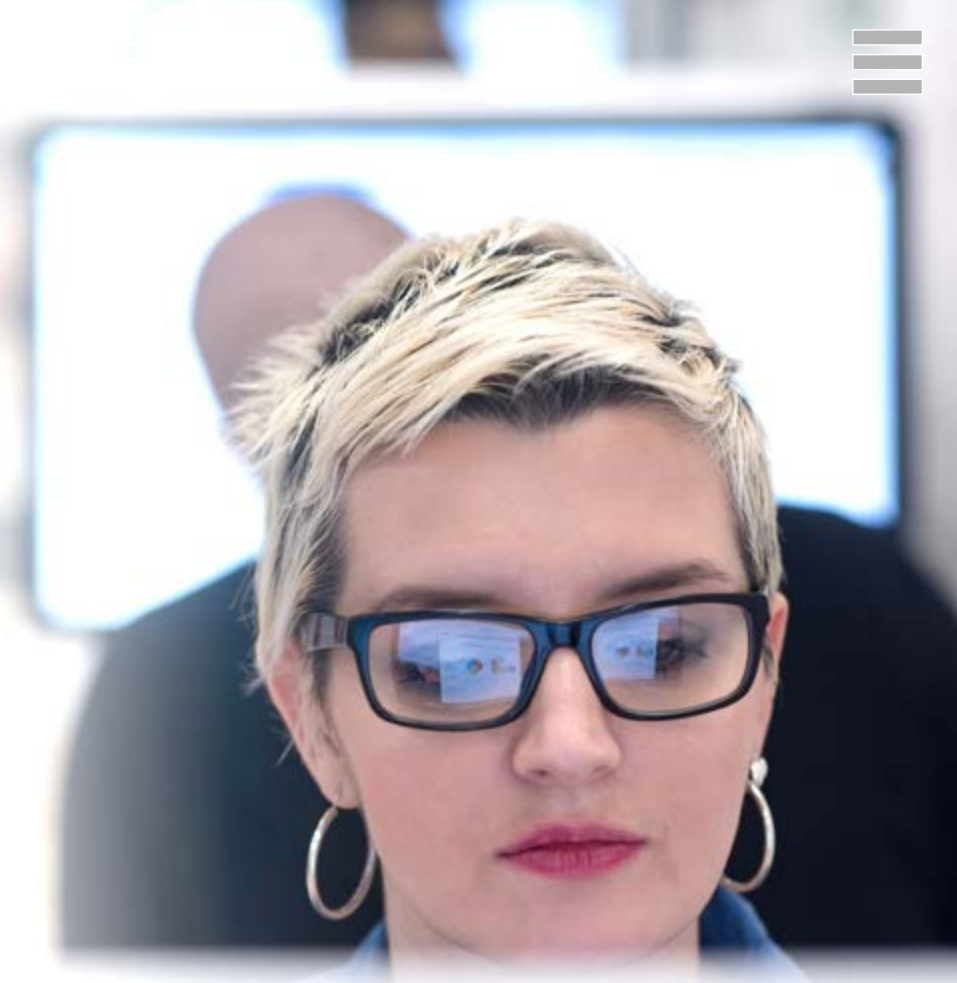
Pero, al mismo tiempo, hay millones de personas que pasaron a usar sus equipos personales, en muchas ocasiones desprotegidos o sin las medidas de seguridad adecuadas. No es lo mismo un equipo de oficina, con una estrategia bien desarrollada en función de la actividad de la empresa, que un ordenador personal que no está sometido a esa protección bien definida por una equipo de personas expertas.

En este contexto, Kaspersky Lab publicó un informe en el que avisa que “todos los dispositivos corporativos, incluidos móviles y portátiles, deben protegerse con el software de seguridad adecuado que permita, por ejemplo, que se borren los datos de los dispositivos que se denuncien como perdidos o robados, separar los datos personales y laborales y restringir las aplicaciones que pueden instalarse”. Esa como una de las medidas que deberían tomarse. Más adelante podrás leer otras.

La misma empresa cuenta que “en España tres de cada cuatro (73%) trabajadores remotos no han recibido ningún tipo de orientación o formación específica de seguridad. Una cifra muy alta si tene-



La bautizada como infodemia, ayuda a COVID-19 a desplegar amenazas a través de la desinformación. Una sociedad sedienta de acceder a fuentes que respondan dudas en plena situación de incertidumbre, se ha mostrado más vulnerable a abrir enlaces dudosos que llegan acompañados de ataques. La Organización Mundial de la Salud u OMS ya advirtió de este fenómeno en marzo de 2020



mos en cuenta riesgos como el aumento del correo basura o los ataques de phishing, además de los peligros de conexión o el llamado Shadow IT (uso de aplicaciones por parte de los empleados que no están bajo el control de los departamentos de seguridad)".

Una persona que trabaje con ordenadores y dispositivos electrónicos, no siempre tiene formación para mantener la seguridad al máximo. De hecho, uno de los grandes retos que confrontan los CISO empresariales, como IT Digital Security analiza en muchas ocasiones, es la falta de formación de personal. Como dicen desde INCIBE, en Instituto Nacional de Ciberseguridad de España, "desarrollar una cultura de seguridad en una organización puede que sea uno de los objetivos más complejos que se pueden plantear. Requiere de una planifica-

ción pormenorizada y de acciones continuadas en el tiempo. Es habitual que los trabajadores vean en los protocolos de seguridad una complicación, un incordio o una molestia", además de la falta de tiempo que a veces se presenta entre las tantas rutinas diarias que hay que llevar a cabo.

A comienzos del mes de junio, como [publicaba la revista IT Reseller](#), "a medida que las empresas dependen en mayor medida del correo electrónico para hacer negocios, los hackers están llevando a cabo lo que los investigadores llaman una estafa "BEC" o timo del CEO". Lo que hace es aprovecharse de la falta de comunicación directa como resultado de las medidas de confinamiento y teletrabajo. Aprovechándose del teletrabajo, un cibercriminal suplanta la identidad de un alto cargo, así como la apariencia visual del correo electrónico para pedir

a los empleados de una empresa que cambien la cuenta bancaria (poniendo una suya) para realizar una transferencia económica como método de pago. Y ahí se roba dinero.

Cómo protegerse de los ciberataques que han surgido con COVID-19

Además de la enorme importancia que tiene hacer algo tan sencillo como no descargar aplicaciones que no sean oficiales ni abrir enlaces si no estás totalmente seguro de su origen, hay diversas precauciones y medidas que tanto ciudadanos, como empresas y CIO y CISO deben tomar.

Para los directivos encargados de mantener la seguridad empresarial, tienen que tener en cuenta que no es que los ciberdelicuentes se hayan vuelto más creativos, sino que siguen recurriendo a los

ataques habituales, como el phishing (normalmente a través de mail, por la creación de páginas web falsas o por herramientas de mensajería instantánea) y el ransomware.

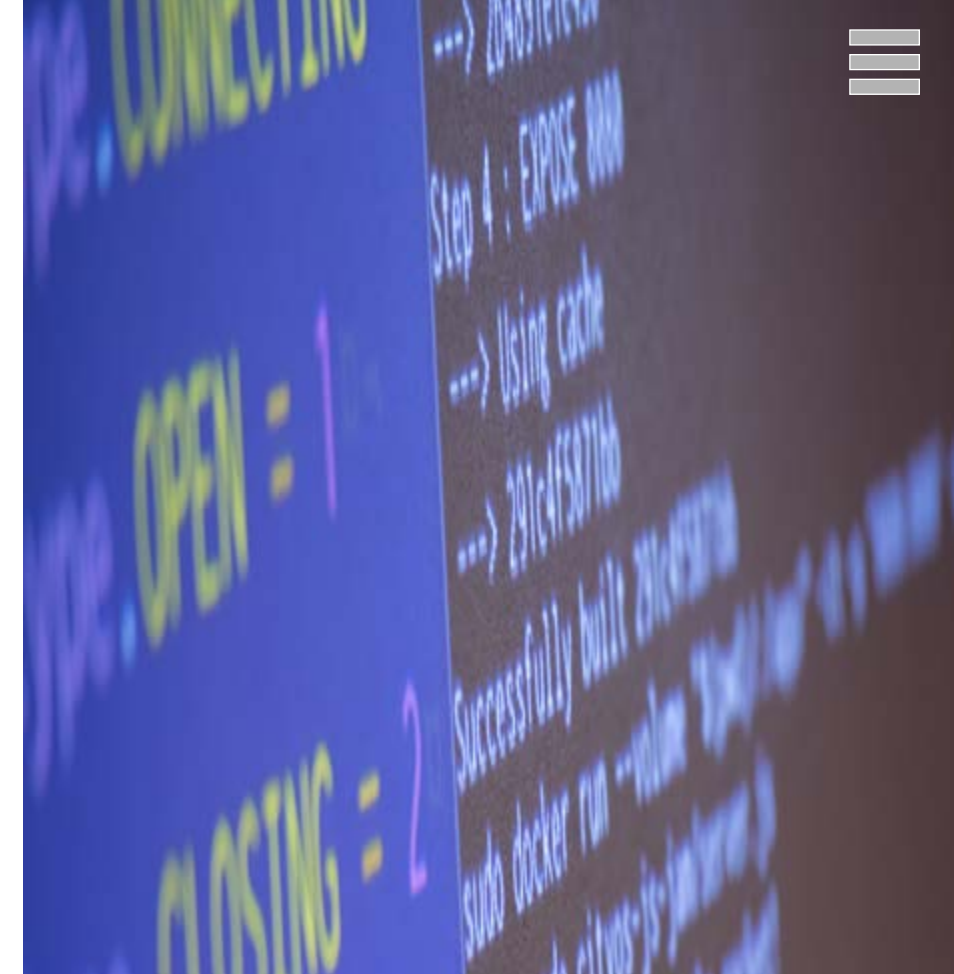
Solo que ahora hay dos novedades: poner el coronavirus como tema esencial de sus ataques (en un momento en el que hay mucha más información que nunca antes y más herramientas e incluso resulta difícil distinguir qué contenidos son reales y cuáles falsos) y también que los empleados de muchas empresas no están dentro de las oficinas bien securizadas y están en sus casas, manteniendo reuniones a distancia y, en muchos casos, usando sus propios dispositivos con herramientas de seguridad más propias para proteger un PC o tablet personal que los datos de mucha relevancia de una empresa con informaciones de miles de clientes y usuarios.

Ahí es donde los CIO y CISO deben:

■ **Educar a los trabajadores en seguridad.** Nunca está de más recordarlo. Y si antes no ha habido el tiempo de dar unas clases básicas de cómo evitar ataques y no caer en las típicas trampas de phishing, haz ahora que esto sea totalmente prioritario. Cabe recordar, de nuevo, que los ciberdelincuentes aprovechan despistes para conseguir que los empleados en remoto abran links que bloquean sus equipos, instalen apps que roban información, por ejemplo. En muchas ocasiones, los mails que reciben los empleados, son supuestamente del equipo de informático o de la dirección de la empresa pidiendo datos privados de la empresa. Es importante que los empleados:

- Rechacen mails que no han solicitado
- Verifiquen el nombre y la dirección del remitente
- Presten atención a los errores ortográficos (muchas veces, las campañas de phishing llegan de

En España tres de cada cuatro (73%) trabajadores remotos no han recibido ningún tipo de orientación o formación específica de seguridad. Una cifra muy alta si tenemos en cuenta riesgos como el aumento del correo basura o los ataques de phishing, además de los peligros de conexión o el llamado Shadow IT, de acuerdo con Kaspersky



otros países ajeno al nuestro propio y eso lleva a que no esté bien redactado el contenido)

- No pinches sobre un enlace si no conocen al remitente o sospechan de que el supuesto remitente no es quien dice ser
- Si hay alguna duda, nunca faciliten datos personales
- Recuerden la siempre importancia de tener contraseñas seguras, fuertes y que no se repitan de unas herramientas y dispositivos a otros

■ **Escoge las herramientas de videollamadas y de videoconferencias que mejor garanticen la seguridad.** El Equipo de Respuesta a Incidentes del Centro Criptológico Nacional, CCN-CERT, avisó en el mes de abril de la detección de una vulnerabilidad en Zoom. Hay empresas que ofrecen este tipo de software que es creado de forma exclusiva para ámbitos empresariales, y suelen



- **Contar con un protocolo para saber cómo actuar en caso de que entre un ataque.** Ese protocolo probablemente ya exista en el entorno de oficina (o debería ser así). Pero ahora hay que llevarlo al nuevo contexto y panorama que la compañía y los equipos que utilizan los trabajadores, están usando. Hay empresas de seguridad expertas en esto, con herramientas apropiadas y que pueden aconsejar al CISO a tomar las riendas de esta nueva normalidad.

Preparación para el futuro

De acuerdo con un estudio realizado por BitDefender, un 55% de las empresas españolas no tenía un plan de contingencia para afrontar adecuadamente la crisis generada por el coronavirus. Este porcentaje es 5 puntos porcentuales por encima de la media global. El coronavirus nos ha enseñado

ser de pago. No está nunca de más invertir en seguridad cuando está en riesgo el prestigio de una empresa y la información privada de los clientes.

- **Implementar un programa de seguridad capaz de securizar muchos equipos situados en diferentes espacios (hogares).** Hay herramientas de escritorio virtual capaces de ayudar a la seguridad. Hay formas de expandir el software antivirus del entorno de oficina, a equipos situados de forma remota. Lo importante es analizar qué herramienta puede servir mejor para el cometido de la empresa.

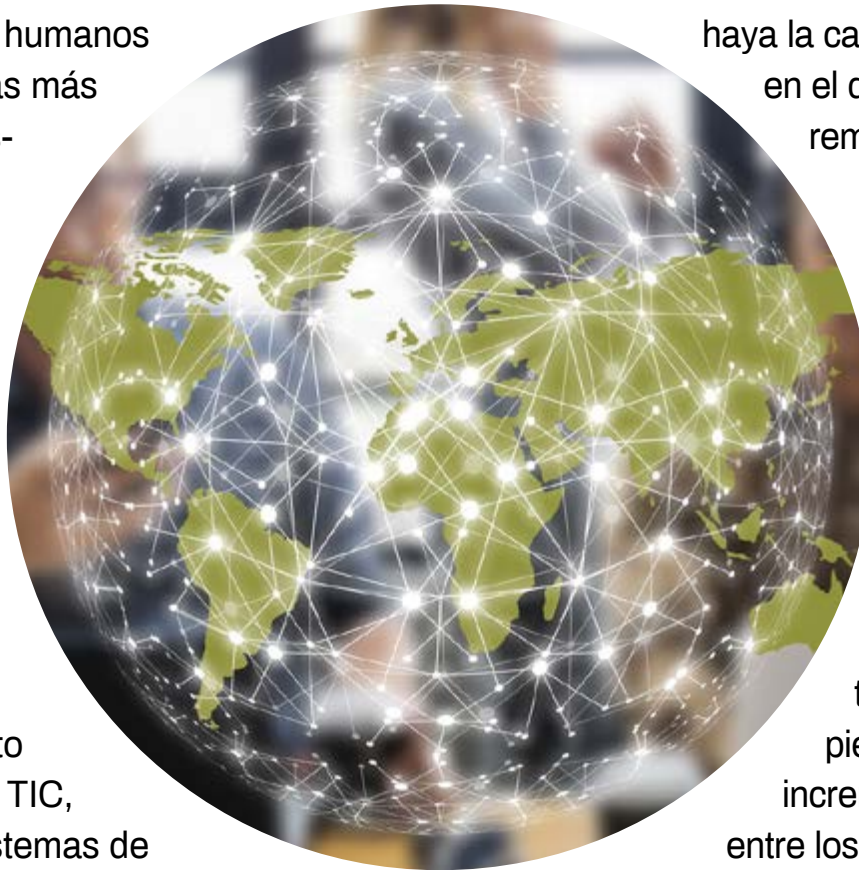
Educa a los trabajadores en seguridad. Si, como CIO o CISO, antes no has tenido tiempo de dar unas clases básicas de cómo evitar ataques y no caer en las típicas trampas de phishing, haz ahora que esto sea totalmente prioritario. Los ciberdelincuentes aprovechan despistes para conseguir que los empleados en remoto abran links que bloquean sus equipos, o instalen apps que roban información, por ejemplo

do muchas cosas. Y los humanos y las empresas, hasta las más potentes y ricas, han visto que nada es eterno, nada está seguro y su vida y actividad puede cambiar para siempre de una semana para otra sin saber cómo seguir.

Para algunas empresas, COVID-19 ha tenido oportunidades que han aprovechado. Por ejemplo, en el ámbito del hardware y software TIC, encontramos que los sistemas de eyetracking, biometría de voz y reconocimiento facial han encontrado un nuevo panorama que los beneficia. Para controlar el acceso a lugares, realizar pagos o controlar una oficina u hogar inteligente. Ayudan a evitar el contacto físico con máquinas.

Para otras, la nueva situación ha llevado a que sus servicios o productos no sirvan o no puedan usarse y muchas empresas han perdido grandes cantidades de dinero en los últimos tres meses.

En el caso de la seguridad empresarial, los expertos y expertas saben ahora que necesitan de un plan para que el futuro no se muestre tan incierto. Y para que, si hay rebrotes de coronavirus, la situación no vuelva a pillarlos por sorpresa, sino que



haya la capacidad de actuar rápido en el despliegue del trabajo remoto.

De acuerdo con el mencionado estudio de Bit-Defender, que se realizó en mayo, si hay que abordar nuevamente cambios rápidos en los patrones de trabajo, el 36% tiene la intención de mantener un servicio de soporte técnico 24/7, un 29% piensa que es necesario incrementar la colaboración entre los responsables de todos los departamentos de la compañía, y un 24% tiene la intención de avanzar en la externalización de los servicios relacionados con la seguridad de sus TI. Solo un 14% afirma haber realizado una inversión significativa para mejorar su seguridad general.

Igual es el momento ahora de aplicar esta labor, antes de que pueda volver a pillar a la economía y las empresas por sorpresa.

Dimensional Research realizó la encuesta a 345 profesionales de seguridad de TI, de los cuales el 94% de los cuales afirmaron estar más preocupados por la seguridad ahora que antes de la pandemia. Las áreas de mayor preocupación de los equipos de seguridad incluyen seguridad de la red

Enlaces de interés...

- [El aumento de las videollamadas dispara el volumen de ciberincidentes](#)
- [El 55% de las empresas españolas carecía de un plan de contingencia de ciberseguridad para afrontar la crisis](#)
- [A los responsables de TI les preocupa más la seguridad tras la pandemia](#)

doméstica de los empleados (58%); aumento de ransomware y ataques de phishing, e ingeniería social (45%); mantener sistemas remotos configurados de forma segura (41%); y mantener sistemas remotos compatibles (38%).

Las empresas de seguridad tienen aquí una oportunidad que no deben perder de vista. Y los responsables de la seguridad empresarial tienen que trabajar en fortificar los equipos de su firma y educar a los empleados, antes de que sea demasiado tarde. 

Compartir en RRSS



¿Confía en la seguridad de sus datos alojados en nubes públicas?

Vea y proteja todo con Sophos Cloud Optix. Combine el poder de la IA y la automatización para simplificar el cumplimiento, administración y monitorización de la seguridad en la nube.

Sophos.com/es/cloud-optix



Cloud  ptix

SOPHOS
Cybersecurity evolved.



El factor humano llega a GravityZone

El factor humano llega a GravityZone

Las personas cometemos errores. Es como crecemos y aprendemos. Pero cuando hablamos de tecnología, con una industria como la del cibercrimen al acecho de cada una de nuestras faltas, cometer un error puede salir muy caro. Se calcula que el 95% de las brechas de seguridad tienen al ser humano como la principal causa; es decir, que si fuésemos capaces de eliminar el error humano de alguna manera, 19 de cada 20 brechas de seguridad no se habrían producido.

Los errores humanos son difíciles de abordar porque en la mayoría de las ocasiones no son intencionados. Van desde la descarga de un archivo malicioso a utilizar contraseñas poco seguras o incluso navegar por páginas web poco apropiadas. Hay que tener en cuenta, además, que los entornos laborales son ahora mucho más complejos, con más herramientas y servicios que requieren un mayor uso de contraseñas. Durante los últimos meses la explosión del teletrabajo ha roto definitivamente el perímetro de seguridad y colocado a los usuarios lejos de los departamentos de TI. Las técnicas de ingeniería social que empujan a los empleados a pinchar en enlaces maliciosos, abrir puertas trase-

ras, descargarse documentos que nunca debieron abrirse o ceder sus credenciales, se han incrementado y profesionalizado. Los ataques, en definitiva, son más dirigidos, y caer en las trampas de los ciberdelincuentes no es tan complicado como pueda parecer.

En medio de esta situación Bitdefender lanza una oleada de innovación que “mejora y fortalece aún más GravityZone como plataforma de seguridad unificada”, explica Nuria Gálvez, Sales Engineer de Bitdefender, en la entrevista en vídeo.

Las capacidades de seguridad de Bitdefender GravityZone cubren todos los elementos del entorno empresarial, desde las estaciones de trabajo físicas/virtuales y servidores, dispositivos móviles,

IoT, recursos y servicios en la nube. Como plataforma de seguridad integrada no sólo detecta amenazas, sino que proporciona visibilidad y contexto, así como contención y respuesta efectiva para incidentes de seguridad independientemente de dónde las amenazas pueden surgir.

La evolución de GravityZone se orchestra en torno a varias novedades más allá de nuevas capacidades de detección y reporte. Por un lado la solución EDR, conocida como Ultra, estará disponible en on-premise, tanto en licenciamiento en bundle como en licenciamiento a la carta. Menciona también Nuria Gálvez novedades en torno a EDR Storage, que hasta ahora era predeterminado de siete días y que a partir de ahora “va a ser posible disponer de almacenamiento para estos eventos de EDR en mayores periodos de tiempo, es decir, 30, 90 o 180 días como add-ons”. Se añade una nueva remediación de ransomware que permitirá hacer copias de seguridad y restauración automática de los archivos en caso de infecciones de este tipo de malware.

Pero quizá lo más destacado sea la nueva capacidad de monitorización de la conducta del usuario; “al módulo existente en Endpoint Risk Analytics (ERA) añadimos Human Risk, lo que nos va a permitir monitorizar los comportamientos de riesgo del usuario”, explica Nuria Gálvez. De forma que si hasta ahora Endpoint Risk Analytics permitía calcular el riesgo de los endpoint de una forma inmediata, pudiendo verificar y corregir la superficie de ataque, a partir de esta nueva release se tendrá en cuenta lo que Nuria Gálvez considera “el activo real de la



Las técnicas de ingeniería social que empujan a los empleados a pinchar en enlaces maliciosos, abrir puertas traseras, descargarse documentos que nunca debieron abrirse o ceder sus credenciales, se han incrementado y profesionalizado



Diálogos **it**

#ContentMarketingIT

**EL FACTOR HUMANO
LLEGA A GRAVITYZONE**

 **CLICAR PARA
VER EL VÍDEO**

Bitdefender lanza una oleada de innovación que mejora y fortalece aún más GravityZone como plataforma de seguridad unificada

empresa, la persona". Añade además la ejecutiva de Bitdefender que esta capacidad "mejora el actual motor de análisis de riesgo y nos va a permitir tener una completa visión de cómo es nuestra seguridad real".

Human Risk Analytics

Desde que apareciera la figura de CISO, el responsable de la seguridad de TI de las empresas, la tensión entre innovación y productividad por un lado,

y cumplir con las restricciones y regulaciones de seguridad por otro, ha sido constante. Muy pocas restricciones pueden generar problemas de seguridad, y demasiadas pueden conducir fácilmente a la frustración y a una caída de la productividad.

Con Human Risk Analytics, Bitdefender quiere buscar un equilibrio entre los dos extremos sin imponer directamente restricciones de seguridad al usuario, sino analizando el comportamiento del mismo de forma que puedan identificarse a los

usuarios que tienen un comportamiento incorrecto porque intenten navegar por sitios comprometidos, hagan un uso inadecuado de las contraseñas o cualquier otra acción que suponga un riesgo para ese usuario y para la empresa. Según la puntuación de riesgo, el administrador de seguridad puede identificar al usuario que se comporta mal y tomar medidas sobre ese usuario en particular. Según Nuria Gálvez este enfoque tiene dos grandes beneficios, por un lado permitir que los usuarios

operen en un clima con restricciones más ligeras, porque sólo se aplicarán cuando sea necesario, y por otro “centrarnos en acciones que mitiguen un riesgo específico y mejoren un comportamiento en particular”.

Tener Human Risk Analytics integrado en una plataforma unificada de seguridad y de análisis de riesgo permite, entre otras cosas, poder cubrir el ciclo entero de seguridad: evaluación de riesgos, prevención, detección y respuesta a las amenazas. También permite una mayor integración entre la evaluación de la postura de seguridad y los controles de seguridad. Específicamente, la mitigación de riesgos puede ser semiautomatizada o totalmente automatizada. Como ejemplo, una vez que se identifica un riesgo debido a la falta de un parche, se va a poder resolver automáticamente a través de un control de seguridad, como puede ser un módulo de gestión de parches. Y cuando se identifica un riesgo generado por el usuario, es posible la recomendación automática de una capacitación de concienciación de seguridad para este usuario y se pueden

monitorizar aún más las mejoras de comportamiento, lo que, en opinión de Nuria Gálvez, “va a ayudar y va a respaldar las necesidades de las personas, haciéndolas mejorar su conocimiento de los riesgos de TI y aumentando concretamente sus habilidades cognitivas”.

Rendimiento

No hace tanto tiempo, cuando el cloud era solo un sueño y la tecnología no había acelerado los sistemas, cada nueva versión de producto solía llevar asociado un impacto en el rendimiento del dispositivo en el que fuera a operar. Durante la entrevista preguntamos a Nuria Gálvez si la nueva funcionalidad de analítica de comportamiento de usuario tendrá algún tipo de impacto en los endpoints.

Explica la ejecutiva de Bitdefender que la funcionalidad estará disponible de forma automática, “es decir, no necesitará ninguna intervención manual por parte del administrador”. Dejando claro este asunto, dice también que GravityZone ya dispone del módulo de Endpoint Risk Analytics (ERA),

Tener Human Risk Analytics integrado en una plataforma unificada de seguridad y de análisis de riesgo permite, entre otras cosas, poder cubrir el ciclo entero de seguridad: evaluación de riesgos, prevención, detección y respuesta

◀ a las amenazas ▶

en el cual se programa un escaneo regular de los endpoint que a partir de ahora va a incluir la parte de Human Risk. “El resultado es que vamos a tener información sobre los riesgos más importantes que se han encontrado en los comportamientos o acciones de los usuarios, así como aquellos usuarios considerados de mayor riesgo por estos comportamientos dentro de la organización”. Estos indicadores son revisados y verificados de forma individual y detallada, e igual que con el escaneo de

indicadores de riesgo en el endpoint que ya estaba disponible desde el año pasado, que era totalmente transparente para el usuario, “el añadir este escaneo Human Risk tampoco penalizarán impactará en la solución”.

A tiempo

“Diría que ha llegado en el momento justo y que a su vez ha llegado el momento de ponernos serios en términos de seguridad de TI”, responde Nuria

Gálvez cuando le preguntamos si la nueva oleada de innovación, y en particular el módulo de monitorización del comportamiento de los usuarios, llega en el momento preciso, ahora que la fuerza laboral se ha desperdigado.

Recuerda que son muchas las estadísticas que asocian parcial o totalmente los errores del usuario a los incidentes de seguridad. “Es necesario cuidar al usuario no controlándolo, sino protegiéndolo tanto a él como a la compañía de lo que podría supo-

Al módulo existente de Endpoint Risk Analytics (ERA) Bitdefender añade el de Human Risk, lo que va a permitir monitorizar los comportamientos de riesgo del usuario





Las políticas
de las organizaciones
no deben limitarse
solamente a garantizar
la seguridad de los
endpoints o de las redes

Enlaces de interés...

- [Bitdefender protege la reputación digital con Digital Identity Protection](#)
- [Bitdefender GravityZone integra nuevas capacidades de defensa de endpoints](#)
- [El 55% de las empresas españolas carecía de un plan de contingencia de ciberseguridad para afrontar la crisis](#)

ner una costosa consecuencia de un posible error”, asegura, al tiempo que añade que durante los últimos meses los ciberdelincuentes han utilizado el COVID-19 como una forma de utilizar a los usuarios como objetivos y en algunos casos han tenido éxito; “el hecho de que ahora mismo se están utilizando redes poco seguras a la hora de conectarse desde casa; la posibilidad de que un amigo o un familiar utilice en un determinado momento el dispositivo corporativo en uso por el empleado; el uso de servicios de mensajería instantánea por parte de los usuarios para compartir información confidencial; la utilización de aplicaciones que pueden no estar permitidas por la compañía; el almacenamiento inadecuado de los datos.... Todo esto se une a la

falsa sensación de seguridad y privacidad que nos ofrece el estar en casa, lo que nos va a provocar la tormenta perfecta”.

En estas circunstancias, las políticas de las organizaciones no deben limitarse solamente a garantizar la seguridad de los endpoints o de las redes. En esta nueva realidad que estamos viviendo, cuando los usuarios actualmente están más fuera del perímetro corporativo que dentro del mismo, el factor humano se ha convertido en un punto clave, por lo que es necesario que las estrategias de ciberseguridad incorporen acciones dirigidas a cada uno de estos elementos: los dispositivos, redes y las personas, pero siempre encontrando un equilibrio entre flexibilidad y control. 

Compartir en RRSS



ENDPOINT, NETWORK, CLOUD, HUMAN

GRAVITYZONE SEGURIDAD UNIFICADA Y GESTIÓN DE LOS RIESGOS

El 7 de julio incluimos también
el Elemento Humano

Bitdefender[®]

WWW.BITDEFENDER.COM





JUAN GRAU

REGIONAL SALES MANAGER DE
BITDEFENDER EN ESPAÑA



El factor humano, la nueva clave de la ciberseguridad

Una gran mayoría de los profesionales de Seguridad de la Información de todo el mundo coinciden en que, tras la gran crisis global que atravesamos, sus organizaciones van a tener que ser capaces de abordar cambios estratégicos con agilidad. De esta forma, la capacidad para cambiar de escenario rápidamente sin aumentar el riesgo se convierte en algo cada vez más crítico para todo tipo de empresas.

Compartir en RRSS



En esta realidad, uno de los mayores desafíos ha sido el haber tenido que adaptar la actividad en muy poco tiempo para permitir que gran parte de los empleados pudieran trabajar desde casa. No hay duda de que esto ha supuesto una oportunidad excelente para los hackers y que ha añadido nuevos retos relacionados con la ciberseguridad de las organizaciones.

Las redes poco seguras a la hora de conectarse desde casa; la posibilidad de que un amigo o familiar utilice en un determinado momento el dispositivo corporativo puesto a disposición del empleado; el uso de correos electrónicos personales o de servicios de mensajería instantánea para compartir información confidencial; la utilización de aplicaciones no permitidas por las políticas corporativas de la empresa y el almacenamiento inadecuado de los datos se unen a la falsa sensación de seguridad y privacidad que ofrecen los hogares para provocar una tormenta perfecta.

En estas circunstancias, las políticas de las organizaciones no deben limitarse solamente a garantizar la seguridad de los dispositivos o las redes. En esta nueva realidad, el factor humano se ha convertido en un punto clave, por lo que es necesario que las estrategias de ciberseguridad incorporen acciones dirigidas a cada uno de esos elementos -dispositivos, redes y personas-, pero siempre encontrando un equilibrio entre flexibilidad y control.

◀ Dar libertad total a los empleados que trabajan des-

de casa es un riesgo demasiado grande, pero implantar unas medidas de seguridad excesivamente severas tampoco es lo ideal, ya que pueden incrementar la frustración de los profesionales y tener un efecto negativo en la productividad de los mismos.

La importancia del control del comportamiento

Conscientes de esta necesidad, en Bitdefender acabamos de añadir el ángulo “humano” al módulo de analítica de riesgos de nuestra plataforma de seguridad GravityZone. Con nuevas capacidades para el análisis de riesgos en el comportamiento humano, Human Risk Analytics logra identificar los comportamientos potencialmente peligrosos de cada usuario, creando perfiles de riesgo individuales, lo que permitirá a los responsables de seguridad actuar con precisión quirúrgica, aumentando los controles o educando al usuario allí donde sea necesario.

El nuevo módulo de Bitdefender no impone ninguna restricción al usuario, sino que analiza su comportamiento y evalúa el riesgo asociado al mismo



GravityZone añade el factor humano a las múltiples capas de seguridad que ya cubría en el pasado: endpoints, red, servicios y recursos cloud para detectar, ofrecer visibilidad y contexto, y proporcionar una respuesta

De esta forma, la plataforma GravityZone añade el factor humano a las múltiples capas de seguridad que ya cubría en el pasado: endpoints, red, servicios y recursos cloud para detectar, ofrecer visibilidad y contexto, y proporcionar una respuesta eficaz ante cualquier posible incidente con independencia del lugar en el que se origine la amenaza.

Es importante destacar que el nuevo módulo de Bitdefender no impone ninguna restricción al usuario, sino que analiza su comportamiento y evalúa el

riesgo asociado al mismo. Así, será posible implantar medidas de seguridad específicas para cada perfil de empleado e incidir en la mejora del comportamiento solo de los que lo necesiten, sin que ello afecte a la actividad del resto.

El sistema ofrece a los responsables de seguridad de la organización la posibilidad de seguir la evolución del comportamiento de cada usuario desde una única consola y ajustar la política de seguridad para mitigar los riesgos que hayan sido generados

por cada uno de ellos, así como medidas destinadas a mejorar la concienciación de los empleados que lo necesiten.

Las empresas saben que una incidencia de seguridad significa jugarse la confianza del mercado y, por tanto, la supervivencia del negocio. Y saben también que la primera línea de defensa debe ser el comportamiento profesional y responsable de todos y cada uno de sus empleados. De nada sirve disponer de las mejores soluciones tecnológicas de seguridad si no van acompañadas del compromiso de las personas que forman parte de la organización a la hora de proteger los datos de la compañía, los clientes y los partners. 

#ITWebinars



Los desastres ocurren...

¿Tienes un plan de continuidad de negocio?

