it Reseller
TECH&CONSULTING

nº 68
JUNIO 2021

CONTENIDOS↓

Oportunidades para el canal de TI en torno a los Fondos NextGenEU, a debate

Inteligencia y analítica de datos como oportunidad para el canal, a debate

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

IA e IoT

Nuevas oportunidades, nuevos retos

EDITORIAL

it Reseller TECH&CONSULTING

it televisión

Director Pablo García Reales
pablo.garcia@itdmgroup.es

Redacción y colaboradores Hilda Gómez, Arantxa Herranz, Reyes Alonso, Ricardo Gómez, Eva Herrero

Diseño revistas digitales

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

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

El canal español sigue creciendo con firmeza

Apesar de la terrible desgracia que el COVID-19 ha arrastrado consigo a todos los niveles, la industria tecnológica se ha sabido aferrar con vigor a sus virtudes desde el primer momento y ha llegado incluso a cosechar guarismos extraordinariamente satisfactorios. El canal TI español, en particular, experimentó el pasado año una progresión ascendente, que se vio culminada en diciembre con un espectacular crecimiento interanual en facturación de un 28%. El sector ha emprendido 2021 sosteniendo niveles de mejoría superiores al 20%, entre los que destaca la fuerte subida experimentada por los canales de consumo, cifrada en un 34%. Pese a la tercera ola de la pandemia y a elementos disruptivos como el temporal Filomena o las elecciones catalanas, el canal se ha visto empujado por la creciente demanda de tecnología, especialmente de dispositivos móviles y soluciones de telecomunicaciones. También están registrando notables repuntes las áreas de software y licencias, así como de consumibles de impresión.

Con respecto a los portátiles, la categoría reina de 2020, su rendimiento ha mantenido su excelencia en prácticamente todos los canales durante las primeras semanas del año, con un crecimiento interanual del 74%. Los retailers han experimentado el comportamiento más destacado en este segmento, seguidos de los resellers corporativos, los distribuidores pequeños y medianos, y los etailers de consumo. Los etailers corporativos han sido los únicos en ver decrecer sus ratios de ventas de portátiles.

El optimismo y la confianza en el presente y el futuro del canal tecnológico siguen siendo halagüeños, amparados por un horizonte entusiasta donde cada día se atisban más cerca los Fondos Europeos de Recuperación. ■

Pablo García Reales

SUMARIO

Junio 2021

it Reseller TECH&CONSULTING

EN PORTADA

IA e IoT: Nuevas oportunidades, nuevos retos

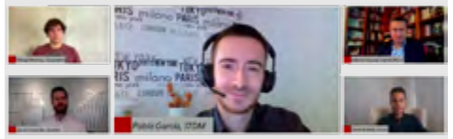
REVISTAS DIGITALES

ANUNCIANTES

ENTREVISTA

George Chen, director general de Newline EMEA

DEBATE



Inteligencia y analítica de datos como oportunidad para el canal, a debate

MESAS REDONDAS GTI

Oportunidades para el canal de TI en torno a los Fondos NextGenEU, a debate

REPORTAJE

El contact center: salvavidas de muchas empresas en la pandemia

TENDENCIAS

NO SOLO it

ACTUALIDAD

SOLUCIONES

SAMSUNG

Portable SSD T7

Super Fast External Storage

WORLD'S
No.1
FLASH MEMORY
SINCE 2002
SAMSUNG

* Source: 2019 Q2 IHS Markit data: NAND suppliers' revenue market share

FRANCISCO TORRES BRIZUELA, DIRECTOR DE CANAL, ALIANZAS Y CLOUD DE NETAPP ESPAÑA

"Con Unified Partner ayudamos al canal a rentabilizar los cambios del mercado"

NetApp acaba de anunciar cambios en su programa Unified Partner, los cuales entrarán en vigor su año fiscal 2022, y que buscan "permitir a nuestro ecosistema de partners aprovechar los cambios que se han producido a raíz de la pandemia". Así lo ha asegurado Francisco Torres Brizuela, director de canal, alianzas y cloud de NetApp España, quien ha reconocido que "la pandemia ha acelerado la transformación digital de las empresas", algo que también "está afectando al canal".

Las mejoras anunciadas proporcionarán a su canal una experiencia más flexible, coherente y simplificada, algo que "les permitirá estar mejor preparados para los cambios" que se están produciendo y que se acelerarán el próximo año. "Queremos expandir nuestro ecosistema de partners a través de nuevos incentivos financieros, acelerando la rentabilidad y

añadiendo nuevas soluciones y servicios mediante especializaciones certificadas".

MÁS INCENTIVOS

Así las cosas, NetApp detalla que las mejoras incluidas en Unified Partner "afectarán a todas las categorías del programa" e incluyen una expansión de la comunidad, que incluirá socios especializados que venden, consumen o influyen en la cartera de la empresa, lo que a su vez potencia el atractivo para captar más tipos de socios.

Además, se van a incluir incentivos simplificados, alineándolos con iniciativas clave y enfocándolos en áreas como la adquisición de clientes, FlexPod, o el consumo y la nube (una de las prioridades de NetApp), entre otras. Estos incentivos vinculados a nuevas especializaciones serán más predecibles a lo largo del ciclo de vida de las ventas.

También se incluirán recompensas para nuevos socios, que obtendrán beneficios por acciones que impulsen el cierre de acuerdos como parte de programas estratégicos, por ejemplo, al establecer reuniones y registrar nuevos acuerdos.

NetApp acaba de anunciar cambios en su programa Unified Partner. El renovado programa de NetApp amplía el ecosistema de socios, ofrece nuevos incentivos financieros y acelera la rentabilidad, además de incorporar nuevas soluciones y especializaciones de Servicios Certificados.

NUEVAS ESPECIALIZACIONES

El programa también ofrece una oportunidad para reconocer y recompensar los conjuntos de habilidades y modelos de comercialización únicos de los partners, con la disponibilidad de nuevas especializaciones de soluciones para Cloud Preferred, FlexPod, SAP, AI/ML, Data Protection, Data Security, Hosting Service Provider, Infrastructure y Spot by NetApp Preferred. La transformación de las Services Certified Specializations incluye Integration Services Certified, Lifecycle Services Certified, y NetApp Keystone Services Certified, lo que garantiza la alineación con las necesidades de los clientes en todo el ciclo de vida de la nube híbrida.

PARTNER CONNECT 2.0 RENOVADO

Finalmente, NetApp destaca Partner Connect 2.0, un rediseño de su localizador de socios, pensado para ofrecer una mejor experiencia de usuario y para ayudar a los clientes a encontrar socios más especializados.

"Nuestro objetivo es ayudar al canal a rentabilizar los cambios del mercado", afirma Torres Brizuela, quien también destaca que "queremos motivar a nuestro canal para que priorice la venta de nuestras soluciones, además de crear una base sólida y flexible para alcanzar nuestros objetivos cloud".

El año pasado, "el sector TI creció de forma importante", algo que benefició al canal. NetApp se ha propuesto que esta tendencia continúe y que sus partners puedan sacar el máximo partido de la transformación digital y la cloud.

"Estamos transformando nuestro Unified Partner Program y evolucionando su estructura para que trabajar en colaboración con NetApp sea más sencillo y rentable que nunca para nuestros partners," explica Chris Lamborn, director del equipo Global Partner GTM & Programs de NetApp. "Estos nuevos cambios no son sino los primeros de una estrategia multifase con la que buscamos incentivar y recompensar a nuestros partners por su experiencia creando soluciones y que, al mismo tiempo, contribuirá a generar más valor para sus clientes". ■

MÁS INFORMACIÓN

- Todas las novedades del nuevo programa de canal de NetApp
- La continuidad de negocio como máxima prioridad
- La oferta de NetApp

Puntos clave del programa de canal

- Un ecosistema para partners aún más extenso
- Incentivos simplificados
- Nuevas recompensas para partners
- Nuevas especializaciones para soluciones
- Nuevas especializaciones para partners Services Certified
- Partner Connect 2.0

Schneider Electric ayuda a sus partners a vender servicios de gestión de energía

El programa Edge Software & Digital Services ofrece a los proveedores de soluciones de IT acceso a la cartera de Software y Servicios Digitales de IT EcoStruxure de Schneider Electric, así como a ventajas económicas, facilidades y apoyo para desarrollar su estrategia de servicios de gestión de energía. Actualmente, sólo el 27% de los proveedores ofrecen estos servicios.

Como parte de su programa de partners de Soluciones IT mySchneider, y en respuesta al importante crecimiento del Edge Computing, Schneider Electric ha presentado su programa Edge Software & Digital Services, que ofrece un conjunto completo de beneficios, herramientas de asistencia y certificaciones a aquellos partners de soluciones de IT que creen una estrategia de servicios de gestión de energía.

Gartner estima que, para 2025, el 75% de los datos generados por las empresas se crearán y procesarán fuera de un centro de datos tradicional y centralizado o de la nube. Sin embargo, dado que la infraestructura edge está distribuida geográficamente, requiere siempre una supervisión y gestión

remotas, lo que abre el camino a grandes oportunidades en la venta de servicios de gestión de energía. Sin embargo, en la actualidad, sólo el 27% de los proveedores de soluciones de IT ofrecen estos servicios. Pues bien, con su nuevo programa, Schneider Electric permite a los proveedores de soluciones de IT obtener ingresos fijos mediante la monitorización y gestión remota de la infraestructura física de las redes de sus clientes, utilizando el software IT y los servicios digitales EcoStruxure.

"La aceleración de Edge Computing presenta una enorme oportunidad para que los proveedores de soluciones de IT aumenten sus ingresos a través de la venta de servicios de gestión de energía", afirma David Terry, vicepresidente de IT Channels en, Schneider Electric Europe. "Hemos creado un programa completo para nuestros partners que simplifica y agiliza el tiempo necesario para desarrollar su estrategia de servicios de gestión de energía. Esto les permitirá atender las necesidades de sus clientes, mediante la supervisión y gestión eficaces de los centros edge, que se consideran ahora una prioridad de vital importancia".

ELEMENTOS DEL PROGRAMA

El programa incluye rebates y fondos de desarrollo de marketing, para facilitar la inversión de los clientes en IT en sus negocios; una guía operativa paso a paso, para acompañar a los partners durante sus operaciones, ofreciendo el apoyo de Schneider Electric; cursos y webinars relacionados con el software de monitorización remota y digital, para que los técnicos puedan sacar todo el partido a la herramienta; y software de TI y servicios digitales EcoStruxure, que proporciona una supervisión remota avanzada, 24 horas al día y 7 días a la semana, y asistencia remota e in situ.