Ante un desastre o un incidente imprevisto, el negocio debe continuar. Para ello es vital reaccionar lo más rápido posible para mitigar cualquier impacto, algo que puede hacerse teniendo implantadas las tecnologías adecuadas.

Los planes de continuidad de negocio deben contemplar los riesgos más variados: aquellos relacionados con la infraestructura, los empleados, las operaciones, la comunicación; el objetivo es gestionar una organización que tenga que enfrentar nuevos desafíos y riesgos y pueda garantizar que se restablecen las operaciones y la producción sin impactar en la cuenta de resultados.

Recientemente, se ha puesto a prueba la continuidad de nuestros negocios con una crisis sanitaria. La adopción masiva del teletrabajo ha tratado de paliar la situación, pero los planes de recuperación deben contemplar muchos otros aspectos: las paradas deben ser mínimas, las copias de seguridad exactas, los fallos reducidos, la recuperación ágil.

Backup basado en cloud, soluciones de recuperación ante desastres como servicio y planes de seguridad gestionados que protegen a las empresas frente a ciberataques sofisticados, forman parte del abanico de opciones que permiten minimizar los riesgos y garantizar la continuidad de negocio ante cualquier eventualidad. Regístrate en este webinar y conoce cuáles son.



REGISTRO



“La ciberseguridad siempre ha formado parte de nuestra actividad”

(Roberto Beitia, Sarenet)

25 años son muchos. Muchos más cuando los enmarcamos en el mundo de la tecnología. Sarenet los cumplió el pasado mes de mayo, en plena pandemia, la misma que ha impedido una celebración por todo lo alto y que ha acelerado la digitalización en la empresa española.

Sarenet nace hace 25 años, en 1995, el mismo año que se fundó Altavista, para dar servicios de acceso a Internet. Un año después, mientras nacía Hotmail, Sarenet diseñaba las primeras soluciones a medida para pymes, y en 1997 crecía un 44% y se convertía en el primer proveedor de Internet con accesos a 56Mbps y en utilizar enlace Satélite directo con EEUU en Marzo.

En 1998, mientras se fundaba Google, Vocento entra en el accionariado de Sarenet, que supera los tres millones de euros de facturación y se convierte en pionera de soluciones de comercio electrónico con la implantación de pago electrónico online.

Un año después Sarenet se convierte en el primer Proveedor de Internet en obtener una licencia de Operador de telefonía. En el mismo año nacía Napster, precursor de Kazaa, eMule o bitTorrent. En el año 2000, mientras el mundo sobrevivía al temido Efecto 2000, Sarenet crecía un 61% y lanzaba Iconoce.

En 2001 la compañía consigue su primer cliente de acceso Internet vía radio con tecnología LMDS. Meses antes había nacido la Wikipedia y Apple presentado su iPod.

Tres años después, sin dejar de evolucionar su oferta, Sarenet abre su primera oficina en Madrid y supera los diez millones de euros de facturación. En 2005 la compañía lanza sus servicios de Voz sobre





"Todas las crisis tienen un efecto acelerador de los cambios que de otra manera hubieran tenido lugar de forma más pausada"

IP, VoIP, y copia de seguridad remota, y en 2006, coincidiendo con el nacimiento de Twitter, abre oficina en Barcelona.

Llegamos a 2007 y Sarenet obtiene la licencia de Operador Móvil Virtual mientras el mercado recibe al iPhone. En 2008 lanza su nuevo gestor de contenidos multimedia de Sarenet, más ágil y efectivo, y

en 2009 inicia el despliegue de infraestructura para ofrecer líneas Ethernet/ Fast Ethernet en Madrid, Barcelona y País Vasco.

En 2010, mientras el tráfico de datos por el móvil supera al de voz, Sarenet lanza su centraliza Sarevoz. En los siguientes cinco años la compañía sigue evolucionando su oferta de servicios cloud, lanzan-

do Iconoce Sentio, conecta su centro de datos a i2Basque y lanza su servicio de telefonía móvil al tiempo que los fundadores compran la participación de Vocento. Mientras, en el mundo Facebook salía a Bolsa y Google abría su sistema de Inteligencia Artificial a todo el mundo.

En 2016 Sarenet activa su primera plataforma IoT y en 2019 completa su portfolio de Ciberseguridad formando un departamento propio de Ingeniería de clientes y Ciberseguridad.

En 2020, Sarenet es uno de los principales operadores de voz y datos especializado en empresas de España. La empresa vasca ofrece soluciones de

analítica de datos, almacenamiento cloud, conectividad y seguridad en el sector empresarial. Roberto Beitia, presidente Sarenet y uno de sus fundadores, responde a algunas preguntas.

Este año se cumplen los 25 de Sarenet, ¿Cómo ha sido la evolución de la compañía?

La evolución de la compañía ha ido muy ligada a la evolución de la tecnología que ha sido y sigue siendo muy dinámica. En paralelo hemos ido cubriendo más áreas de negocio para dar respuesta a las necesidades de nuestros clientes, básicamente Pymes. A la conexión Internet y alojamiento Web inicial se sumó la telefonía IP y la Centralita Virtual, después de la integración con la telefonía móvil. En cuanto a los servicios de alojamiento Web, han evolucionado desde los servicios Housing y Hosting a Servidores Virtuales, servicios Cloud y plataformas SaaS.

¿Cuál es la situación Actual de Sarenet, ¿dónde está haciendo foco?

El foco sigue siendo ofrecer soluciones de voz y datos de calidad diseñadas a medida para las Pymes que consideran las comunicaciones un aspecto crítico para el buen funcionamiento de su negocio. La seguridad, disponibilidad, privacidad... de los datos son clave para nuestros clientes y nosotros no podemos fallarles. Podemos mencionar como actuaciones que se han lanzado recientemente la fibra segura dual, la segmentación de redes industriales y los servicios Cloud orientados a la Analítica de datos y al Aprendizaje automático.

A lo largo de su carrera, ¿Cómo ha visto la evolución del papel del CISO?

La evolución del papel del CISO en las empresas ha estado siempre asociada al nivel del riesgo que han experimentado en cuestiones de Ciberseguridad. En un principio la actuación de las empresas era reactiva y ante la proliferación de ataques han tenido que tomar cartas en el asunto y establecer políticas y sistemas para prever cualquier amenaza.

"En un principio la actuación de las empresas era reactiva y ante la proliferación de ataques han tenido que tomar cartas en el asunto"





"La ciberseguridad es un servicio transversal a todas las TICs y como tal ha evolucionado también muy rápidamente"

Hay que tener en cuenta que, cada vez más, las empresas dependen de las TICs para sus operaciones. El aumento de eficiencia es espectacular pero al mismo tiempo hay que cuidar más todos los detalles para garantizar la continuidad de los sistemas y las aplicaciones. Eso implica contar con la figura del CISO y su integración en los departamentos de Sistemas.

Otro de los grandes cambios pasa por la migración al cloud y al mundo del as-a-service. ¿Cómo se han reinventado empresas como Sarenet para hacer frente a este cambio de negocio?

Más que una reinención se trata de añadir capas de servicios a las actividades que ya se venían realizando. Contamos además con una gran ventaja y es que nosotros mismos somos los primeros usuarios de servicios Cloud para toda la gestión interna, para operar la Centralita Virtual, el DNS, el Correo electrónico, etc. Muchos de estos servicios ya se venían ofreciendo en forma de SaaS. La capa de valor que hemos añadido este año es la de Contenedores y Kubernetes.

Más recientemente se han convertido en un proveedor de servicios de ciberseguridad, ¿qué peso tiene ahora la oferta de ciberseguridad y cuál es su estrategia en este terreno?

La ciberseguridad siempre ha formado parte de nuestra actividad porque hay que tener en cuenta que los operadores somos uno de los blancos pre-

feridos de los ciberdelincuentes. Podemos afirmar que la ciberseguridad es un servicio transversal a todas las TICs y como tal ha evolucionado también muy rápidamente. Llevamos años instalando cortafuegos en nuestras Redes Privadas Virtuales y MPLS y más recientemente el servicio se presta en modo "virtualizado".

¿Qué papel juegan los servicios gestionados de ciberseguridad en el mercado? ¿Cómo están creciendo?

Juegan un papel determinante porque ofrecen ventajas indudables frente al esquema clásico de los



industry 4.0



Enlaces de interés...

- | [Blog Sarenet](#)
- | [Sarenet y Nozomi Networks se alían para asegurar los entornos ICS y SCADA](#)

cortafuegos en casa del cliente. Es la solución que nosotros aplicamos por defecto a cualquier nuevo cliente de conectividad.

El IoT, los entornos industriales, se ha convertido en temas candentes desde el punto de vista de la ciberseguridad, pero también de la conectividad. ¿Cómo está afrontando Sarenet este cambio?

Desde el 2018 pasado estamos muy activos en la “segmentación de redes industriales” para permitir la adopción del IoT. En dicha segmentación la ciberseguridad es la clave. Los entornos industriales han estado desconectados en muchos casos por miedo a los ataques; ahora con el advenimiento del IoT se tiende al todo-conectado pero lógicamente observando todas las medidas de ciberseguridad requeridas. Sarenet está de lleno en este proceso y

por ello se creó en 2018 el departamento de Ciberseguridad e Ingeniería de clientes.

Entre otras muchas cosas, dicen de COVID-19 que es el impulsor de adopción de tecnología de los últimos años, ¿qué opina?

Todas las crisis tienen un efecto acelerador de los cambios que de otra manera hubieran tenido lugar de forma más pausada. Lo hemos visto en esta crisis y en todas las crisis precedentes. La cuestión es si merece la pena el “impulso” teniendo en cuenta el alto precio que se paga en cualquier crisis. En mi opinión la balanza entre el efecto acelerador y las desgracias inherentes a una crisis siempre es negativa; creo que lo pertinente es evitar la crisis en su origen cuando se está gestando, es decir, cuando se pueden tomar medidas para atajarla.

Compartir en RRSS



La documentación TIC, a un solo clic



La transformación tecnológica del sector de la construcción

En el sector de la construcción se prevé un crecimiento del 85%, hasta alcanzar los 15,5 billones de dólares en 2030. Sin embargo, a pesar de esta expansión, existe una baja productividad debido a la falta de inversión en tecnología digital. Finalcad ha elaborado un informe en el que plasma el futuro de la transformación digital en la construcción tras conocer la opinión de 200 encargados de obra y 200 directores de oficina.



Creación de aplicaciones seguras en los entornos financieros

Las organizaciones de servicios financieros operan según determinadas normas. Es algo lógico, ya que los activos y la información que gestionan son valiosos, sensibles y pueden ser objeto de sofisticados ciberataques. Pero si bien las diferentes regulaciones y normas emplean diferentes enfoques, requieren el mismo planteamiento en materia de seguridad: tener visibilidad de los riesgos y las vulnerabilidades de su software y sus sistemas, y planificar para abordar las vulnerabilidades. Este documento ofrece cinco pasos para la creación de aplicaciones más seguras, incorporando la seguridad desde el inicio del desarrollo del software.



Índice de interconexión global

Este estudio de Equinix muestra que, para acelerar su transformación digital, los líderes de TI de hoy deben aprovecharse de la interconexión (intercambio de tráfico directo y privado entre partners de negocio clave) para eliminar la distancia entre los servicios de TI y los usuarios. Ésta es la única forma de mejorar rápida y exponencialmente el rendimiento del negocio digital, impulsado por la dinámica interacción entre personas, sistemas, aplicaciones, datos y nubes en la vanguardia digital.



Informe Global CIO 2020: cómo la IA resuelve la complejidad del cloud

Este informe ilustra los retos a los que se enfrentan las empresas mientras luchan contra las complejidades del cloud empresarial, y los motivos por los que el viaje hacia unas operaciones en el cloud autónomas controladas por IA está marcando las agendas de los directores de sistemas de información (CIO) en 2020.



“Ahora se están prestando muchos más servicios”

(Laia Salas, Secura by Factum)

Hasta hace unos meses era la CEO de Secura. Lo fue durante once años, hasta que, con una facturación cercana a los cuatro millones de euros anuales, la compañía que fundara junto con Israel Zapata, fue vendida a Factum, un integrador, también español, que completaba con esta adquisición su oferta de seguridad. Hablamos con Laia Salas, responsable de Secura by Factum.

Secura by Factum, que es como se ha bautizado a la nueva unidad de negocio, generará el 70% de los ingresos de la compañía, está compuesta en su mayor parte por los empleados de Secura, dirigida por Laia Salas y, en esencia, no ha cambiado respecto a la Secura original.

Dice Laia Salas que no temen perder el apoyo de sus clientes, esos que buscan una empresa no demasiado grande, esos que buscan una atención personalizada que no priorice las hojas de Excel sino un trabajo bien hecho y una buena experiencia del cliente. Reconoce la responsable de Secura by Factum que con la entrada en Factum se han hecho un poco más grandes, que ahora tienen más

fuerza para poder hacer más cosas, pero que ha sido un proceso muy pensado y que han buscado un colaborador “muy definido”; “no queríamos asociarnos con un gran partner que diluyera nuestra especialización, nuestra marca, nuestra manera de trabajar con los clientes”.

Dice Salas que lo único que ven los clientes es que “ahora podemos hacer proyectos en otras áreas, que podemos reforzar la parte de servicios gestionados con el apoyo de más recursos que ahora nos están demandando los clientes”. Dice también que desde el primer momento han querido transmitir a los clientes una imagen de tranquilidad y de continuidad, y que “nadie nos ha puesto ninguna pega, sino todo lo contrario. También es cierto que lo estamos llevando con mucha normalidad,



que seguimos haciendo exactamente lo mismo, no hay ningún cambio, lo que hacemos es crecer”.

Cuando una figura del canal de seguridad desaparece o forma parte de una adquisición, como es el caso, hay dos grupos que contienen el aliento. Por un lado los clientes, que no parecen haberse visto impactados. Al fin y al cabo las caras visibles, la cultura, es la misma. La otra parte son los fabricantes con los que cada una de las partes trabaja. Lo ideal es que sean complementarios, pero pueden ser competidores, y entonces hay movimientos. En el caso de Factum y Secura, no ha habido grandes movimientos, principalmente porque el negocio

de la primera en el mercado de la ciberseguridad no estaba muy extendido. Dirigida por expertos en ciberseguridad, el portfolio de Secura es mucho más rico y con players que están pegando fuerte en el mercado.

Sobre la oferta de fabricantes con la que se trabaja ahora, dice que ha habido sinergias. Destaca la de CrowdStrike que sí que tenían en el radar y con la que Factum ya había firmado un acuerdo de distribución; “ya estamos recibiendo incluso peticiones activas de nuestros clientes para trabajar con ellos y nos parecen muy interesantes”. También menciona Salas a Veritas, que ya venía trabajando con Factum, “con

“No queríamos asociarnos con un gran partner que diluyera nuestra especialización, nuestra marca, nuestra manera de trabajar con los clientes”



Iosu Arrizabalaba y Laia Salas durante la firma del acuerdo de compra.

quien tienen mucha relación y mucho negocio”, o Trend Micro, a quien ya se le había echado el ojo y con el que están trabajando muy a gusto; “habíamos detectado necesidades en torno a la solución de Virtual Patching y hemos aprovechado que en Factum tienen más relación y técnicos cualificados; así tenemos mucha más facilidad de empezar”.

Sobre la selección de fabricantes, dice Laia Salas que la misión es ofrecer tecnologías con las que

“nos sintamos cómodos, en las que ya seamos especialistas, que tengamos alguna experiencia. Al final nosotros no vendemos por vender, sino que vendemos cosas en las que de verdad creemos y consideramos que podemos ayudar a los clientes”.

No habla la responsable de Secura by Factum de eliminar a fabricantes del portfolio de Secura, pero sí de centrarse en los que tienen una tecnología que se esté demandando ahora mismo “y por el

"Antes que la tecnología se está viendo como necesidad imperiosa reforzar la parte humana, la parte de recursos humanos"

camino se irán perdiendo algunos que, no digo que no tengan buenas soluciones, pero por la razón que sea no termina de cuajar en nuestros clientes”.

2020, al año de...

Surge en este momento de la entrevista el topic de seguridad industrial, sobre la que dice Salas que es “una espinita que tenemos todos”. Habla de tener paciencia y de una gran oportunidad “que vendrá en su momento”. Es uno de los sectores que “ha cortocircuitado el coronavirus”; la seguridad industrial se había convertido en un tema de conversación recurrente, pero con todo lo que está ocurriendo, el cierre de fábricas por todos los lados y muchos procesos parados “yo creo que iremos un poco hacia atrás” en torno a este tema.



Si la seguridad industrial no va a ser el rey de la fiesta en 2020, ¿quién lo será? 2020 será el año de... “Lo que sí sé es que va a cambiar el paradigma absolutamente de todo”, asegura Laia Salas añadiendo que quizá aún es pronto para que las empresa asuman, o puedan reconocer, que de verdad van a tener que cambiar su escenario, su protección, sus necesidades, sus prioridades, todo.

Recuerda Salas que en la primera fase se agotaron los ordenadores, el mercado se volcó en el teletrabajo, se habló de la nube como la solución indispensable para hacer frente a un cambio tan drástico. Estamos ahora en un momento de espera, de ver qué va a pasar en septiembre, en otoño. Vamos a ver qué escenario hay que afrontar para que se replanteen nuevos paradigmas de seguridad y de protección. “Si estamos todos en casa la mitad del tiempo, la mitad de la plantilla fuera, habrá que

plantearse las cosas de otra manera, pero yo creo que aún es pronto para que la gente se dé cuenta de hacia dónde vamos a tener que ir”.

Durante esta crisis uno de los productos estrella han sido los firewalls, asegura Laia Salas; también la seguridad endpoint, tanto en lo que se refiere a nuevos proyectos como a la ampliación de algunos existentes; “clientes que no lo tenían y otros que han aprovechado para adoptar soluciones más completas”.

Menciona un fabricante, Splunk, cuyo nombre está subiendo como la espuma ya desde el año pasado. Dice Salas que es una de las soluciones con las que empezaron a trabajar el año pasado y que aporta una capa de visibilidad de todo lo que está pasando en la empresa para tenerlo todo controlado. De repente los empleados están todos desperdigados y “se necesita esa capa de visibilidad, de



INFORME SOBRE CIBERAMENAZAS 2020 DE SONICWALL

El Informe sobre Ciberamenas 2020 de SonicWall proporciona información detallada y un análisis exhaustivo del panorama de ciberamenazas.

Entre los principales hallazgos del informe se incluyen que el Internet de las Cosas (IoT) es un tesoro para los ciberdelincuentes; que el cryptojacking continúa desmoronándose; que las amenazas cifradas todavía están en todas partes o que los ataques de canal lateral están evolucionando.



saber que está pasando, de controlar que no se caiga nada, que todo el mundo esté aquí, tienen las VPN bien, etcétera”.

De forma que en cuanto a tecnologías podríamos decir que COVID-19 ha impulsado la venta de firewalls, y soluciones de seguridad endpoint y de visibilidad y control. Además, apunta Salas, se ha notado un incremento de la demanda de servicios profesionales, “por un lado para adecuar y gestionar mejor las herramientas que ya tenían, y por otro lado para apoyarles en determinados proyectos.

Está claro que la situación desbordó a los departamentos de TI. Tanto como para que mientras unos se volcaban en las nuevas necesidades, se sub-



contrataran servicios para dar a poyo en la gestión; “esto ha sido una oportunidad para potenciar más los servicios. Creo que antes que la tecnología se está viendo como necesidad imperiosa reforzar la parte humana, la parte de recursos humanos”.

Habla también Laia Salas de accesos seguros o doble factor de autenticación como otros elementos o tecnologías que ha potenciado la crisis sanitaria que ha obligado a todo el mundo a trabajar de otra manera. Durante los primeros momentos se cubrieron necesidades, “pero hay vida más allá de aquel mes de marzo y mes de abril; el problema no es que nos haya desbaratado estos dos o tres meses, sino que todavía hay incertidumbre y está todo un poco parado”.

Enlaces de interés...

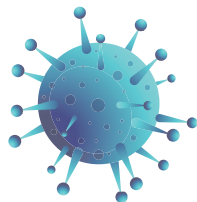
- [Secura creció un 67,51% en 2019](#)
- [Los servicios gestionados impulsan las cuentas de Secura](#)
- [Factum afianza su oferta de servicios de ciberseguridad con la compra de Secura](#)

Hay que ver cómo se asientan las cosas, dice la responsable de Secura by Factum. Por ejemplo, es poco probable que se despliegan proyectos de redes WiFi en oficinas si las previsiones son las de un rebrote. Independientemente, “yo creo que esto ha sentado las bases ya de un cambio que se necesitaba y que va a venir bien a todos”, dice la directiva. No sólo hablamos de una más y mejor conciliación, de una reducción del gasto estructural porque quizá no haya que invertir tanto en oficinas, ni defender un perímetro de seguridad que ya se ha perdido, es que ya, sí o sí, tenemos que empezar a pensar más en el cloud, en esa nube que soñamos y sobre la que se han hecho castillos en el aire, nunca mejor dicho. En realidad, quizá la tecnología de 2020 no es otra que el triunfo, definitivo e inexorable, de la nube. 

"Nosotros no vendemos por vender, sino que vendemos cosas en las que de verdad creemos y consideramos que podemos ayudar a los clientes"

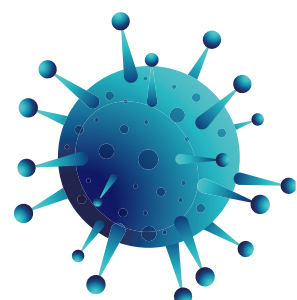
Compartir en RRSS





Ayúdanos a conocer la realidad digital

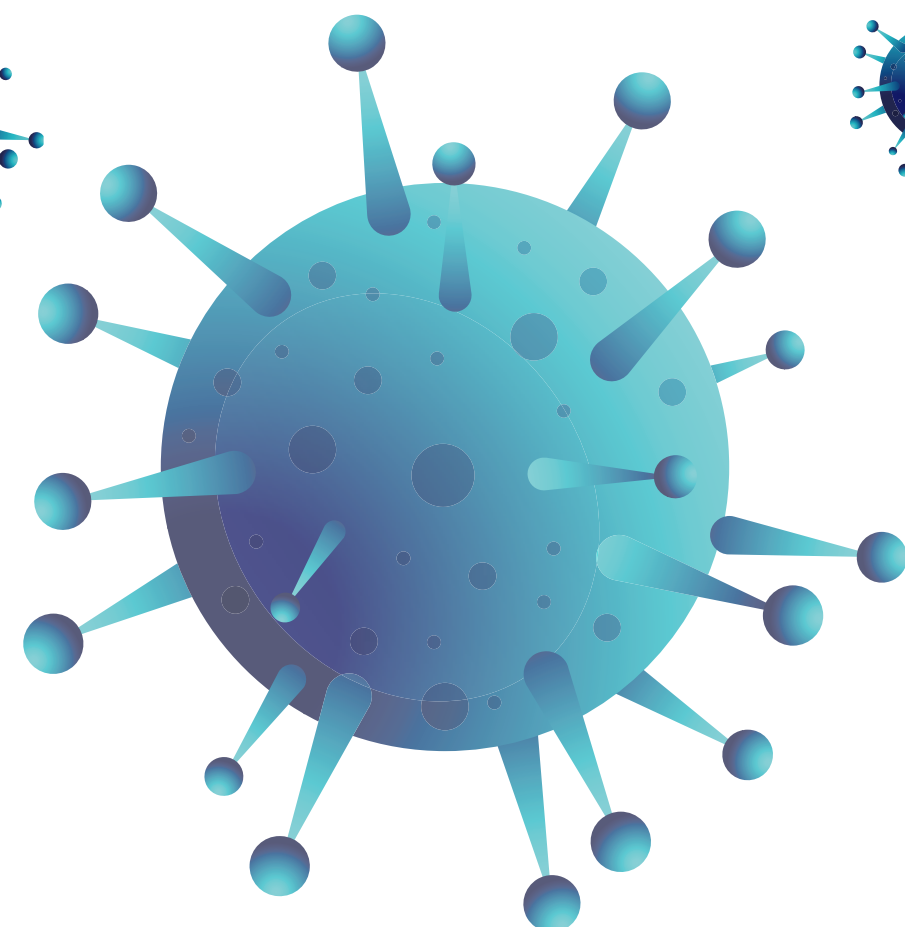
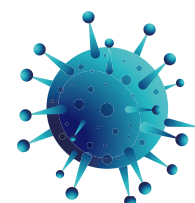
COVID-19, ¿cuánto y cómo ha influido en las estrategias de TI?



¡PARTICIPA!

en nuestra Encuesta

it **RESEARCH**





Cadena de suministro, el peligro acecha

Las empresas, todas, se basan en terceras partes para la entrega de productos o servicios a sus clientes. Esos terceros, esa cadena de suministro, los proveedores, son indispensables, pero al mismo tiempo también suponen un enorme riesgo de seguridad para el ecosistema digital de las empresas. ¿Les conoces?

Un tercero es una entidad con la que una empresa tiene un acuerdo para proporcionar un producto o servicio a la propia empresa o sus clientes en nombre de dicha organización. Hoy en día es casi imposible encontrar una empresa que no interactúe con proveedores o vendedores externos. ¿Quién puede ser un tercero? Un call center, una agencia de marketing, una gestoría, el proveedor de telecomunicaciones, servicios de desarrollo de software, proveedor de ciberseguridad, alojamiento web, pagos online, y un largo etcétera.

Esta cadena de suministro suele acceder a los sistemas o recursos de las empresas, y se termina compartiendo con ellos datos confidenciales y rutas de acceso. Esa capacidad de acceder a información confidencial es lo que lleva a estos terceros, a estos proveedores, a convertirse en un objetivo muy tentador para los ciberdelincuentes como punto de entrada de un objetivo concreto. ¿Por qué? Porque al final se busca el camino de menor resistencia y los ciberatacantes ya saben que desde hace años las empresas están reforzando sus defensas; de forma que en lugar de lanzar ataques directos, comprometen la cadena de suministro o un proveedor clave para conseguir acceso.

Llegados a este punto se entiende por qué conocer a los proveedores se convierte en un aspecto decisivo para la seguridad empresarial. Si una empresa está sujeta a ciertas regulaciones, contratos e incluso elabora una gestión de riesgos em-

presariales y mantiene el riesgo dentro de un cierto umbral, sus proveedores externos deben cumplir automáticamente con estos requisitos. Los terceros deben ser evaluados e incluso monitorizados continuamente con respecto a su compromiso con la tolerancia al riesgo de la empresa, el cumplimiento normativo y los requisitos contractuales. Al hacer esto, se asegura de que no representen un riesgo innecesario para la organización.

En realidad, los terceros no son un nuevo reto desde el punto de vista de seguridad. Son muchos los titulares que hacen referencia a brechas de seguridad en las que el origen son los proveedores externos de la víctima. Baste recordar el incidente de Target de hace seis años, que se originó por el uso de credenciales robadas de una empresa que proporcionaba



Compartir en RRSS





What are the most common attack vectors for hackers or phishers or fraudsters using these third-party vendor "carriers" to infiltrate large companies? What are some of the most surprising techniques that have actually worked?

FRED KNEIP

CHRIS SIENKO

INFOSEC INSTITUTE

¿SON LOS PROVEEDORES TU PRINCIPAL PROBLEMA DE SEGURIDAD?

CLICAR PARA VER EL VÍDEO

El incidente de Target de hace seis años se originó por el uso de credenciales robadas de una empresa que proporcionaba servicios de climatización al minorista

Diagnostics a través de una agencia asociada para el cobro de deudas. También se tiene conocimiento de cómo un ciberdelincuente tuvo acceso a datos de millones de solicitantes de tarjetas de crédito de Capital One a través de un contenedor en la nube de Amazon mal configurado.

Está claro que las brechas de terceros pueden obligar a una organización a responder a incidentes de seguridad. Aunque es posible que no tenga la obligación de responder conforme a las normas vigentes, la organización aún podría sufrir daños considerables en su reputación como resultado del incidente.

Por otra parte, los costes de una brecha de seguridad suelen ir más allá de la mitigación inicial y el impacto de la pérdida de datos. Son múltiples los factores que pueden incrementar el coste de la brecha de unos 5,5 millones de dólares a más de ocho. [El Data Breach Calculator](#) de IBM, que permite a las empresas revisar factores que pueden impactar

servicios de climatización al minorista. Además de los costes propios de la brecha, Target tuvo que enfrentarse a una multa de 18 millones de dólares

La brecha de Equifax se originó en la aplicación Apache Struts, que expuso la información personal de más de 147 millones de personas y generó una multa de 700 millones de dólares a la compañía. El año pasado, un usuario no autorizado tuvo acceso a datos de once millones de pacientes de Quest



RIESGO CIBERNÉTICO DE TERCEROS:

8 CONSIDERACIONES CLAVE

En este documento, veremos por qué es importante el riesgo de seguridad de terceros, qué es lo que está transformando este espacio y cómo priorizar el riesgo. Durante el proceso, profundizaremos en los principios para obtener calificaciones justas y precisas y por qué es importante la seguridad de los proveedores,

además del coste real de administrar el cuestionario de seguridad de un tercero y cómo incorporar la monitorización continua en su programa de riesgos de terceros.

White Paper

Third-Party Cyber Risk:
8 Key Considerations



riskrecon

Evaluar miles de entidades asociadas a una empresa para ver si han implementado controles para salvaguardar razonablemente los datos es un desafío formidable

en el coste total de un incidente de seguridad, recoge que, en igualdad de condiciones, la participación de un tercero aumenta el coste de 7,3 a 8,1 millones de dólares; si además se combina la migración a la nube, y por tanto la adopción de servicios con más proveedores, el coste de una brecha de seguridad puede alcanzar los 8,6 millones de dólares.

En general se calcula que el 60% de las brechas de seguridad están asociadas a terceras partes, un porcentaje que puede incrementarse conforme la adopción de plataformas digitales aumente y se extiendan nuevos modelos que requieran compartir datos con socios y proveedores. Incluso la normativa PSD2, que entró en vigor el 13 de enero de 2019, obliga a los principales bancos europeos a permitir que terceros proveedores de gestión de cuentas y de servicios de pago autorizados accedan a sus datos internos, incluida la información de clientes; lógicamente la normativa busca transparencia y flexibilidad, pero representa un riesgo de seguridad para los bancos.

La transformación digital ha creado enormes oportunidades, ha promovido la innovación, ha mejorado la productividad. Y ha creado nuevas vulnerabilidades. Ya lo dicen los expertos: con una media de



varias decenas de proveedores interactuando con una empresa, no se trata de si los datos estarán expuestos, sino de cuándo, y cuál será el impacto de la reputación corporativa por la pérdida de confianza.

Los perímetros de seguridad, que llevan años desdibujándose poco a poco, casi han desaparecido en medio de una pandemia sanitaria que obligaba a las empresas a abrir la mano con el teletrabajo y a rendirse definitivamente a los servicios cloud y plataformas de compartición de archivos como DropBox, Google Drive o OneDrive.



Tan necesario como tener control sobre los activos empresariales es saber quiénes son los proveedores que hacen negocios con una organización

Las organizaciones controlan sus propios entornos, pero tienen un control limitado sobre las medidas de seguridad tomadas por los proveedores. Si bien las relaciones comerciales con terceros dependen de la confianza, no está de más establecer procesos de verificación. La ciberseguridad incorpora las diferentes políticas, procedimientos y controles necesarios para proteger un ecosistema de datos. Las empresas pueden incluir autorizaciones basadas en roles o autenticación multifactor, y pueden enseñar a los empleados la conciencia de ciberseguridad.

La estrecha relación que se mantiene con los proveedores, sobre todo en un mundo tan digitalizado es prácticamente simbiótica porque la protección debe ser mutua y cualquier cambio puede generar un gran impacto. Esa estrecha relación e interdependencia está fomentando la adopción de sistemas de visibilidad de activos, de herramientas de gestión de identidades y accesos, y, como no podía ser de otra manera en estos casos, de soluciones de gestión de riesgos de terceros.

55,000+

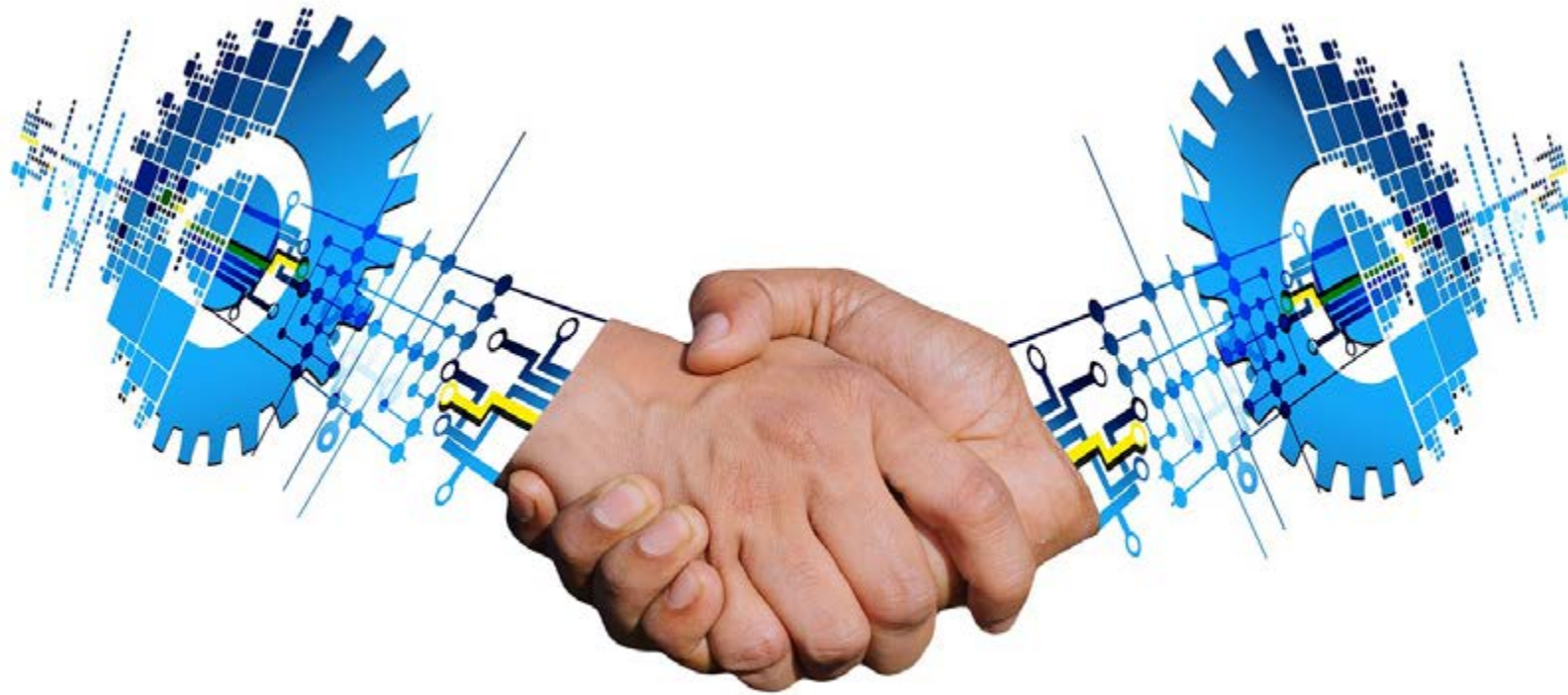
third-party risk assessments delivered across clients

www.deloitte.com/us/thirdpartyriskmanagement

Deloitte.

GESTIÓN DE RIESGOS DE TERCEROS

CLICAR PARA VER EL VÍDEO



En igualdad de condiciones la participación de un tercero aumenta el coste de una brecha de seguridad de 7,3 a 8,1 millones de dólares

Los riesgos de la transformación digital

Recientemente se han publicado los resultados de un estudio elaborado por Ponemon Institute a petición de CyberGRX, un proveedor de soluciones de ciber riesgo, en el que se han encuestado a casi 900 profesionales de seguridad de TI y ejecutivos de nivel C de diferentes sectores (financiero, salud, industrial, sector público y minorista). [El estudio](#)

destaca que si bien se entiende que la transformación digital es crítica, su rápida adopción está creando vulnerabilidades significativas para la mayoría de las organizaciones.

Un 82% de los encuestados cree que sus empresas sufrieron al menos una brecha de seguridad como resultado de la transformación digital; y un 55% dice con certeza que al menos una de las infracciones que afectan a su organización fue causada por un tercero.

Recoge también el estudio que la transformación digital ha incrementado la dependencia de terceros, entre otros los proveedores de nube o de soluciones de IoT, y que la mayoría de las empresas no cuenta con un programa de gestión de riesgos de terceros. Es más, un 63% de los encuestados dice que sus organizaciones tienen dificultades para garantizar un entorno de nube seguro y el 54% de los profesionales de ciberseguridad dicen que evitar

Controlando los terceros

Cuando se trata de establecer el riesgo de seguridad que pueden generar los proveedores de una empresa, hay algunas preguntas básicas que todo responsable debería plantearse:

- **¿Sabes quiénes son tus terceros?**
- **¿Sabe a qué tipo de datos tienen acceso esos proveedores?**
- **¿Sabe qué prácticas emplean los proveedores en sus empresas?**
- **¿Sabe en qué terceros confía su cadena de suministro para proporcionar el servicio que utiliza?**

Los riesgos tecnológicos continuarán manifestándose, y el papel de la gestión de riesgos de terceros no es eliminarlos, sino identificar estos problemas y disminuir su impacto potencial en la empresa. En un mundo cada vez más interconectado, no podemos permitirnos el lujo de ignorar el riesgo que representan los proveedores. Al contrario, debemos ser conscientes de ello y administrar estratégicamente los recursos para abordar dichos riesgos.

las vulnerabilidades es un desafío. Además, el 56% de los ejecutivos de nivel C dice que a sus organizaciones les resulta un desafío garantizar que los proveedores, o terceros, tengan políticas y prácticas que garanticen la seguridad de su información.

Con respecto a las inversiones, dice el estudio que “los presupuestos son y seguirán siendo inadecuados para asegurar el proceso de transformación



Los cuestionarios de gestión de riesgos de terceros generalmente se completan antes de la incorporación del proveedor y luego se actualizan a intervalos regulares

digital". Según los datos la mayoría de las organizaciones no tienen un presupuesto adecuado para proteger los datos; de hecho, solo el 35% de los encuestados dice que tiene ese presupuesto. Debido a los riesgos creados por la transformación digital, los encuestados creen que el porcentaje de seguridad de TI asignado a la transformación digital en la actualidad casi debería duplicarse de un promedio del 21% al 37%. En dos años, el porcentaje promedio será solo del 37% y los encuestados dicen que idealmente debería ser del 45%.

Gestionando los riesgos

La implementación de un programa de third-party cyber risk management (TPCRM), o gestión de

ciberriesgos de terceros, se ha convertido en algo esencial para asegurar el ecosistema de cualquier organización evitando los riesgos a los que una organización está expuesta

Hay varios componentes importantes involucrados en la creación de un buen programa de TPCRM, comenzando por identificar y priorizar la cartera de terceros por el riesgo inherente que representan para una organización; después habría que aplicar el nivel adecuado de la debida diligencia para que se puedan tomar decisiones informadas sobre con quién comprometerse y con quién no. Para hacer esto de manera efectiva, un enfoque de TPCRM debe ser escalable y dinámico para que pueda evolucionar junto con su ecosistema.



MAPEO Y GESTIÓN DE RIESGOS DE TERCEROS

¿Cómo gestiona los riesgos de protección de datos cuando una gran parte de los datos que origina viajan más allá de su control?

Los directores ejecutivos clasificaron las ciberamenazas entre los cinco principales riesgos para las perspectivas de crecimiento. Las empresas experimentan incidentes de ciberseguridad todos los días que pueden ser perjudiciales, costosos y dañar su reputación de manera significativa.

Sin embargo, las grandes empresas en el centro de vastos ecosistemas de datos se enfrentan a un problema particularmente espinoso: la gestión de los riesgos de cibernética y privacidad en torno a la información que viaja a terceros y más allá.



Hoy, muchas empresas comparten datos con proveedores de servicios y subcontratistas para mejorar la prestación de servicios y reducir los costos. En el proceso, los datos cambian de propietario varias veces y la documentación que contiene información sensible e identificable viaja por todo el ecosistema. ¿Cómo hacer frente a ese riesgo?

Seguros al rescate

Dependiendo de los requisitos comerciales, algunos proveedores pueden verse obligados a llevar una cobertura de incumplimiento específica como parte del programa de gestión de riesgos. De forma que las empresas pueden requerir que sean nombradas como asegurados adicionales en las políticas de proveedores para esas áreas de cobertura.

El ciberseguro es un área de cobertura especializada de rápido crecimiento. Según datos del informe The Cyber Insurance Market Report, publicado por Allied Market Research, se espera que el mercado mundial de cobertura de riesgo cibernético genere ingresos de 14.000 millones de dólares para 2022, registrando un crecimiento medio anual de casi el 28% durante el período 2016-2022.

Se calcula que el 60% de las brechas de seguridad están asociadas a terceras partes, un porcentaje que puede incrementarse conforme la adopción de plataformas digitales aumente

En todo caso, el primer paso es el de involucrar a la dirección empresarial. Ha de tenerse en cuenta que las empresas gastan mucho tiempo y dinero en lograr su nivel de seguridad interna hasta el punto de proteger su información más crítica; esfuerzos que pueden desperdiciarse si al final los datos se

comparten con un tercero menos seguro. De forma que los expertos concuerdan en que debe defenderse una estrategia que permita a los equipos de seguridad de las empresas proteger adecuadamente a las organizaciones en el mundo interconectado en el que vivimos, lo que pasa por contar con las herramientas y recursos necesarios para administrar la cartera completa de terceros independientemente de que no todos los proveedores necesitarán del mismo nivel de diligencia. Esto significa que uno de los primeros pasos deber ser el determinar quién representa un riesgo significativo y por lo tanto lo mejor es empezar por hacer un inventario de proveedores.

Por lo tanto, tan necesario como tener control sobre los activos empresariales es saber quiénes son los proveedores que hacen negocios con una organización. Parece tarea fácil, pero es más complicado de lo que parece, especialmente teniendo

en cuenta el aumento en el uso de aplicaciones en la nube y el Shadow IT. De hecho, una fuente señaló que para 2027, el 90% del gasto en TI se realizará fuera de la organización de TI. Por esta razón es importante descubrir todas las relaciones de la cadena de suministro, idealmente usando una herramienta de descubrimiento de activos, y luego determinar el nivel de riesgo para cada proveedor.

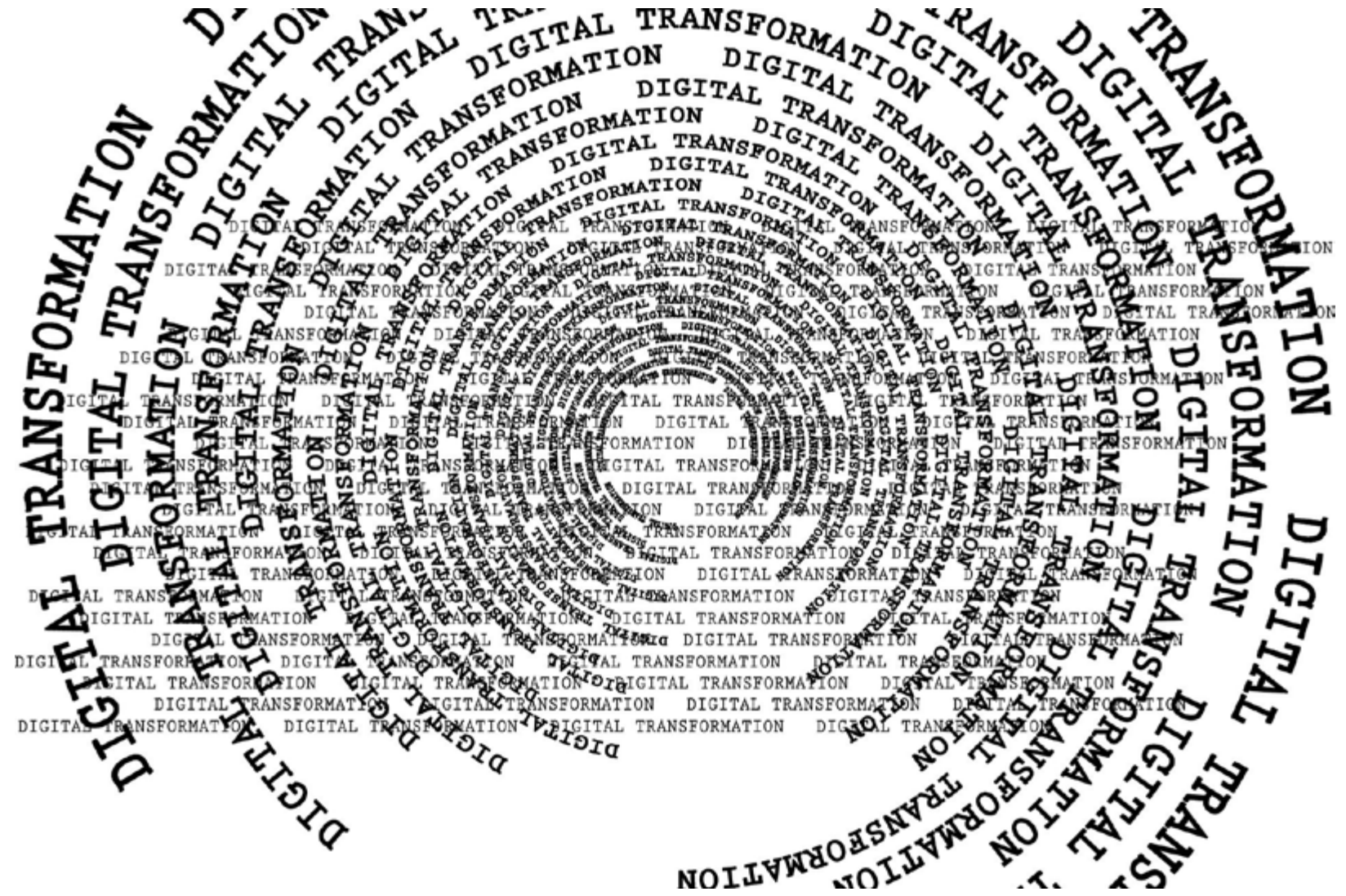
Desde PwC se proponen una serie de soluciones para poder gestionar los riesgos que se pueden generar a través de los proveedores. La primera es mapear el flujo de datos, priorizando el gobierno de los mismos así como los mecanismos para hacer un seguimiento, sean digitales o analógicos, desde su creación hasta su eliminación. Se trata de custodiar los datos implementando controles en el sistema, monitorizando y aplicando políticas de seguridad así como procedimientos de manejo de datos y auditoría.



La consultora también propone realizar evaluaciones en torno a cómo esos terceros protegen los datos identificando primero a los proveedores en función de una serie de atributos, como el volumen de transacciones, los datos regulados y la sensibilidad de dichos datos. En este paso hay que tener en cuenta las leyes de privacidad y realizar evaluaciones de los controles de seguridad implementados por estas entidades en torno a la protección o acceso a la información de la organización.

En este punto hay que tener en cuenta que cada industria ha reconocido las mejores prácticas que deberían guiar la forma en que su organización gestiona las evaluaciones de riesgos de seguridad de la información, como NIST e ISO. También hay estándares específicos, como PCI DSS. Por lo tanto es importante consultar las pautas específicas de cada industria.

Lo habitual es enviar cuestionarios a los proveedores para consultar sobre sus prácticas y controles de seguridad internos. Los cuestionarios de gestión de riesgos de terceros generalmente se completan



Las organizaciones controlan sus propios entornos, pero tienen un control limitado sobre las medidas de seguridad tomadas por los proveedores

antes de la incorporación del proveedor y luego se actualizan a intervalos regulares. Estas evaluaciones de seguridad son vitales para reducir el riesgo de terceros. Los cuestionarios deben personalizarse para el nivel de riesgo particular del proveedor, según el tipo de acceso a los datos que tenga. Las mejores soluciones son automatizadas, lo suficientemente flexibles para que se puedan utilizar plantillas de cuestionarios estándar o permitirle crear

la suya propia, o tan útiles como las que permiten verificar el cumplimiento de regulaciones como GDPR.

Aunque los cuestionarios de seguridad son útiles, no deberían ser el único componente de una evaluación de riesgos de seguridad de terceros, porque los riesgos de ciberseguridad cambian constantemente. Por esa razón es importante complementar los cuestionarios con otros métodos de evaluación,



Enlaces de interés...

- I [La identificación de riesgos, fundamental para fortalecer la cadena de suministro](#)
- I ['La seguridad es prioritaria siempre, por encima de cualquier otra cosa' \(AWS\)](#)
- I [En 2020 aumentarán las brechas originadas por terceros y la superficie de ataque](#)

como las calificaciones de seguridad y la monitorización continua.

Por otra parte, los informes de inteligencia de ciberamenazas proporcionan datos de terceros en comparación con prácticas y estándares de la industria, y esta información podría ser la base para crear los perfiles de riesgo.

La inteligencia de amenazas juega un papel importante en la evaluación de los riesgos de los proveedores. Explica la consultora que evaluar miles de entidades asociadas a una empresa para ver si han implementado controles para salvaguardar razonablemente los datos es un desafío formidable que se hace aún más difícil por la proliferación de servicios basados en la nube.

Por ejemplo, el análisis de grandes volúmenes de datos no estructurados requiere que varias organi-

zaciones tengan acceso ilimitado a los datos, lo que puede provocar una proliferación desconocida de datos confidenciales almacenados en ubicaciones inseguras. En este entorno, es importante usar inteligencia de amenazas y herramientas de monitorización continua para comprender mejor a dónde van sus datos y quién accede a ellos. Esta monitorización continua puede ayudar a identificar más claramente su exposición al riesgo. No sólo se debe identificar a esos terceros según el riesgo en función de atributos como el volumen de transacciones, los datos regulados y el tipo de sensibilidad de datos, sino que se deben tener en cuenta los impactos de la evolución de los datos y las leyes de privacidad en función de dónde se procesan los datos.

Finalmente aconseja PwC el crear un plan de respuesta ante incidentes que contemple no sólo

la capacitación de la empresa en general, sino la realización de ensayos y planificación anticipada, y la asignación de responsabilidad para comunicarse con los medios y las partes interesadas.

En este año, que seguramente quedará marcado para siempre en nuestras vidas, los CISO deben abogar por la creación de culturas más resilientes, por convertir la ciberseguridad en una responsabilidad de todos, y aceptar que la mayoría de las veces las amenazas llegan a través de los proveedores, muchos de los cuales tienen acceso a información sensible de la empresa. No sólo deben evaluar a esos terceros en busca de potenciales vulnerabilidades, sino adoptar soluciones que les permitan identificar datos reales que un tercero expuso inadvertidamente para responder de manera más inmediata. 

thalesgroup.com

THALES

¿Cuál es la estrategia de cifrado de su empresa?

Que sus datos estén en reposo, en movimiento o en uso, **puede** confiar en Thales para proteger sus datos sensibles

#EncryptEverything



#ITWebinars

N CIPHER

Transacciones electrónicas europeas: cumpliendo con eIDAS

¿Sabes por dónde empezar?

Transacciones electrónicas europeas: cumpliendo con eIDAS

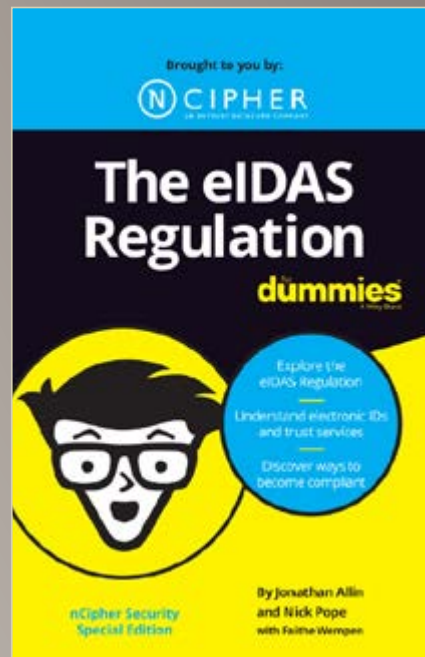
El eIDAS es el Reglamento Europeo para el Reconocimiento de Identidades Electrónicas, se creó con el objetivo de garantizar las interacciones electrónicas entre ciudadanos, empresas y autoridades públicas dentro de la Unión Europea.



¿Por qué es tan importante eIDAS? ¿Qué impacto tienen los negocios? Con la ayuda de José María Pérez, ingeniero para el sur de Europa en nCipher, respondemos a estas y otras preguntas en un #ITwebinars que, entre otras cosas, pone de manifiesto que

el Reglamento eIDAS ofrece oportunidades significativas.

Pero empecemos por el principio, ¿qué es eIDAS? Explica José María Pérez que bajo las siglas en inglés de Electronic Identification Authentication and Trust Services se esconde este reglamento que



EIDAS FOR DUMMIES

Este libro explica de manera fácil qué es eIDAS, qué son los servicios de confianza o por qué los HSM, o módulos de cifrado por hardware, están tan íntimamente relacionados con la normativa. Descubre además las diez maneras en las que nCipher Security puede ayudarte a tratar con eIDAS.

explica cómo se rigen las transacciones electrónicas dentro de la Comunidad Europea que entró en funcionamiento el 1 de julio de 2016. “Lo primero que aporta eIDAS es la plena validez legal”, dice el directivo añadiendo que una firma electrónica tiene la misma validez que una firma manuscrita y que esto se aplica a firmas digitales, sellado de tiempo y cualquier otra forma de autenticación electrónica.

¿Por qué es tan importante eIDAS? Dice José María Pérez que si algo ha puesto de manifiesto esta pandemia sanitaria “es que tenemos que estar preparados y ser flexibles para una forma de trabajar nueva. Tenemos que ser capaces de poder manejar una operativa distinta como la conocíamos hace unos meses”, un entorno en el que priman los procesos electrónicos. eIDAS no sólo ayuda en la transformación digital de las empresas, sino que “aborda la falta de seguridad legal que teníamos en el anterior reglamento de 1999. eIDAS tiene herramientas suficientes como para olvidarnos del papel y de los procedimientos ordinarios”, asegura José María Pérez.

eIDAS no sólo ayuda en la transformación digital de las empresas, sino que aborda la falta de seguridad legal que teníamos en el anterior reglamento de 1999

Dentro de eIDAS está la figura de los Trust Service Providers, o TSP, ¿qué papel juegan dentro de esta normativa? “Son las empresas encargadas y reconocidas dentro del marco de eIDAS para prestar estos servicios de confianza. Y aquí hay una palabra que toma una mayor importancia, que es cualificación. Estos servicios no van a ser sólo digamos servicios digitales, sino que van a estar cualificados”, explica el directivo de nCipher. Un





TRANSACCIONES ELECTRÓNICAS EUROPEAS:
CUMPLIENDO CON EIDAS



CLICAR PARA
VER EL VÍDEO

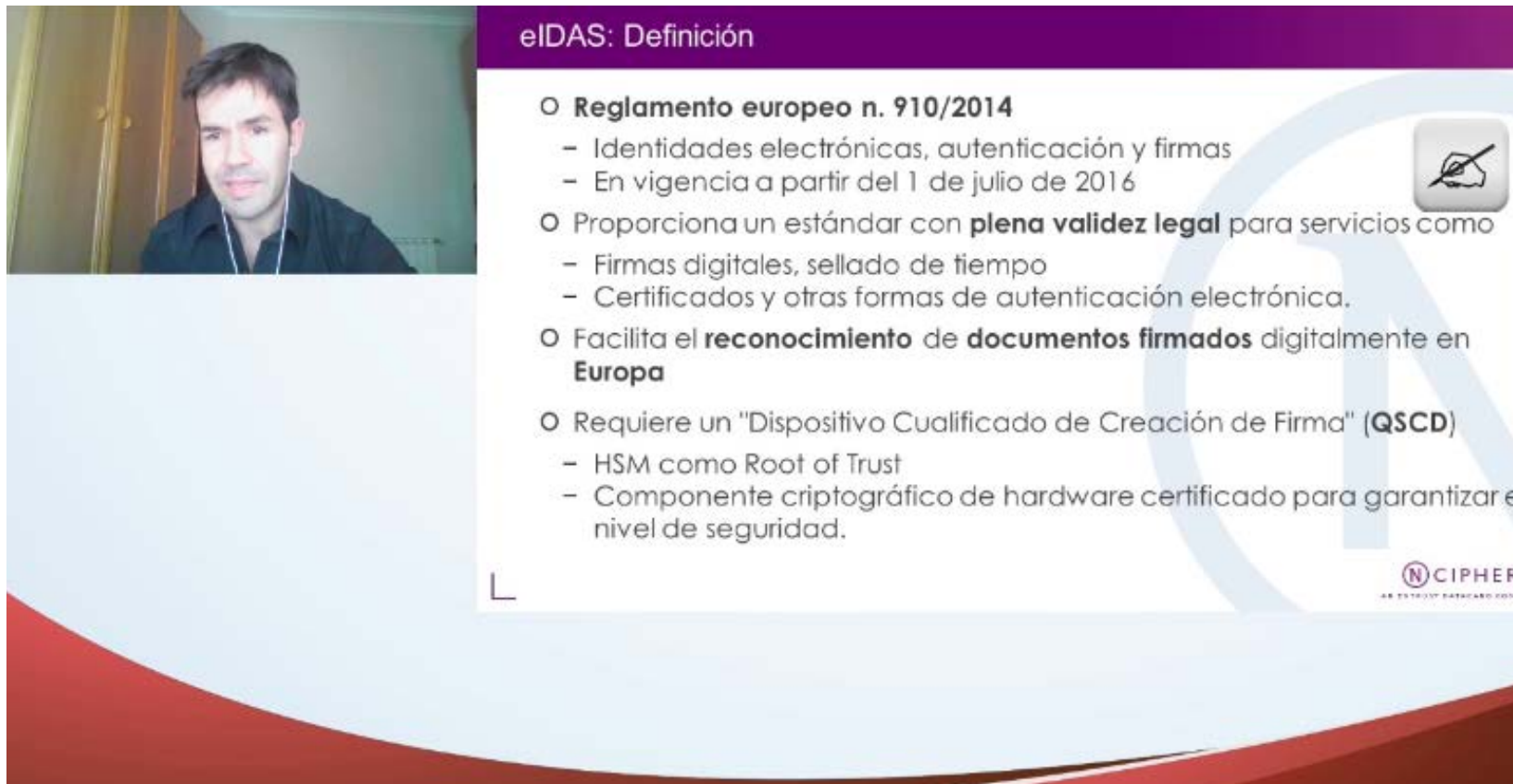
Si algo ha puesto de manifiesto esta pandemia sanitaria es que tenemos que estar preparados y ser flexibles para una forma de trabajar nueva

ejemplo de esta cualificación de la que habla José María Pérez, es la firma digital avanzada, que añade el haber sido creada dentro de un dispositivo seguro de creación de firma, un QSCD, por una entidad que cuenta con un certificado que garantiza que puede ofrecer sus servicios. Es decir, un Trust Service Provider. Tal es su importancia que existe un buscador para encontrar a estos TSP y saber cuáles son los servicios cualificados que están ofreciendo.

eIDAS y nCipher

Los HSM, o Hardware Security Module, son dispositivos criptográficos que juegan un papel clave en todo el entorno de eIDAS, y nCipher es uno de los principales fabricantes de módulos HSM, módulos que utilizan los Trust Service Providers para poder ofrecer sus servicios de confianza.

Explica durante su presentación José María Pérez, que los HSM se utilizan para generar claves y que con estos módulos “estamos otorgando a estos



eIDAS: Definición

- **Reglamento europeo n. 910/2014**
 - Identidades electrónicas, autenticación y firmas
 - En vigencia a partir del 1 de julio de 2016
- Proporciona un estándar con **plena validez legal** para servicios como
 - Firmas digitales, sellado de tiempo
 - Certificados y otras formas de autenticación electrónica.
- Facilita el **reconocimiento** de **documentos firmados** digitalmente en **Europa**
- Requiere un "Dispositivo Cualificado de Creación de Firma" (QSCD)
 - HSM como Root of Trust
 - Componente criptográfico de hardware certificado para garantizar el nivel de seguridad.

L

N CIPHER

Enlaces de interés...

- I [eIDAS, ¿sabes por dónde empezar?](#)
- I [Primeros pasos con eIDAS](#)
- W [Explotando las oportunidades de eIDAS](#)
- W [eIDAS for Dummies](#)

TSP de una herramienta de seguridad para utilizar esas claves con el grado que les exige esa certificación. Y dado que contamos con esta seguridad, los HSM son la raíz de confianza para todos los servicios de confianza digitales y permiten a los TSPs cumplir con todos los estándares transfronterizos de la Unión Europea”.

La familia de HSM de nCipher se llama nShield, y dado el rendimiento y las especificaciones que requiere la normativa eIDAS, la propuesta de la compañía pasa por dos productos: el HSM de red que es el nShield Connect y el HSM PCI, que es nShield Solo. “Al final, tanto uno como otro cumplen el perfil de protección, las especificaciones que se

requerían para el entorno de QSCD de eIDAS. Es decir, estos HSM pueden generar, usar y almacenar claves criptográficas de una forma completamente certificada y por lo tanto, cumplir con la política de uso de las claves”, asegura el directivo de nCipher.

Añade el ingeniero para el sur de Europa en nCipher que las empresas que estén dentro del marco de eIDAS, es decir, que estén realizando transacciones electrónicas, tienen que cumplir con este estándar, con las especificaciones de eIDAS “y los TSP, que son los que están en primera línea, tienen que contar con la arquitectura de QSCD (dispositivo cualificado de creación de firma). Como fabricante de un HSM, nCipher está aquí para echar una mano”. 

Compartir en RRSS



**NUEVO
INFORME**

DOCUMENTO EJECUTIVO

Teletrabajo en 2020: el futuro se hace presente



ELABORADO POR **itRESEARCH**

◀ Descarga este **documento ejecutivo** de **itRESEARCH** ▶



En busca de la conectividad inteligente

EN BUSCA DE LA CONECTIVIDAD INTELIGENTE



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, Belén Juárez

Eva Herrero

Favorit Comunicación, Alberto Varet

Ania Lewandowska

Diseño revistas digitales**Producción audiovisual****Fotografía**

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

El show debe continuar y la tecnología puede hacerlo posible



No está siendo una época fácil para las organizaciones. El parón provocado por la pandemia está haciendo que muchas hayan visto interrumpidas sus actividades, perdido tiempo en reajustarse a la situación y caer sus negocios. Otras han sabido adaptarse, tener capacidad de resiliencia para absorber el impacto y salir del paso amoldando personal y negocio a los tiempos que corren.

Muy buena parte de esa respuesta ágil se ha debido a las habilidades directivas para organizarse frente a la crisis, pero también la tecnología ha tenido su protagonismo y lo tendrá aún más para devolvernos a esa "nueva normalidad" que va a regir nuestro día a día en los próximos meses y años.

Es el momento de acelerar esa transformación digital de las organizaciones, no solo pensando en el teletrabajo, sino en estrategias tecnológicas que garanticen la conectividad inteligente y ágil de espacios físicos, empleados y otros elementos que intervienen en la toma de decisiones empresariales; que permitan ganar productividad; que garanticen el acceso seguro a las aplicaciones y datos ubicados en la nube; en definitiva, prácticas tecnológicas que, sumadas a las decisiones corporativas, den lugar a organizaciones fuertes y capaces de dar respuesta a las necesidades cambiantes del mercado.

Este trimestre en IT Trends hemos puesto el foco en tres áreas que permiten todo esto. En este número podrás leer ampliamente sobre ello, además de poder ver a sus protagonistas. En el IT Webinars [La era de la conectividad](#), abordamos cómo 5G, WiFi, SD-WAN, el open networking y el acceso remoto seguro, facilitan a las empresas afrontar las más exigentes demandas de

conexión ante un entorno en el que las necesidades se multiplican y los volúmenes de datos a transmitir crecen de manera exponencial. Participaron en la sesión Citrix, HPE, VMware, Sonicwall, Dell Technologies y D-Link.

Uno de los objetivos de las organizaciones es sacar mayor provecho de todo lo que hacen. Las tecnologías de automatización inteligente de tareas lo hacen posible. En las siguientes páginas podrás leer nuestro [Especial RPA: la automatización que te hará ganar agilidad corporativa](#), con las principales claves de esta tecnología ofrecida de la mano de Appian, ABAI Group y Automation Anywhere.

Y por último, la identidad; esa pieza única que debería darnos acceso a redes, datos y aplicaciones para garantizar la total seguridad de la información que manejan las compañías. Empleados, clientes y proveedores juegan un papel fundamental a la hora de blindar esta muralla que debe levantarse entorno a la información. Este fue el tema central del IT Webinars [Autenticación y gestión de identidades, el nuevo perímetro de seguridad](#), en el que participaron CyberArk, Micro Focus, Fortinet, Thales, Check Point, F5 Networks, One Identity, Akamai y SonicWall.

Y no podíamos finalizar el trimestre sin ofreceros los resultados de nuestra encuesta: **Teletrabajo en 2020**, el futuro se hace presente, que [podéis leer aquí](#).

No nos queda más que deseáros una buena lectura (recuerda que tienes cientos de enlaces y vídeos para bucear tanto como quieras en la información) y... ¡un feliz verano! ■

Arancha Asenjo
Directora de IT Trends

www.ittrends.es

Encuentros **it**TRENDS



La inteligencia artificial (IA) es una rama amplia de la ciencia de la computación que se ocupa de construir máquinas inteligentes capaces de realizar tareas que generalmente requieren inteligencia humana. La IA es una ciencia interdisciplinaria con múltiples enfoques, pero los avances en el aprendizaje automático y el aprendizaje profundo están creando un cambio de paradigma en prácticamente todos los sectores de la industria.

¿Cómo puedo mejorar los procesos empresariales utilizando Inteligencia Artificial?
¿De qué manera puedo sacar provecho para mi organización de las capacidades que esta tecnología propone?

23 de septiembre de 2020 - 11:00 (CET)

REGISTRO



6 de cada 10 organizaciones fueron víctimas de ransomware en 2019, una cifra que va en aumento año a año debido al incremento en los pagos de rescates. Más de un tercio de las organizaciones experimentaron seis o más ataques exitosos, y el 69% esperan sufrir uno este año.

Aunque inicialmente el ransomware se utilizaba de manera aleatoria, infectando usuarios a los que se pedían rescates de cientos de dólares por recuperar el control de sus ordenadores, los ataques se han hecho mucho más dirigidos y ambiciosos, llegando a colapsar empresas e incluso ciudades. Nadie está a salvo de una amenaza difícil de rastrear.

¿Cómo hacer frente a la amenaza? ¿Por qué no es suficiente con tener un buen backup? ¿Qué sectores están más expuestos? Podrás conocer todas las respuestas en este webinar.

30 de septiembre de 2020 - 11:00 (CET)

REGISTRO



Tecnología, habilitador de la “nueva normalidad”

Durante lo peor de la crisis sanitaria por la COVID-19, las organizaciones han estado utilizando la tecnología para mantener su maquinaria en marcha y, a su vez, minimizar los riesgos para la salud. Esto ha desvelado el gran potencial de la nube, las aplicaciones colaborativas y las comunicaciones de nueva generación, pero también ha revelado la gran brecha digital que afecta a las empresas y sus trabajadores.

Una vez que pase la pandemia, gran parte de la tecnología implementada va a seguir en uso, y los expertos coinciden en que esto transformará para siempre las estructuras empresariales y el propio mercado laboral, en el que las habilidades tecnológicas tendrán más importancia que nunca.

A raíz de la pandemia, las organizaciones han tenido que implementar a marchas forzadas nuevas tecnologías para seguir operando mientras sus empleados se encontraban reclusos en sus hogares. Este cambio ha sido absolutamente disruptivo para ciertas empresas, que hasta ahora no se habían planteado seriamente el uso de nuevas tecnologías ni la necesidad de abordar la transformación digital. Ahora, ante las condiciones de bloqueo impuestas por los gobiernos de los países más afectados, muchas han optado por usar las tecnologías digitales para el trabajo rutinario con aplicaciones empre-

sariales, para habilitar el trabajo colaborativo o para celebrar reuniones a distancia.