El programa también ofrece dos nuevas vías de certificación, adaptadas al enfoque específico de los partners, ya sea para la reventa de software y servicios o para la supervisión y gestión de servicios completos. Los partners certificados tienen acceso a un Partner Success Manager especializado y con experiencia que les guiará a lo largo de su trayectoria de desarrollo y agilizará la obtención de ingresos. Todos los participantes en el programa tienen acceso a las herramientas de diseño, así como a la Plataforma Exchange de Schneider Electric, una plataforma abierta que conecta a los expertos del sector y a los partners tecnológicos, para aumentar el posicionamiento competitivo y la innovación empresarial. ■

MÁS INFORMACIÓN

- APC by Schneider Electric intensifica su apuesta por el canal en la península Ibérica
- HPE reconoce el papel de Schneider Electric en el campo de la computación Edge
- Tech Data, Cisco y Schneider Electric ponen en marcha el Edge Tour

El potencial de la gestión de la energía

Se calcula que la venta de servicios de gestión de la energía ofrece un potencial de aumento de los ingresos anuales equivalente a 1,5 veces el coste inicial de la solución. Además, pueden ayudar a mejorar la resiliencia de estos espacios con un mantenimiento proactivo, e identificar las actualizaciones de hardware, para ayudar a reducir los gastos operativos de sus clientes. Para compensar los costes iniciales, el programa Edge Software & Digital Services incorpora una bonificación a lo largo del ciclo de vida de la relación con el cliente, incluyendo la conexión, la supervisión, el mantenimiento y la actualización de los activos del cliente.

Mayorista autorizado

El universo de Apple

¡Ya en Esprinet!

iPhone Mac iPad Watch AirPods Music TV

esprinet®

Campus 3·84 - Nave 1, Calle Osca, 2
Pol. PLAZA - 50197, Zaragoza, España
info_es@esprinet.com / (+34) 976766110

Wolters Kluwer contribuirá a la digitalización de España como socio de la CEOE

La compañía participará en las comisiones y grupos de trabajo de la confederación, y colaborará conjuntamente en el desarrollo de propuestas para impulsar la innovación y transformación de las empresas, aportando su experiencia como proveedor de soluciones tecnológicas en los ámbitos laboral, fiscal, contable y de gestión.

Wolters Kluwer Tax & Accounting España ha firmado un acuerdo de colaboración con la Confederación Española de Organizaciones Empresariales (CEOE) para convertirse en una de sus empresas asociadas, con el objetivo de contribuir a la digitalización de las empresas a partir de su liderazgo y experiencia como proveedor de soluciones tecnológicas expertas en los ámbitos laboral, fiscal, contable y de gestión. Para Tomàs Font, director general de la compañía en España, este acuerdo "consolida a Wolters Kluwer como un actor con impacto real en la sociedad y en el ecosistema empresarial. Nuestro objetivo es brindar a los profesionales la capacidad de hacer crecer, administrar y proteger sus negocios y los de sus clientes en un mundo en constante movimiento y cambio".

Como miembro asociado de la CEOE, la compañía participará en las comisiones y grupos de trabajo de la confederación que abordan cuestiones de interés para su ámbito de actividad y para la reactivación empresarial, y colaborarán conjuntamente en el desarrollo de propuestas para impulsar la innovación y transformación de las empresas. "La digitalización es vital y desde Wolters Kluwer les acercamos las herramientas expertas, que combinan conocimiento y tecnología, que la hacen posible", señala Font.

"Wolters Kluwer es una compañía que trabaja de forma muy activa para la digitalización del tejido empresarial, fundamental para la recuperación económica, y en lo que tenemos que centrar buena parte de nuestros esfuerzos actualmente", asegura Antonio Garamendi, presidente de la CEOE, que ha destacado que "es un importante aliado para ofrecer nuevos servicios de valor a nuestros asociados, formada por más de 200 organizaciones de todos los sectores productivos y territorios del país. Las soluciones de Wolters Kluwer suponen un activo para cualquier tipo de negocio en una realidad cada vez más digitalizada". ■

MÁS INFORMACIÓN

Wolters Kluwer reorganiza la dirección de la División de Tax & Accounting en España

Adaptación al sistema TicketBAI

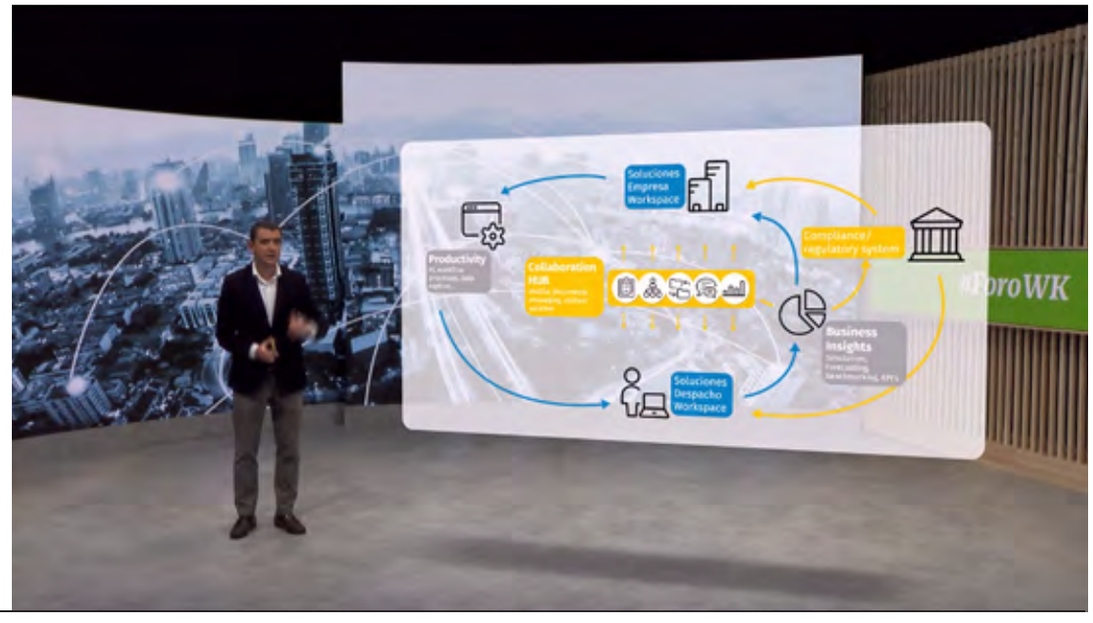
Wolters Kluwer Tax & Accounting España confirma que ha adaptado sus soluciones de facturación para hacer frente a los cambios que establece el nuevo sistema TicketBAI de control de la facturación, que entrará en vigor a partir del 1 de enero de 2022 en el País Vasco.

Creada con el objetivo de reducir el fraude fiscal, TicketBAI es una iniciativa común de las tres Diputaciones Forales y el Gobierno vasco para establecer un sistema que garantice la trazabilidad de todos los movimientos de venta que se emitan por cualquier persona física o jurídica que tenga sede fiscal en el País Vasco. Con Ticket BAI, los despachos profesionales, pymes y autónomos tendrán que gestionar esta emisión de facturas de venta o tickets con un software de gestión que garantice la no vulnerabilidad del dato y su veracidad. En el caso de Bizkaia, TicketBAI forma parte de un proyecto más amplio (Batuz), que también contempla un acercamiento de la Hacienda a los contribuyentes con la creación de borradores de los impuestos de IVA y Sociedades y la llevanza en sede electrónica de los libros de operaciones económicas.

A partir de ahora, a3factura, a3ASESOR | ges y a3ERP ya incluyen todas las especificaciones técnicas para realizar este proceso de manera automatizada y sin impactar de ninguna forma práctica al usuario, que puede seguir realizando sus gestiones del día a día. En el caso de a3factura, al ser una solución cloud, todos los cambios a que obligue la normativa se incorporarán en tiempo real de forma totalmente automática. La compañía también está adaptando las soluciones contables específicamente dirigidas al despacho profesional a3ASESOR | con y a3ASESOR | eco (que también se adapta a lo que obliga Batuz).

Foro Asesores 2021, también online

Wolters Kluwer prepara una nueva edición de Foro Asesores, el evento de referencia para Despachos Profesionales y asesorías, un espacio donde analizar y compartir intereses comunes haciendo foco en la excelencia y abriendo nuevos horizontes para crear oportunidades para el sector. Para ofrecer todas las garantías de seguridad, el evento se celebrará los días 9 y 10 de junio en formato online, pudiendo asistir a todas las ponencias en streaming desde cualquier parte y acceder a contenidos adicionales a la carta. Foro Asesores es la cita ineludible para el profesional del despacho. El evento se dirige a profesionales de los ámbitos laboral, fiscal y contable: asesores laboralistas, asesores fiscales-contables, técnicos tributarios, economistas, consultores..., que podrán compartir estrategias y herramientas de crecimiento de la mano de expertos, representantes de la Administración y de Colegios Profesionales, y estar al día de las tendencias del sector para, innovar, hacer crecer y transformar el despacho. Se prevé que más de 25.000 asistentes compartan experiencias y estrategias para la transformación digital del sector.



Mitel amplía el valor de su Programa Global de Partners

Reforzando su enfoque de comercialización únicamente a través de partners, Mitel ha presentado un mejorado programa global de canal, que reconoce el papel fundamental que los partners desempeñan en el ciclo de vida de las comunicaciones de los clientes mediante la introducción de nuevos recursos, formación, herramientas e incentivos, que responden a la mayor demanda de soluciones en la nube por parte del mercado e impulsan la capacidad de los partners para sacarle partido.

"La forma de trabajar cambió drásticamente el año pasado y nuestros partners han estado en primera línea de esa transformación, garantizando la continuidad del negocio de innumerables clientes gracias a su profundo conocimiento de cada uno de ellos y con la ayuda de la tecnología de Mitel", afirma Lana King, VP Partner Programs, Training & Enablement de Mitel. "Gracias a las inversiones que estamos realizando para ampliar el valor de nuestro Programa Global de Partners, el objetivo de Mitel es ayudarles a fortalecer aún más esas relaciones y, al mismo tiempo, facilitarles la maximización de los ingresos y el crecimiento de su negocio".