Esto está siendo beneficioso en un sentido muy definido, que es el de la modernización de las empresas que se habían mostrado tímidas o indiferentes en cuanto a la transformación digital. Pero a su vez ha puesto de relieve una falta de habilidades digitales entre buena parte del tejido empresarial, y también en los propios trabajadores. De cara al futuro próximo, muchas empresas seguirán utilizando buena parte de las tecnologías que les están permitiendo seguir adelante durante la pandemia, pero para hacerlo correctamente deberán enfrentarse a la brecha digital.

Numerosas organizaciones alertan de los peligros que tiene implementar las nuevas tecnologías sin contar con los conocimientos necesarios en materias como la seguridad cibernética. Como muestra de ello, los últimos estudios revelan que gran parte de las empresas no están preparadas para efectuar el cambio definitivamente, sin antes resolver ciertos problemas básicos. Por ejemplo, en el reciente informe *"Flexibility at Work"* realizado por Randstad, los expertos destacan los graves problemas a los que se enfrentan tanto las empresas como los trabajadores españoles para abordar estos cambios en el futuro cercano.

EL TELETRABAJO COMO EJE DEL CAMBIO

Si algo ha demostrado la pandemia es que, a igualdad de condiciones, las empresas con ma-

yor grado de automatización han sido más capaces de mantener las operaciones durante lo peor del confinamiento. Lo mismo se puede decir de aquellas que han podido implementar a tiempo el teletrabajo, permitiendo a sus empleados continuar con la mayor parte de sus funciones sin que se produzcan efectos negativos importantes para el negocio. En este sentido, según la investigación de Randstad, el 42% de las empre-

sas españolas han implantado sistemas de trabajo remoto para seguir funcionando en estos meses de confinamiento. Según este análisis, lo positivo es que, a pesar de verse obligadas a tomar estas medidas, lo que causó una sorpresa inicial y cierta indignación, el 58% de los trabajadores españoles afirma que antes de esta crisis su empleo ya reunía las condiciones propicias para convertirse en un puesto de trabajo remo-



5 HABILIDADES EMPRESARIALES PARA SALIR REFORZADOS DE LA CRISIS DE LA COVID-19

Las empresas tecnológicas comienzan a recuperar fuerzas

El impacto de la pandemia en las empresas tecnológicas ha sido serio, ya que los clientes han reducido al mínimo el gasto en tecnologías no esenciales, pero a su vez se están generando nuevas oportunidades. Una reciente investigación realizada por la asociación tecnológica CompTIA señala que el ambiente general de los negocios tecnológicos se está estabilizando, con claras señales de mejoría a corto plazo. Esto está motivado por la creciente demanda de servicios de seguridad, computación en la nube y otras áreas que están cobrando importancia para las organizaciones a raíz de la pandemia.

Según indican los datos de este estudio, el porcentaje de empresas tecnológicas que ha experimentado un aumento en las consultas de nuevos clientes y en las oportunidades comerciales fue del 83% en abril y del 84% en junio, un aumento significativo frente al 76% registrado en marzo. Como explica Nancy Hammervik, vicepresidenta ejecutiva de relaciones industriales de CompTIA, "sigue habiendo mucha incertidumbre sobre el impacto de la pandemia en el futuro, pero es una señal esperanzadora de que la tecnología se vea como una solución para ayudar a las empresas

a navegar en estos tiempos inciertos". Las principales prioridades de inversión para las organizaciones son los productos y servicios relacionados con la seguridad cibernética, como informa el 42% de las empresas encuestadas. Le sigue el cambio de infraestructura o aplicaciones locales a la nube (42%), los servicios de TI gestionados y subcontratados (40%) y la consultoría general de ayuda para adoptar las tecnologías virtuales (40%). Y también destacan que el área de personal está demandando nuevos servicios tecnológicos para apoyar las estrategias de contratación de cara al futuro.

to. Y el 68% de los trabajadores ya demandaba esta forma de trabajo como medio para mejorar su calidad de vida y su conciliación familiar, pero su empresa lo impedía.

Pero esto se debe mirar con lupa, ya que la realidad es que existe un desconocimiento general muy profundo sobre ciertas cuestiones fundamentales relativas al trabajo remoto en la era digital. Sobre todo, en materia de ciberseguridad, ya que los entornos domésticos y profesionales no se pueden mezclar de forma segura sin seguir ciertas pautas y contar con ciertas tecnologías, algo que desconoce la mayoría. Además, a pesar de sus demandas de teletrabajo, gran parte de la población activa se puede considerar en etapas tempranas de la alfabetización digital, ya que desconocen las características y particularidades de muchas de las tecnologías necesarias para trabajar desde casa.

IMPACTO DE LA AUTOMATIZACIÓN EN EL MERCADO DE TRABAJO

No todos los sectores han podido solucionar los problemas que ha planteado el confinamiento con trabajo remoto, ya que muchas empresas requieren operarios físicos para realizar el trabajo. Por ejemplo, el transporte, la sanidad o la industria manufacturera, y estas empresas ponen sus miras en una estrategia que combine la posibilidad del trabajo remoto con mayores capacidades de automatización.



Y esto significa menos personal humano imprescindible y más automatización a través de maquinaria, robótica y software autónomo.

En estos ámbitos se prevé que la destrucción de empleo podría ser importante en la próxima década, a medida que las fábricas, los almacenes minoristas, o el transporte de mercancías y personas se automaticen más y más. De hecho, muchos fabricantes están planificando la posibilidad de acelerar las próximas etapas del proceso de automatización en el que se han embarcado a largo plazo. Y empresas que no lo consideraban posible, ahora se lo están planteando para prepararse de cara al futuro, tanto por competitividad como por resiliencia frente a situaciones de emergencia como la que estamos viviendo.

Para los expertos en el mercado laboral esto va a tener un impacto radical en el mercado de trabajo,

ya que no solo se reducirá la plantilla en muchas empresas, sino que los requisitos para acceder a los puestos de trabajo estarán cada vez más vinculados a las habilidades tecnológicas, y los trabajadores deberán adquirir nuevos conocimientos y especializarse más. Según la investigación de Randstad Research, en los países de la OCDE el 30% de los empleos se verá modificados tras la pandemia, mientras que el 70% de los trabajos actuales desaparecerá, cifras mucho más desalentadoras que las de investigaciones anteriores.

NUEVOS CONOCIMIENTOS TECNOLÓGICOS PARA CONSEGUIR EMPLEO

Mientras que hasta hace relativamente poco los expertos consideraban que la digitalización y la automatización generarían nuevas y excitantes posibilidades en el mercado laboral, ahora el fu-

turo se percibe con muchas más dificultades para los trabajadores. Los expertos han apoyado la automatización como medio de modernizar la economía, proporcionando puestos de trabajo más dignos y estimulantes a las personas, pero ahora perciben notas más negativas en este avance, ya que la posibilidad de que se repita una situación como la generada por la pandemia de la COVID-19 genera mucho temor e incertidumbre.

Ante esta situación, muchas empresas están buscando en la tecnología una forma de garantizar la continuidad de las operaciones, independientemente de que sus empleados deban quedarse en casa, y esto pasa por una mayor automatización y un aumento del uso de tecnologías digitales en los puestos de trabajo restantes. Así, los empleados del futuro (y no muy lejano), deberán adquirir nuevas habilidades para encajar en la nueva realidad del mercado de trabajo, ya sea que estén en una empresa en proceso de cambio o que quieran acceder a un puesto de trabajo.

Los entornos domésticos y profesionales no se pueden mezclar de forma segura sin seguir ciertas pautas ni tecnologías



Como explica en su informe Valentín Bote, director de Randstad Research, “el teletrabajo no va a ser el único avance tecnológico obligado que nos va a traer la pandemia. La automatización va a ver crecer su protagonismo por la importancia de evitar aglomeraciones, lo cual, lejos de amenazar al empleo, va a generar nuevas oportunidades. Para los profesionales interesados en aprovecharlas, es recomendable seguir de cerca la evolución del mercado laboral y apostar por la formación continua”. Porque un elevado porcentaje de las empresas está teniendo dificultades para encontrar personal cualificado, ya que la brecha digital es muy amplia en general, y es preciso trabajar para reducirla lo antes posible, tanto para los trabajadores en activo como para los futuros profesionales de todas las industrias.

AUMENTA EL RIESGO DE PRECARIEDAD

Los analistas de Randstad prevén que, tras la pandemia, se producirá un movimiento mucho más veloz de lo previsto hacia los empleos a tiempo parcial, las contrataciones temporales, de personal autónomo y a las subcontrataciones a través de ETTs y otras empresas especializadas. Como ejemplo citan el cambio que se produjo en Estados Unidos entre 2005 y 2015, cuando estas modalidades de trabajo pasaron del 10,7% al 15%, una tendencia que se está acelerando peligrosamente y que lo hará aún más a raíz de la pandemia.

Uno de los conceptos que para Randstad va a ponerse más de moda es el de Gig Economy, una modalidad laboral basada en pequeñas tareas o encargos que se pueden llevar a cabo a través de plataformas digitales. Mientras que sus impulsores venden este concepto como una forma de revalorizar el trabajo, en realidad este planteamiento puede esconder un grave problema de precariedad. Porque muchas empresas aprovechan estas plataformas para proponer trabajos puntuales muy mal pagados, por los que una masa creciente de desempleados o trabajadores necesitados compiten, impulsando los salarios a la baja.

Además, en muchos casos esto exige que los trabajadores tengan ciertas habilidades tecnológicas que las empresas dan por hechas, pero que deberán adquirir y costear por sí mismos, en un delicado equilibrio coste-beneficio. Según afirman los responsables de este estudio, el uso de las plataformas de Gig Economy ha aumentado un 30% entre 2016 y 2019, y solo en la Unión Europea esta modalidad de trabajo se ha convertido en la principal fuente de ingresos para el 2% de los adultos.

Aunque el riesgo de precariedad no va a frenar esta forma de microeconomía, más aún teniendo en cuenta que las empresas van a



Muchas empresas seguirán utilizando buena parte de las tecnologías que les están permitiendo seguir adelante durante la pandemia, pero, para hacerlo correctamente, deberán enfrentarse a la brecha digital

apostar por contratar a trabajadores freelance para muchas tareas puntuales, periódicas y específicas. Esto genera oportunidades por las que los trabajadores deberán luchar, y necesitarán contar con nuevas habilidades digitales para poder capitalizarlas, a la vez que luchan por unas condiciones razonables.

GRANDES OPORTUNIDADES PARA LA ROBÓTICA

La automatización suena más que nunca a robótica, ya que las tecnologías implicadas en esta tendencia se basan en una combinación de software y maquinaria cada vez más sofisticada, inteligente y autónoma, que se asemeja cada vez más a los conceptos de robots que la ciencia ficción ha imaginado desde los años 50 del siglo pasado. Ahora hay sectores que pueden sacar partido del impresionante avance que ha dado la robótica, gracias a la combinación de nuevas tecnologías en el campo de la ingeniería mecánica y la automática con la parte de TI. En esta se incluye tanto el hardware de visualización, monitorización y

computación autónoma como el software, donde diversas ramas de la inteligencia artificial han sido absolutamente disruptivas.

Esto está impulsando campos como el de la robótica móvil y la fusión cada vez mayor de las tecnologías de la información con las tecnologías operativas clásicas en las fábricas y en otros entornos. Ahora, además de su tradicional aplicación en las cadenas de montaje de las fábricas, los robots están irrumpiendo en nuevos entornos como el mantenimiento mecánico, los almacenes y centros de intercambio logístico y áreas donde hasta ahora sus aplicaciones eran muy limitadas, como el de la atención médica, donde se han convertido en herramientas fundamentales para la limpieza y la higienización de objetos, superficies y salas completas.

Pero, así como la revolución industrial impulsó un cambio radical en el mercado de trabajo en el siglo XIX, la transformación digital y la automatización a través de la robótica tienen el potencial para generar cambios a gran escala en el mercado de trabajo. Según la investigación de Rands-

tad, la compra de robots ha aumentado un 16% en todo el mundo en la última década. En España, concretamente, hay 157 robots industriales en las fábricas por cada 10.000 trabajadores, con una tasa de robotización del 1,57%, mientras que en Europa este índice es de un 1,06%.

Y se sitúa por delante de otros países fundamentales en la economía de la Unión, como es Francia (1,37%), y de otras economías fuertes como la de Suiza (1,29%) o la propia China (0,97%). Aunque queda bastante por debajo de otras economías fuertes de nuestro entorno, como Alemania (3,22%), Suecia (2,40%) o Dinamarca (2,30%), y de otras economías de primer nivel, como Corea del Sur (7,10%), Singapur (6,58%), Japón (3,08%) o Estados Unidos (2%).

Otro aspecto que destacan los expertos es la relación entre la robotización y el envejecimiento de la población, y señalan que donde habrá más robots será en los países que envejecen más tarde, sobre todo por el impulso que se dará en el campo de la atención sanitaria a personas mayores.

LOS NUEVOS ENTORNOS DE TRABAJO REQUIEREN NUEVOS PERFILES

A pesar de que las nuevas tecnologías aplicadas a las empresas y las nuevas formas de trabajo remoto, externalización y microempleo están alterando radicalmente el mundo laboral, no todo se ve turbio en el futuro. Con la expansión de las nuevas tecnologías y la popularización de nue-

5G y la nube en el borde, tecnologías clave para la recuperación económica

Desde que dio comienzo el confinamiento, las empresas comenzaron a cambiar su estrategia operativa para dar cabida al teletrabajo, y para automatizar al máximo cualquier interacción con los usuarios y clientes y minimizar el riesgo de contagio. Muchos de estos cambios han llegado para quedarse, porque las empresas están aprendiendo a trabajar de otra forma, que en muchos casos es incluso más eficiente y permite reducir costes tradicionalmente fijos, como los relativos a los puestos de trabajo.

Pero esto también tiene su propio coste, ya que las infraestructuras tecnológicas y las redes empresariales no estaban bien preparadas para una situación como la que estamos viviendo, por lo que muchas organizaciones públicas y empresas han tenido que adoptar soluciones poco ortodoxas para salir del paso. Ahora que los efectos de la enfermedad están mitigándose ya se está comprobando que nada volverá a ser exactamente igual que an-

tes de la pandemia, y mucho menos en las empresas, que ahora deberán escoger si consolidan sus estrategias adoptadas “temporalmente” para superar la crisis o si darán el paso final hacia una transformación definitiva.

Según los expertos de [ABI Research](#), esta segunda opción parece ser la que tomarán buena parte de las empresas, que apostarán por modelos que ya han adoptado parcialmente, y que les aportan beneficios operativos y comerciales. Pero modificar la arquitectura de la red empresarial para ser más flexibles y dinámicos a través del teletrabajo y las nuevas tecnologías exige implementar toda una nueva gama de sistemas, entre los que los expertos destacan las infraestructuras cloud-Edge y las redes 5G.

La consultora pronostica en uno de sus últimos informes que estas dos tecnologías van a ser clave para la recuperación económica, ya que estarán íntimamente ligadas a la transformación digital que buscan

las empresas. Y tendrán un papel aún más importante si se produce lo que muchos temen: un rebrote virulento de la enfermedad, ya sea este mismo otoño-invierno o en temporadas posteriores. Y estas tecnologías no solo impactarán en ciertos sectores, sino que generarán un mercado floreciente en diferentes eslabones de la cadena de suministro tecnológico, e impulsarán grandes beneficios comerciales para industrias como la de telecomunicaciones o las de diferentes categorías de servicios TI.

Como explica en su informe Don Alusha, analista senior de ABI Research, “una combinación de cómputo en la nube y conectividad 5G ultra confiable de baja latencia será la base para impulsar el crecimiento posterior a la COVID-19. Este crecimiento no es solo para las telecomunicaciones, sino también para una multitud de industrias pesadas en activos, que están adoptando los primeros procesos y operaciones digitales”. Con esto se refiere a la

sinergia entre 5G y la computación cloud en el borde, que proporcionará grandes oportunidades a los proveedores de servicios de comunicaciones (CSP), que se enfrentan a un cambio importante en la propia naturaleza de los servicios que demandan sus clientes.

Además, la transformación que ha impulsado la pandemia abarca otros sectores relacionados, como es el de los operadores hiperescala, que ahora deben afrontar sus propios cambios. Según dice Alusha, “los proveedores de hiperescala como Amazon y Microsoft están aprovechando sus operaciones de pequeña escala para lanzar sus ofertas cloud-edge. Tienen la visión de desarrollar capacidades cercanas al límite, pero no necesariamente tienen la penetración y distribución de las capacidades de red que tienen los CSP. Claramente, hay una oportunidad lista para ser abordada por alguien, pero aún no se sabe quién captura qué partes del emergente borde de la nube y el ecosistema 5G”.

EN BUSCA DE LA CONECTIVIDAD INTELIGENTE

vos paradigmas de entorno laboral se generan retos, ya que es imprescindible que los trabajadores cuenten con toda una nueva serie de habilidades. Pero si los profesionales y las empresas trabajan juntos para superar el bache, se abren nuevas oportunidades para la modernización de profesiones tradicionales y para la creación de otras nuevas, impulsadas por la tecnología.

Si actualmente las habilidades tecnológicas son cada vez más determinantes en la cualificación de los trabajadores, tras la pandemia lo serán aún más. De hecho, determinarán casi completamente la capacidad de las personas para obtener y mantener un empleo, así como para progresar en su carrera profesional. Pero actualmente la brecha digital es muy grande, y un 25% de las grandes empresas de los países miembros de la OCDE se ven en dificultades para encontrar trabajadores cualificados para determinados perfiles tecnológicos. Resolver esto no es tarea fácil, pero

las organizaciones empresariales, las instituciones académicas y los gobiernos están impulsando nuevos planes de formación tecnológica más acordes a las necesidades reales de las empresas.

Con ello pretenden reducir lo antes posible la escasez de talento tecnológico, un factor que frena la competitividad de los países y sus industrias en la economía globalizada. Esto irá acompañado de los grandes cambios que ya se están produciendo en la estructura de las organizaciones públicas y privadas, dos complicaciones que al confluir enturbian el futuro del mercado laboral. Para abordar este problema creciente, los expertos de Randstad recomiendan reavivar el diálogo social para involucrar a todos los actores de la sociedad, para conocer tanto la opinión como las necesidades de las personas y de las empresas, y cómo toda la estructura de la sociedad puede aportar su grano de arena para sentar las bases de la futura economía, no solo de las empresas sino de la sociedad. ■



MÁS INFORMACIÓN



[La tecnología cambiará un tercio de los empleos](#)



[Un CEO debe llevar la tecnología en su ADN](#)



[El mercado 5G de consumo se ralentiza, mientras que el empresarial sigue creciendo](#)



[El mercado de robots autónomos en almacenes crecerá con fuerza hasta 2025](#)



[Crece el gasto en soluciones de conferencia basadas en la nube](#)



[Avanzan los planes para crear una nube europea](#)



[Guía mundial de gasto en transformación digital](#)



[Informe Economía Digital en España](#)

Si te ha gustado este artículo,
compártelo



**NUEVO
INFORME**

DOCUMENTO EJECUTIVO

Teletrabajo en 2020: el futuro se hace presente



ELABORADO POR **itRESEARCH**

◀ Descarga este **documento ejecutivo** de **itRESEARCH** ▶

La era de la conectividad

Las nuevas propuestas de computación requieren mayores velocidades de transmisión y una transformación de los centros de datos y las redes de comunicación. ¿Cuál es el siguiente nivel? Las empresas están construyendo sus infraestructuras de muy diferente manera aprovechando tecnologías como 5G, Wifi, SD-WAN, entornos multicloud; incorporando el IoT; y aumentando la velocidad de conexión. Estas nuevas redes requieren, además, herramientas de monitorización que garanticen la agilidad y productividad, y medidas de seguridad para proteger estas vías de comunicación.

A continuación, puedes leer un resumen de las intervenciones y acceder al vídeo de cada uno de los participantes en el webinar de IT Trends, La era de la conectividad, emitido el pasado junio, o ver la sesión completa en este [enlace](#). Participaron Citrix, HPE, VMware, Sonicwall, Dell Technologies y D-Link. ■



NUNO SILVEIRO, DELIVERY NETWORKS SPECIALIST, CITRIX

“SD-WAN conecta con fiabilidad los CPD y las nubes. Aporta una visión amplificada y una capa de seguridad”

Las organizaciones distribuidas necesitan desplegar tecnología que conecte sus diferentes sedes, pero las redes WAN tradicionales tienen ciertas limitaciones de ancho de banda y gestión. La irrupción del concepto de SD-WAN (redes WAN definidas por software) viene a resolver los problemas de fiabilidad y resiliencia de las líneas y mejora la calidad de la experiencia de los usuarios. También resuelven las circunstancias que describía Nuno Silveiro, Delivery Networks Specialist en Citrix durante el IT Webinars [“La era de la conectividad”](#), celebrado en IT Trends. “La mayoría de las empresas se cambian a modelos de negocio digitales porque hay cada vez más competidores”, señaló. Además, las amenazas cibernéticas son una realidad latente en las empresas. “Desde el phishing que busca información oculta hasta la capacidad de los malware de robar datos de los ordenadores de los usuarios. Las compañías han de adquirir sistemas para paliar estos ataques a



NUNO SILVEIRO, DELIVERY NETWORKS SPECIALIST, CITRIX

EN BUSCA DE LA CONECTIVIDAD INTELIGENTE

la vez que optimizan procesos administrativos y de negocio”, prosiguió Silveiro.

Existe una conectividad entre las apps, los datos y la ubicación de los datos. “Están muy distribuidos en aplicaciones SaaS, y en distintas nubes donde los usuarios tienen que conectarse y consumir, lidiando con los retos que hemos identificado previamente. Esto genera un estrés a nivel de conectividad y experiencia del usuario que obliga a las compañías a replantearse un nuevo modo de pensar sobre la conectividad dentro de sus redes en cuanto a optimización y en términos de seguridad”, explicó.

“Abogamos por mantener las aplicaciones con la máxima experiencia de usuario y con seguridad, pero que permitan elegir a las empresas. Queremos que consuman datos en el CPD, en la nube pública, en la nube privada o con multi nubes híbridas, donde ellos quieran, no que tengan solo que centrarse en único producto obligatoriamente”, detalló Silveiro. “Nosotros permitimos a los usuarios que, independientemente de si se conectan por Wi-Fi o por datos, pueden hacerlo a todas las apps y puedan ser lo más productivos posible. Ahí es donde SD-WAN puede ayudar, ya que se conecta con fiabilidad a los CPD y a las nubes. Tiene una visión ampliada de lo que se produce en el entorno desde un punto de vista central e incluye una capa de seguridad a través de sus conectividades”, comentó este especialista de Citrix. “El objetivo es proveer una buena expe-

riencia de usuario con seguridad y posibilidad de elección para que las empresas se muevan de un entorno a otro y nosotros somos un facilitador de ese cambio. Acompañamos a nuestros clientes sea cual sea su objetivo”, añadió.

Tras la pandemia de la covid-19 y el viraje repentino hacia el teletrabajo de muchas compañías, se ha creado mucho estrés en las organizaciones ya que no tienen centralizada la información. “Han tenido que pensar en la seguridad del acceso y de transporte de todo dispositivo. Nosotros permitimos que los empleados y colaboradores se conecten de un modo efectivo y que se pueda controlar quién accede al sistema y desde dónde accede pues el teletrabajo ya es una realidad”, aseguró Silveiro. “Tenemos que entregar la capacidad de que las empresas tengan seguridad corporativa porque las tradicionales VPN no garantizan la seguridad necesaria pues no controlan ni todos los accesos ni todos los contenidos”, prosiguió.

Y es que, en Citrix, la seguridad es prioritaria. “Hay organizaciones que han migrado escritorios virtuales a la nube sin tener en cuenta que en casa hay más gente que usa la red y puede ser atacada. Hemos desarrollado una solución que permite trabajar en conjunto con la red preinstalada. Es fácil de desplegar y permite un control de la aplicación. Garantiza la política de seguridad al 100%”, concluyó Silveiro.

[Puedes ver aquí la intervención de Citrix.](#) ■



TECNOLOGÍA SD-WAN PARA POTENCIAR EL ESPACIO DE TRABAJO DIGITAL

La tecnología SD-WAN ayuda a las empresas a aprovechar al máximo su inversión, independientemente de que las personas trabajen desde una sucursal o

remota lejos del centro de datos. Permite utilizar todo el ancho de banda disponible, optimizar el rendimiento para aplicaciones virtuales, Web y SaaS como Office 365, además de otras apps de uso intensivo de ancho de banda como VoIP y garantizar conexiones siempre listas con la mejor calidad posible.



Si te ha gustado este artículo,
compártelo

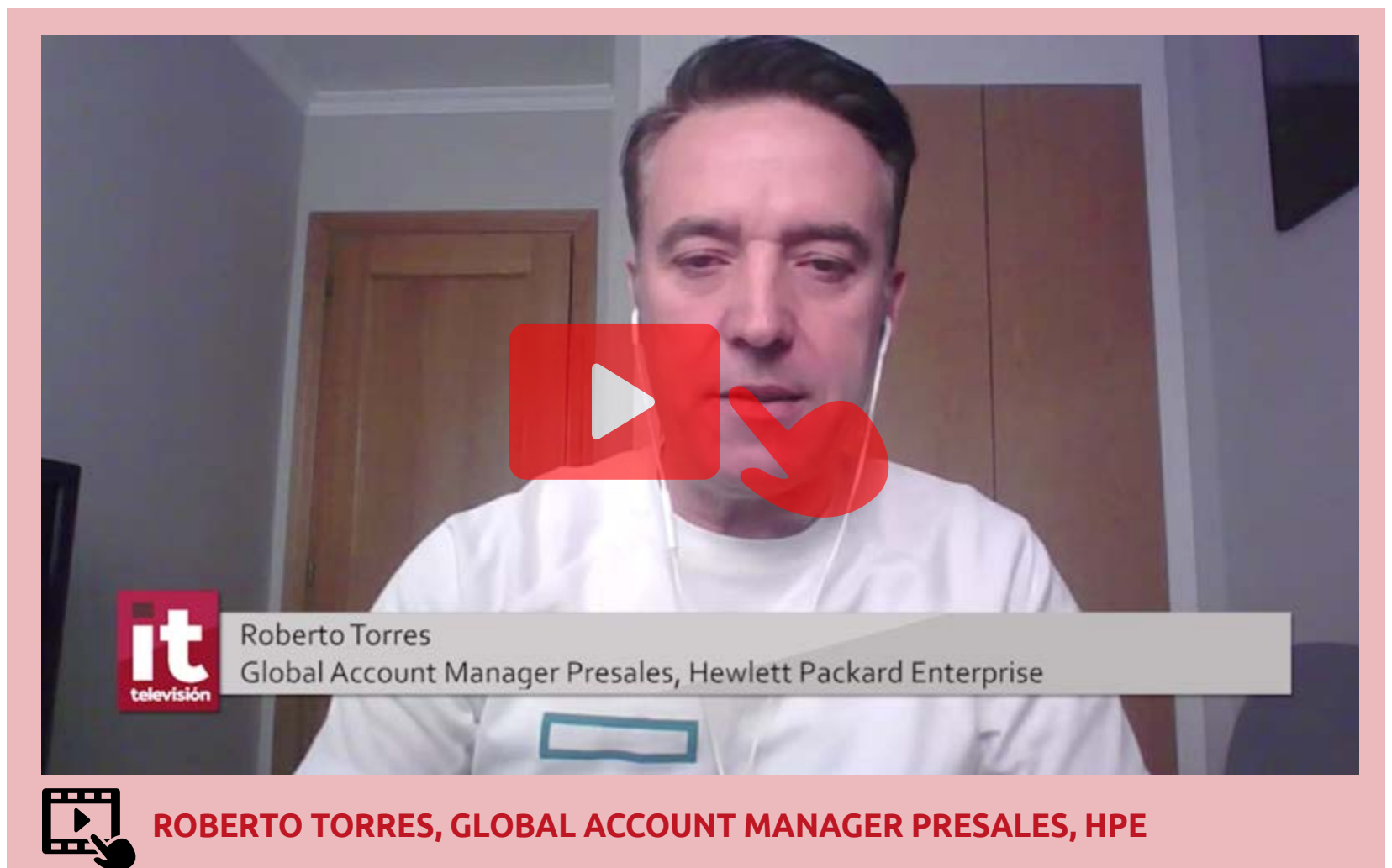


ROBERTO TORRES, GLOBAL ACCOUNT MANAGER PRESALES, HPE

“El empuje de la Industria 4.0 requerirá mayores conexiones y capacidades que 5G puede resolver”

5 G será uno de los motores de movilidad este año. El mercado de infraestructura 5G alcanzará los 4.200 millones de dólares y dos tercios de las empresas desplegarán esta tecnología en 2020 según Gartner. 5G es una alternativa a sus redes actuales con menor latencia y mayor ancho de banda. Esto implica más dispositivos conectados con más capacidades como inteligencia artificial, edge computing o automatización.

“Hay un empuje bestial hacia la industria 4.0 para obtener un mayor rendimiento productivo. La parte VR y AR de realidad aumentada es un caso de uso que va a venir con las nuevas tecnologías de comunicación. Con las gafas de realidad virtual, los empleados se van a poner en frente de las máquinas y leerán el manual de forma virtual”, comenzó Roberto Torres, Global Account Manager Presales en HPE, su intervención en el webinar [“La era de la conectividad”](#), sobre la necesidad de redes

**ROBERTO TORRES, GLOBAL ACCOUNT MANAGER PRESALES, HPE**

móviles más potentes que den capacidad de comunicación a las nuevas demandas de conectividad.

“Ayudará a que los navegadores de los coches estén conectados entre sí y no solo muestren las líneas verdes o rojas, sino que se verá en tiempo real dónde está el cruce, el semáforo o el peligro y se avisarán unos a otros. Las smart cities con telemetría y sensores ya son una realidad en España. En distintos monumentos se sabe cuándo hay menos personas para limpiar, hacer reformas etc; en sanidad, los doctores usarán esta tecnología para operar en remoto o detectar patologías de manera digital conectando su sistema con el de otros hospitales”, explicó Torres.

Pero, además, 5G traerá cambios fundamentales para las telcos. “Habrá cambios en las funcionalidades. Tiene que cambiar el acceso radio, aunque los teléfonos coexistirán con 4G también. Se producirán modificaciones en las funciones de red de cómo se implementa en el core”, desarrolló Torres. Además, se montarán redes virtuales dentro de la propia red física. “Desde el punto de vista de acceso y movilidad hemos visto la evolución del 1G al 5G. Con 5G se alcanzan velocidades de hasta 10GB por segundo”, prosiguió.

Esta tecnología de 5G convivirá con los equipos Wifi para proporcionar la cobertura necesaria según los casos. “Los disposi-

tivos móviles con imágenes en 4k, cámaras de video con mayor movilidad, más ancho de banda. Hay que evolucionar a microservicios y Kubernetes. Necesitamos crecimiento y la velocidad de despliegue tiene que ser máxima”, señaló Torres. “Las redes de Wifi 6 salen del mismo panel de control de 5G con más dispositivos conectados, más ancho de banda y movilidad entre edificios así que podemos unirlos y ahorrar costes a las grandes telcos”, añadió.

Para este tipo de cliente, HPE propone una línea de servidores ruggedizados para el despliegue de redes 5G. “Siempre hemos tenido servidores especializados para el mundo telco. No valen los servidores tradicionales porque hay que llevarlos al Edge. Llevamos tiempo desarrollando equipamientos preparados para aguantar entornos hostiles. Hay mucho polvo y altas y bajas temperaturas, así que hemos tenido que poner equipos especiales. Tenemos la gama tradicional y la Carrier-grade para equipos de telecomunicaciones con despliegues más específicos. Todo es auto programable y definido por el software”, subrayó Torres. “Podemos desplegar entornos de inteligencia artificial, GPUs para desplegarlas en máquinas virtuales o kubernetes donde el IoT pueda orquestar todo este tipo de tecnologías”, concluyó.

[Ve la intervención de HPE en este webinar.](#) ■



LAS VENTAJAS DE LA TECNOLOGÍA 5G

Una red de acceso sólo es posible con un núcleo que sea verdaderamente 5G.

Para HPE es importante la gestión de datos de suscripción y de sesión a través de un entorno de

datos compartidos unificados y centralizados, proporcionar el servicio adecuado para cada caso de uso con una división de la red, acelerar los ciclos de desarrollo a través de una arquitectura abierta de nubes nativas y el enfoque DevOps.



Si te ha gustado este artículo, compártelo



JOAQUÍN GÓMEZ, NSX SALES ACCOUNT EXECUTIVE, VMWARE

“Hemos añadido a la red SD-WAN, el cloud y los usuarios, de manera que tenemos todo en SD-WAN, no solo oficina o campus”

La empresa distribuida y ubicua requiere, de igual manera, redes distribuidas, ubicuas, disponibles para dar servicio, con conexiones fiables y estables y fácilmente gestionables; capaces de interconectar esos entornos de TI híbridos y multicloud donde se alojan las aplicaciones y datos corporativos.

Para VMware, el contexto viene marcado bajo un paradigma de nuevas tecnologías. “Nos estamos moviendo muy deprisa en cuanto a trabajo remoto y dispositivos. Necesitamos muchas más conectividades y de una forma diferente. En VMware nos hemos preguntado dónde está mi red, las apps, y cómo conectarnos de manera óptima”, afirmó Joaquín Gómez, NSX Sales Account Executive, en VMware, durante el IT Webinars [“La era de la conectividad”](#).

“Cualquier dispositivo ha de poder conectarse a tu infraestructura, desde cualquier app y cualquier plataforma. Hay que cambiar cualquier entorno de ejecución porque las apps deben ser



accesibles desde cualquier dispositivo. Todas las operaciones han de ser comunes y la seguridad está embebida en la plataforma”, señaló. Así, la solución de VMware da prioridad a la seguridad y a la migración. “Proponemos diseñar el data center como si fuera cloud (aunque sea en casa). De esta manera, el almacenamiento y las redes serán definidas por software y lo que hago en casa lo puedo hacer en cualquier nube. Después, hay que poner políticas de Zero Trust o políticas de seguridad sobre quién puede hablar con quién dentro de mi centro de datos virtual; también se necesita visibilidad analítica para proteger el contexto y la app en la zona más cercana desde donde se produzca el ataque. Una vez tengo el data center con lo que me interese, lo puedo mover a la cloud aplicando las mismas políticas de segmentación y seguridad”, argumentó Gómez.

En una red cloud, todo está hiperconectado. “Las apps están muy distribuidas. A partir de NSX podemos hacer una infraestructura con piezas pequeñas en diferentes clouds. Esas piezas consiguen eliminar el cerebro de quien ejecuta el trabajo. El cerebro está concentrado en mi data center (en el controller) y hay que poner a trabajadores en diferentes clouds para optimizar, mejorar y acelerar el tráfico de la aplicación poniéndolo cerca de donde se encuentre. Analiza qué usos se hacen en la aplicación, además de prevenir ataques”, explicó Gómez.

“Las redes SD-WAN se han diseñado para conectar oficinas o campus con el data center. Nosotros hemos hecho algo distinto. Hemos añadido a la red SD-WAN, el cloud y los usuarios, de manera que tenemos todo en SD-WAN, no solo oficina o campus. Así se hace una extensión al cloud storage, cloud de seguridad, destination cloud, apps, SaaS, Oracle o cualquier herramienta. Hay muchos tipos de cloud y necesitamos que SD-WAN participe dentro de esta infraestructura, no solo para conectar las ramas de la oficina con el data center, sino también la parte de arriba, es decir, los aplicativos”, comentó Gómez.

En VMware creen que solo puede coexistir seguridad y red a través de la visibilidad. “Tenemos una serie de soluciones con una capa de visibilidad. Hay que ver si el tráfico que va en los diferentes clouds de mi data center, oficinas en el cloud, etc, lo voy a agregar y ver quién habla con quién; después trazo un mapa y lo aterrizo en una solución agregada NSX Intelligent. Con esta solución me voy a conectar con elementos hardware en modo cloud, switches, routers, SD-WAN, etc. Tenemos unos sensores que diferencian los distintos tipos de dispositivos con inteligencia artificial. Para que se conecte todo con seguridad tiene que haber visibilidad y transparencia”, concluyó Gómez.

[Si quieres ver la intervención de VMware, accede en este enlace.](#) ■



EL IMPACTO ECONÓMICO DE CLOUD NETWORKING

Las aplicaciones ahora se ejecutan en todos los puntos de este espectro, y son críticas para la capacidad de las empresas de ganar en mercados hipercompetitivos. Sin embargo, incluso cuando el éxito de los negocios se ha vuelto más dependiente de esta

nueva arquitectura y la cantidad de datos que fluyen a través de las conexiones ha aumentado, muchas organizaciones todavía carecen de un enfoque unificado para la gestión, automatización y seguridad. La Red de Nube Virtual (Virtual Cloud Network) ofrecida en la tecnología NSX, VMware pretende abordar estos problemas, permitiendo a las organizaciones aprovechar una abstracción de software para conectar, operar y asegurar las arquitecturas de extremo a extremo que soportan las aplicaciones donde residan.



Si te ha gustado este artículo, compártelo



LUIS FISAS, DIRECTOR PARA SUR DE EUROPA, SONICWALL

“Políticas de acceso muy permisivas, no autenticar con doble factor, passwords muy sencillas o antivirus basados en listas o firmas, son los fallos más comunes al proteger la red”

La red empresarial está sometiéndose a un constante cambio y evolución. El périmetro se está perdiendo de manera acelerada sumando a marchas forzadas a los hogares. Se incorporan los dispositivos IoT y nos conectamos a la cloud. El rendimiento de la red y su expansión son críticos y los ciberataques se están multiplicando.

Luis Fisas, director para sur de Europa en Sonicwall, evalúa en su intervención en el IT Webinars [“La era de la conectividad”](#), la realidad que vivimos: “Disponemos de más de un millón de sensores en todo el mundo que recopilan información en tiempo real. Existe un crecimiento del ransomware de un 56% frente al año pasado y la covid-19 ha provocado un aumento de ataques que se focalizan en documentos de PowerPoint y PDF”. Además, el 70% de lo que circula por internet está encriptado. “Esto produce que no sea fácilmente analizable por un firewall normal y provoca que las empresas adopten nuevas tec-



LUIS FISAS, DIRECTOR PARA SUR DE EUROPA, SONICWALL

nologías para descryptar y encriptar este tráfico. Solo un 5% de los clientes están inspeccionando este tráfico así que es un peligro para el 95% de empresas restantes”, añadió Fisas.

Por otra parte, el teletrabajo ha cambiado la manera de plantearse la seguridad de las empresas. “En dos meses hemos implementado un plan de trabajo en remoto que se iba a ir desarrollando en siete años. Ahora los puntos de entrada a los servidores no están en un edificio sino en múltiples sitios, lo que amplía el riesgo de ciberataque”. Fisas ejemplifica el momento actual con un símil: “Hemos pasado de tener un castillo con una muralla a un modelo aeropuerto donde entra y sale todo el mundo”.

Es un nuevo paradigma. “Las empresas han de saber si la persona es quien dice ser y que no está suplantando la identidad de otra. El dilema es la autenticación, pero gracias a una plataforma de capture cloud con dispositivos y elementos de ciberseguridad, distinguimos si los dispositivos que se conectan son correctos”, afirmó Fisas.

En Sonicwall enfocan este desafío en tres áreas: asegurando el acceso remoto o móvil, protegiendo el acceso a las aplicaciones cloud y salvaguardando los dispositivos en el puesto de trabajo. “Lo hacemos a través de equipos SMA que defienden estas credenciales”, añadió el directivo. Además, “invertimos en sistemas de autenticación y protección de los correos como

Google Suite, Office 365 y para clouds como One Drive o Dropbox. Después hay que proteger el PC analizando el comportamiento de las apps. Además, el gran peligro de los malware no son los que ya existen, sino los que no conocemos porque se están desarrollando. Conviene tener sistemas de protección con inteligencia artificial puesto que el nivel de desarrollo y variación es rápido y de gran volumen”, dijo Fisas.

Las empresas se ven abocadas a cambiar su infraestructura, pero a veces, cuando se hace de manera rápida, se cometen errores. “Políticas de acceso muy permisivas, no autenticar con doble factor, nivel de las passwords muy sencillos o antivirus basados en listas o firmas y no análisis de comportamiento son los fallos más comunes”, destacó.

Lo que está claro es que después del confinamiento, el teletrabajo ha venido para quedarse. “Hemos pasado de un 20% a un 100% de trabajadores en muchas empresas y algunos clientes se plantean cerrar o reducir el espacio en oficinas porque no van a necesitar tanto espacio. Muchas empresas ofrecerán el 50% del tiempo de trabajo en remoto, lo que permitirá más flexibilidad laboral y otras van a ofrecer remoto siempre. Los sistemas de seguridad de muchas empresas han de cambiar y ser más robustos para garantizar su propia protección”, concluyó Fisas. [Para ver la intervención de Sonicwall, accede aquí.](#) ■



¿SON SUS OFICINAS REMOTAS UNA PUERTA ABIERTA A LOS CIBERATAQUES?

Los investigadores de amenazas de Capture Labs de SonicWall registraron 9.900 millones de ataques de malware en 2019. Durante los últimos cinco años, los ciberdelincuentes han atacado a las organizaciones con un ingente volumen de ataques. Su objetivo era sencillo: lanzar una red lo más grande posible y recoger los frutos. Las soluciones SD-Branch son una de las herramientas ideales para una seguridad sin límites en entornos empresariales distribuidos.



Si te ha gustado este artículo, compártelo



GONZALO DE ANTONIO, SALES EXECUTIVE, DELL TECHNOLOGIES

“El open networking garantiza protección, velocidad en la inversión y agilidad en las empresas”

Uno de los conceptos que ha venido a revolucionar las redes es el open networking que describe una red que utiliza estándares abiertos y hardware commodity, es decir, que tiene la capacidad de ser abierta en términos de compatibilidad de componentes, tanto software como hardware. “Las redes son piezas de la infraestructura que están ancladas en el pasado, pero el open networking viene a renovar la industria con una aproximación totalmente abierta frente a los modelos que han regido tradicionalmente dicha infraestructura”, señaló Gonzalo de Antonio, Sales Executive en Dell Technologies en el IT Webinars [“La era de la conectividad”](#). “Nosotros viramos al open networking hace 6 años. Es una transformación de distribuciones propietarias o arquitectura tradicional o de un solo fabricante, a un modelo en el que cada componente puede ser fabricado en una compañía distinta. Esto garantiza protección, velocidad en la inversión y agilidad en las empresas”, prosiguió.



GONZALO DE ANTONIO, SALES EXECUTIVE, DELL TECHNOLOGIES

“Dell diseña el hardware del servidor, pero se puede desplegar software de otras compañías como Linux o Microsoft. Esto ha sido una revolución en el mundo del cómputo y cambió el mercado. Se ha producido una desagregación total de la infraestructura: hay diferentes proveedores y diferentes capas”, señaló de Antonio, cuya compañía está convencida de que el open networking es el futuro de las redes. “La separación de capas la llevamos a la práctica con distintos proveedores de chips. De ahí diferentes puertos; diferentes CPU, diferentes memorias, etc”, comentó este especialista de Dell Technologies. “Si somos nosotros los que desplegamos y vendemos un software, garantizamos el soporte y garantía de la solución. De esta manera vamos al mercado con una aproximación diferente según las necesidades de cada cliente – se le proporciona hardware, un sistema operativo o soporte, pero también podemos suministrar software solo, pero dando un soporte total”, añadió.

“Las ventajas son la arquitectura abierta, la posibilidad de elección, estandarizar hardware, bajar los costes porque si se quiere cambiar el hardware no se tiene por qué renovar el software y viceversa y eso se traduce en un ciclo de vida más largo y una mayor protección de cada inversión”, matizó. Bajo este principio, Dell Technologies cubre todos los componentes de la red involucrados en una infraestructura moderna para cualquier empresa. “Damos una

solución completa definida por software que puede integrarse fácilmente en el entorno existente. Huimos de cuando las empresas dicen: deshágase de su infraestructura legacy”.

Toda la red se conforma y trata como un único elemento lógico, aunque haya centenares de elementos en la red. “Se pueden tratar y gestionar fácilmente. Ese elemento lógico puede estar distribuido en diferentes localizaciones, pero se puede gestionar desde un único punto de gestión, no hay que conectarse a cada uno de los switches. De esta manera facilitamos las operaciones y la gestión”, comentó de Antonio, quien continuó detallando las capacidades de la propuesta de Dell en el mercado: proveer de forma automática los puertos a los que se conectan las máquinas virtuales; ser inteligente e identificar los flujos de tráfico que entran y aplicar políticas diferenciadas de segmentación; o proporcionar información a la empresa para identificar problemas y resolverlos sin usar herramientas externas. “Sabemos lo que ocurre a tiempo real y lo que ocurrió en el pasado. Es decir, si un servidor se cayó o no funcionaba bien”, añadió.

La compañía también dispone de soluciones de SD-WAN para sedes remotas, asegurando la calidad de la experiencia del usuario. “La solución es completa. Las redes han de cómo los paracaídas: funcionan mucho mejor cuando están abiertas”, concluyó. [Para ver la intervención de Dell Technologies, accede en este enlace.](#) ■



OPEN NETWORKING PARA ACELERAR LA AGILIDAD DE LAS EMPRESAS

La infraestructura de red en muchas empresas está envejeciendo y se ha quedado obsoleta. Sus componentes propietarios y las interfaces que utilizan pueden obstaculizar los planes de una empresa para avanzar. La red está de alguna manera bloqueada, o cerrada por el hardware y software propietarios del fabricante desplegado, lo que limita el ritmo de la innovación en comparación con el rápido avance de los entornos informáticos de computación abiertos.



Si te ha gustado este artículo, compártelo



ANTONIO NAVARRO, COUNTRY MANAGER IBERIA, D-LINK

“Necesitamos mayor ancho de banda a nivel LAN e inalámbrico. Habrá que aumentar los gigas; apostamos por conexiones de 1GE y 10GE”

La transformación digital ha incrementado la importancia de la red, especialmente en el extremo donde clientes, empleados, aplicaciones cloud y dispositivos IoT se conectan a la empresa. “En D-Link creemos que la transformación digital es una oportunidad de negocio porque necesitamos dar acogida a miles de dispositivos conectados y eso necesita infraestructuras de red. Necesitaremos mayor ancho de banda a nivel LAN e inalámbrico. Habrá que aumentar los gigas. Lo mismo en wireless. Necesitaremos movilidad y escalabilidad ilimitada; llegan tecnologías como 5G. El PoE, las Smart cities, y las industrias 4.0 necesitan soluciones específicas que nosotros abordaremos”, expuso Antonio Navarro, Country Manager para Iberia de D-Link, sobre las claves del presente y futuro de la tecnología de conectividad en el webinar [“La era de la conectividad”](#) de IT Trends.

Para solventar estas necesidades, desde el proveedor apuestan, dentro de la tecnología de



ANTONIO NAVARRO, COUNTRY MANAGER IBERIA, D-LINK

conmutación, por las conexiones 1GE y 10GE. “Tenemos que dar cabida a esas velocidades. Democratizar que una PYME pueda tener una conexión a gran velocidad y una empresa grande, incluso un nivel mayor”. El crecimiento tiene dos vertientes. “Primero en soluciones como data center y core de red de alto rendimiento de 10, 25, 40 o 100 GB. Por otro lado, vamos a presentar un switch no gestionable puramente de 10 GB”, dijo Navarro. Junto a estas propuestas, el director general de D-Link en Iberia apuntó estas otras tendencias en conectividad.

❖ **PoE (Power over Ethernet):** Es una subtecnología que cada vez cobra mayor importancia. “Es la que más crece por los puntos de acceso, cámaras IP o telefonía IoT. Antes estaba limitado a 100 metros de distancia, pero ahora alcanza hasta 250 metros. Es muy importante para la videovigilancia exterior porque se ahorran costes y así, no se depende de equipos intermedios”, explicó Navarro.

❖ **Switching industrial.** “Se usa para todo lo relacionado con digital signage, transporte, industria 4.0, video vigilancia y Wireless exterior porque necesitaremos resistencia a altas o bajas temperaturas y esto lo aportan los equipos robustos”.

❖ **Wi-fi:** “cubrimos el Wireless de tres maneras: a nivel tradicional con controladores Wireless, a través de gestión de proyectos de control mediante plataformas basadas en software o con una plataforma pura en cloud.

Con estos sistemas tenemos diferentes velocidades y dispositivos específicos para hoteles, por ejemplo. Permite gestionar la política de seguridad, los escenarios multi-side, la gestión del ancho de banda, hotspots etc”.

❖ **Cloud:** “nuestra solución tiene una escalabilidad ilimitada y ventajas como equipos que se auto provisionan y permiten un ahorro de costes de desplazamiento. Damos gestión cloud centralizada tanto en la parte inalámbrica como en la cableada y tenemos más de siete modelos a los que iremos sumando más a lo largo del año”.

❖ **Gateways SD-WAN:** “Es nuestro complemento porque vamos a ver cada vez más entornos críticos en cloud. Controla y asegura el tráfico de red, se dota de muchas funcionalidades a nivel seguridad, servicios VPN, firewall, DPI, etc. Con esta tecnología sabemos lo que está pasando, y cómo controlarlo en cada momento”.

Asimismo, en la sesión, Navarro hizo referencia a la convivencia de Wifi 6 y 5G. “Van a cohabitar y se van a ayudar mutuamente. Sacaremos equipos en todas las plataformas. Estas tecnologías tienen ventajas muy parejas: mayor velocidad, mucha menor latencia, mucha mejor gestión de usuarios concurrentes, mayor densidad de usuarios por celda y mucho menor consumo”, concluyó Navarro.

[Si quieres ver la intervención de D-Link, puedes acceder en este enlace.](#) ■



SOLUCIONES DE CONMUTACIÓN PARA EL CENTRO DE DATOS



Este ebook repasa las principales arquitecturas de red para el data center y las soluciones de switching que dan respuesta a las demandas actuales del CPD.

Si te ha gustado este artículo,
compártelo



Autenticación y gestión de identidades, el nuevo perímetro de seguridad

La identidad se ha convertido en el nuevo perímetro de seguridad. Saber quién accede, desde dónde, con qué dispositivo y a qué recursos es uno de los pasos más complicados de la migración a la nube.

La manera de afrontarlo pasa por la autenticación basada en contexto y de múltiples factores, una autenticación no sólo de las personas, sino también de las aplicaciones y dispositivos, y de una manera centralizada.

No nos olvidemos de la gestión de cuentas privilegiadas, un aspecto muy importante teniendo en cuenta que, según Forrester, el 80%

de las violaciones de datos tienen una conexión con credenciales privilegiadas comprometidas, como contraseñas, tokens, claves y certificados.

Las empresas necesitan mejorar la protección de las identidades, amenazadas por una gestión poco hábil de las contraseñas, un panorama digital en constante cambio o una gran rotación de los empleados, lo que genera la necesidad de gestionar el aprovisionamiento y el desaprovisionamiento de credenciales. Desde una perspectiva de capacidad de administración y cumplimiento, esto representa

una gran amenaza para proteger los datos de su empresa

Dentro de las actividades trimestrales de IT Trends, el pasado abril se emitió la sesión online **Autenticación y gestión de identidades, el nuevo perímetro de seguridad**, a cuya sesión completa puedes acceder [aquí](#), con la participación de CyberArk, Micro Focus, Fortinet, Thales, Check Point, F5 Networks, One Identity, Akamai y SonicWall. También puedes pinchar, en la siguiente página, en cada una de las imágenes de los portavoces para acceder a sus intervenciones en nuestra web. ■



EN BUSCA DE LA CONECTIVIDAD INTELIGENTE



Carlos Luaces de Santiago
Sales Engineer Iberia, CyberArk

Carlos Luaces de Santiago, CyberArk



Ramsés Gallego
Security International Director, Micro Focus---

Ramsés Gallego, Micro Focus



Raúl Tejeda
System Engineer, Fortinet

Raúl Tejeda, Fortinet



Guillermo Martín Soto
Regional Sales Manager Iberia & North Africa, Cloud Protection & Licensing Identity and Access Management, Thales

Guillermo Martín Soto, Thales Iberia y Magreb



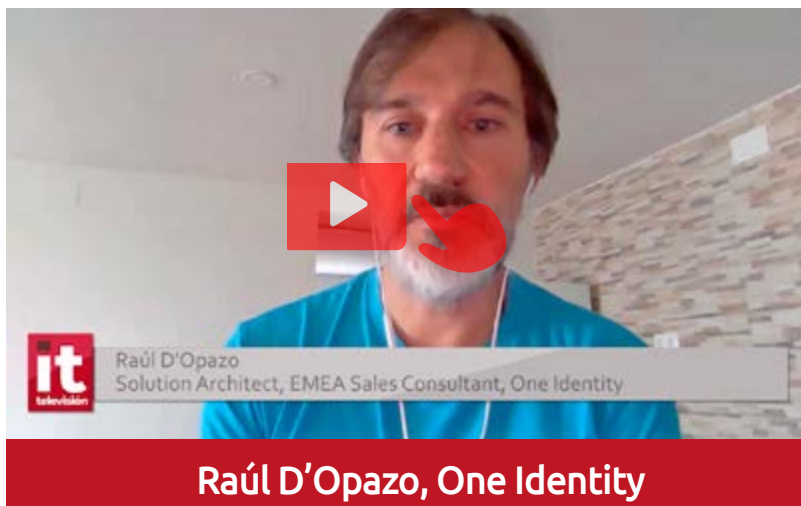
Eusebio Nieva
Director Técnico, Check Point

Eusebio Nieva, Check Point



Daniel Varela
Solutions Engineer Security, F5 Networks

Daniel Varela, F5 Networks



Raúl D'Opazo
Solution Architect, EMEA Sales Consultant, One Identity

Raúl D'Opazo, One Identity



Enric Mañez
Enterprise Security Sales, Akamai

Enric Mañez, Akamai



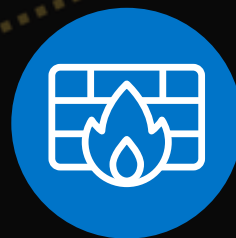
Sergio Martínez
Director General, SonicWall Iberia

Sergio Martínez, SonicWall Iberia

NO SOMOS SOLO FIREWALLS.

SonicWall ofrece ciberseguridad sin límites para la era hiperdistribuida y una realidad laboral en la que todo el mundo teletrabaja con múltiples dispositivos en un entorno poco seguro.

La plataforma en la nube SonicWall Capture Cloud integra la seguridad, la gestión, el análisis y la inteligencia de amenazas en tiempo real en la cartera de productos de redes, correo electrónico, dispositivos móviles y de seguridad en la nube de la empresa.



Firewalls físicos y virtuales



Sandbox multi-motor en la nube



Seguridad en la nube pública y privada



Antivirus de nueva generación



Correo electrónico seguro



Seguridad Cloud



SD-WAN



Acceso Remoto Seguro



Wifi Seguro



Visibilidad e informes unificados



www.SonicWall.com

SONICWALL®

 @SonicWallSpain

El teletrabajo ha llegado para quedarse Trabajamos como vivimos

Santiago Campuzano,
Country Manager
de Citrix Iberia



Y por fin llegó la calma. Parece que, muy lentamente, la situación generada por la crisis del coronavirus se estabiliza en toda la sociedad, tanto en el plano personal como en el profesional. Han sido unos meses muy duros que, especialmente en España, no se olvidarán y que han supuesto un reto muy difícil de superar. Desde el punto de vista profesional y, en concreto, en el ámbito de la tecnología ha sido un reto enorme para las organizaciones mantener la capacidad productiva a través del plan de continuidad de negocio, con grandes retos en las áreas de infraestructuras, comunicaciones y movilidad extrema, con implementación de programas de teletrabajo.

Un reto para todos, aunque mayor en empresas donde ni existía la posibilidad tecnológica ni la cultura o el liderazgo para llevarlo a cabo. Después de ser partícipes en proyectos con la mayoría de las grandes empresas y organizaciones públicas, podemos decir que la continuidad de negocio ha sido muy exitosa y con una fuerte implementación de los modelos de acceso remoto. Y digo

modelos de acceso remoto y no teletrabajo porque evidentemente lo que estamos viviendo en estos días no es un modelo de teletrabajo y, mucho menos, de smartworking. Sin embargo, se ha demostrado que la tecnología y las personas están sobradamente preparados para aceptar que, probablemente, el teletrabajo ha llegado para quedarse. Aunque quedan muchas tareas pendientes para que pueda ser efectivo y beneficioso para las personas, las empresas y la sociedad.

Desde el punto de vista de las personas quizás nos hemos llevado lo peor del teletrabajo y ninguna de sus ventajas. Entre otras vicisitudes hemos vivido unas jornadas de trabajo interminables, escasa comunicación dentro de la organización informal, falta de medios para tener un espacio físico de trabajo mínimamente preparado, tener que adecuar el hogar para que todo el mundo pudiera cumplir con sus obligaciones o formativas, carencias en las comunicaciones, problemas para conciliar el entorno profesional y el familiar o, en algunos casos, incluso llevar el ordenador físico

desde la oficina a casa. Visto así, sinceramente no es un panorama muy halagüeño. Después de haber vivido prácticamente toda mi carrera profesional en entidades que permitían y fomentaban el teletrabajo, esto no es teletrabajo.

En el plano personal los beneficios, en un entorno bien gestionado, son muchos. Facilidad en la conciliación familiar, mayor productividad personal al evitar las horas punta de tráfico o mejora en algunos hábitos de vida como la alimentación o el deporte. En definitiva, un modelo motivador en casi todos los aspectos, ofreciendo ventajas profesionales y personales. Para las empresas ha sido una lucha contrarreloj y, en muchas ocasiones, sin un destino muy claro. Evidentemente los objetivos de los planes de continuidad de negocio eran conocidos, sin embargo, más allá del puro ámbito tecnológico. Pero si bien se ha demostrado que tecnológicamente es un reto superado, desde el punto de vista cultural y desde el liderazgo quedan aún tareas pendientes. Para empezar, el teletrabajo supone un ejercicio de responsabilidad bidireccional.

EN BUSCA DE LA CONECTIVIDAD INTELIGENTE

Por parte de los miembros del equipo tienen que ser capaces de gestionar su tiempo, sus actividades y sus objetivos; y, por parte de los managers se deben fijar medidas de control basadas en KPI's, al tiempo que se huye del micromanagement.

A decir verdad, todos los equipos tienen que entender que la situación vivida, a pesar de estar con una teórica mayor disponibilidad, requiere una mayor flexibilidad con menor carga de reuniones virtuales y, sobre todo, ayudando a proteger el individuo dentro de su espacio y fuera de la organización no funcional de la empresa. En definitiva, garantizar la productividad global sin sobrecargar a las personas porque exigir resultados no tiene que ver con controlar el trabajo. Además, existen ahorros relevantes en los gastos asociados a los edificios e infraestructuras, se producen reducciones significativas del absentismo y, en la sociedad multigeneracional en la que vivimos, supone un factor importante de atracción de talento.

Más que nunca el trabajo es lo que se hace, no donde se hace. Por último, desde el punto de vista social también el teletrabajo tiene un impacto relevante. Aparte de permitir reducir el tráfico general, con la consecuente reducción de la contaminación, también ahorra tiempo a todos los trabajadores que se ven afectados por la reducción del tráfico en la hora punta. Por supuesto, también se disminuyen los incidentes y accidentes de tráfico en el tiempo de desplazamiento al lugar de trabajo. Más allá de hacer demagogia acerca de modelos de

transformación digital, que en muchos casos poco tienen que ver con el teletrabajo o el smartworking, debemos ser pragmáticos en entender por qué la llamada nueva normalidad va a afectar también a la forma en la que las personas trabajan.

Como consecuencia de la revolución socio-tecnológica de los últimos años nuestra forma de entender el uso de dispositivos y aplicaciones ha cambiado, siendo una parte intrínseca casi de nuestra naturaleza humana actual, por ello adaptarnos a usarlo no ha sido complicado, aunque sí gestionarlo en la situación vivida. Ahora más que nunca trabajamos como vivimos.

Sin embargo, también es cierto que la experiencia digital se ha convertido en un componente, diríamos, que intrínseco a nuestra forma de vida. Por ello, la selección correcta de la tecnología es si cabe más crítica que nunca. Ya que no en vano buscamos de forma nativa una experiencia digital óptima, que ayude a satisfacer las expectativas del usuario, permita entornos flexibles y dinámicos desde el punto de vista de IT y, por supuesto, lo haga en un entorno de seguridad.

Nuestra experiencia nos ha permitido a ayudar a que más de medio millón de personas trabajen desde sus casas en estos días y creemos que únicamente es viable con una visión holística del proceso, por ello, cuando hablamos de los espacios de trabajo inteligentes o digitales y de la transformación del puesto, pensamos en una forma de acceso única que no cambie la experiencia del



CÓMO TRANSFORMARSE EN UN ESPACIO DE TRABAJO DIGITAL

Ya no es suficiente almacenar de forma segura sus archivos. Debe poder trabajar con esos archivos en tiempo real con sus compañeros, clientes y partners. Su espacio de trabajo

digital debe extenderse más allá del uso compartido de archivos para apoyar una plataforma de colaboración de contenido que se centre en la seguridad, los flujos de trabajo y la movilidad y productividad de los usuarios.



cliente con la máxima seguridad, independientemente del dispositivo y de donde esté el usuario y adaptándose a ese contexto; y, lógicamente, acompañado del modelo adecuado de infraestructura, ya sea cloud u on premise en función de la estrategia de la organización. ■

Si te ha gustado este artículo, compártelo



La urgente necesidad de proteger las credenciales privilegiadas

Anastasia Sotelsek,
Principal Sales
Engineer de
CyberArk Iberia



Si mejorar la seguridad de credenciales privilegiadas no es una de las prioridades principales de los responsables de seguridad, debería serlo. Los atacantes externos y los intrusos malintencionados actúan constantemente sobre cuentas privilegiadas para robar información confidencial, fingir ser una persona de confianza o interrumpir aplicaciones y servicios críticos para el negocio.

Según el último Informe de CyberArk, Global Advanced Threat Landscape, menos de la mitad de las organizaciones tiene implementada una estrategia de seguridad de acceso privilegiado para DevOps, IoT, RPA y otras tecnologías que son fundamentales para las iniciativas digitales. Esta debilidad facilita que los atacantes asalten el acceso privilegiado que les permita moverse lateralmente a través de una red para avanzar en su ataque.

Las cuentas privilegiadas son ubicuas. Existen en sistemas, bases de datos y aplicaciones;

residen en las instalaciones y en la nube, y son utilizadas por personas, aplicaciones, procesos automatizados, máquinas y bots. Las organizaciones deben localizar y proteger cientos, o incluso miles, de cuentas privilegiadas dispersas en la red.

Para mitigar el riesgo, estas credenciales deben protegerse con fuertes medidas de seguridad de acceso privilegiado. Implementar un programa efectivo de gestión de acceso privilegiado (PAM) es un desafío para muchas organizaciones, ya que el panorama de amenazas es amplio, complejo y en constante evolución.

LA UBICUIDAD CONDUCE A LA VULNERABILIDAD

A medida que las organizaciones migran a plataformas en la nube y adoptan nuevas tecnologías como la automatización de procesos robóticos (RPA), el número de identidades no humanas, de servidores y de aplicaciones en

cada organización aumenta exponencialmente. Las organizaciones deben adaptar continuamente sus sistemas y prácticas PAM para seguir el ritmo de esta innovación, así como la evolución paralela del panorama de amenazas.

CONOCER NUESTRO GRADO DE EXPOSICIÓN

Muchas organizaciones confían en procesos manuales ineficientes para asignar y monitorizar credenciales de cuentas privilegiadas. Las contraseñas y las claves a veces permanecen sin cambios durante meses, o incluso años, después de su creación. Los ex empleados, integradores y fabricantes a menudo mantienen el acceso a aplicaciones y sistemas críticos mucho después de su salida de la empresa, exponiéndolas a violaciones de datos y ataques maliciosos.

Los empleados descontentos o los atacantes externos pueden actuar sobre cuentas inactivas o contraseñas sin cambios para realizar ataques sofisticados. Una vez que un atacante inteligente

te obtiene acceso a credenciales de cuentas privilegiadas, puede moverse lateralmente y acceder a otros recursos empresariales críticos en solo minutos. Los adversarios pueden pasar de penetrar un puesto de trabajo a obtener derechos de administrador completos en un controlador de dominio en menos de 20 minutos.

Al pensar como si fueran un atacante, las organizaciones pueden defenderse de las técnicas que estos suelen usar para acceder a cuentas privilegiadas, robar datos y eliminar sistemas.

PLANIFICAR CON ÉXITO LAS ACCIONES PAM

Tener un marco de seguridad priorizado por fases para alinear las iniciativas PAM con la posible reducción de riesgos, ayuda a las organizaciones a abordar sus responsabilidades lo más rápido posible.

Los responsables de seguridad deben seguir estos pasos:

1. Identificar las cuentas privilegiadas, las credenciales y los secretos más críticos, y enfocarse en las cuentas que podrían poner en peligro la infraestructura de misión crítica o exponer datos confidenciales desde una perspectiva de riesgo de la organización.

2. Desarrollar un plan priorizado para reducir las vulnerabilidades y fortalecer la seguridad. Establecer qué acciones son las más importantes, qué elementos se pueden lograr

rápidamente y con recursos mínimos, y cuáles requieren un tiempo y esfuerzo significativos.

3. Una vez que el plan esté implementado, debe ser reevaluado y mejorado continuamente para abordar las amenazas en evolución y las nuevas tecnologías.

APROVECHAR AL MÁXIMO LA INVERSIÓN

Los atacantes perfeccionan continuamente sus habilidades, encontrando nuevas formas de penetrar en las redes y evitar ser detectados. Los equipos de TI y seguridad pueden superar estos desafíos y minimizar los riesgos de acceso privilegiado al observar cómo los atacantes vulneran el acceso privilegiado, y preguntarse: ¿cuáles son los vectores de ataque de acceso privilegiado más comunes y cómo piensa y se comporta el perpetrador en cada caso?

Para evitar el robo de credenciales, las organizaciones deben discontinuar los procesos desarticulados manuales de gestión de secretos y credenciales, introducir un repositorio digital (Vault) seguro, para almacenar y monitorizar de forma centralizada las credenciales de cuentas privilegiadas, y rotar automáticamente las contraseñas y las claves según las políticas de seguridad.

Siguiendo estas recomendaciones, las organizaciones pueden fortalecer su estrategia de seguridad, reducir riesgos y aprovechar al máximo sus inversiones en tecnología. ■



LAS CINCO GRANDES RAZONES PARA DAR PRIORIDAD A LOS PRIVILEGIOS

El acceso privilegiado es una puerta de entrada a los activos más valiosos de una organización y la base de casi todas las filtraciones graves de seguridad.



Las organizaciones deben contar con una estrategia tanto para gestionar y supervisar el acceso privilegiado como para detectar y responder a amenazas si quieren reducir el riesgo de convertirse en el blanco de los ataques avanzados que existen en la actualidad.

Si te ha gustado este artículo, compártelo





ASEGURE ACCESO REMOTO A SISTEMAS INTERNOS CRÍTICOS

Acceso Zero Trust, Autenticación Multifactor
Biométrica y Aprovisionamiento Just-in-time
con CyberArk Alero.

SOLICITE UNA DEMO



El impacto de la era Exascale en nuestro modo de vida y trabajo

Adriano Galano,
AI and HPC sales
specialist en HPE



Cada segundo en la tierra se producen cantidades gigantescas de datos en todos los ámbitos de la vida. Los datos son hoy la energía que mueve la economía de cualquier país. Toda decisión debe estar soportada por los datos y gracias a los datos somos capaces de predecir y anticiparnos a cualquier evento o necesidad futura. Para 2025, IDC predice que, en todo el mundo, los datos crecerán hasta 175 zettabytes, y será fundamental convertir estos datos en conocimientos accio-

nables, utilizando combinaciones de modelado, simulación, análisis de datos, aprendizaje automático e inteligencia artificial (IA). Los conocimientos prácticos impulsan los negocios.

Pero ¿están nuestras organizaciones preparadas para tratar y analizar estas bastas fuentes de información? Los sistemas exascale son capaces de dar respuesta y muchas de las innovaciones que estamos desarrollando en esos grandes sistemas muy pronto la llevaremos a sistemas de cualquier tamaño, lo que

permitirá a la supercomputación, el HPC y el IA a organizaciones de cualquier tamaño:

- ❖ Dar respuesta a la “explosión cámbica” en las tecnologías de cómputo: una mayor diversidad de tipos y modelos de computación: procesadores, aceleradores, FPGA, de propósito específicos.