Desarrollado a partir de un exhaustivo proceso de participación de los partners, el Programa 2021 introduce puntos de programa mejorados y reconocimiento para los partners que van más allá de los criterios mínimos de certificación para lograr competencias técnicas y de ventas avanzadas. Entre las distintas oportunidades que tendrán los partners para reforzar sus conocimientos, se encuentra la nueva certificación relativa a la implicación en el ciclo de vida del cliente (Customer Lifecycle Engagement Certification), diseñada para ayudar a los partners en la gestión general de los clientes a lo largo de su ciclo de vida. La certificación se centra en las renovaciones de garantía de software, en los esfuerzos de retención y en el apoyo a los clientes en sus iniciativas de modernización tecnológica, desde asegurar que las organizaciones están aprovechando la última versión y funcionalidades, hasta guiarlas en su migración a la nube o a las ofertas de suscripción. La certificación está prevista para la segunda mitad del año.

PUNTOS DE RENDIMIENTO

Mitel también anuncia nuevos puntos de rendimiento que recompensarán a los socios por acelerar las ventas de soluciones en la nube y de los nuevos servicios de suscripción. Además, en el transcurso del año, la compañía tiene previstas nuevas inversiones para respaldar la experiencia general del programa, incluyendo herramientas de cotización simplificadas, mejoras en el Centro de Interacción con Partners de Mitel y en los equipos de soporte del programa, así como nuevos y exclusivos programas de marketing que están programados para ser lanzados este verano. ■

El Programa 2021 recompensa el papel que los partners desempeñan en el ciclo de vida de las comunicaciones de los clientes mediante la introducción de recursos e incentivos. "El objetivo de Mitel es ayudarlos a fortalecer aún más esas relaciones y, al mismo tiempo, facilitarles la maximización de los ingresos y el crecimiento de su negocio", señala Lana King, de Mitel.

MÁS INFORMACIÓN

Mitel amplía el valor de su Programa Global de Partners

TS-h973AX

NAS con QuTS hero, SSD NVMe U.2 y conectividad 10GbE/2,5GbE

Alta integridad de los datos y uso del almacenamiento

El sistema operativo QuTS hero basado en ZFS admite tecnologías de reducción de datos basadas en bloques (deduplicación y compresión de datos en línea) y optimización SSD para priorizar la utilización del almacenamiento.

Potencia los SSD y el almacenamiento por niveles

Instala SSD U.2 NVMe PCIe Gen 3 x4 de alto rendimiento o SSD SATA 6Gb/s en las ranuras para SSD dedicadas para garantizar la aceleración de la caché y una E/S aleatoria mejorada.

Conectividad de alta velocidad de 10 GbE y 2,5 GbE

Un puerto 10GBASE-T Multi-Gig y dos puertos LAN 2,5GbE aceleran la virtualización, el acceso intensivo a los archivos, las tareas de copia de seguridad y restauración, y la transferencia multimedia.

Protección integral de datos y copias de seguridad de nivel empresarial

Disfruta de un centro de copia de seguridad de clase empresarial, compatible con la copia de seguridad y restauración de datos de la nube y máquinas virtuales (incluyendo Google ™ Workspace, Microsoft 365®, VMware® y Hyper-V).

www.qnap.com

QuTS hero edition ZFS QuTS hero NAS

TS-h3088XU-RP

Solución de almacenamiento all flash con alto rendimiento y capacidad y baja latencia

intel XEON inside

Alta integridad de los datos y uso del almacenamiento

El sistema operativo QuTS hero basado en ZFS admite tecnologías de reducción de datos basadas en bloques (deduplicación y compresión de datos en línea) y optimización SSD para priorizar la utilización del almacenamiento.

Potencia la transferencia de datos de alta velocidad con 4 puertos de 25 GbE

Acelere su virtualización, acceso intensivo a archivos, y grandes tareas de copia de seguridad / restauración con SFP28 de 25 GbE y RJ45 de 2,5 GbE.

Gran capacidad de E/S con expansión PCIe

Incluye tres ranuras PCIe Gen 3 que permiten el uso de varias tarjetas de expansión para aumentar el potencial de las aplicaciones. (Se incluye una ranura preinstalada con una tarjeta de red 25GbE de dos puertos).

Expansión de almacenamiento flexible y asequible

Obtén una capacidad de almacenamiento a escala de petabytes conectando hasta dieciséis Cajas de expansión de almacenamiento SAS de 12 Gb/s TL-1620Sep-RP al TS-h3088XU-RP.

www.qnap.com

Syneto financia a sus partners la compra de infraestructura con Syneto 0%

Además de ofrecer formación y márgenes muy competitivos al canal, Syneto ofrece esta iniciativa de financiación al 0% con el objetivo de hacer crecer su red de socios y el número de operaciones de valor en Iberia. La compañía ha reunido ya a 12 socios estratégicos activos y certificados, cuatro a nivel nacional y ocho a nivel local.

Syneto ha anunciado la puesta en marcha de la oferta "Syneto 0%", una nueva iniciativa de financiación para el canal en España a través de la cual partners de la compañía podrán adquirir infraestructura Syneto con un 0% de interés real en 12 o 24 meses. La promoción será válida para pedidos realizados antes del 31 de julio, con valor de 11.000 hasta 75.000 euros, sujeta a estudio y aprobación previa por la entidad financiera y Syneto, y no es acumulable a cualquier otra promoción, descuento, oferta o rebate previo. Para solicitar esta oferta solo hay que confirmar interés en la oferta y solicitud de la misma; confirmar datos de la operación (producto y plazos) y del cliente final (CIF y datos de contacto); esperar confirmación de Syneto y de la financiera; y y finalmente procesar el pedido en el mayorista siguiendo las instrucciones de Syneto.

Los partners de Syneto han valorado muy positivamente esta iniciativa que les permite ofertar la plataforma como pago

CONTENIDOS↓

por uso en muchas ocasiones en las que el cliente no está interesado en hacer un desembolso inicial grande y prefieren una financiación a 12 o 24 meses.

"El canal es fundamental en la estrategia de la compañía y por eso tenemos que ofrecerles un valor añadido. Con esta oferta, buscamos dar todas las facilidades a nuestros partners a la hora de apostar por nuestras soluciones", afirma Eduardo García Sancho, Sales & Channel Manager de Syneto para España. "Con esta iniciativa queremos ayudar a nuestro canal de distribución no sólo desde el punto de vista económico, sino planteando la posibilidad de establecer una variante financiera a la hora de adquirir la plataforma hiperconvergente de Syneto. Los socios de canal que trabajen con nosotros siempre tendrán la posibilidad de contar con un enorme apoyo por nuestra parte en todos los aspectos, tanto de producto, como técnicos y económicos a la hora de obtener la mejor oferta posible de cara a sus clientes".

CANAL CUALIFICADO

Desde la puesta en marcha del programa de canal "Channel Challenge", hace 9 meses, Syneto ha reunido ya a 12 socios estratégicos activos y certificados, cuatro a nivel nacional y ocho a nivel local, que han llevado a cabo proyectos en todo el territorio nacional. El objetivo de la compañía es duplicar su canal cualificado al finalizar el año, consiguiendo un elenco de partners especializados en el entorno pyme. Según Eduardo García Sancho, "buscamos una red de partners que se desenvuelvan en operaciones con mejora de su valor añadido en entorno pyme, que tengan clientes con gran interés en mejorar o actualizar sus sistemas tradicionales obsoletos con una solución avanzada que además de ofrecer hiperconvergencia permita elevar el nivel de servicio con sistemas avanzados de protección del dato, incluso anti malware". ■

MÁS INFORMACIÓN

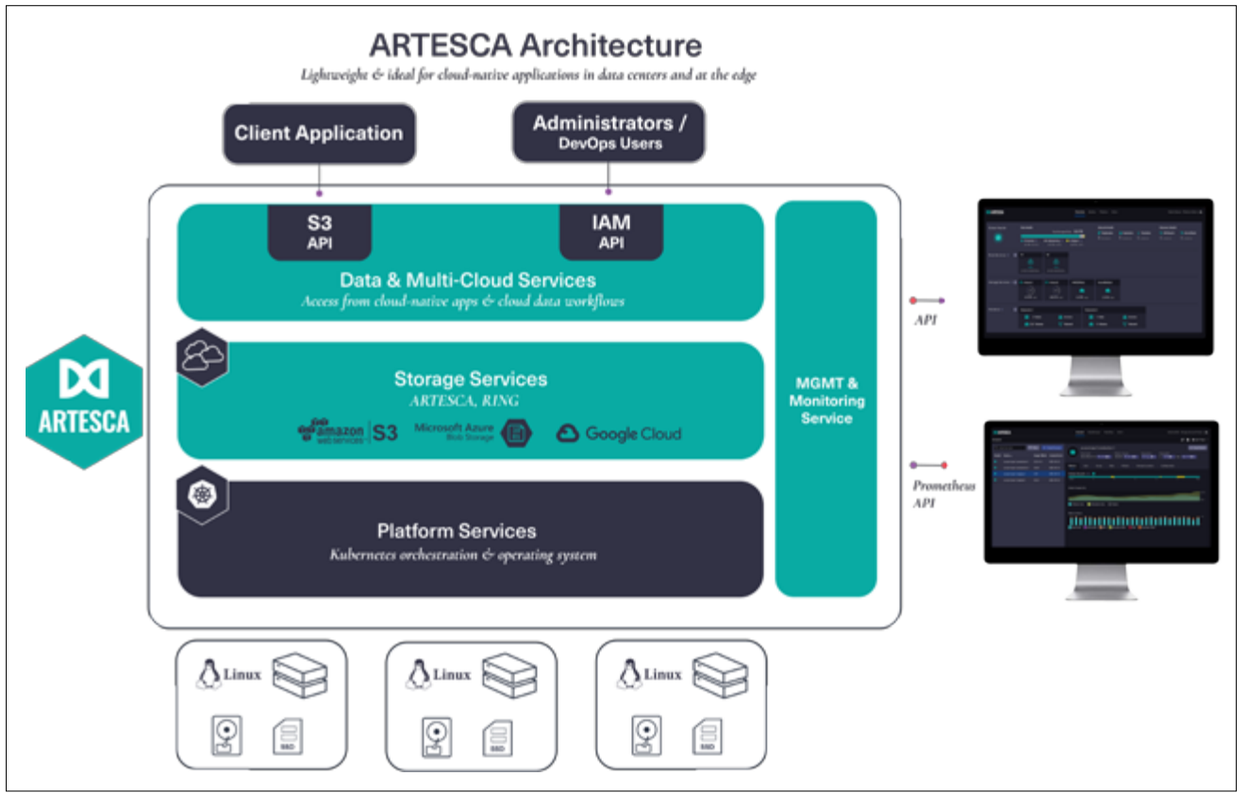
- Syneto ofrece las claves para para proteger el activo más valioso, el dato
- Syneto espera duplicar su canal cualificado en España con el programa Channel Challenge

Syneto ayuda a las pymes a simplificar, acelerar y proteger sus operaciones de TI

La revolución de la hiperconvergencia no se detiene. Al contrario, se acelera. Prueba de ello son las nuevas versiones de la solución de infraestructura hiperconvergente HYPERSeries 2000 y 3000 de Syneto, que ofrece virtualización, copias de seguridad nativas integradas, restauración instantánea y recuperación ante desastres en un único dispositivo plug-and-play simple, rápido y seguro. Con HYPERSeries, Syneto propone una solución que protege los datos, garantizando su protección y dando la oportunidad de recuperarlos de forma inmediata, sin importar el motivo de la pérdida. El proceso de recuperación se realiza en 15 minutos como máximo. En una infraestructura Syneto, las copias de seguridad se pueden programar para que se creen automáticamente y de forma casi instantánea cada minuto, lo que garantiza la recuperación en un momento determinado desde un minuto antes de un evento negativo, como un ataque de malware. Además, cualquier máquina virtual se puede recuperar en menos de un minuto, independientemente de su tamaño.