- ❖ A las nuevas tendencias en sistemas de almacenamiento y memoria. Permitiendo realizar la visión que esbozamos hace algunos años ya sobre el “Memory Centric Computing”

“Los sistemas exascale son capaces de dar respuesta y muchas de las innovaciones que estamos desarrollando en esos grandes sistemas muy pronto la llevaremos a sistemas de cualquier tamaño”

❖ Sistemas de interconexión como CRAY Slingshot, que aporta los beneficios de el alto rendimiento y baja latencia de las redes de comunicación, pero soportado en estándares del mercado como Slingshot. Y la evolución a los sistemas de interconexión fotónicos y nuevos estándares que romperán las fronteras de los centros de datos tal y como los conocemos hoy.

❖ Seremos capaces de dar soluciones a los datos allí donde se originen, desde el extremo (Edge) hasta los grandes supercomputadores.

❖ Y todo con los elementos de software que permitirá a los clientes tener la potencia de un supercomputador con la experiencia de usar un Cloud.

Todo esto lo llevaremos a los clientes de modo ágil, simple, flexible. Con la libertad de elección que nos da el mundo híbrido y con modelos de

pago por uso y fórmulas financieras que garantizarán que toda esta innovación sin barreras pueda llegar a las organizaciones y la sociedad.

Concluyendo, se espera que la computación a exascale resuelva problemas que antes estaban fuera de nuestro alcance, con avances en nuevas soluciones energéticas, asistencia sanitaria, predicción meteorológica, ciencia de los materiales y mucho más. Permittiéndonos crear una industria más competitiva, con empresas más ágiles centradas en el dato y sociedades más resilientes, capaces de mitigar los desastres y centrado en los seres humanos. ■

Si te ha gustado este artículo,
compártelo



GUÍA DE PLANIFICACIÓN DE VIRTUALIZACIÓN DE CLIENTES HPE SIMPLIVITY

Hewlett Packard Enterprise ha probado implementaciones de escritorios virtualizados a gran escala usando las soluciones VMware y Citrix® en la infraestructura hiperconvergente HPE SimpliVity. Los resultados han sido validados y publicados en forma de varios informes técnicos sobre arquitecturas de referencia y rendimiento. Estos documentos proporcionan un proyecto para diseñar e implementar infraestructura hiperconvergente altamente resiliente y escalable para implementaciones de virtualización de clientes.



No consolidar la infraestructura de ciberseguridad plantea desafíos al 99% de las empresas del mundo

Mario García,
director general de
Check Point para
España y Portugal



La pandemia de la COVID-19 ha provocado un cambio en la cultura de trabajo, puesto que los efectos han sido globales, rápidos y generalizados donde evaluar las inversiones en ciberseguridad es más necesario que nunca. Como norma general, en ciberseguridad no hay segundas oportunidades, pero ahora más que nunca, es fundamental dar un paso adelante y contar con una estrategia de seguridad adaptada a los nuevos tiempos. Los datos de una encuesta que hemos llevado a cabo recientemente reflejan que el 69% de las empresas de todo el mundo está de acuerdo en que dar prioridad a la consolidación de los proveedores llevaría a una mejor seguridad IT, dejando una conclusión muy clara: la era de la consolidación de las estrategias e infraestructuras de protección en el mundo digital también ha llegado para quedarse.

Todavía hoy, muchas empresas establecen su estrategia de ciberseguridad de entornos y dispositivos corporativos desde la falsa premisa de que un mayor número de productos se traduce en una mayor seguridad, aunque se tiende a olvidar los retos que esto supone: mayor complejidad para establecer una estrategia óptima, dificultades técnicas, posibles puntos sin protección, etc. Sin embargo, en esta situación, es fundamental que se produzca un cambio de enfoque por parte de los responsables de ciberseguridad, que, sin duda, deben apostar por la simplicidad. En ocasiones como esta, la frase de “menos es más” adquiere un significado trascendental para el bienestar de todos los activos corporativos, y por ende, de la salud de cualquier modelo de negocio. Contar con una solución de ciberseguridad consolidada que permita a las

empresas reforzar y centralizar sus defensas, así como agilizar los tiempos de respuesta a la hora de hacer frente a cualquier tipo de amenaza cibernética, se ha convertido en un aspecto clave.

LA EXPANSIÓN DE LA SUPERFICIE DE ATAQUE, UN RETO MAYÚSCULO PARA LA CIBERSEGURIDAD

A medida que el panorama de amenazas evoluciona y los ciberataques se hacen cada vez más sofisticados, el 99% de las empresas que utilizan múltiples soluciones de distintos proveedores afirman que esto ha planteado nuevos desafíos a su organización. Como consecuencia del teletrabajo, se ha producido un cambio de tablero de juego, ya que se ha pasado de un foco central de desarrollo de actividad profesional (oficina) a múltiples ubicaciones. Esto ha derivado

en un aumento de los dispositivos y redes personales que se utilizan para trabajar, lo que se traduce en una mayor superficie de ataque y, por tanto, más y mayores riesgos para la seguridad corporativa.

En este sentido, la ecuación es muy sencilla: cuantos más dispositivos hay que securizar, mayor es el número de potenciales objetivos para los atacantes y menor es la confianza en su nivel de ciberseguridad. La nueva realidad de trabajo mixto ha supuesto un examen para muchos CISOs, puesto que proteger una red de dispositivos cada vez más amplia es un reto para 9 de cada 10 empresas. A esto, además, hay que sumarle el factor añadido de que equipos como los smartphones, tabletas e incluso ordenadores portátiles apenas cuentan con medidas de seguridad instaladas, por lo que son un objetivo fácil para los ciberdelincuentes y una puerta abierta que da acceso a toda la red de datos y dispositivos de una empresa.

La sensación de urgencia y cambio constante en la que se encuentran muchas compañías en la actualidad les ha hecho optar por soluciones en las que se implementan nuevas herramientas de seguridad para proteger estos equipos. Nuestros datos indican que casi la mitad de las empresas utilizan entre 7 y 40 productos de seguridad distintos en su día a día, lo que aumenta de manera exponencial la complejidad a la hora de gestionar de todos estos recursos y servicios. Estas prácti-

cas hacen que, lejos de aumentar sus niveles de protección, las empresas tengan nuevos focos de vulnerabilidades o brechas de seguridad.

LA VISIBILIDAD, EL ENEMIGO A BATIR EN LA NUEVA ERA DE LA ESTRATEGIA DE SEGURIDAD CONSOLIDADA

Ante este escenario, no cabe duda de que consolidar y centralizar la estrategia de ciberseguridad se ha convertido en una necesidad, por lo que uno de los principales obstáculos a solventar es la falta de visibilidad. Tener alto nivel de visibilidad garantiza la eficacia necesaria para hacer frente y evitar los ciberataques más sofisticados por lo que, sumado a la gestión unificada, completan la arquitectura de seguridad.

La realidad es que la práctica totalidad de las empresas de todo el mundo utilizan múltiples plataformas de gestión de herramientas y productos de ciberseguridad, lo que dificulta la visibilidad. Además, para casi 8 de cada 10 profesionales de ciberseguridad, trabajar con varios proveedores supone un reto, puesto que actividades como el mantenimiento, las actualizaciones de las diferentes versiones, la renovación de los contratos y otras acciones relacionadas con el cuidado y la provisión de una solución de seguridad exigen un tiempo y unos recursos muy valiosos.

No tener una visión integral de la situación de las amenazas de una empresa complica la res-

puesta ante incidentes, lo que aumenta el grado de vulnerabilidad y, por tanto, la posibilidad de que los ataques de un ciberdelincuente tengan éxito y afecten a los datos, infraestructuras o dispositivos. Además, reducir proveedores proporciona un mayor nivel de ciberseguridad, puesto que hay una mayor integración y se minimizan las brechas entre producto, así como una reducción en el tiempo, el coste y los recursos de los sistemas de reparación de incidentes.

LA ESCALABILIDAD, ELEMENTO CLAVE EN LA CONSOLIDACIÓN DE LA ESTRATEGIA DE CIBERSEGURIDAD

No cabe duda de que el primer paso que deben dar las empresas consiste en reconocer cuál es el reto que tienen ante sí. Sin embargo, este no es el único obstáculo, puesto que todavía tienen que dar algunos pasos más en el camino hacia una nueva realidad cibersegura. En este sentido, es evidente que deben elegir una postura y una herramienta de protección que permita unificar y simplificar la gestión de toda la infraestructura de ciberseguridad, sobre todo en estos momentos en los que la movilidad y accesibilidad a los datos en remoto son un pilar fundamental para el desarrollo de las tareas profesionales.

Ante este nuevo escenario, la propuesta que hacemos desde Check Point se centra en un concepto clave: la escalabilidad. Las redes de las empresas son cada vez más extensas y cuentan

con un mayor número de dispositivos conectados, por lo que es necesario contar con herramientas que puedan crecer e hiperescalar a la misma velocidad que lo hacen las infraestructuras corporativas. En nuestro caso, contamos con productos como Check Point Maestro, la primera solución de seguridad de red realmente hiperescalable de la industria. una nueva arquitectura hiperescalable que ofrece a los negocios de cualquier tamaño, la potencia y flexibilidad de las plataformas de seguridad de nube y la posibilidad de expandir sus pasarelas de seguridad existentes hasta una capacidad de hiperescalar sin interrupciones (seamless).

Asimismo, también contamos con nuestra solución Infinity NEXT, una arquitectura de seguridad cloud nativa consolidada que está diseñada para proteger cualquier punto dentro de una red corporativa en cualquier lugar gracias a la innovativa tecnología de nanoagentes y un completo panel de más de 60 soluciones y servicios de protección y prevención de amenazas. Infinity NEXT, además, ofrece protección sin interrupciones y actualizaciones constantes para cualquier red, dispositivos móviles, así como entornos IoT y cargas de trabajo multi-cloud. De esta forma, las empresas pueden elegir entre utilizar la totalidad de las tecnologías disponibles en la suite de Infinity Next o implementar aquellos módulos específicos que se adaptan a sus necesidades inmediatas

con total flexibilidad y facilidad de manejo desde un único panel de control.

Soluciones como estas llegan para dar respuesta a las demandas y necesidades actuales de las empresas que, en condiciones normales, cambian a una gran velocidad, pero que en la nueva realidad que nos toca vivir varían de forma vertiginosa. La combinación de ambas herramientas llega para ofrecer a las compañías de cualquier tamaño lo que verdaderamente necesitan: productos que reducen procesos, minimizan costes y simplifican las tareas relacionadas con la protección de los entornos y activos corporativos. Asimismo, ayuda a consolidar la estrategia de ciberseguridad de las empresas, ofreciendo estabilidad y aportando las medidas necesarias para hacer frente a los nuevos retos que surgen como consecuencia de la nueva realidad de trabajo mixta.

En resumen, la transformación digital empodera a las organizaciones, pero no deben perder de vista el enfoque de ciberseguridad adecuado, puesto que, de lo contrario, expone a las empresas a una gran variedad de amenazas. La pandemia del Covid-19 ha supuesto un cambio radical para las empresas, que han visto cómo tenían que implantar una serie de cambios significativos en su forma de trabajo para poder hacer frente a la situación actual. El teletrabajo es sin duda uno de ellos, pero para que pueda instaurarse de forma definitiva, es imprescindible hacerlo de forma segura. Por tanto, nos en-



CHECK POINT CLOUDGUARD SAAS, MÁS QUE UN CASB

Como explica el documento, CloudGuard SaaS es la solución de prevención más efectiva para malware y ataques zero-days en aplicaciones SaaS. Utiliza la tecnología SandBlast de Check Point y bloquea las amenazas zero-day antes de que lleguen a los usuarios, ofreciendo contenido seguro en segundos, utilizando emulación avanzada de amenazas y tecnología de extracción.



contramos en las etapas iniciales de una nueva era centrada en consolidar las estrategias de ciberseguridad corporativas. ■

Si te ha gustado este artículo, compártelo





CHECK POINT INFINITY

SECURE YOUR EVERYTHING™

Más información



La escalabilidad y el rendimiento de las aplicaciones, claves en la SD-WAN para teletrabajadores

José Luis Laguna,
Director Systems
Engineering Fortinet
España y Portugal



El estado de alerta ha traído consigo la implementación a gran escala del teletrabajo. Muchas organizaciones que dimensionaron su firewall en función del número de delegaciones que tenían, y no del número de usuarios que podrían tener que conectarse a distancia, se enfrentan a graves problemas de escalabilidad. Afortunadamente, algunos fabricantes proporcionamos una alta escalabilidad en las conexiones VPN, al no limitar ni licenciar el número de conexiones VPN. Pero ofrecer conexión a los teletrabajadores es solo la mitad del desafío al que se enfrentan los CISOs y CSOs. La conectividad en sí misma no es suficiente. Incluso para aquellas organizaciones que han logrado escalar las conexiones VPN SSL o IPSec de los teletrabajadores a la red central, conseguir que las aplicaciones críticas para el negocio se ejecuten de la forma correcta, sigue siendo un reto.

El tráfico de aplicaciones que antes se cursaba en la LAN interna de alto rendimiento ahora tiene que utilizar los escasos recursos de ancho de banda de

la conectividad WAN. Por ejemplo, el uso de las videoconferencias es tan elevado en este momento que la experiencia del usuario remoto a menudo se ve gravemente degradada. Esto significa que todas esas conexiones entre los trabajadores remotos y la red central a través de una conexión VPN gratuita también deben equilibrarse y gestionarse. Y las aplicaciones críticas - ya sea en la red local o en la nube - necesitan ser priorizadas, que es precisamente el tipo de desafío para el que SD-WAN fue diseñado. El problema comienza con las limitaciones de muchas redes domésticas. La mayoría de esas redes tienen que soportar una gran variedad de dispositivos y tecnologías, a menudo porque hay más de un adulto que necesita trabajar en casa. A ello se suma que puede haber niños conectados a sus clases online, que interactúan con sus compañeros a través de las redes sociales o los juegos online, o que acceden a plataformas de streaming de entretenimiento.

En la mayoría de las circunstancias, una red doméstica soporta la participación de un usuario en

una videoconferencia. Pero cuando varias personas necesitan utilizar la misma aplicación de vídeo al mismo tiempo -especialmente si también necesitan compartir su pantalla - el rendimiento puede degradarse rápidamente. Trabajar con un proveedor de servicios de Internet para mejorar el ancho de banda disponible es una posible solución. Pero incluso entonces, la priorización de las aplicaciones sigue siendo crítica.

EL VALOR DE SD-WAN PARA LOS "SUPER-USUARIOS"

Este desafío es especialmente difícil para los super-usuarios remotos de una organización, un grupo en el que se encuentran los administradores de sistemas que gestionan la red a distancia, personal de asistencia técnica que necesita solucionar los problemas de los dispositivos de los trabajadores remotos o ejecutivos que necesitan acceso en tiempo real a grandes volúmenes de datos. Su capacidad para realizar su trabajo - responsabilidades en las que confían otros trabaja-

EN BUSCA DE LA CONECTIVIDAD INTELIGENTE

dores - puede verse especialmente afectada por el escaso rendimiento de las aplicaciones debido al limitado ancho de banda.

En estas circunstancias, un pequeño FortiGate como dispositivo de escritorio puede ser una potente solución para administrar un ancho de banda limitado, a la vez que se optimiza y se prioriza el uso de la aplicación. Una solución FortiGate de escritorio incluye SD-WAN y LTE incorporado por defecto, de modo que cuando una aplicación de videoconferencia comienza a experimentar pérdida de paquetes y fluctuaciones debido a que otro dispositivo de la red doméstica está consumiendo ancho de banda, puede detectar que la conexión se está degradando y cambiar automáticamente a la conexión LTE incorporada para garantizar la integridad de la aplicación. La misma funcionalidad está disponible para miles de aplicaciones SaaS, desde Office 365 hasta Salesforce, pasando por el almacenamiento basado en la nube.

Estos potentes dispositivos de escritorio también pueden proporcionar una conectividad WiFi fiable y de alto rendimiento para los dispositivos inalámbricos, lo que les permite estar aislados de la red doméstica abierta. Y también soportan y aseguran el tráfico de voz, permitiendo a los super-usuarios tener acceso total a todos los servicios telefónicos de los que dependen para su trabajo a través de una aplicación de tipo softphone - todo ello apoyado por una ruta extra de conectividad LTE para asegurar la continuidad de la apli-

cación. Y su función de gestión centralizada permite a los administradores ajustar la seguridad, la conectividad y el rendimiento de las aplicaciones para que se puedan hacer cambios sobre la marcha en función de diversos parámetros.

EL TELETRABAJO ES PARTE DE LA NUEVA NORMALIDAD Y SD-WAN ES SU ALIADO

Cuando salgamos de esta crisis, es probable que las cosas no vuelvan a ser como antes. Algunos usuarios pueden insistir en la opción de trabajar desde casa, al menos en ocasiones. Muchas organizaciones apreciarán la flexibilidad de una fuerza de trabajo que pueda responder a las demandas de la empresa, ya sea en el lugar de trabajo o en el hogar. Y los equipos encargados del plan de continuidad de negocio y de recuperación en caso de desastre (BCDR de sus siglas en inglés) tendrán que considerar que proporcionar a los trabajadores remotos la tecnología de acceso remoto suficiente tiene que formar parte de dicho plan. Y para muchos de esos trabajadores, el acceso a la VPN por sí solo no será suficiente. Hay que valorar el impacto comercial por no tener el nivel adecuado de rendimiento o disponibilidad de la aplicación, especialmente para determinados usuarios.

La ventaja fundamental de extender la funcionalidad SD-WAN a los teletrabajadores individuales, especialmente a los super-usuarios, no solo es que pueden disfrutar de un acceso remoto



LOS CENTROS DE DATOS HÍBRIDOS DISTRIBUIDOS REQUIEREN CAPACIDADES ADICIONALES DE NGFW

La evolución de los modernos centros de datos ha llevado a que las aplicaciones y los datos se distribuyan cada vez más a través de infraestructuras hí-



bridadas. Si bien esto contribuye a permitir una mayor agilidad para los flujos de trabajo críticos para el negocio, simultáneamente amplía la superficie de ataque de la organización a la vez que complica la visibilidad e inhibe los controles.

on-demand, sino que también pueden obtener un rendimiento escalable de forma dinámica e independientemente de la disponibilidad de su red local. Es en estos momentos, en el que nuestros trabajadores confían en que pueden hacer su trabajo de forma rápida y eficiente, cuando la funcionalidad SD-WAN cobra mayor protagonismo como elemento diferencial. ■

Si te ha gustado este artículo, compártelo



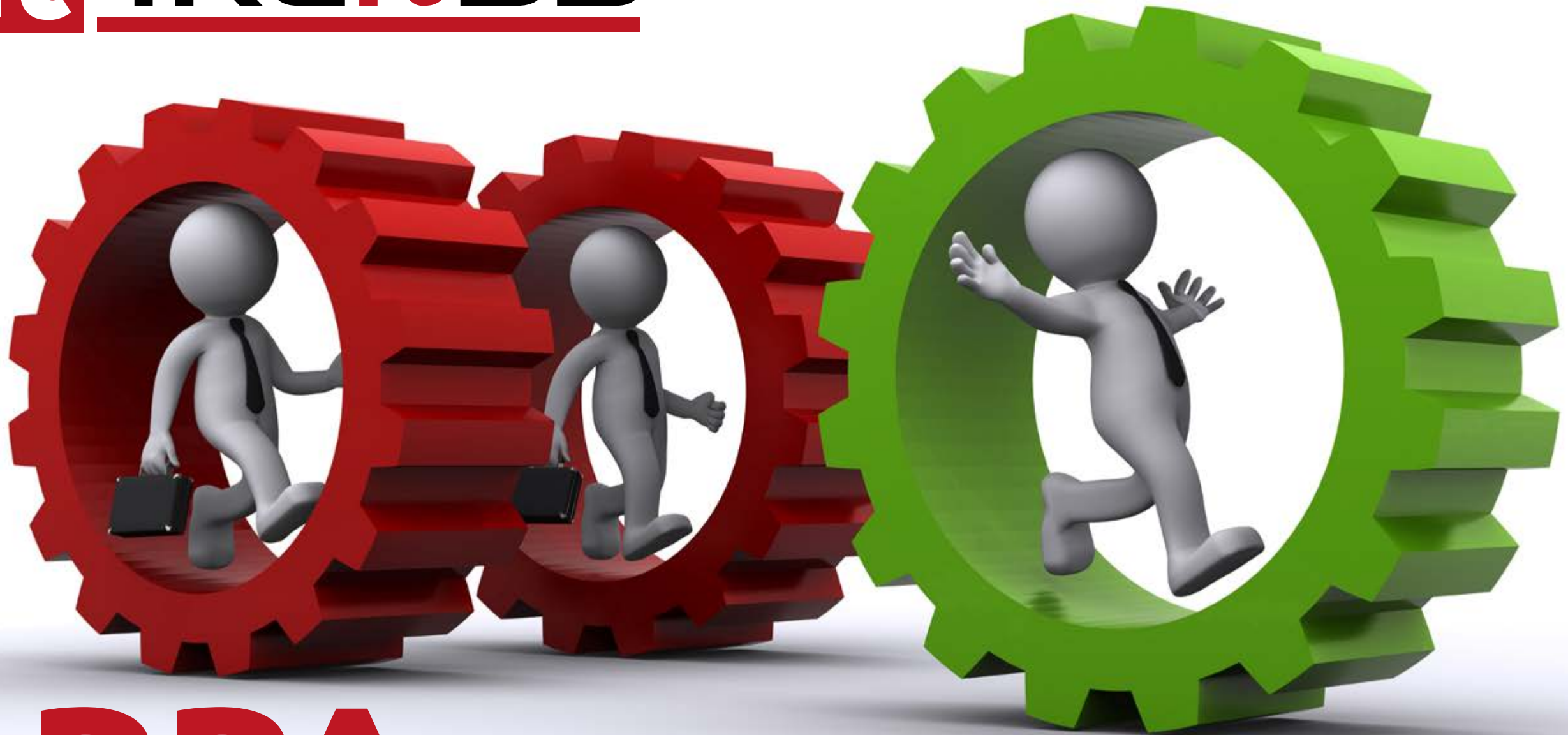


DISEÑADO PARA EL TELETRABAJO SEGURO

Poder adoptar el teletrabajo rápidamente es crítico para la continuidad del negocio y la seguridad. Las soluciones de Fortinet para el teletrabajo ayudan a las organizaciones a garantizar un acceso remoto seguro para todos sus empleados en cualquier ubicación.

SABER MÁS





RPA: la automatización que te hará ganar agilidad corporativa

Patrocinadores:

ABAI GROUP
YOUR BUSINESS PARTNER

Appian

A AUTOMATION
ANYWHERE

Uno de los anhelos de las empresas es seguir avanzando en sus procesos de Transformación Digital con el objetivo de incrementar su eficiencia y su productividad y, para ello, no sólo se necesitan herramientas y conocimientos, sino transformar todos los procesos del negocio y la relación con los clientes. Una de las claves para poder digitalizar los procesos es la automatización, que aporta no sólo esa eficiencia deseada, sino también la eliminación de los errores humanos en estos procesos, permitiendo, además, liberar este valor que aportan los profesionales a labores más productivas para el negocio.

Automatizar para una transformación de los procesos eficiente y productiva



Las siglas RPA responden al concepto Robotic Process Automation, Automatización Robótica de Procesos, que, aunque el nombre puede llevar a alguno a pensar en un mundo poblado por robots de apariencia futurista y cinematográfica, es tecnología orientada a la automatización de tareas vía software para reducir las interacciones e intervenciones humanas en el uso de las herramientas informáticas, sobre todo cuando se trata de tareas repetitivas en las que el talento humano no aporta un valor diferencial. Estos robots de software nos permiten, por tanto, reducir el posible error por intervención humana y aumentar la eficiencia y efectividad de los procesos de los que estemos hablando.

Pero ¿es RPA un concepto nuevo? La verdad es que no. No se trata de una tendencia surgida en este momento, pero lo cierto es que en los últimos tiempos ha vivido una evolución importante y, como han adelantado algunos expertos, el gasto generado alrededor de este tipo de herramientas y procesos automatizados denota su creciente papel en el engranaje de las operaciones empresariales.

EL MERCADO DE SOFTWARE RPA CRECE DE FORMA EXPLOSIVA

Durante el año 2018, el mercado mundial de software de Automatización Robótica de Procesos ya creció más de un 63%, dando un impulso sin precedentes al sector, que se está viendo reforzado hoy por la gran demanda de los nuevos modelos

de negocio digital y la necesidad de dar continuidad a los negocios. Y en ello está teniendo mucha influencia la creciente sinergia con otras tecnologías de automatización, como la Inteligencia Artificial o el reconocimiento de texto y voz.

Según Gartner, en su [informe sobre el mercado de RPA](#) hace dos años los ingresos alcanzaron los 846 millones de dólares, y se esperaba que durante 2019 la tendencia continuara, hasta elevar la cifra a unos 1.300 millones (los datos

confirmados de 2019 todavía no se han publicado). Como señaló en su momento Fabrizio Bisconti, vicepresidente de investigación de Gartner, “el mercado de RPA ha crecido desde nuestro último pronóstico, impulsado por las demandas de los negocios digitales a medida que las organizaciones buscan un procesamiento directo. La competencia es intensa, con nueve de los 10 principales proveedores cambiando la posición de participación de mercado en 2018”.



RPA: beneficios y retos de la automatización de procesos basados en robótica

Una situación que define mucho este campo es que los cinco principales proveedores acapararon el 47% del mercado de RPA en 2018, aunque es destacable que los que ocupaban la sexta y séptima posición vieron un crecimiento de ingresos de tres dígitos, lo que indica que

los puestos del ranking mundial no están garantizados y, según Biscotti, esto se extiende a los cinco primeros de la lista.

Como señalan los expertos de Gartner, aunque las soluciones RPA se pueden encontrar en todas las industrias, sus principales clientes

son los bancos, las aseguradoras, las empresas de telecomunicaciones y las de servicios públicos, ya que pueden integrar con efectividad esta tecnología en sus numerosos sistemas heredados, lo que les permite avanzar mejor en la Transformación Digital.

Cinco mejoras que RPA está aportando al sector público

El camino hacia una mayor automatización ha comenzado tanto en las empresas privadas como en las administraciones y empresas públicas. Y la RPA está demostrando ser la tecnología que más rápido encuentra su lugar en las organizaciones. En el caso del sector público está contribuyendo de forma decisiva a agilizar los procesos, sobre todo los que involucran burocracia y que tradicionalmente han obligado a tener plantillas muy numerosas, compuestas por trabajadores que realizaban tareas repetitivas.

1 Pero ahora, gracias a la adopción de RPA, este panorama está cambiando de forma radical y, a pesar de que existen muchos miedos sobre la pérdida de empleos asociada a esta tecnología, los expertos opinan que se trata más bien de un cambio de las tareas asignadas. De hecho, pensando en el sector público, los cinco benefi-

cios más positivos e importantes, con un mayor impacto en los próximos años son, primero, **mejor servicio al ciudadano**, ya que, gracias a la automatización robótica de procesos, determinados servicios que las administraciones públicas solo ofrecían en horario comercial podrán prestarse durante las 24 horas, algo que los ciudadanos demandan cada vez más. Esto se lograría integrando robots y chatbots, lo que permitirá a la infraestructura responder automáticamente a los mensajes y las consultas de los ciudadanos.

2 En segundo lugar, **más rapidez en el procesamiento de consultas**, y es que la burocracia en el sector público lastra las operaciones a niveles que generan una gran frustración a los ciudadanos. Con la introducción de RPA se puede lograr un salto enorme en agilidad y en nivel de servicio

a los ciudadanos. Empleando robots y otros sistemas automatizados se pueden escanear documentos automáticamente, validar los datos, verificar las características de un demandante y su idoneidad para acceder a un servicio... acelerando procesos sin que tengan que intervenir los funcionarios y trabajadores.

3 Tercero, **más precisión en la entrada de datos**, porque mediante RPA es más fácil que la información sea verificada en cada paso, sin que se produzcan errores en la recopilación de datos. Además, los ciudadanos y los propios empleados de la administración cuentan con más herramientas para verificar que la información es correcta, como portales web, aplicaciones de soporte o escritorios remotos, y la resolución de problemas por errores en los datos puede hacerse mucho más deprisa.

4 Cuarto, **integración de sistemas de bajo coste**, debido a que las herramientas de RPA pueden ayudar a una mejor integración de los sistemas heredados con las nuevas tecnologías, facilitando la gestión de la información y la transferencia de datos entre distintos sistemas. Este es un problema constante para las empresas del sector público, organizaciones donde el gasto en TI es contenido y donde el personal no siempre cuenta con las capacidades necesarias para implementar nuevas tecnologías y trabajar con ellas.

5 Por último, **mejoras de conciliación y presentación de informes**, debido a que RPA proporciona una agilidad sin igual para el trabajo con los datos necesarios para elaborar esos informes, como la verificación de cuentas y saldos en los sistemas, y la localización y administración de las discrepancias e inconsistencias en la información.

Un tema que considerar, y al que Gartner da mucha importancia, es que este entorno va a cambiar mucho en los próximos años, porque las grandes empresas como IBM, Microsoft y SAP, que dominan el mercado tecnológico, están buscando asociarse con otras empresas del sector o adquirirlas, para aumentar su conocimiento, sus clientes y su impulso. Pero, a su vez, las nuevas compañías están adaptándose con más agilidad a las nuevas demandas de los clientes de la era digital, añadiendo capacidades como el procesamiento de eventos y el análisis en tiempo real, lo que atrae a clientes de diferentes ámbitos y escalas.

Estas estrategias harán que, según Deloitte, el mercado de soluciones de automatización crezca a un ritmo anual del 20%, alcanzando los 5.000 millones de dólares en 2024. A nivel general, 2020 va a ser un gran año para estas tecnologías, ya que las compañías se encuentran en plena adopción de automatizaciones inteligentes.

RPA + INTELIGENCIA ARTIFICIAL

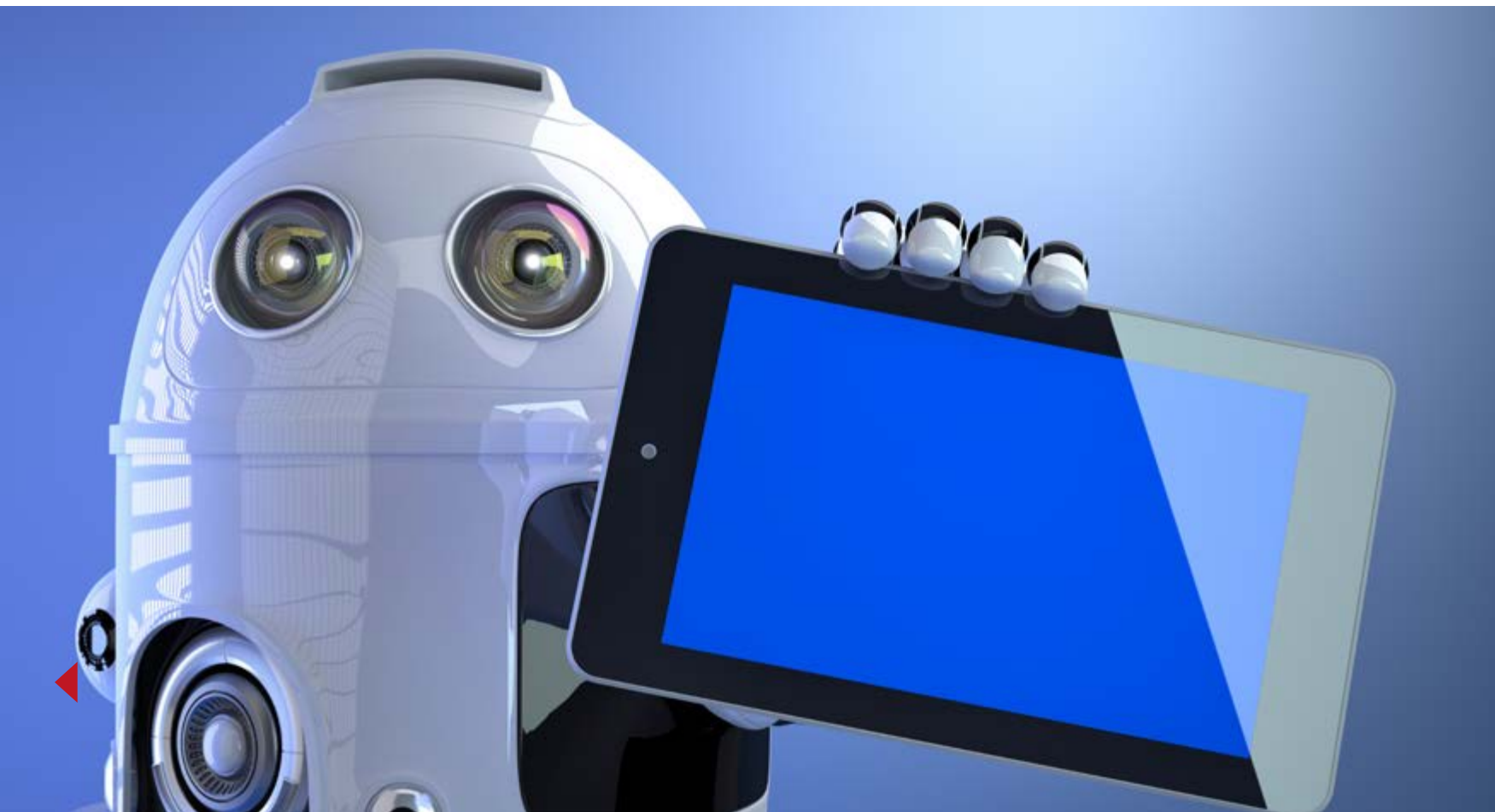
El estudio [Automation with intelligence. Reimagining the organisation in the Age of With](#), pronostica un crecimiento sólido no solo de las soluciones de automatización robótica de procesos, sino que las automatizaciones que

se produzcan serán inteligentes e integrarán Inteligencia Artificial.

Según los datos, extraídos de entrevistas a 523 directivos de compañías de 26 países de todo el mundo, el 47% afirma que combina RPA con Inteligencia Artificial como parte de su estrategia de implementación de automatización inteligente. Además, están consiguiendo buenos resultados, ya que organizaciones que combinan estas dos tecnologías reportan un incremento del 9% en sus ingresos, frente al 3% que registran aquellas que sólo emplean RPA.

Por tanto, concluye Deloitte que la implementación de procesos de automatización inteligente sigue superando las expectativas. Además, las organizaciones que emprenden pruebas piloto perciben de media un retorno alrededor de los 15 meses tras su incursión, mientras que las que se encuentran en fase de escalada lo registran ya de media a los nueve meses. Según Santiago Gómez Rebollo, socio de consultoría de la firma, “2020 será el año clave para la automatización inteligente, a medida que las organizaciones combinen la automatización de procesos con robots con Inteligencia Artificial y otras tecnologías que permitan nuevas maneras de trabajar”.

En su opinión, las automatizaciones trascenderán de la rutina a la innovación, desde recolectar información a predecir datos, analizando y apoyando para la toma de decisiones. “Las empresas que reconfiguren su manera de trabajar, que tomen ventaja de la combinación



El sector financiero, pionero en aprovechar la automatización que le ofrece la RPA

Según el informe elaborado por la firma de investigación Juniper Research, la RPA en el sector financiero tendrá un crecimiento espectacular.

Esta industria ha sido una de las primeras en identificar el gran valor que puede aportar la automatización robótica de procesos a sus operaciones, y los analistas afirman que entre 2018 y 2023 la adopción de es-

tas soluciones crecerá un 400% entre estas empresas, generando unos ingresos que pasarán de los actuales 200 millones de dólares a 1.200 millones al final del período. Las regiones más importantes en este mercado serán Norteamérica y Europa Occidental, que ahora mismo abarcan casi el total del mercado.

Pero, según indican ciertas voces de la industria, esta evolución se enfrenta a determinadas trabas, ya que la adopción de las herramientas RPA está en sus fases iniciales en muchas de las empresas del sector. Esto supone que no existe una gran comprensión de esta tecnología, lo que retrasa la obtención de

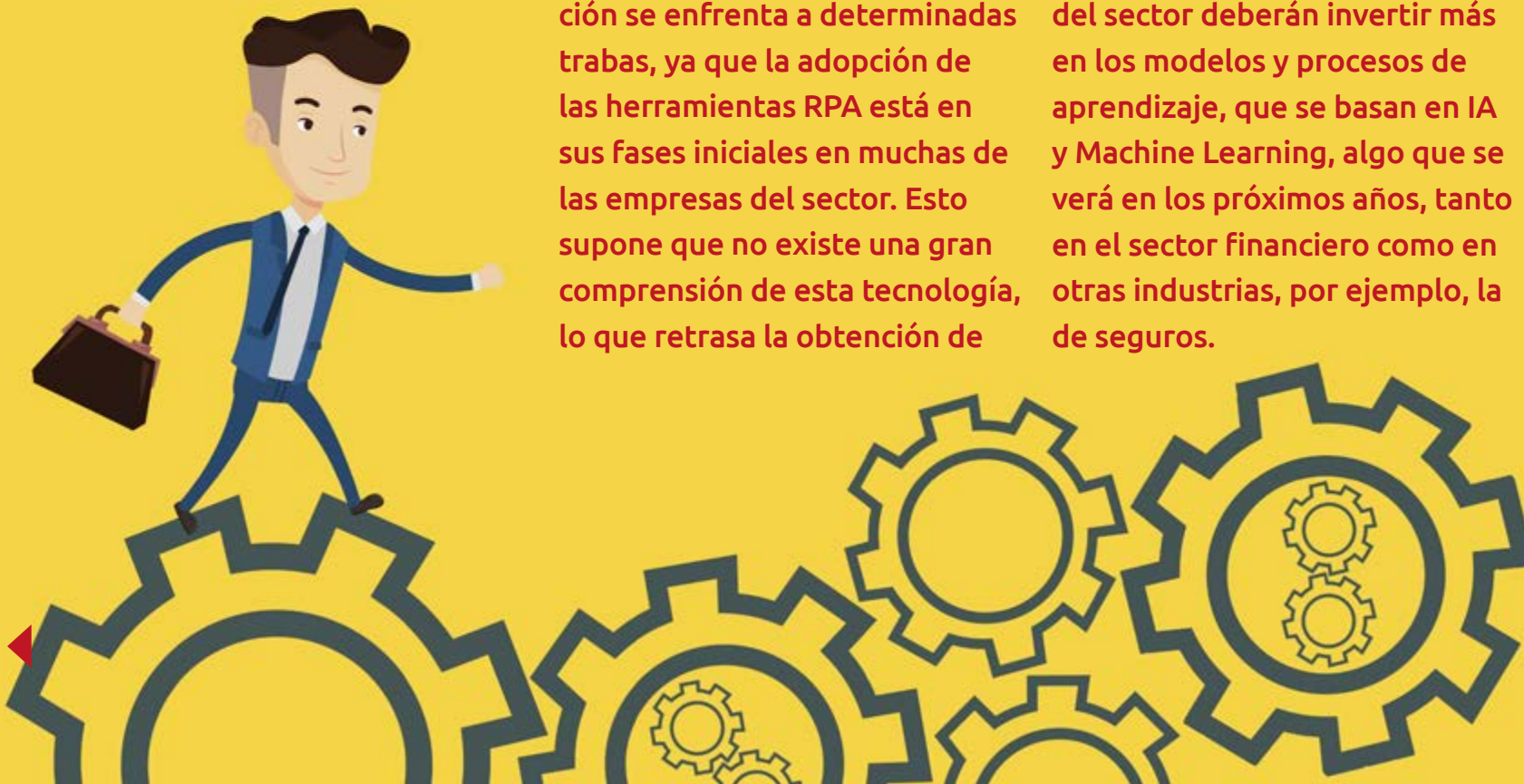
beneficios en estas inversiones. Por ahora, las aplicaciones RPA que más se han adoptado en la industria financiera son los chatbots, que prometen una interacción más ágil, intuitiva y sencilla para el usuario, lo que mejorará la experiencia del cliente. Pero todavía necesitan pulir su funcionamiento y mejorar su inteligencia para alcanzar todo su potencial. Para ello, las empresas del sector deberán invertir más en los modelos y procesos de aprendizaje, que se basan en IA y Machine Learning, algo que se verá en los próximos años, tanto en el sector financiero como en otras industrias, por ejemplo, la de seguros.

entre las personas y las máquinas ejecutando nuevos procesos, y que tengan las habilidades y el conocimiento para impulsar la automatización inteligente serán las mejores posicionadas para aprovecharse de las oportunidades que esta tecnología les puede aportar”, añade.

LA INVERSIÓN ESPAÑOLA EN RPA CRECERÁ MÁS DE UN 35% HASTA 2022

Esta evolución en los datos globales tiene su reflejo en nuestro país. La consultora IDC, en colaboración con Microsoft, presentaba recientemente [un informe en el que analizan cómo optimizar las operaciones de las empresas y la manera de satisfacer mejor a clientes y empleados](#). Y son varias las conclusiones, como el hecho de que el año próximo la mitad de los ingresos de las compañías tendrán su origen en la transformación de modelos de negocios digitales, basados, además, en economías de plataforma y monetización de datos. Una cifra que ascenderá hasta el 80% en 2023.

Según se desprende de esta investigación, las organizaciones deben evolucionar hacia una plataforma tecnológica que pase a ser un núcleo inteligente, que debe estar definido por capacidades cognitivas como la analítica avanzada, la Inteligencia Artificial o Machine Learning. Todo ello apoyado en despliegues en la nube. Es fundamental que la relación entre las organizaciones y sus clientes sea a tiempo real. Al hilo de este informe, ahora, con la Inteligencia Artificial, se aña-



de valor a cada una de las capas de análisis de datos, permitiendo automatizar tareas específicas y mejorar las actividades relacionadas y el proceso general de apoyo a la decisión. De hecho, la inversión en automatización de procesos en Europa crecerá a una tasa del 35% hasta 2022 según IDC. En España, incluso por encima de esta tasa.

Otra investigación, ésta de [Kaizen Institute](#), destaca dos cifras muy importantes y que generan mucha controversia. La primera es que, con las tecnologías actuales, solo el 5% de los trabajos en Europa pueden ser completamente

automatizados. Y la segunda es que en el 60% de los empleos se pueden automatizar hasta un 30% de las actividades que desarrollan los trabajadores, principalmente las tareas repetitivas y de poco valor añadido para los trabajadores.

La implementación de estas tecnologías comenzó en las grandes corporaciones y en determinados sectores, pero actualmente la Automatización Robótica de Procesos ha calado hasta otros niveles de la economía, llegando a las pequeñas y medianas empresas. Un ejemplo de ello es España, donde el 53% de las PYMES ya ha aplicado

RPA a sus procesos como parte de su estrategia de digitalización, de acuerdo con dicho estudio.

Los analistas han puesto énfasis en los enfoques actuales de RPA, que solo requieren instalar un software en las máquinas de cada empleado y llevar a cabo una configuración sencilla, que resulta muy intuitiva para casi cualquier perfil de trabajador. Gracias a esto, el proceso resulta rápido (generalmente menos de seis meses) y requiere una inversión mínima, lo que ha permitido llevar esta tecnología a empresas de menor tamaño en un tiempo bastante corto.



Aunque las soluciones RPA se pueden encontrar en todas las industrias, sus principales clientes son bancos, aseguradoras, empresas de telecomunicaciones y de servicios públicos, ya que pueden integrar con efectividad esta tecnología en sus numerosos sistemas heredados (Gartner)

Otra ventaja de RPA es que resulta más flexible y escalable que otras estrategias.

En palabras de Javier Langa, manager de Kai-zen Institute para Europa Occidental, “aunque sigue existiendo cierto temor en la sociedad a la pérdida de puestos de trabajo ligado a la automatización, la realidad es que el avance de nuevas tecnologías genera un saldo total positivo de puestos de trabajo, y permite sacar mucho más potencial de los trabajadores, liberándoles de las tareas tediosas de poco valor añadido para las que no es necesario el potencial del cerebro humano y enfocarse en proyectos que involucren un proceso creativo”.

EL RECELO DEL TRABAJO AUTOMATIZADO

Pese a las promesas empresariales de ahorro de costes, eficiencia, o productividad, existe entre los empleados el temor a la pérdida de su puesto de trabajo. El último estudio de Ipsos sobre [el progreso de la automatización en España](#) muestra que el temor a la automatización y la consiguiente pérdida del empleo es mayor en los mercados emergentes.

Como ya hemos mencionado anteriormente, tecnologías como la Inteligencia Artificial y el aprendizaje automático están abriéndose paso en el entorno empresarial, proporcionando nuevas formas de abordar las tareas diarias, especialmente de carácter administrativo, que suelen ser más repetitivas y tediosas. Pero poco a poco, de la mano de esos nuevos asistentes digitales, las

En España, el 53% de las PYMES ya ha aplicado RPA a sus procesos como parte de su estrategia de digitalización

tecnologías de automatización van a poder aplicarse a trabajos de otro nivel, como a ciertas tareas relacionadas con la organización y la gestión. Porque la IA y el ML ofrecen numerosas posibilidades en el ámbito de las empresas, muchas de ellas todavía por descubrir. Claro, que esto va a tener un impacto importante en el mercado laboral, ya que muchos trabajos actuales van a desaparecer o van a transformarse hasta el punto de ser irreconocibles en unos años.

Según la encuesta de Ipsos, realizada en 28 países distintos, un 35% de la población ve probable que su puesto de trabajo sea automatizado en los próximos 10 años. Mientras tanto, un 54% piensa que es poco probable que esto se produzca y un 11% no está seguro de lo que sucederá.

En opinión de Vicente Castellanos, director de estudios sociales de Ipsos España, “la digitalización supone automatizar cada vez más los puestos de trabajo. Del estudio de IPSOS se desprende que cuanto mayor parte de nuestro trabajo se dedique a la toma de decisiones, menos nos sentimos

amenazados por la digitalización, y aceptamos de mejor grado que la toma de decisiones se base en herramientas que nos ayuden a decidir mejor”.

Como conclusión, el 69% de los entrevistados durante esta investigación opinan que podrán mantener su empleo a pesar de los cambios que traerá la automatización. En el caso de España, el 66% se siente seguro de tener las habilidades necesarias para que su puesto de trabajo deba mantenerse.

LA IA Y LA AUTOMATIZACIÓN REQUERIRÁN PERSONAL CON MÁS INTELIGENCIA EMOCIONAL

Lo que está claro es que la introducción de la IA y la RPA demandarán nuevas habilidades, pues para trabajar con Inteligencia Artificial y con la automatización hacen falta profesionales con cualificación técnica, pero también con otras habilidades transversales, como es la inteligencia emocional (IE). Según una investigación de la firma [Capgemini](#), la demanda de estas competencias se multiplicará por seis en los próximos 3 a 5 años.

Este estudio, denominado [Emotional Intelligence – The essential skillset for the age of AI](#), tiene como objeto analizar cómo están introduciéndose capacidades humanas como requisitos fundamentales para el trabajo en entornos de automatización e Inteligencia Artificial. Uno de sus principales pronósticos es que la demanda de inteligencia emocional para este tipo de empleos se multiplicará por seis en los

El mercado de soluciones de automatización crece a un ritmo anual del 20% y se espera que alcance los 5.000 millones de dólares en 2024 (Deloitte)

próximos 3 a 5 años. Pero, sin embargo, menos de una de cada cinco empresas está formando a los trabajadores que no tienen funciones de supervisión en este campo.

Esto es un freno importante para alcanzar la cualificación necesaria para la automatización dentro de las organizaciones, dada la opinión de empleados y directivos, que creen que la inteligencia emocional es una capacidad clave, junto con la conciencia de uno mismo, la autogestión, la conciencia social y la gestión de las relaciones. Y creen firmemente que esto se convertirá en un requisito fundamental para tener éxito en los próximos años.

Pero, según las respuestas obtenidas en esta investigación, la inmensa mayoría de las organizaciones no ha modificado sus procesos de selección y formación de personal para implementar este enfoque. Y esto impedirá que se pueda aprovechar el potencial de la inteligencia emocional para mejorar la satisfacción del

empleado, reducir la rotación de personal, generar más ingresos y reducir costes.

Entre las principales conclusiones de este informe destaca que el avance de la automatización y de la IA en las empresas propiciará un cambio de percepción sobre el valor que habilidades como la inteligencia emocional tienen en la organización. Esto será importante para el trato con el cliente, ya que las tareas rutinarias automatizadas dejarán espacio para que los empleados dediquen más tiempo al trato personal, como opina el 76% de los directivos encuestados. Y otros tantos creen que los empleados deberán asumir tareas que requieren competencias emocionales. Por ello, para el 61% de encuestados la IE se va a convertir en una competencia clave en un plazo de 1 a 5 años.

Otro asunto importante en este sentido es que los trabajadores se muestran preocupados por la introducción de la Inteligencia Artificial y la automatización, y ven peligros para su puesto de trabajo. Esto pone el foco en otras habilidades que permitirán progresar en la organización a largo plazo, como son este tipo de soft skills. Esta idea se ve reforzada por los datos, ya que las organizaciones con una plantilla más dotada en materia de IE ya están percibiendo beneficios. Por ejemplo, un 60% de ellas afirma estar consiguiendo unos resultados un 20% mejores en diversos factores de negocio, como la productividad, la satisfacción del empleado, la cuota de mercado o la atención al cliente. ■



MÁS INFORMACIÓN



[Beneficios de la monitorización de red para la automatización industrial](#)



[Beneficios empresariales de la automatización y la orquestación](#)



[Impacto de la automatización en las operaciones de IT](#)

Si te ha gustado este artículo, compártelo



Convierta Desafíos En Oportunidades

Impulse La Continuidad Del Negocio Con
Una Fuerza De Trabajo Digital Inteligente

No todas las tecnologías de automatización robótica de procesos (RPA) son iguales. Cuando se producen cambios, necesita una solución que se adapte e implemente rápidamente. Automation Anywhere ofrece la única plataforma RPA con inteligencia artificial integrada, creada para la nube y con un interfaz web para satisfacer las necesidades de hoy y prepararlo para las incertidumbres del mañana.

automationanywhere.com/la/products/enterprise/a2019



La automatización de procesos, motor de la eficiencia en las empresas españolas

España está inmersa en el proceso de desescalada. Tras más de dos meses de confinamiento, la nueva normalidad empieza a hacerse notar y con ella, los cambios en las empresas para ser 100% seguras y eficientes. Y es que, si hay lecciones aprendidas de esta situación vivida, además de demostrar que el teletrabajo es factible en nuestras organizaciones, entre ellas figura la necesidad de automatizar procesos para que nuestras empresas sean más ágiles, productivas y eficientes.

Dicha necesidad puede cubrirse desde varios frentes, pero desde hace unos años, el concepto de RPA o automatización robótica de procesos, está sonando en las organizaciones con mayor fuerza como esa tecnología que les permitirá alcanzarlo. “Permite automatizar tareas manuales y repetitivas, de gran volumen y basadas en reglas, que no aportan generalmente valor a la empresa pero que suelen tener un elevado coste al necesitar de la intervención humana”, explica Víctor Ayllón, Vicepresidente RPA COE de Appian Corporation.

Por su parte, Óscar Martínez, Regional Sales Director de Automation Anywhere, apunta que se trata de una tecnología intuitiva y fácil de usar: “es capaz de interactuar con cualquier sistema o aplicación a través de la interfaz de usuario, lo que permite a los



usuarios de negocio construir automatizaciones o bots por sí mismos y obtener un retorno de la inversión en cuestión de días o semanas en lugar de meses o años, como es el caso de otras tecnologías donde se requiere una inversión inicial mayor y más recursos técnicos”.

Generalmente se suele asociar la automatización con la destrucción de puestos de trabajo. Sin embargo, ABAI Group quiere desmarcarse de esa idea. “La RPA es un medio para un fin con más transcendencia. El ser humano aporta una función de valor que nunca podrá ser sustituida por robots porque aporta creatividad, juicio y empatía. Lo que queremos potenciar son esas habilidades hacia un automatismo para mejorar la experiencia del empleado, pero sin perder el foco de la máxima eficiencia y mínimos costes”, agraga Carlos Fernández, responsable de soluciones de negocio de ABAI Group.

UNA PROPUESTA EN ALZA

La automatización robótica de procesos es una tendencia global y organizaciones de todas las industrias y regiones ya han automatizado al menos alguno de sus procesos de negocio. Aunque las cifras pueden ser dispares (un informe de HfS Research señala que en 2021 el volumen de negocio de este sector será de 12.700 millones de dólares, mientras que Morgan Stanley aumenta la cifra a 54.000 millones), lo cierto es que hay un gran interés. En España, según IDC, el 58% de los CIO considera que la automatiza-

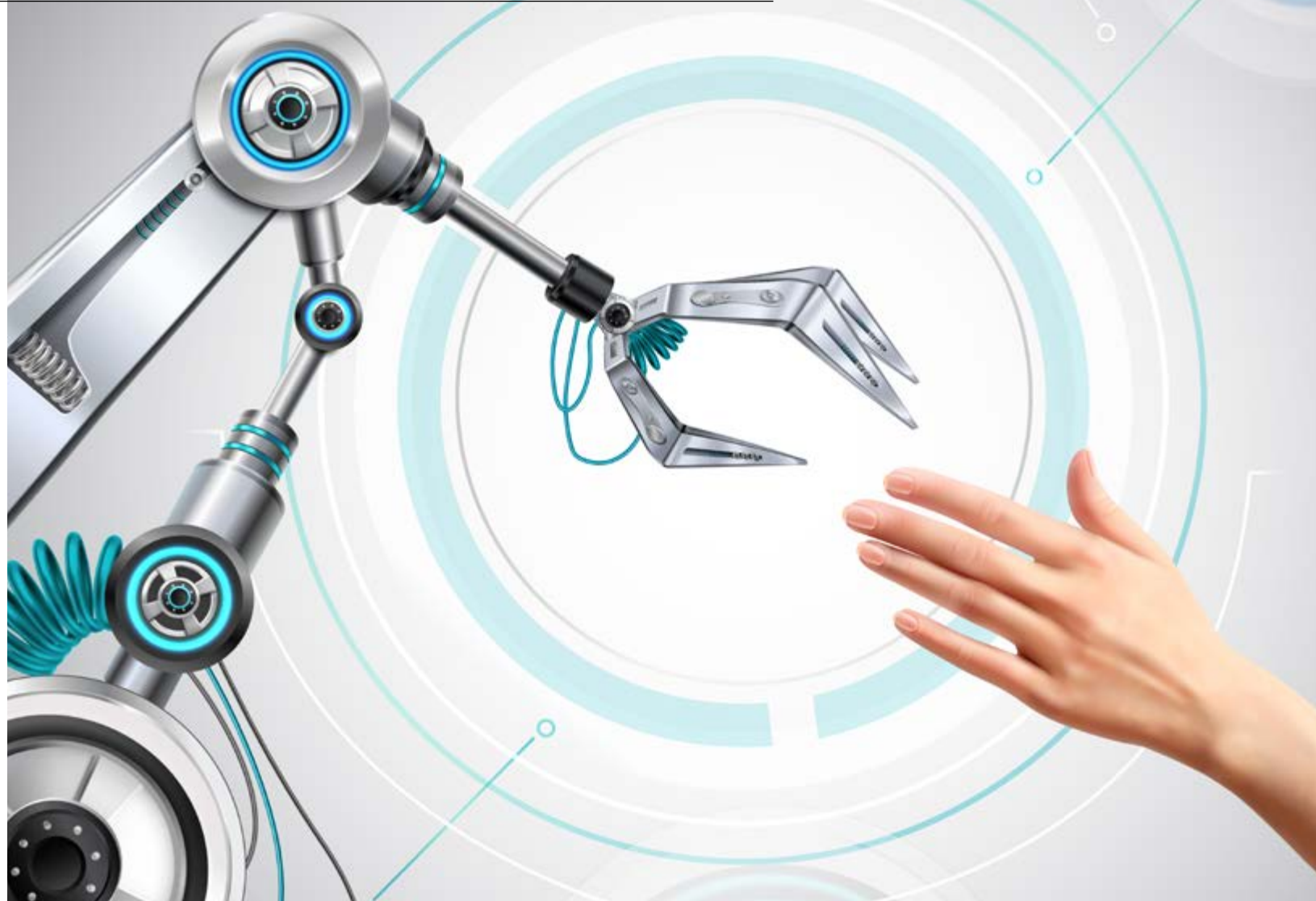
ción de procesos y la IA serán la principal prioridad de inversión. La consultora señala, también, que el mercado de RPA en nuestro país se duplicará en los próximos años.

“Entre los sectores más avanzados en la automatización inteligente, destacan Banca y Servicios Financieros, BPO, Utilities, IT y Manufacturing. No obstante, el contexto actual, en el que las organizaciones necesitan combinar la continuidad del negocio con la particularidad impuesta por la COVID-19 de evitar la interacción física y ser más ágiles a la hora de dar respuesta al cliente, está favoreciendo la aceleración de proyectos de automatización en todas las industrias, convirtiéndola en una necesidad. En este sentido, existe interés y necesidad en prácticamente todos los sectores, como el sector sanitario, la banca, las compañías aseguradoras, las operadoras de telecomunicaciones, el sector de la energía, el retail, la Administración Pública e, incluso, en el ámbito turístico”, asegura Ayllón.



“La crisis por la pandemia pone de manifiesto que las compañías deben estar preparadas para el cambio y garantizar la continuidad de su negocio. Las plataformas de automatización son sus aliadas para enfrentarse a este nuevo escenario”

VÍCTOR AYLLÓN, APPIAN



“RPA interactúa con cualquier sistema o aplicación, permite a los usuarios de negocio construir bots por sí mismos y obtener un ROI en cuestión de días o semanas en lugar de meses o años, como es el caso de otras tecnologías”

ÓSCAR MARTÍNEZ, AUTOMATION ANYWHERE

office y unificación de bases de datos. Sin embargo antes de que llegue 2025 va a ampliarse el nicho. “Nuestro día a día está lleno de tareas repetitivas. Envío de informes, datos de hojas de cálculo, recordatorios, evaluaciones de ratios etc. El cómputo de ese tiempo no es una cuestión menor y es que la RPA no solo cubre la capa básica de las tareas, sino que puede ampliarse a todas las actividades de procesos mecánicos que aportan poco valor”, afirma Fernández; “cuando las empresas midan los tiempos se darán cuenta del poco valor que les sacamos a las cualidades de nuestros empleados”.

“Entre nuestros clientes hay varias empresas del IBEX 35 -entre otros Santander Consumer- en las que estamos implementando proyectos junto con la ayuda inestimable de nuestro canal, gran cantidad de multinacionales con oficinas en España y que tienen como plataforma de automatización Automation Anywhere y un número importantes de oportunidades en diversos sectores”, apunta el responsable de ventas de la compañías, quien destaca, en estos momentos, la oportunidad que la aplicación de RPA tiene para hacer frente a los efectos de la COVID-19, y al uso que gobiernos y empresas están haciendo de sus robots RPA para combatir los desafíos que presenta la pandemia. No es un caso de nuestro país, pero puede servir de ejemplo: “colaboramos con varios hospitales, como el Hospital General de Northampton en Londres, para automatizar la monitorización

constante del suministro de oxígeno del centro médico, reducir el riesgo de errores y apoyar el tratamiento de pacientes con COVID-19”.

También desde Appian están obteniendo grandes referencias de clientes en nuestro mercado. “Los principales bancos españoles como Santander o Bankia utilizan nuestra aplicación y la administración pública está empezando a incorporar esta tecnología en sus procesos”, añade Ayllón, quien destaca también el Centro de Excelencia Robotics de Deloitte, “donde se han automatizado más de 100 procesos robóticos con Appian RPA, con más de 41.000 horas de uso en un año. Han amplificado sus capacidades de automatización de procesos a gran escala, con un importante impacto, tanto en operaciones internas de su área Business Process Outsourcing (BPO) como en procesos críticos para clientes de diferentes industrias”.

Por su parte, Fernández destaca que, “en ABAI Group implementamos RPA en telco, utilities y logística. El objetivo es separar el tiempo de gestión del tiempo de relación con el cliente. La automatización alivia sistemas, aplicaciones y tiempos de espera”.

AUTOMATIZACIÓN DE PROCESOS, COMBINACIÓN DE TECNOLOGÍA Y CAPACIDAD HUMANA

Además de generar oportunidades para las empresas, y en contra de la leyenda negra que acarrea la automatización, la RPA no significa destrucción

de empleo. Aún más, según el World Economic Forum (WEF), las profesiones emergentes resultantes de la automatización podrían representar 6,1 millones de empleos en todo el mundo entre 2020 y 2022. “La robotización puede potenciar las habilidades humanas y generar nuevas oportunidades laborales”, destacan desde Appian.

La creación de estas plataformas de software para la automatización de procesos se ha venido enriqueciendo en los últimos años sumando tecnologías. “Nuestros esfuerzos en I+D van encaminados a permitir a toda organización automatizar de forma integral sus procesos, de extremo a extremo. Para ello, combinamos diferentes tecnologías bajo una única plataforma que ayuden a nuestros clientes en todos los pasos de la automatización en sí: descubrir, analizar, diseñar, automatizar, medir, monitorizar y reevaluar; un concepto que va más allá de la RPA y que se conoce como hiperautomatización”, afirma Óscar Martínez.

“Nuestro día a día está lleno de tareas repetitivas y el cómputo del tiempo que empleamos en realizarlas no es una cuestión menor. La RPA puede ampliarse a todas las actividades de procesos mecánicos que aportan poco valor”

CARLOS FERNÁNDEZ, ABAI GROUP

Bajo este precepto, la solución de Automation Anywhere ofrece una propuesta en la nube, con un interfaz web, que se implementa en cuestión de minutos y es accesible desde cualquier dispositivo. Su plataforma combina RPA, inteligencia artificial, aprendizaje automático y análisis de datos en tiempo real, para ayudar a las organizaciones a iniciar rápidamente su proyecto de automatización de procesos y luego poder escalarlo fácilmente y de forma ilimitada. “Nuestra propuesta permite el uso de la automatización desde las aplicaciones más comunes como Salesforce, Excel o G Suite y, por tanto, solventa uno de los problemas de la automatización que, según Gartner, es el número limitado de procesos automatizados en las implantaciones existentes”.

Por parte de Appian, “entendemos la automatización de procesos como una manera de repensar los trabajos para combinar de la for-



ma más eficiente capacidades humanas, inteligencia artificial y robots, entendiendo cada una de estas piezas como “trabajadores” de un mismo workflow”. En base a ello, han construido una plataforma con la que “hemos conseguido un mayor control de la base instalada de bots así como la posibilidad de desplegar bots más sofisticados para tareas más complejas. La capacidad de orquestar fácilmente la próxima generación de mano de obra combinada: personas, software, robots e IA en flujos de trabajo sin fricción (incluso en ausencia de API), nos da una potente administración de robots para aumentar la escala y el rendimiento, y ejecutamos Appian Cloud, segura y disponible a nivel mundial”, relata Ayllón, quien destaca, además, la incorporación de Novayre Solutions SL, desarrolladores de Jidoka RPA, como un punto de

inflexión en su oferta. “Con la incorporación de este activo, Appian ha conseguido permitir a los clientes la opción de utilizar la funcionalidad de automatización full-stack (iBPMS, RPA, AI y gestión de caso) a través de Appian Cloud con la expectativa de que estas soluciones mantengan su rápido y fácil desarrollo y entrega, así como un ROI elevado y plazos muy cortos para recuperar la inversión”.

En el caso de ABAI Group, la compañía ha diseñado su solución RPA junto a su partner White Pass. “Ofrecemos un portfolio integral. Para ello hemos diseñado aplicaciones de negocio personalizables que sirven como interfaz entre las personas y el robot. Queremos reducir a cero el tiempo de petición y tramitación. Además, los robots no son infalibles y menos en procesos complejos, así que para ofrecer esa experiencia

integral cubrimos esos procesos haciendo que las gestiones no finalizadas se envíen a los especialistas. Es un marco digital sin carga y descarga de ficheros y sin tiempos vacíos por procesos manuales”, explica Fernández.

La oportunidad de la automatización está ahí. Hoy más que nunca las organizaciones deben estar preparadas para el cambio, para repensar sus negocios, para ganar agilidad. Y las cifras esperadas del mercado de automatización indican que están en el camino de querer y poder aprovechar las capacidades que esta propuesta tecnológica les brinda para seguir avanzando en su transformación. ■



MÁS INFORMACIÓN



[Entrevista completa con Óscar Martínez \(Automation Anywhere\)](#)



[Entrevista completa con Víctor Ayllón \(Appian\)](#)



[Entrevista completa con Carlos Fernández \(ABAI Group\)](#)

Si te ha gustado este artículo,
compártelo

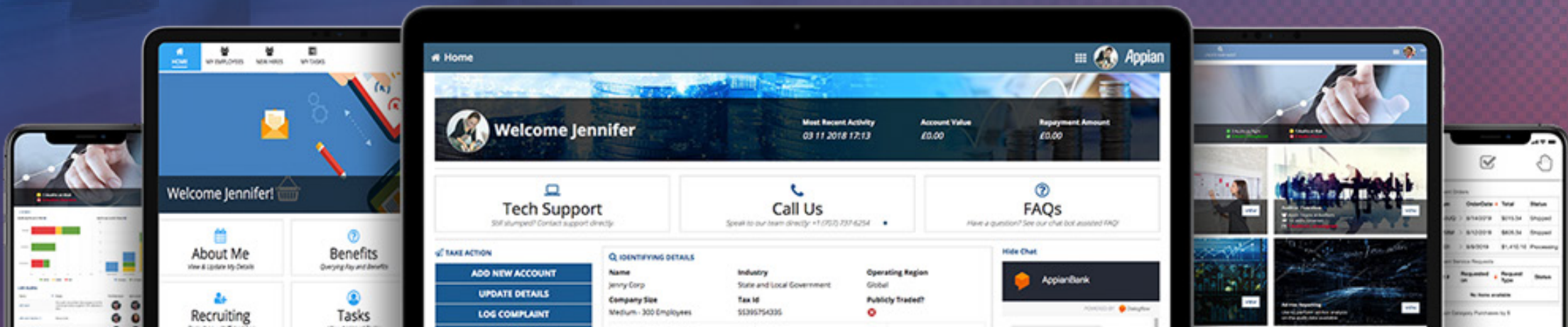


Automatizar las tareas.
Mejorar la productividad.
Todo con una plataforma potente.

Prueba hoy el RPA de Appian



Appian



Automatización inteligente para acelerar la transformación digital

ÓSCAR MARTÍNEZ,
Regional Sales
Director de
Automation Anywhere



Según Gartner, en los dos últimos años, la Automatización Robótica de Procesos o RPA ha sido el segmento de software de más rápido crecimiento. Para finales de 2023, el 90% de las organizaciones grandes o muy grandes habrán implementado alguna forma de RPA como pieza clave de sus iniciativas de transformación digital, en comparación con el 55% que ya lo hacían en 2019.

La Automatización Robótica de Procesos (RPA) es una forma de automatización no invasiva, intuitiva y fácil de usar, que interactúa con cualquier sistema o aplicación involucrada en un proceso a través de la interfaz de usuario.

Permite a los usuarios construir bots para auto-

matizar tareas comerciales basadas en reglas al imitar las actividades de un usuario y en general es más fácil de implementar, de forma que se obtiene un retorno de la inversión en cuestión de días o semanas en lugar de meses o años, como es el caso de otras tecnologías donde se requiere una inversión inicial mayor y más recursos técnicos.

Además, un gran número de organizaciones aplica ya diferentes tecnologías de Inteligencia Artificial para complementar y aumentar las posibilidades de la RPA (un 80% de las empresas para 2022, según Gartner), como por ejemplo en el procesamiento inteligente de documentos (IDP), donde se utiliza inteligencia

artificial para procesar datos no estructurados de correos electrónicos, contratos, documentos escritos a mano, etc.

En Automation Anywhere creemos que todo proceso que puede ser automatizado dentro de una organización debería ser automatizado para desbloquear el potencial humano, liberar a los empleados de esas tareas tediosas y repetitivas, y que así se puedan centrar en las cosas que sólo los humanos pueden hacer: como el pensamiento crítico y la creación de valor a través de la innovación.