Scality responde a la demanda creciente de almacenamiento de objetos

Los grandes analistas coinciden en destacar que en los próximos tres años se van a generar más datos que en las tres últimas décadas, y que el 80% de esos datos son no estructurados, provenientes cada vez con mayor frecuencia de los ecosistemas IoT y de los 80.000 millones de dispositivos que se encuentran permanentemente conectados. Una de las derivadas de esta tremenda explosión en la generación de datos estriba en su soberanía. Es decir, en si tanto las organizaciones públicas como privadas controlan realmente sus datos, teniendo en cuenta que el universo multicloud es ya una realidad, y que el 70% de las empresas europeas tienen dos o más proveedores para la nube. En este contexto están confluyendo una serie de tendencias como la aparición de nuevas cargas de trabajo para dar respuesta a las aplicaciones que demandan inteligencia artificial y analítica; el desarrollo de nuevas aplicaciones nativas en cloud vinculadas a la contenerización y a las prácticas DevOps; la necesaria reducción de latencias; y al auge del almacenamiento de objetos como opción preferente en materia de almacenamiento primario.



Para dar respuesta a todas estas corrientes, Scality, fabricante especializado en el almacenamiento masivo de datos no estructurados, acaba de presentar Artesca, su nuevo software de almacenamiento de objetos ligero para kubernetes. Se trata de la segunda gran innovación tecnológica en la historia de la compañía, tras el lanzamiento en 2010

El fabricante especializado en almacenamiento masivo de datos no estructurados ha lanzado Artesca, la segunda mayor innovación tecnológica de su historia, consistente en un software de almacenamiento de objetos ligero para kubernetes.

de Ring, su propuesta para el almacenamiento de archivos.

El almacenamiento de objetos se despliega, cada vez con mayor frecuencia, entre sistemas basados en flash, y se está erigiendo en una tecnología vital de almacenamiento para las aplicaciones modernas. El entorno nativo de la nube exige adaptabilidad, portabilidad y eficiencia, atributos que las soluciones de almacenamiento tradicionales no siempre consiguen igualar. Artesca ha sido creada específicamente para los desarrolladores a la vez que cumple con las más altas exigencias de seguridad a nivel empresarial. Compatible con una amplia cartera de servidores de almacenamiento de datos inteligentes all-flash e híbridos de HPE -fabricante que ha participado en su desarrollo-, Artesca permite abordar múltiples casos de uso, desde el Edge hasta el núcleo y la nube, especialmente en aplicaciones cloud-native, de inteligencia artificial y aprendizaje automático, de analítica de big data y de tecnologías 'In-memory'.

MODELO DE DISTRIBUCIÓN

HPE, junto a su canal, disfrutará durante los primeros seis meses de la distribución en exclusiva de Artesca. A partir de ahí se abrirá su comercialización al resto del canal y de socios tecnológicos con los que cuenta Scality, como Cisco, Lenovo o Supermicro.

En su versión hasta 100 TB se trata de un producto gratuito, y a partir de esa línea el cliente podrá escoger un modelo de suscripción a 1, 3 o 5 años. Como explica Israel Serrano, nuevo responsable de Scality para el sur de Europa, el perfil del cliente de Artesca puede oscilar "desde una pequeña start-up que quiera comercializar sus soluciones en la nube hasta grandes corporaciones, interesadas en el almacenamiento de objetos". ■

Los grandes **analistas coinciden** en que en los **próximos tres años** se van a **generar más datos que en las tres últimas décadas**, y que el **80% de esos datos son no estructurados**

MÁS INFORMACIÓN

- Scality. El futuro del almacenamiento: Abriendo nuevos caminos
- Los fabricantes de almacenamiento y memoria podrían elevar sus costes por el aumento de precio de materiales CCL
- Siete consejos para ser eficientes en almacenamiento y recuperación de datos

Nuevo Site exclusivo de HP en Vinzeo

- Todas las herramientas relacionadas con la marca en un único portal:
  HP Útiles
- Promociones de fabricante a un solo click:
  Cash Rewards
- Promociones HP Vinzeo a un solo click:
  Vip & Promos
- **Localiza fácilmente tus contactos** para atender y resolver tus dudas y preguntas

Accede

vinzeo

hp

Esprinet finaliza el primer trimestre con un sólido crecimiento del 28%

La Junta Directiva de Esprinet ha aprobado los resultados económicos provisionales correspondientes al primer trimestre de 2021, finalizado el 31 de marzo, un período en el que las ventas de la compañía ascendieron a 1.166 millones de euros, un 28% más en comparación con los 913,8 millones de euros del primer trimestre de 2020. Estos buenos resultados se debieron tanto al crecimiento orgánico registrado por la compañía, cifrado en un 23%, como por los 42,8 millones de euros derivados de las actividades de Grupo GTI en España y Dacom e idMAINT en Italia.

El beneficio bruto, que asciende a 56,1 millones de euros, muestra un aumento del 33% con respecto al mismo trimestre del año anterior, debido tanto a mayores ventas como a la mejora del margen porcentual, que se sitúa en el 4,81% (frente al 4,63% del año pasado), a pesar de que el peso de las ventas de PCs y smartphones ha aumentado aún más.

El EBITDA ajustado, que coincide con el EBITDA dado que no registró costes no recurrentes, ascendió a 20,3 millones de euros, lo que supone un incremento anual del 70%, y el beneficio antes de impuestos ascendió a 14,1 millones de euros, en comparación con los 5,9 millones de euros del primer trimestre de 2020. Los ingresos netos, que aumentaron un 159%, ascendieron a 10,2 millones de euros.

El compromiso constante por mejorar los índices de satisfacción de los clientes

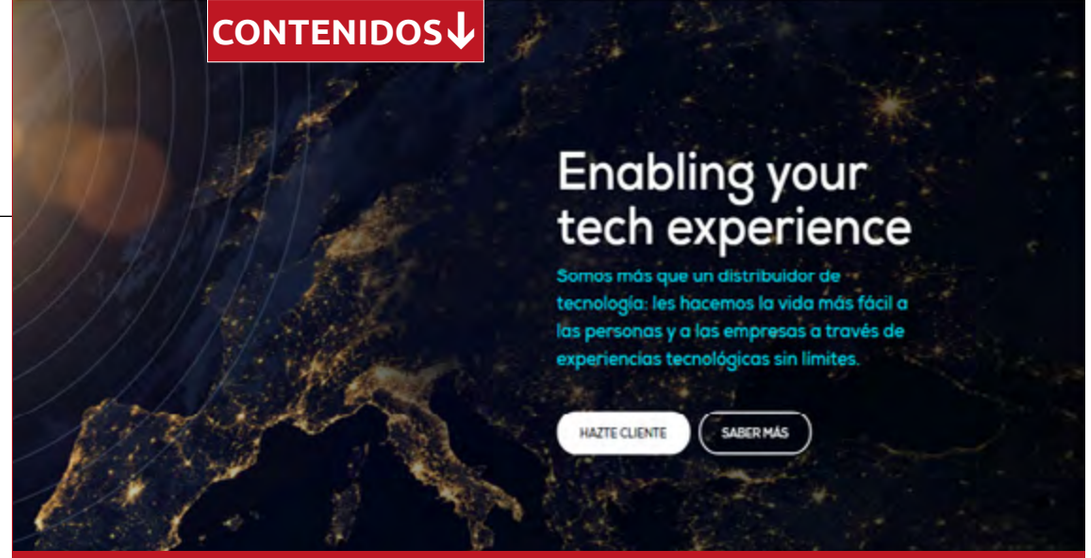
El Grupo registró una importante aceleración en Advanced Solutions, división que creció un 48%, gracias a la contribución de las adquisiciones del Grupo GTI en España, y de Dacom e idMAINT en Italia. En las áreas de IT Clients y de Consumer Electronics, el Grupo registró incrementos notables en todas las categorías, destacando PCs y smartphones.

ayudó al Grupo en ambos segmentos de clientes. En los primeros tres meses de 2021, el mercado registró un crecimiento del 18% en el segmento empresarial y del 23% en el segmento de consumo. Las ventas del grupo registraron un crecimiento por encima del mercado tanto en el segmento empresarial (39%) como en el segmento de consumo (25%).

El Grupo registró una importante aceleración en Advanced Solutions, división que creció un 48%, también gracias a la contribución de las adquisiciones del Grupo GTI en España, líder en el segmento Cloud, y de Dacom e idMAINT en Italia, líderes en Identificación Automática y Captura de Datos. En IT Clients, el Grupo registró incrementos notables en todas las categorías: PCs (41%), Impresión (6%) y otros productos de TI (54%). También en el área de Consumer Electronics, las ventas aumentaron en todas las categorías: smartphones (23%), Línea Blanca (29%), Gaming (8%) y otros productos CE (17%).