Automation Anywhere es la única plataforma de RPA que democratiza el uso de la automatización de procesos con una combinación de

“Todo proceso que puede ser automatizado dentro de una organización debería ser automatizado para desbloquear el potencial humano”

facilidad de uso y la fiabilidad necesaria para acelerar las iniciativas de transformación digital de cualquier empresa.

Entonces, si el camino más rápido hacia la transformación digital es la automatización, ¿por qué es todavía tan difícil para muchas organizaciones hoy? La razón se debe a que la mayoría de las empresas tienen sistemas y aplicaciones informáticas tanto en front como en back office que trabajan en silos y nunca fueron diseñados para trabajar juntos. ¿Cuál es la principal ventaja de las empresas nativas digitales más exitosas? Estas empresas modernas nacieron ya en un mundo dominado por procesos digitales e integran las herramientas de front y back office y las aplicaciones de productividad que usan todos los empleados para obtener una ventaja significativa en términos de costes y velocidad de ejecución.

Hoy en día, las empresas tradicionales no solo se enfrentan a la competencia de estas compa-

ñías nativas digitales, sino también a otros factores externos como la reciente pandemia de COVID-19. RPA puede ayudar, es el ecualizador entre la empresa tradicional y las organizaciones nativas digitales.

Si bien ciertas soluciones de automatización puntuales pueden ayudar con ciertos pasos del proceso en el front o back office, solo una solución completa de automatización permitirá derribar los silos. De esta forma, las organizaciones pueden comenzar con cualquier proceso sabiendo que puede llegar a ser en una empresa totalmente automatizada y cerrar la brecha entre el front office, el back office y todos los empleados.

Esta transformación digital por medio del uso de la Automatización Inteligente a través del front y back office, permite a las empresas obtener las siguientes ventajas competitivas:

❖ Tomar medidas más rápidas bajo la restricción de recursos reducidos

❖ Mantener la continuidad del negocio con una fuerza laboral digital 24/7

❖ Preservar la conexión con todas las partes interesadas a través de múltiples sistemas

❖ Asegurar una buena atención al cliente durante picos en el volumen de llamadas

❖ Ayudar a proteger las funciones y operaciones comerciales más críticas durante los actuales momentos de incertidumbre

Automation Anywhere ofrece la única plataforma de automatización inteligente con una arquitectura diseñada para la nube y con un interfaz web, por lo que se implementa en cuestión de minutos y es accesible desde cualquier dispositivo. Combina RPA, inteligencia artificial, aprendizaje automático y análisis de datos en tiempo real, para ayudar a las organizaciones a iniciar rápidamente su proyecto de automatización de procesos y luego poder escalarlo fácilmente y de forma ilimitada. ■

Si te ha gustado este artículo,
compártelo



El equipo de Rainbow y Extel CRM somos ahora

ABAI GROUP
YOUR BUSINESS PARTNER

ABAI Group es una compañía de servicios de
relación con clientes y externalización de procesos

Para más información sobre nuestras soluciones de
gestión omnicanal, Back Office, RPA, Text&Speech
Analytics, Chatbot y Big Data consulta nuestra web

www.abagroup.com



RPA: de necesidad empresarial en confinamiento a ventaja competitiva frente al cambio

VÍCTOR AYLLÓN,
Vicepresidente RPA
Centro de Excelencia
de Appian Corporation



La automatización no es un fenómeno nuevo. Ha estado presente a lo largo de la historia como una oportunidad para generar más valor a partir del equilibrio del paradigma clásico de personas, procesos y tecnología. Sin embargo, no ha sido hasta hace unos años, cuando los “robots software” RPA empiezan a ganar tracción a un ritmo acelerado en el tejido empresarial español, sobre todo, en el sector TIC, Industria, Banca y Utilities. Prueba de ello, son los datos que ofrece IDC. La consultora revela que en España la inversión en automatización de procesos se duplicará hasta 2021.

La capacidad que tiene el RPA de liberar a los trabajadores de tareas de gran volumen, repetitivas y lineales, que requieren un elevado esfuerzo manual, y traspasarlas a una “plantilla digital” de robots software, aportando rapidez

y precisión a los procesos, permite a las organizaciones evolucionar rápidamente hacia un paradigma más productivo, ágil y eficiente. Es por ello que RPA está ganando tracción a un ritmo acelerado, siendo, según la consultora Gartner, la categoría de software empresarial de más rápido crecimiento en los últimos años.

Aun así, en la mayoría de los procesos aún hay tareas “robóticas” que se ejecutan de forma manual y que requieren una elevada dedicación humana, restando recursos a actividades de mayor valor. Según los expertos, el mercado RPA aún tiene mucho margen de crecimiento y un largo recorrido por delante.

COVID-19, CATALIZADOR DEL CAMBIO

Antes del COVID-19, Deloitte vaticinaba que, en 2020, el 72% de las entidades habría empe-

zado a adoptar esta tecnología. Sin embargo, el coronavirus ha acelerado esta tendencia al evidenciar que la automatización robótica de procesos es una necesidad para todas las empresas en pleno confinamiento.

El aislamiento social impuesto como medida para frenar la propagación del virus ha paralizado organizaciones de sectores como el aéreo o el turístico y ha puesto bajo presión a las de sectores como el sanitario o el comercio electrónico, que se han visto obligadas a buscar nuevas fórmulas para continuar operativas al tiempo que protegen la salud de sus trabajadores. En ambos casos, RPA ha permitido dar respuesta a estos desafíos. Para las primeras, la automatización es una forma de reducir costes en un momento de inactividad y para las segundas, una necesidad para escalar su ca-

pacidad operativa. La repentina dispersión de los equipos de trabajo ha dejado claro que los procesos de negocios deben poder ser operados, gestionados y coordinados de forma similar independientemente de dónde se encuentren los trabajadores.

Con este panorama, muchas organizaciones pisan el acelerador para abordar proyectos de automatización. Estamos observando como los directivos precipitan sus inversiones en automatización como consecuencia del COVID-19, principalmente porque, además de los beneficios mencionados, esta tecnología presenta particularidades que hacen factible una adopción generalizada en un momento como el actual. Hablamos de su versatilidad para automatizar procesos muy diferentes, su rápida implementación o su desarrollo, que no interfiere con sistemas corporativos ya implantados.

Hay muchas empresas que están aprovechando la coyuntura para empezar a construir ahora lo que serán los procesos en la época post COVID-19, convencidas de que la automatización robótica de procesos les aportará una ventaja competitiva clave.

La pandemia del COVID-19 ha dejado patente que vivimos un momento repleto de incertidumbres por un virus que se manifiesta y propaga de manera caprichosa y que la relajación de las medidas de confinamiento nos devolverá a una normalidad en la que nada volverá a ser como antes. En este escenario, la única certeza es que

RPA será un valor diferencial para que las compañías estén preparadas para el cambio.

RPA INTELIGENTE Y EN EL CLOUD

Con el objetivo de dar respuesta a un entorno empresarial repleto de interrogantes y rápidamente cambiante, se abordarán despliegues de RPA en el Cloud que, además de proporcionar conectividad a los procesos y dotar de continuidad al negocio, permitirá dimensionar la capacidad de ejecución con rapidez y agilidad en función de las necesidades del mercado. También se le dotará de inteligencia artificial (IA) con el objetivo de identificar, diseñar, medir y administrar procesos automatizados en toda la empresa.

Tradicionalmente y de forma equívoca, se ha pensado que la automatización reemplazaría a los humanos. Superada esta asociación y demostrado que, lejos de eliminar puestos de trabajo, genera nuevas oportunidades laborales- según el World Economic Forum (WEF), las profesiones emergentes resultantes de la automatización podrían representar 6,1 millones de puestos de trabajo entre 2020 y 2022-, la automatización robótica de procesos se convierte en una pieza fundamental en la transformación digital de la empresa.

DEL RPA 1.0 A LA HIPERAUTOMATIZACIÓN

La tecnología RPA muestra sus mayores ventajas y rentabilidad en procesos mecánicos,

basados en reglas, con una entrada y una salida bien definida, aunque no todos los casos de uso pueden ser abordado como proyectos “puros” de RPA. Gartner recientemente ha introducido el término “Hiperautomatización” que es la confluencia de tecnologías RPA, BPM e Inteligencia Artificial para poder ofrecer una automatización de procesos que sea efectiva y que aborde procesos complejos y completos.

En este contexto, RPA desarrolla todo su potencial para proporcionar la adaptabilidad y la resiliencia necesaria para que las organizaciones sean competitivas en una economía globalizada en la que también la capacidad de innovación se “contagia”.

Estamos inmersos en una imparable revolución tecnológica: la forma de operar de las empresas y el papel del trabajador humano está evolucionando rápidamente. Y la actualidad deja claro que, hoy más que nunca, las compañías deben estar preparadas para el cambio. La automatización de procesos, que combina el potencial de RPA con las tecnologías de IA y las capacidades humanas, es un aliado fundamental para enfrentarse a este nuevo escenario. ■

Si te ha gustado este artículo,
compártelo



RPA

automatización y agilidad corporativa



it **TRENDS** Especial

¡DESCÁRGALO AQUI!



Diálogos itTRENDS



“La inteligencia del espacio de trabajo está ligada a la productividad y a las interrupciones”
(Mar García, Citrix)



“HPE propone IA y alta computación para acelerar la búsqueda de la cura de la COVID-19”
(Fran Yañez, HPE)



“Los atacantes utilizan todo lo que está a su alcance para sofisticar sus ataques, y sabemos que la IA no es una excepción” (José Luis Laguna, Fortinet)



“La monitorización de las funciones serverless es fundamental” (Eusebio Nieva, Check Point)

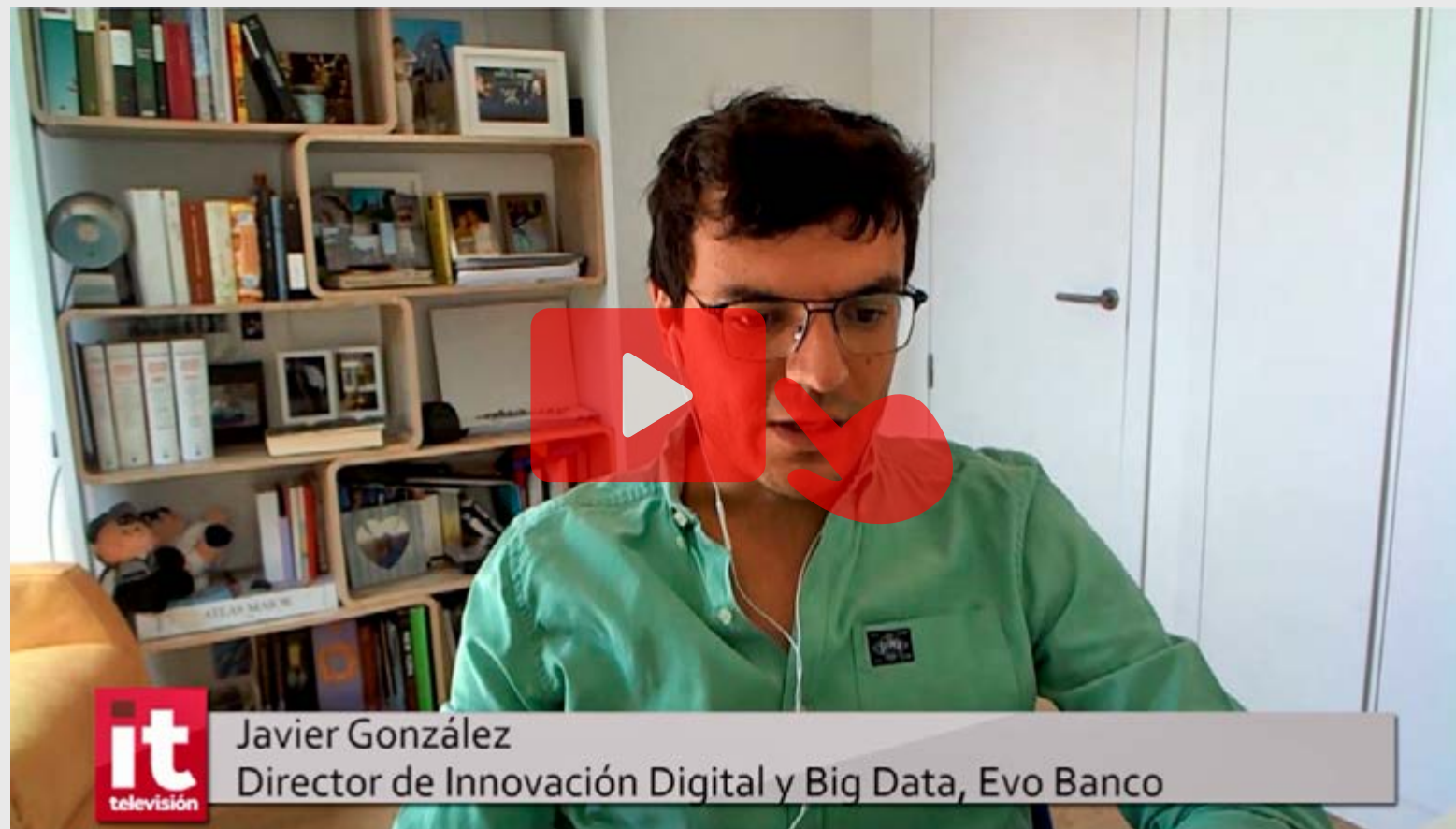


“El ADC se necesita siempre, la gran diferencia es cuándo y cómo necesito balancearlo”
(Joaquín Gómez, VMware)



“Por cada empleado puede haber hasta 10 cuentas privilegiadas” (Albert Barnwell, CyberArk)

Diálogos itTRENDS



EVO Banco plasma en una hipoteca digital su filosofía tecnológica

El sector de la banca ha hecho tradicionalmente un uso intensivo de las tecnologías para procesar sus datos, gestionar las transacciones, estudiar los cambios en el mercado, poner la atención en los usuarios y generar nuevos productos como la hipoteca digital de EVO Banco. En IT Trends, hablamos con Javier González, Director de Innovación Digital y Big Data de EVO Banco, sobre las tecnologías que se esconden tras este producto, así como tras la TI corporativa de la entidad.

Cada mes en la revista,
cada día en la web.



**JUAN CARLOS PASCUAL****CYBERSECURITY SERVICES MANAGER
EN CAPGEMINI**

Juan Carlos Pascual, estudió ingeniería informática por la UNED y Programa ejecutivo de Innovación en Ciberseguridad por la Universidad de Deusto, trabaja desde 2014 en Grupo Capgemini en el área de ciberseguridad. Ha centrado su carrera en el sector tecnológico dentro de áreas relacionadas con la seguridad, cloud y las comunicaciones.

Seguridad Cloud:

La capacidad de extender la empresa más allá de los límites



La nube es un nuevo paradigma en la empresa. Hasta hace no mucho había quien aún alojaba reticencias sobre la adopción de la nube. Con todo, las circunstancias actuales han abierto los ojos a aquellos que lo veían como una opción incierta y lejana.
¿Cómo renunciar a los beneficios que proporciona este entorno?

Compartir en RRSS

Una de las principales prioridades de las empresas es contar con un sistema robusto. Los retos planteados por las amenazas existentes y las nuevas normativas de protección de datos y seguridad en las redes hacen necesario que una de las patas de la transformación digital sea la ciberseguridad, que debe estar alineada con el negocio para ayudarle a conseguir sus objetivos. A la hora de definir las conexiones y trabajar con los

recursos de información de la empresa, es necesario tener en cuenta varios puntos:

■ **Seguridad del dispositivo.** La respuesta sobre el uso de dispositivos abarca un amplio rango de productos, PCs domésticos, dispositivos móviles, los propios portátiles corporativos..., todos ellos con una protección y aislamiento adecuados y con una gestión de la logística que incluya seguridad del endpoint y parches de seguridad actualizados.

■ **Seguridad del usuario** para poder hacer frente a las amenazas de un entorno ajeno a la oficina. Ingeniería social, phishing y otros tipos de ataques dirigidos deben encontrar usuarios concienciados. El primer firewall es un usuario concienciado.

■ **Continuidad del negocio y recuperación de desastres** ante los que un entorno en la nube es ideal, dada la capacidad de dimensionamiento de los recursos cloud, la habilitación de entornos redundantes y las arquitecturas de redundancia adaptadas a las necesidades de disponibilidad, recuperación en caliente o “cold sites” virtuales.

■ **Seguridad de las conexiones** para garantizar que la información que se comparte no resulta accesible para los posibles atacantes. Hay que tener en cuenta que los datos de la empresa no solamente pueden ser confidenciales. También pueden estar protegidos legamente, como los datos personales, y transmitirlos sin precauciones puede aparejar multas además de una pérdida de reputación. Las redes privadas virtuales (VPN)



Hay que tener en cuenta que los datos de la empresa no solamente pueden ser confidenciales



Aprovisionar un entorno seguro y garantizar la protección es otra de las capacidades de un puesto de trabajo en la nube

partir información, realizar videoconferencias y trabajo en grupo ha supuesto un reto importante para las empresas. Los paquetes de colaboración en la nube, como Office 365 o GSuite garantizan el uso de software de confianza, con la ventaja añadida de poder controlar el consumo de las licencias de manera adecuada. En este caso, la seguridad viene unida a la economía.

son soluciones al alcance de todos y las bondades que proporcionan están fuera de toda discusión.

- **Seguridad y homogeneidad del entorno.** El ecosistema de aplicaciones resulta controlado en el ámbito de una empresa, pero es difícil hacerlo cuando se teletrabaja. Aprovisionar un entorno seguro y garantizar la protección es otra de las capacidades de un puesto de trabajo en la nube. La seguridad se actualiza automáticamente de manera homogénea.
- **Seguridad de las herramientas de colaboración.** La proliferación de herramientas para com-

- **Seguridad en las aplicaciones de negocio.** La seguridad irá orientada por un análisis de riesgos. Existen excelentes soluciones nativas en cloud y otras complementarias de fabricantes que aportan una mayor flexibilidad en la gestión de claves y trabajan con componentes de cifrado, ya sea manejo de algoritmos como custodia de claves.
- **Las auditorías de seguridad** son clave para comprobar que los controles funcionen. Las empresas deben asegurar periódicamente que el funcionamiento y las configuraciones de seguridad son las correctas, que las aplicaciones se han desarrollado con la debida seguridad y que



La evaluación y gestión de riesgos será la que determine los puntos en los que es necesario reforzar las configuraciones

están actualizadas. En este punto, los entornos cloud disponen de monitores de configuración que facilitan la tarea, obviamente la evaluación y gestión de riesgos será la que determine los puntos en los que es necesario reforzar las configuraciones con elementos adicionales a las provistas por el cloud.

Una vez están definidas todas las características de seguridad de la red, es necesario hacer una monitorización de seguridad, en la que se puedan detectar incidentes de seguridad y responder adecuadamente, así como realizar análisis forenses tras un ataque. Es fundamental conocer qué ocurre

Enlaces de interés...

- I [T-Systems y Check Point abordan la seguridad en entornos cloud híbridos](#)
- I [SASE: Cinco pasos hacia un enfoque moderno de la ciberseguridad](#)
- I [Los ataques externos a cuentas cloud han crecido un 630%](#)

en el entorno cloud de la empresa y actuar de manera proactiva, para que los ataques no consigan su objetivo y para poderlos identificar de manera que cualquier incidente similar en el futuro quede identificado y pueda pararse.

Es indiscutible que el camino a la nube en muchos sitios ha resultado complicado y ha planteado muchos interrogantes, pero actualmente, habilitar entornos masivos de teletrabajo es una tarea rápida y sencilla, sin dejar de lado la ciberseguridad, que puede ser incluida dentro del propio entorno totalmente adaptada a las necesidades más exigentes. **it**



nº 58
JULIO-AGOSTO 2020



La ciberseguridad en 2020
y las oportunidades
para el canal, a debate



**Digital
Signage:**

el valor de la imagen



Reseller
TECH&CONSULTING



Cada mes en la revista,
cada día en la web.



JORGE DÍAZ-CARDIEL

**SOCIO DIRECTOR GENERAL DE ADVICE
STRATEGIC CONSULTANTS**

Autor de “Éxito con o sin crisis”, “Recuperación económica y Grandes Empresas”, “La victoria de América”, “Innovación y éxito empresarial”, “Las empresas y empresarios más exitosos de España”, “Digitalización y éxito empresarial” y “Digitalización, productividad y competitividad: empresas más exitosas gracias a la transformación digital”.

Contexto geoestratégico de la guerra tecnológica entre EE.UU. y China



“A veces, lo barato, sale caro”. Además de ser un dicho popular, es una frase pronunciada por el presidente norteamericano Donald Trump en entrevista televisada con María Bartiromo, la periodista económica y de negocios más influyente de Estados Unidos, editora de “Sunday Futures” y “Mornings with María Bartiromo” de FoxBusiness Network.

Compartir en RRSS





Trump se refería, en respuesta a Bartiromo, al “outsourcing” o subcontratación de la producción de productos tecnológicos norteamericanos a empresas chinas con sede en China continental (por contraste con Taiwan, también llamada, China insular) y a la subcontratación de la producción de coches norteamericanos a México. Como sabemos, es una cuestión de menores costes laborales: Silicon Valley subcontrata la producción de chips, semiconductores, redes, ordenadores, servidores y teléfonos móviles a empresas chinas, porque los costes laborales en el país asiático son infinitamente menores que en Estados Unidos. Lo mismo sucede con los tres grandes fabricantes de automóviles de Detroit, que, al trasladar la producción a México, reducen costes, sí, pero como sucede en Silicon Valley, dejan el mercado laboral americano convertido en un erial o, como diría el gran escritor británico-estadounidense T.S. Elliot, “en tierra baldía”.

Sin embargo, enmarcar el enfrentamiento (sea en Tecnologías de la Información o en automóviles) entre Estados Unidos y China en la constreñida

cuestión de los costes laborales es de una gran pobreza intelectual. El marco, el contexto y el trasfondo son mucho mayores. Lo que está en cuestión es la primacía de Estados Unidos como primera potencia económica, empresarial y militar del mundo. Los norteamericanos somos paranoicos. Como escribió Andy Grove, expresidente y CEO de Intel: “only the paranoics survive” (sólo los paranoicos sobreviven). La paranoia está instalada en la psicología norteamericana y, en el caso que nos ocupa, desde los

políticos y los empresarios a la población general, la pregunta está en el aire, cuando menos desde 2009: “¿perderá Estados Unidos su condición de primera potencia mundial a favor de China?”. Es la cuestión central de uno de los libros del experto en política internacional y buen amigo, Fareed Zakaria (CNN, Time, Newsweek, Foreign Affairs), “The Post American World”, libro de cabecera del presidente Barack Obama, también amigo (y exjefe). La lectura de esta obra llevó a Obama a preguntarse en el dis-

Sin embargo, enmarcar el enfrentamiento (sea en Tecnologías de la Información o en automóviles) entre Estados Unidos y China en la constreñida cuestión de los costes laborales es de una gran pobreza intelectual

curso sobre el Estado de la Unión de enero de 2020 sobre si “¿no debíamos haber sido nosotros los que construyéramos el tren bala de Shanghái en vez de China?”. Diez años después, la pregunta se mantiene y explica en buena parte la victoria de Trump en las elecciones presidenciales de 2016 con su lema “America First”.

Tras la caída de la Unión Soviética en 1991, Estados Unidos queda como única superpotencia

mundial. Primero Bush padre y, después, Bill Clinton, impulsan la globalización y los tratados de libre comercio que, junto al desarrollo intensivo y fuerte de las Tecnologías de la Información e Internet impulsan el comercio mundial y, en Estados Unidos se vive una época de excepcional crecimiento económico (media de crecimiento del PIB del 5% durante la década de los años noventa y 24 millones de nuevos puestos de trabajo). Entonces empieza la subcontratación de la fabricación norteamericana a China y otros países asiáticos. Pero, conforme a la “destrucción creativa” de Schumpeter, al tiempo que se destruyen negocios y empleos en Estados Unidos (manufactura, agricultura, los que luego votaron a Trump), se crean otros nuevos al albur de la nueva economía del conocimiento.

La globalización no para durante los ocho años de presidencia de George Bush Jr, pero, tras los atentados del 11S y las guerras de Oriente Medio, las prioridades de Estados Unidos cambian y buena parte de los recursos públicos van a financiar las guerras en Afganistán, Iraq y, después, Siria. Apareció la crisis financiera o gran recesión de 2007-2009, la peor para Occidente desde la Gran Depresión de 1929-1946. Y Estados Unidos necesita financiación: China se la ofrece. En 2010, el 32% de los bonos del Tesoro norteamericano están en manos chinas. Una venta masiva hubiera desestabilizado fuertemente más la economía norteamericana. Pero, con Barack Obama, en junio de 2009, acaba la recesión y comienza el período más extenso de crecimiento económico

y creación de empleo en 50 años: entre junio de 2009 y febrero de 2020 la economía crece una media del 3% en PIB y se crean 32 millones de empleos, dejando tasa de paro en 3,5%. Barack Obama puso los fundamentos y Donald Trump continuó construyendo. Pero, al mismo tiempo, los norteamericanos dejan de ver en los productos que compran el famoso “Made in América”, que es sustituido por el “Made in China”. Millones de empleos en manufactura se pierden en Estados Unidos a favor de muchos más millones de chinos que cobran un dólar diario y un cuenco de arroz para estar en forma y trabajar 18 horas diarias seis días a la semana. Al abrir la caja de un iPhone se lee: “Diseñado en Estados Unidos” y “Fabricado en China”. Apple, HP, HPE, Microsoft, Intel, Google... subcontratan la fabricación a China, por ejemplo, a una -entre muchas otras “ciudades/fábrica”, así se llaman en chino- empresa como Foxconn, con un millón de empleados. Las compañías de telecomunicaciones, como Verizon, AT&T, T-Mobile / Sprint, Comcast delegan la fabricación de redes en conglomerados chinos como Huawei. Igualmente, los fabricantes de chips/microprocesadores, como Intel, Nvidia y AMD.

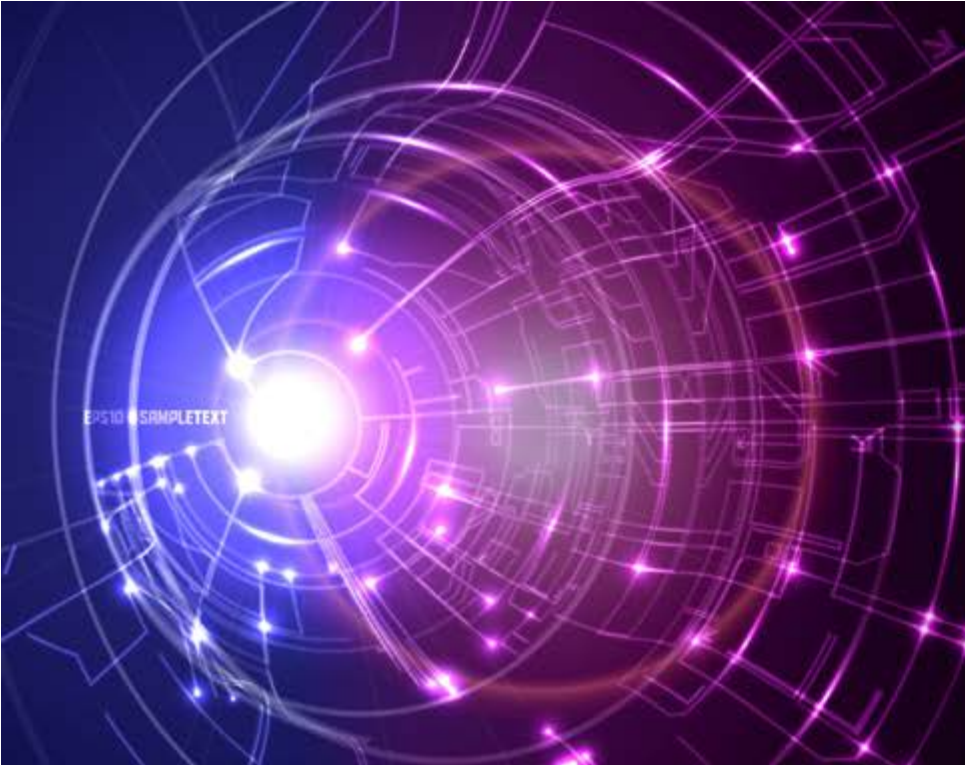
El descontento social es tan grande en Estados Unidos que obreros y agricultores votaron a Donald Trump en noviembre de 2016, quien les promete restaurar la gloria de América y repatriar empleos y beneficios empresariales. Trump, con el “America First” ofrece una fiscalidad muy favorable a las empresas TI que decidan traer a casa los beneficios



Trump, con el "America First" ofrece una fiscalidad muy favorable a las empresas TI que decidan traer a casa los beneficios en lugar de dejarlos en las filiales extranjeras

en lugar de dejarlos en las filiales extranjeras: en vez de pagar el 25% del impuesto de sociedades, pagarán un 10% y Apple y HP, Microsoft e Intel, se “apuntan”. Apple llega a poner en marcha una fábrica para 10.000 empleados en Texas y dos viejos enemigos, Tim Cook y Donald Trump, se hacen amigos.

Igualmente, Amazon (Jeff Bezos) ve amenazado su liderazgo mundial en comercio electrónico por Alibaba, propiedad de un ciudadano chino educado en mi alma mater, Harvard, Jack Ma, aunque su empresa vale en bolsa la mitad que Amazon. Trump otorga a Amazon la mitad del contrato de cloud más grande de la historia, convocado por el



La paranoia está instalada en la psicología norteamericana y, en el caso que nos ocupa, desde los políticos y los empresarios a la población general, la pregunta está en el aire, cuando menos desde 2009: "¿perderá Estados Unidos su condición de primera potencia mundial a favor de China?"

Pentágono en 2017 y destinado en principio íntegramente a Amazon, pero son años en que Bezos y Trump se llevan mal. Hasta que Bezos pide ayuda a Trump y éste, para recompensar a Bezos "por su humildad" y por la vanidad que le genera al presidente, da marcha atrás en su decisión de otorgar enteramente a Microsoft Azure el proyecto de cloud computing (JEDI) y lo divide a partes iguales entre Amazon y Microsoft. Jeff Bezos y Donald Trump se hacen amigos y, a cambio, Trump pide ayuda a Bezos para luchar contra China, contra Alibaba, para ser exactos. Satya Nadella, CEO de Microsoft no se ofende por llevarse solo la mitad del concurso del Pentágono. Su karma es budista y su alma es pacifista: mejor la mitad que nada, piensa Nadella.

Oracle no queda fuera, porque Larry Ellison puede sacar pecho por tener el contrato de Inteligencia Artificial más potente de la historia que le otorga la Agencia Central de Inteligencia. La unión, con estos y otros muchos ejemplos, entre las empresas TI y la administración americana no es sino una vuelta a la colaboración que ya hubo durante la Guerra Fría, solo que con un enemigo distinto: de la extinta Unión Soviética a China.

Primero, Trump desata la guerra comercial contra China, imponiendo aranceles a la importación de productos chinos. Luego, resumiendo mucho, "enfila" empresas concretas chinas porque son una amenaza para la Seguridad Nacional de Estados Unidos y para las grandes empresas

TI norteamericanas: Facebook, Alphabet-Google, Amazon, Microsoft, Apple se quejan de una competencia desleal de Tencent, Baidu, Alibaba, Xiaomi, Huawei, entre otras. El caso de Huawei es quizá el más conocido porque vende equipos de telecomunicaciones, teléfonos móviles y redes. Sin ir muy lejos, en España, Telefónica tuvo sus redes en manos de Huawei para el despliegue de 5G. Al igual que Orange, Vodafone, Deutsche Telecom y todas las operadoras de telecomunicaciones europeas. Y norteamericanas, porque también Verizon, AT&T, Comcast, T-Mobile/Sprint dependían de Huawei. Y, también el sector de chips/microprocesadores, con Intel, Nvidia y AMD dependiendo de Huawei.

**Enlaces de interés...**

V [Maria Bartiromo entrevista a Donald Trump en Fox Business](#)

Primero, Trump desata la guerra comercial contra China, imponiendo aranceles a la importación de productos chinos

Así que llegaron las sanciones de Trump a la empresa china que, como su propio presidente ha dicho públicamente, “ha restado 12 billones de dólares a nuestra facturación anual”. Personalmente, no creo que una alianza de Nokia-Ericsson-Alcatel Lucent sea suficiente para contrarrestar a Huawei. Sería como comparar a “Los Panchos” -con todo respeto- con “The King”, Elvis Presley.

Pero la cuestión de Huawei, Tencent, Xiaomi, Baidu... es sólo una parte de la cuestión. China ha entrado en recesión. El 21 de mayo de 2020, por vez primera desde 1978, el gobierno chino ha reconocido que no conseguirá su objetivo de creci-

miento económico este año. Y aprieta las tuercas a Taiwán y a Hong-Kong, a pesar de que ellas quieren seguir siendo independientes. Estados Unidos se retira de la Organización Mundial de la Salud, porque cree que está al servicio de China quien, por su parte, “insufla” dos billones de dólares a la OMS; China está construyendo islas artificiales militares en el Mar de China y en el Mar de Japón, lo que ha llevado a Corea del Sur, Japón y Australia a pedir ayudar militar norteamericana. Trump ha respondido con el despliegue de varias divisiones del Cuerpo de Marines (USMC) en los tres países. Y ha enviado la Séptima Flota (70 bar-

cos y submarinos, 300 aviones y más de 40.000 marines) al Pacífico para proteger Corea del Sur, Taiwan, Japón y Australia. El coste de la defensa norteamericana lo pagan los países defendidos, excepto la Séptima Flota.

Me preguntaron la semana pasada si era cierto que Estados Unidos y China irían a la guerra (militar). Respondí que no. Por ahora, Trump “se contenta” con exigir a las empresas cotizadas chinas en los mercados de valores estadounidenses, los mismos requerimientos de transparencia informativa que se exige a las empresas norteamericanas. 

¿Cuál es la situación de la empresa española en relación con la digitalización?

¿Qué tecnologías son las que están impulsando la transformación digital?

Descubra las últimas tendencias en el **it** Centro de Recursos **User**

Tecnología

para tu **Empresa**

Con la colaboración de:



servicenow

SAMSUNG