Sobre la base de los resultados obtenidos en los tres primeros meses de 2021 en términos de rentabilidad y cuotas de mercado consolidadas, el Grupo Esprinet ve el año en curso de forma positiva. El primer semestre debería confirmar una comparación favorable con el año anterior; por el contrario, el segundo semestre abre una serie de escenarios, ante

Las **ventas del grupo** registraron un **crecimiento por encima del mercado** tanto en el segmento **empresarial (39%)** como en el de **consumo (25%)**



Nueva web

Esprinet presenta su nueva web completamente rediseñada, para facilitar la experiencia de navegación de los usuarios. Realizada en inglés, español y portugués, para ser compartida en todos los países en los que opera el Grupo, la plataforma web presenta una organización de secciones y contenidos orientados a acercar la dimensión institucional con el alma comercial del mayorista, convirtiéndose en una herramienta no solo para mejorar la comunicación con todos sus públicos objetivo sino también para la generación de negocio.

Desarrollado en colaboración con Boraso, el sitio cuenta con un área dedicada a la información del Grupo -con páginas específicas de Sostenibilidad, Gobernanza, Inversores, Medios y posibles nuevos Talentos- y las secciones Comercial y Marketing, con descripciones generales de los diversos grupos de productos, información sobre las marcas y los servicios de la cartera. Con esta estructura, Esprinet renueva su enfoque de apertura y relación con el mercado, con el objetivo de facilitar la relación con prospectos, clientes y proveedores. Los nuevos gráficos juegan un papel fundamental, creados con el objetivo de afirmar una Identidad Visual única y distintiva, acorde con el nuevo contenido.

La nueva plataforma web se convierte así en un importante canal de comunicación e interacción entre Esprinet y sus grupos de interés, un punto de contacto que acogerá nuevas formas de análisis en profundidad útiles para la consecución de los objetivos del Grupo. Un elemento distintivo es la exhaustividad y claridad de los contenidos, orientados a resaltar las fortalezas de la oferta, además de la estrategia y los valores corporativos.

la persistencia de un marco de incertidumbre ligado a la pandemia. En base a estas premisas, y con la expectativa de una mayor demanda de los consumidores en la recta final del año, este año la compañía prevé que se superarán unas ventas de 5.000 millones de euros y un EBITDA ajustado de más de 80 millones de euros. ■

MÁS INFORMACIÓN

- Alessandro Cattani, Esprinet: 'Cerramos 2020 sabiendo que fue el mejor año de nuestra historia'
- Dacom e IdMaint ya son 100% propiedad de Esprinet
- Un nuevo equipo de liderazgo dirigirá las actividades de Esprinet

Más empleados en España

En el año de su vigésimo aniversario, el Grupo Esprinet ha alcanzado una facturación de 4.500 millones de euros, lo que representa un crecimiento del 14% de los ingresos. El mayorista superó todas las expectativas, gracias al compromiso y la dedicación de un equipo de más de 1.600 profesionales, y, en agradecimiento a su gran adaptabilidad y cohesión mostrada durante 2020, Esprinet les ha hecho entrega de una prima extraordinaria por valor de 600 euros.

Durante 2020, el Grupo Esprinet contrató a 259 personas nuevas. La selección y el proceso de captación de nuevos candidatos continuó incluso durante el periodo de confinamiento y las nuevas incorporaciones pudieron comenzar a trabajar directamente en smartworking gracias a la entrega a domicilio de todo el equipamiento tecnológico necesario. Ahora, en el primer semestre de 2021, están previstas 110 nuevas contrataciones, 56 de ellas en la Península Ibérica, de las cuales 41 son adicionales, distribuidas entre las delegaciones de Madrid, Zaragoza, Oporto, Barcelona y Bilbao. Estas contrataciones ampliarán el equipo de trabajo, principalmente en las áreas de venta y marketing.

it whitepapers

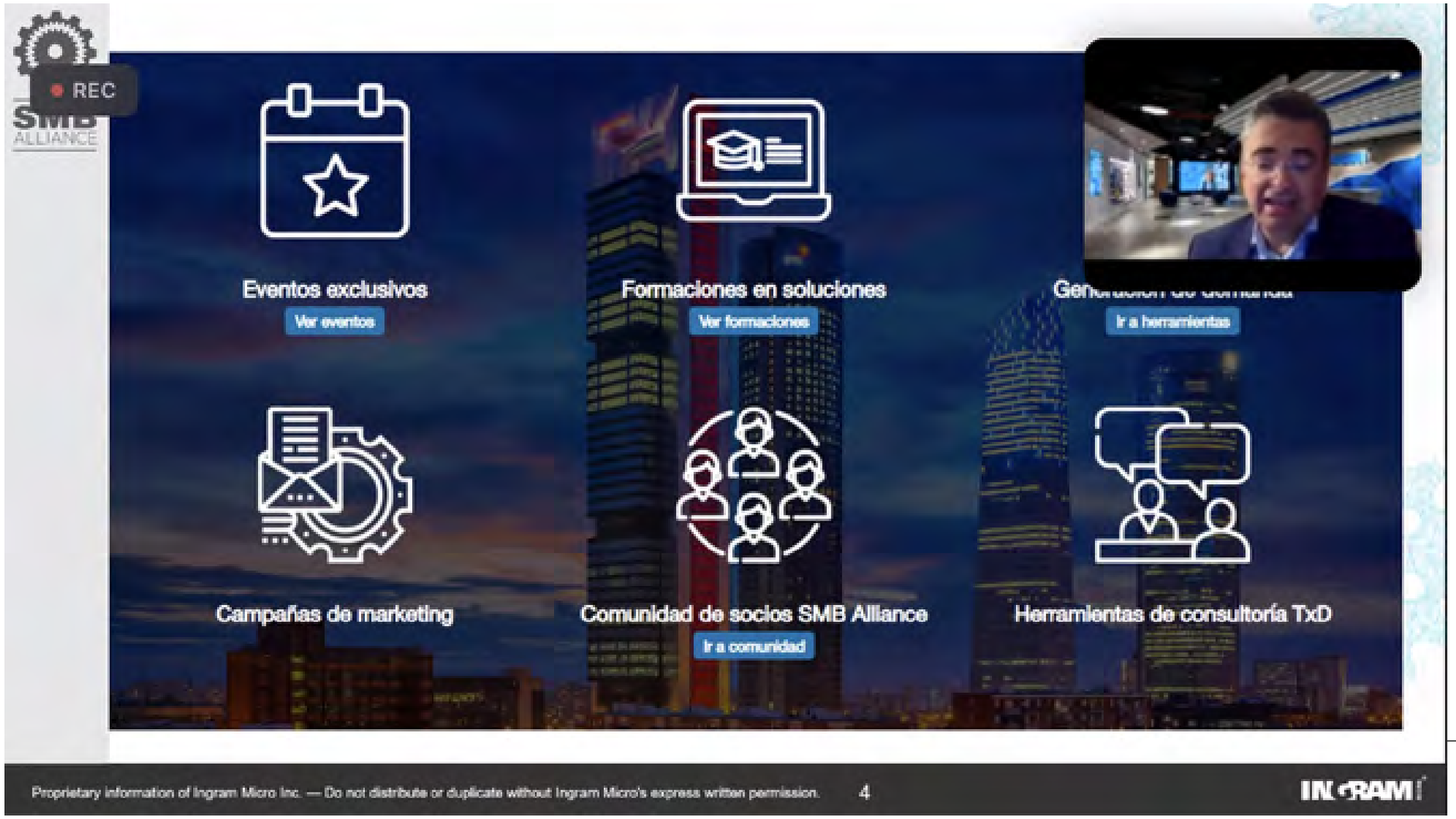
INFORME: HACIA LA EMPRESA HIPERINTELIGENTE

IT Research ha realizado para MicroStrategy un estudio acerca de la toma de decisiones en la empresa y las herramientas utilizadas. Según el informe, un 86% de los consultados afirma que la información interviene en más del 40% de las decisiones que se toman en su organización. Además, un 71% considera que en su compañía estas decisiones se llevan a cabo con la información lo más actualizada posible; un 29% cuestiona esta posición.

Ingram Micro e IDC arropan al canal en su impulso a la digitalización de las pymes

La economía española y el gasto TI están en período de recuperación, siendo las categorías de servicios TI y tecnología empresarial las que están creciendo más rápidamente. Teniendo en cuenta que las pymes conforman el 99,8% del tejido empresarial español, sorprende que estas representen únicamente el 15% del gasto TI. Según IDC, la idea es que este porcentaje crezca dos puntos respecto a 2020.

Las pymes ya se han habituado al trabajo remoto, y ya han comenzado su andadura en la automatización de procesos, y ahora es el momento de apostar por la nube híbrida y por una migración de la seguridad del



El tejido productivo español está dominado por pymes que apenas representan el 15% del gasto TI. Conscientes del papel clave del canal como acelerador de la digitalización de estas empresas, IDC e Ingram Micro han puesto en marcha el proyecto SMB Alliance con el fin de "capacitar al canal para que sea un consultor tecnológico para la pyme", señala Alberto Pascual, director ejecutivo de Ingram Micro.

perímetro a la seguridad del datos. "Para ello se requiere una nueva propuesta de valor y de nuevos actores con conocimientos y habilidades para que las pymes lleven a su vez su propuesta de valor al cliente final", señala José Antonio Cano, director de análisis y consultoría de IDC Research España. Ahí es donde entra el canal de TI.

Según Cano, "una cuarta parte de los partners cambiarán de enfoque, modificarán su estrategia, serán comprados o dejarán de operar en 2021". Se requerirá un enfoque de partner centrado en servicios, y se priorizará la experiencia/especialización de los partners y su capacidad para obtener resultados. Pero el principal desafío sigue siendo la escasez de habilidades en el canal, y ese es precisamente uno de los objetivos de la iniciativa SMB Alliance de IDC e Ingram Micro.

ABANICO DE HERRAMIENTAS

La SMB Alliance dota al canal de una serie de herramientas, incluidos eventos exclusivos por verticales, para dar pistas a los partners de los criterios de cada industria, casos de uso y skills; formaciones y campañas de marketing. Asimismo, para cada vertical se determinan una serie de soluciones y se fomentan entornos de colaboración con otros partners del sector. Para que todos estos procesos

sean escalables, se ofrece la herramienta de Diagnóstico Digital Online, que diagnostica la situación digital de la empresa por cada una las áreas de negocio y emite recomendaciones para cada área de negocio. Asimismo, para identificar vulnerabilidades de seguridad en el entorno de las compañías y blindarlas se ofrecen las herramientas CyberGram y SpyGlass.

"Lo que queremos es capacitar al canal para que sea un consultor tecnológico para la pyme" apunta Alberto Pascual, director ejecutivo de Ingram Micro. El objetivo es darle la máxima visibilidad en el mercado para que toda esta capacidad transformadora llegue a las pymes. El canal que forme parte de la SMB Alliance estará bajo el paraguas de TecnoHub Consulting, una marca que agrupará las soluciones de TI, los recursos, las soluciones financieras y todo el elenco de partners, y que pretende ser "un integrador

Alianza con UiPath

La Automatización Robótica de Procesos (ARP) es una de las tecnologías de más rápido crecimiento. De hecho, la amplia y especializada cartera de Advanced Solutions de Ingram Micro empezó a ofrecer Inteligencia Artificial (IA) y ARP hace unos años y se ha convertido en una de las divisiones con más rápido crecimiento a nivel global de la compañía. Pues bien, para impulsar su crecimiento en este mercado, el mayorista amplía su oferta en IA con un acuerdo de distribución global con UiPath, por el que suministrará su cartera de software de automatización y de ARP a nivel mundial.

La relación de Ingram Micro con UiPath se inició a principios de 2021 y se ha expandido rápidamente de Norteamérica a América Latina y ahora a Europa, Oriente Medio, África y Asia Pacífico. El equipo de Ingram Micro cuenta con un maduro equipo de expertos de UiPath y dedicado cuya misión es dar soporte a los partners durante todo el ciclo de ventas, incluyendo identificación de oportunidades, tratamiento de diseño, servicios de asesoramiento, licencias y formación. Con el apoyo de los Centros de Excelencia de Ingram Micro, los socios de canal que venden UiPath se benefician de las mejores prácticas compartidas, servicios de apoyo "follow the sun" y recursos globales diseñados para satisfacer las variadas demandas del mercado a nivel local, regional y global.

de integradores", una suma de los integradores más relevantes del mercado.

MARCO DE ADHESIÓN

Por otra parte, consciente de que junto con el empuje de la pyme es necesario el impulso de la Administración Pública, Ingram Micro ofrece un marco para facilitar al canal la adhesión a los procesos de licitación y contratación gubernamentales.

Actualmente, unos 100 partners forman parte de la SMB Alliance, los cuales disponen de la capacitación necesaria para abordar las soluciones de TI que se están impulsando o muestran interés por capacitarse. Se trata de partners con un perfil de pequeño y mediano integrador que satisfacen el criterio de capilaridad geográfica necesaria para llegar a pymes de todos los sectores. En cuanto al canal enfocado en el sector público, actualmente lo forman unas 30 figuras con el mismo criterio de capacidad y alcance geográfico.

"Estamos ejecutando una transformación del modelo económico del país, un cambio exponencial en el que es necesario adelantarse a las tendencias, construir soluciones y preparar al canal para gestionar ese cambio. Para llegar a ese tejido empresarial tan heterogéneo como son las pymes el canal es clave", asegura Alberto Pascual.

Por su parte, Jorge Gil, director general de IDC Research España, concluye señalando que el objetivo de SMB Alliance es "poder contar con un canal integrador sumamente potente para poder ayudar a la pyme en su digitalización". ■

MÁS INFORMACIÓN

- "El canal es muy consciente del momento histórico que estamos viviendo": Jaime Soler (Ingram Micro)
- IDC e Ingram Micro acompañan al canal en los planes de digitalización de sus clientes

it whitepapers

ESPAÑA EN LA ERA POST-COVID

La COVID-19 ha trastocado la vida de empresas y ciudadanos que ven con incertidumbre el futuro. A la preocupación sanitaria se le unen unas previsiones económicas, y de desempleo, nada esperanzadoras. Descubre en este IT Research cuáles son las principales previsiones para España y cuál es el papel que va a jugar la tecnología en la recuperación a través de más de 40 gráficos, divididos en seis bloques, y las opiniones de diversos analistas del sector.

KIOXIA

Comparte tu mundo

Memoria USB TransMemory U365 3.2

DMI Computer

www.dmi.es

Tech Data incrementa su nómina de marcas en el mes de mayo

El mayorista incorpora las soluciones de HPE Financial Services, Secureworks y Digitate a sus distintas divisiones.

Tech Data no ceja de ampliar su catálogo de marcas y el mes de mayo ha sido una muestra incuestionable de esta estrategia. Por un lado, ha sumado a HPE Financial Services (HPEFS) como partner financiero de su propuesta Tech-as-a-Service (TaaS) B2B solution.

"Estamos especialmente satisfechos de poder ayudar a los socios de las pymes a acelerar su adopción de los modelos de suscripción como servicio. El profundo conocimiento del mercado de TI que tiene HPEFS significa que ya están familiarizados con muchos partners clientes, lo que agilizará el proceso de incorporación y aprobación", señala Roman Rudolf, vicepresidente de estrategia y servicios de Tech Data.

Para Patrick Leoni, director de Canal de HPEFS, EMEA&APJ, "Tech Data TaaS B2B es una oferta líder en el mercado y Tech Data está ayudando a los resellers a satisfacer la demanda de soluciones flexibles de los clientes. En HPEFS compartimos el mismo enfoque sobre los resellers y el resultado de negocio del cliente en su recorrido de consumo de sistemas TI".

Utilizando el generador de suscripciones, que está totalmente integrado en la plataforma InTouch, de Tech Data, los partners pueden combinar hardware, software y servicios de múltiples fabricantes en una sola solución y ofrecerla en forma de suscripción a sus clientes finales. La plataforma de generación de suscripciones TaaS también está disponible como solución de marca blanca para los partners.

"Con TaaS, los partners pueden disfrutar de una experiencia totalmente digitalizada con verificaciones de crédito automáticas e instantáneas y presupuestos personalizados, entregados en cuestión de minutos. Tech Data está comprometida estratégicamente con el desarrollo de una atractiva oferta de servicios y una experiencia digital mejorada que ayude a nuestros partners a impulsar su transformación desde un modelo de estrictamente compra directa de activos a modelos basados en la suscripción", añade Rudolf.

CONTENIDOS↓

TAEGIS XDR DE SECUREWORKS

Secureworks continúa reforzando su estrategia de canal en el mercado europeo. Esta vez ha alcanzado un acuerdo con Tech Data, por el que este pone a disposición de sus partners en la región el porfolio nativo de Cloud Secureworks Taegis, que abarca Secureworks Taegis XDR (Extended Detection and Response), Secureworks Taegis Managed XDR, Secureworks Taegis VDR y Secureworks Incident Management Retainer, para respuesta proactiva y de emergencia a incidentes.

Los complejos entornos de hoy en día han aumentado los riesgos para los usuarios finales de nube, redes y puntos de conexión. En este sentido, la plataforma Taegis de Secureworks unifica la detección y la respuesta en entornos de puntos de conexión, red y Cloud. La solución utiliza análisis avanzado e inteligencia aplicada a comunidades, mediante detección y conclusiones basadas en IA extraídas de la participación en más de 1.400 respuestas a incidentes, para detectar, investigar y responder a ciberataques.

"Consideramos que la plataforma Taegis XDR puede ayudar a los MSP, MSSP y resellers a gestionar las amenazas a las que se enfrentan los clientes de forma mucho más efectiva. También crea una oferta diferenciada de servicios de ciberseguridad que da como resultado una relación estrecha y estable con los clientes. Estamos muy satisfechos de poder trabajar con Secureworks para llevar estas soluciones al mercado europeo", comenta David Ellis, vicepresidente para Europa de ciberseguridad y movilidad de Tech Data.

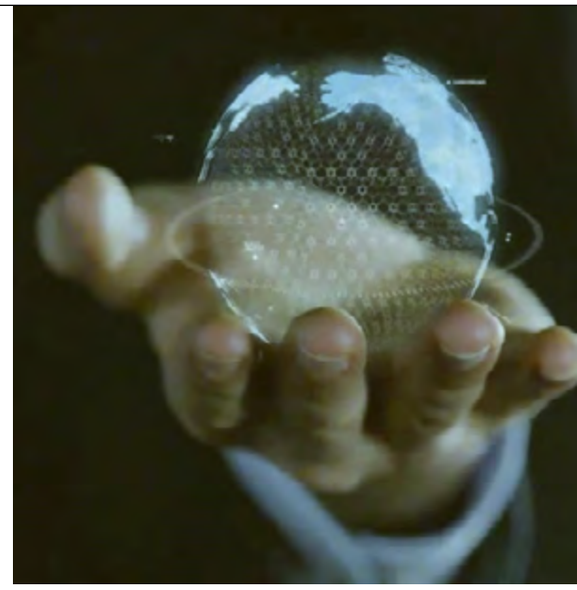
Para ayudar a los partners a ofrecer un negocio rentable basado en la tecnología de Secureworks, Tech Data ofrece una serie de programas y recursos de capacitación, entre ellos una evaluación de referencia sobre ciberseguridad, desarrollada por Tech Data en colaboración con Canalys; acceso al programa Practice Builder de Tech Data para ayudar a los partners a adoptar nuevos modelos de negocio y desarrollar conocimiento experto en segmentos tecnológicos en crecimiento; formación en ventas y marketing a través de la plataforma Channel Academy de Tech Data; formación técnica a través del equipo de Academy del mayorista; y acceso a una gama flexible de soluciones de financiación para permitir que los partners aceleren sus inversiones.

CON EL SOFTWARE EMPRESARIAL DE DIGITATE

Tech Data ha firmado un acuerdo europeo con Digitate, que brinda a los socios del mayorista en toda Europa la oportunidad de ofrecer la gama completa de soluciones Digitate, basadas en la plataforma de software ignio de la compañía. Esto incluye su producto insignia de inteligencia artificial para operaciones de TI (AIOps), una de las seis soluciones de Digitate a las que los socios pueden acceder.

Ignio de Digitate aplica inteligencia artificial (IA) y aprendizaje automático (ML) para proporcionar a los equipos de operaciones de TI conocimientos que permitan la predicción, prevención y solución de problemas y riesgos. La plataforma de software puede identificar y reparar automáticamente los incidentes y fallos de TI sin intervención humana, a la velocidad de la máquina.

Gartner predice que para 2023, el 40% de los equipos de infraestructura y operaciones de las grandes empresas utilizarán la automatización aumentada por IA, y las soluciones de aprendizaje automático serán la opción preferida para muchas empresas. Tech Data ha creado una cartera integral de análisis de datos para ayudar a los partners a abordar esta oportunidad y ofrece soporte especializado a través de sus expertos en datos y soluciones de IoT, la metodología de Solutions Factory y los programas Practice Builder. ■



MÁS INFORMACIÓN

- Tech Data complementa su oferta de servicios con la compra de Finance Technology
- Tech Data orienta al canal TI en la gestión de los fondos Next Generation EU
- El COVID-19 ha dado impulso a los modelos de consumo de TI como servicio

Arrow ECS suma dos nuevos fabricantes en su región EMEA

El mayorista incorpora las soluciones de datacenter de Submer y la propuesta de seguridad de Secureworks.

Arrow ECS sigue ampliando su ya nutrido porfolio. Por un lado, ha sellado un acuerdo con Submer para proporcionar computación de alta eficiencia y alta densidad a clientes empresariales en EMEA (Europa, Oriente Medio y África). Arrow unirá las soluciones avanzadas de refrigeración por inmersión de Submer con las soluciones OEM de Dell Technologies, junto con su soporte y servicios personalizados, para ofrecer soluciones llave en mano. Al combinar la cadena de suministro mundial, los servicios de ingeniería y las capacidades de soporte de Arrow con la innovadora solución de inmersión de Submer, el mayorista podrá facilitar el despliegue de soluciones de centros de datos sostenibles a escala global.

"Arrow Electronics está entusiasmado de formar equipo con Submer para proporcionar una plataforma para nuevas capacidades en el borde y ofrecer mejoras de eficiencia energética para nuestros clientes", afirma James Stannard, vicepresidente de ventas del negocio de servicios globales de Arrow en EMEA. "Durante más de 85 años, hemos estado guiando a las empresas en su viaje de innovación con una amplia oferta de productos y servicios globales. Nuestra capacidad para ayudar a las empresas a escalar les permite centrarse en acelerar sus negocios", apunta".

Por su parte, Daniel Pope, CEO y cofundador de Submer, señala que "Submer tiene la misión de proporcionar la tecnología que permite entornos óptimos para la máquina, allanando el camino para una nueva generación de centros de datos refrigerados por inmersión, y Arrow y Dell son compañeros clave en este viaje. Gra-

cias a nuestra tecnología de refrigeración por inmersión, somos capaces de aportar eficiencia, densidad y tranquilidad a aquellos que desean ejecutar cargas de trabajo complejas y de alta densidad de una manera sostenible".

SECUREWORKS TAMBIÉN EN EUROPA

Por otro lado, Arrow ha firmado un nuevo acuerdo de distribución paneuropeo con Secureworks, por el que ofrecerá un porfolio completo de software y servicios de seguridad adicionales y escalables para el canal en Europa. "Estamos muy contentos de ampliar nuestra relación con Arrow, permitiéndoles comercializar y revender los principales productos de software y servicios de respuesta a incidentes de Secureworks a su amplia red de distribuidores de valor añadido en toda Europa", afirma Maureen Perrelli, directora de canal de Secureworks. "Arrow ha sido un distribuidor preferente de Secureworks en Norteamérica, y está bien posicionado a nivel mundial para habilitar a nuestra comunidad de socios de canal para ofrecer los productos y servicios de Secureworks al mercado europeo de ciberseguridad".

A medida que las empresas crecen en complejidad técnica debido a la digitalización, hay un número cada vez mayor de endpoints y aplicaciones que se abren a la amenaza de los ciberataques, especialmente en entornos cloud y en la infraestructura de la red. La colaboración entre Arrow y Secureworks pretende ofrecer a las empresas la posibilidad de digitalizarse y hacerlo de forma segura.

Secureworks proporcionará a Arrow una forma simplificada de satisfacer la creciente demanda de ciberseguridad de los clientes. Los productos y servicios que estarán disponibles tras este nuevo acuerdo de distribución son Secureworks TaegisTM XDR (Detección y Respuesta ampliada), Secureworks Taegis ManagedXDR, Secureworks Taegis VDR y Secureworks Incident Management Retainer, para la respuesta proactiva y de emergencia frente a incidentes. ■

MÁS INFORMACIÓN

- Arrow refuerza su cartera con la suite de productos para ciberataques de OPSWAT
- Arrow Electronics distribuirá las soluciones de Liqid en la región de EMEA

GRANDES IDEAS PARA TUS REUNIONES
SOLUCIONES COMPLETAS DE ALTA CALIDAD

Descubre los kits tres en uno compuestos por:

Un monitor interactivo, una barra de videoconferencia y ordenador

Monitor interactivo Traulux TLM80
de 65 o 75 pulgadas cn android 8.0 embebido
+ Soporte de pared

Unidad de videoconferencia
POLY Studio USB Auto Track 4K

Módulo PC-OPS i5 con 8Gb de RAM
+ Windows 10 PRO preinstalado

El versátil conjunto garantiza su compatibilidad con cualquiera de los servicios más usados en la nube y plataformas para videoconferencia más reconocidas

Descubre más en charmex.net

¿Tienes dudas? ¿Hablamos?

Escríbenos para que podamos ayudarte

Visita nuestras redes sociales
Charmex Internacional s.a

ACTUALIDAD

V-Valley lanza V-Valley Academy para potenciar la formación de sus partners

A fin de reforzar los conocimientos de sus partners, V-Valley presenta V-Valley Academy, una herramienta diseñada para proporcionarles acceso a formaciones y contenidos especializados, así como un centro de soluciones y certificaciones tanto propias como de los distintos fabricantes. En V-Valley Academy se podrá acceder a una serie de webinars, trainings y contenidos en torno a las diferentes soluciones del negocio de Advanced Solutions, propias o de los distintos fabricantes, a fin de facilitar a los partners contenido que les ayude en la toma de decisiones y, en definitiva, en su día a día. Además, y con motivo del despliegue de los Fondos Next Generation de la Unión Europea, se ha desarrollado todo un ciclo de formaciones para orientar y guiar a los clientes en la obtención de las ayudas destinadas a la digitalización de la pyme.

La herramienta les da acceso a una serie de webinars sobre las diferentes soluciones del negocio de Advanced Solutions, además de formaciones y contenidos especializados en los Fondos Next Generation de la UE. También pone a su disposición un centro de soluciones para pilotos y pruebas de concepto y un centro de certificaciones oficiales de Pearson VUE.

CENTRO DE SOLUCIONES

A través de V-Valley Academy los partners también podrán acceder al Centro

de Soluciones de V-Valley, para aumentar las posibilidades de que los partners puedan realizar pilotos y pruebas de concepto. En el centro, puede llevarse a cabo la simulación de entornos en producción de un centro de datos, de tal forma que los clientes de V-Valley pueden realizar todo tipo de pruebas usando lo último en tecnología hardware y software para centros de datos. Para ofrecer un valor añadido, V-Valley ha creado un equipo de especialistas con gran experiencia para dar formación y hacer demostraciones a través de este centro.

Por último, V-Valley cuenta con un centro de certificaciones oficiales de Pearson VUE disponible para todos aquellos clientes interesados en obtener este tipo de certificaciones oficiales. ■

MÁS INFORMACIÓN

- HPE y V-Valley acercan al canal los beneficios de la plataforma HPE GreenLake
- V-Valley acerca al canal TI las claves para acceder a los fondos Next Generation

Mayorista de Salicru

Salicru ha firmado un acuerdo con Esprinet por el que se integra en el portfolio de V-Valley, la división de valor del Grupo. Este tipo de alianzas se enmarca en la estrategia de crecimiento y expansión de Salicru, que podrá disponer de la experiencia de uno de los mayores mayoristas de tecnología en el Sur de Europa, lo que le permitirá acceder con sus equipos a nuevos clientes y mercados.

A partir de ahora, V-Valley ofrecerá a su canal de distribución los Sistemas de Alimentación Ininterrumpida (SAI-UPS) de Salicru, una completa gama de soluciones de protección y seguridad energética de equipos tecnológicos entre los que destacan los equipos de mediana y gran potencia para uso profesional, como son las series SPS ADVANCE RT2, SLC TWIN RT2, SLC TWIN PRO2, SLC ADAPT, SLC X-PERT y SLC CUBE4. Este nuevo acuerdo ofrece también la posibilidad de implementar soluciones tecnológicas personalizadas y de gran relieve capaces de resolver las necesidades de sus clientes en el ámbito de la protección y seguridad de sus equipos y procesos industriales.

V-Valley aporta su experiencia en proyectos y soluciones orientadas al mercado B2B, contando con un gran elenco de profesionales certificados en las tecnologías más punteras, pudiendo desarrollar servicios avanzados en el área de valor, desde el inicio del proyecto hasta su puesta en marcha, incluyendo la formación, transferencia tecnológica y soluciones financieras, a medida y acordes a cada proyecto, a sus partners. Adicionalmente El Grupo Esprinet proporciona servicios tradicionales de venta al por mayor, servicios de venta al consumo, servicios logísticos y otros servicios financieros a sus más de 31.000 clientes.

ALSO estrecha lazos con IBM a través de su marketplace

ALSO ha firmado un acuerdo con IBM por el que incorpora las soluciones de nube híbrida e Inteligencia Artificial de IBM Cloud al ALSO Cloud Marketplace. Los clientes de ALSO podrán acceder así a los más de 200 servicios cloud que ofrece IBM a través de un único punto de acceso y con un modelo de subscripción y pago por uso.

"Desde ALSO queremos ayudar a nuestros distribuidores en el proceso de digitalización de sus clientes, desarrollando sus ventajas competitivas y proponiendo las soluciones que más se adaptan a sus necesidades. Para alcanzar este objetivo y reforzar la adopción de la tecnología cloud en el mercado español tenemos el placer de contar con IBM como proveedor estratégico. Este acuerdo nos permite expandir nuestro portafolio de productos y servicios Cloud con una de las tecnologías que más se ajustan a nuestra nueva realidad, donde el Hybrid Cloud es eje central", asegura Montserrat Peidró, directora general de ALSO Cloud España.

CLOUD MARKETPLACE

ALSO Cloud Marketplace ofrece la posibilidad de implementar de manera personalizada los servicios en la nube que permitan agilizar el funcionamiento de las empresas, adoptar nuevos modelos de negocio y mejorar los procesos y las operaciones para ser más eficientes y poder competir en el mercado. Los clientes de ALSO podrán contar ahora con las soluciones de nube híbrida de IBM tales como IBM Cloud Satellite, IBM Cloud Pak for Data como Servicio en IBM Cloud y Red Hat OpenShift en IBM Cloud. También podrán contar con soluciones de Inteligencia Artificial como IBM Watson Assistant y de ciberseguridad como IBM MaaS360.

"Compañías españolas de todo tipo están acelerando la adopción de las tecnologías de nube híbrida porque están experimentando sus ventajas y aportación de competitividad. Ampliar nuestras capacidades de nube híbrida a través de socios del ecosistema como ALSO es fundamental para que IBM llegue a sus clientes. Estamos muy satisfechos de que ALSO confíe en las tecnologías de IBM y refuerce con ellas su oferta cloud en el mercado español", afirma Mónica Cernuda, IBM Public Cloud Market Leader SPGI. ■

La importancia de la nube

Con la pandemia de COVID, el número de empresas que recurren a la nube para dar apoyo a sus estrategias digitales no deja de crecer. De hecho, según la última encuesta a consejeros delegados de todo el mundo realizada por IBM, en España el 80% de los directivos cree que el cloud es una de las tecnologías que más cambiarán sus negocios en los próximos años. Para Peidró, "éste es el momento para los resellers en España de acelerar la adopción de la nube entre sus clientes. Todas las empresas necesitan digitalizarse, ya sean grandes o pequeñas, y todas ellas requerirán de un partner que te lo ponga fácil, te ayude y asesore en el proceso, y precisamente en ALSO tenemos mucha experiencia en dar soporte en la transición hacia un cloud rentable".

Los partners de ALSO podrán contar ahora con las soluciones de nube híbrida de IBM tales como IBM Cloud Satellite, IBM Cloud Pak for Data como Servicio y Red Hat OpenShift en IBM Cloud. "Desde ALSO queremos ayudar a nuestros distribuidores en el proceso de digitalización de sus clientes", afirma Montserrat Peidró, de ALSO Cloud España.

MÁS INFORMACIÓN

- ALSO aumenta su facturación un 11,3% ayudado por la demanda de servicios cloud
- ALSO se alía con Barcelona Tech City para su desembarco en España

MCR Mobile prevé triplicar su facturación apoyado en nuevas marcas y líneas de negocio

MCR ha celebrado un webcast virtual para analizar, de la mano de expertos, analistas y marcas líderes del sector el mercado de la telefonía y la movilidad, así como mostrar la estrategia de MCR Mobile, la división de movilidad de MCR, las principales oportunidades que existen para el canal en la actualidad, las tendencias más importantes y las previsiones para este mercado en los próximos meses. Bajo el título de MCR CONNECT MOBILE, el evento ha contado con fabricantes como Oppo, Samsung, SwissVoice o ZTE y la participación de más de 100 empresas distribuidoras.

En palabras de Alex Cabo, director de MCR Mobile, "desde MCR hemos organizado esta jornada de análisis porque, como en el resto de nichos de la tecnología, nuestro objetivo es estar siempre preparados para ofrecer al canal lo último en innovación. De ahí que sea importante abordar no sólo las cifras y estrategias, sino también las principales tendencias y oportunidades que se están abriendo con el 5G y los nuevos casos de uso".

Tras la presentación inicial de los ponentes, han intervenido por parte de la consultora Ideas Originales David García, director Comercial, e Iñaki Martínez, director de Estudios, Sistemas e Información, analizando los temas que, en positivo y en negativo, están afectando al mercado de la movilidad. En este sentido, entre las nubes grises que se ciernen sobre el mercado destaca la escasez de componentes claves, como chips y pantallas, siendo Europa uno de los mercados más dañados por esta escasez. Se espera que esta falta de componentes impacte entre un 25 y un 30% en la falta de producto en el sector.

MESA DE EXPERTOS

Tras ello dio comienzo la mesa de expertos, donde los participantes han tratado diversas cuestiones de interés relacionadas con este mercado. En concreto, junto a Alex Cabo han estado Álvaro Galán, director de Producto y Estrategia de Oppo Mobile Iberia; Anna Coll, B2B Channel Sales Manager de Samsung Electronics Iberia; Frédéric Vincey, Country Manager de Swissvoice; e Iván Sánchez, Sa-

El evento MCR CONNECT MOBILE ha reunido a fabricantes como Oppo, Samsung, SwissVoice y ZTE y a representantes de más de 100 empresas distribuidoras para, como señala Alex Cabo, director de MCR Mobile, "abordar no sólo las cifras y estrategias, sino también las principales tendencias y oportunidades que se están abriendo con el 5G y los nuevos casos de uso".

les Director de ZTE. Tras sus intervenciones, se pasó finalmente al turno de preguntas, donde los asistentes al webinar pudieron exponer sus dudas y comentarios directamente a los ponentes.

"Estamos muy contentos con la respuesta de los fabricantes, los cuales admiten que afrontan con miedo la escasez de componentes, principalmente de chips. En el webinar han explicado sus estrategias para 2021, cómo afrontan la falta de inventario prevista a mitad de año y su apuesta por 5G, que va a tener un empuje especial", señala Cabo. "Nuestra labor desde MCR Mobile será dar disponibilidad ante la falta de productos que va a haber".

BALANCE DEL PRIMER AÑO

Tras un año de existencia, el balance que hacen los responsables de la división de telefonía y movilidad de MCR es muy positivo. El año 2020 ha sido un gran año para el sector, especialmente el último trimestre, lo que ha permitido a MCR Mobile superar con creces sus expectativas. También el mercado de Portugal ha avanzado con solidez durante los últimos meses, demostrando una gran fortaleza y unas expectativas muy buenas.

"MCR Mobile se ha posicionado muy bien en los tres principales canales (retail, consumo y operadoras), y se han superado con creces las expectativas de negocio, especialmente en el apartado de retail, con el gran dinamismo del negocio vinculado a las grandes superficies, sobre todo durante este primer trimestre del año", explica Alex Cabo, cuyos planes para este año pasan por ampliar el catálogo en un 50% y triplicar la cifra obtenida en el año anterior a nivel de facturación.

NUEVOS ACUERDOS Y LÍNEAS DE NEGOCIO

Se espera así firmar dos o tres nuevos acuerdos con grandes marcas a lo largo del segundo y tercer trimestre del año. A este respecto, el director de MCR Mobile afirma que "no buscamos incorporar nuevas marcas porque sí. La oferta tiene que tener sentido, y queremos marcas que cubran segmentos que no están cubiertos". Por ejemplo, la marca Honor prevé lanzar a principios del verano nuevos dispositivos que cubren el ámbito online, y que permitirán a MCR reforzar los canales digitales.

Por otra parte, el mayorista trabaja para ampliar su oferta en líneas de negocio, con accesorios de telefonía y con wearables, haciendo crecer sus ecosistemas IoT. "La clave está en que es necesario un ecosistema conectado, y el centro de control es el propio dispositivo, lo que genera una gran oportunidad de cross-selling", explica. "Todos los fabricantes tienen su ecosistema propio, y nosotros como mayorista de referencia añadimos a nuestro porfolio cada vez más referencias para cubrir nuevos nichos de mercado y ofrecer más líneas de negocio rentables para nuestro canal", concluye Alex Cabo. ■

MÁS INFORMACIÓN

- MCR Mobile incorpora la nueva gama de smartwatches de Ulefone
- MCR Mobile suma a su cartera la marca de accesorios UAG

SZLamp y sus productos LED

MCR PRO ha firmado un acuerdo con SZLamp para la distribución de sus productos en Iberia. "Este acuerdo con SZLamp refuerza nuestra apuesta por la especialización en el segmento de la tecnología LED y por la penetración en aquellas líneas de negocio donde detectamos mayores oportunidades para nuestro canal", destaca Enrique Hernández, director de la división MCR PRO.

La pantalla LED está a punto de comenzar un punto de inflexión y de robar protagonismo y hegemonía al display clásico. La versatilidad y flexibilidad de la tecnología LED para prácticamente cualquier solución, le augura un futuro prometedor, y la división MCR PRO LED ha nacido precisamente para dar servicio a la demanda de tecnología LED en el sector.

SZLamp, sub empresa de la compañía de señalización LED Unilumin Group, ha ido abriéndose paso por el mercado europeo, cumpliendo todos los certificados CE, RoHS y EMC necesarios para su distribución en la UE. Con un diseño ligero, robusto y con un mantenimiento extremadamente sencillo, tanto por la parte frontal como por la trasera, el modelo GN se ha establecido como un estándar para la gran mayoría de soluciones Retail, Horeca y Corporate desde su lanzamiento.

TENDENCIAS

El proceso de digitalización en empresas y Administraciones Públicas se ha acelerado

En los últimos meses el proceso de digitalización se ha acelerado de forma exponencial. Así lo pone de manifiesto el IV Estudio sobre el estado de digitalización de las empresas y Administraciones Públicas españolas de Vodafone, que muestra cómo todas las empresas y Administraciones Públicas, independientemente del segmento al que pertenecen, comparten la opinión sobre la importancia de las nuevas tecnologías para su actividad en el horizonte del próximo año.

A medida que aumenta el tamaño de las empresas, mayor protagonismo ha desempeñado el teletrabajo durante los meses de la pandemia. En el caso de las grandes empresas la implantación del teletrabajo asciende al 94%, mientras que el teletrabajo en microempresas se ha duplicado hasta alcanzar un 30% durante los meses de pandemia. En el futuro todas las organizaciones planean reducir el teletrabajo, pero las empresas de todos los tamaños continuarán en niveles ligeramente superiores a la situación previa a la pandemia. Sin embargo, en el caso de

La conectividad a Internet y los servicios vinculados al cloud se mantienen como las soluciones más implantadas, mientras avanzan nuevas aplicaciones relacionadas con el teletrabajo como sistemas de videoconferencia, herramientas de colaboración, acceso remoto al puesto de trabajo y sistemas de seguridad.

las Administraciones Públicas el porcentaje de teletrabajo podría mantenerse en un 55%, previéndose así un incremento notable respecto a la situación previa.

Las empresas españolas consideran que contaban con las soluciones necesarias para la implementación del teletrabajo en la pandemia. De hecho, la mayoría de las empresas se autopercibe como "preparada", siendo el segmento de las grandes empresas y las pymes donde esta percepción obtiene sus mayores porcentajes (87% y 84% respectivamente). Sin embargo, las Administraciones Públicas creen que han estado menos preparadas para hacer frente a esta práctica laboral.

A mayor tamaño de la empresa se incrementa la importancia atribuida a las nuevas tecnologías para un futuro inmediato. Consideran estas como muy importantes o bastante importantes un 57% de las microempresas, un 68% de las pymes, un 82% en el caso de las grandes empresas y para el 84% de las AAPP.

Todos los tipos de empresas como Administraciones Públicas coinciden en citar la crisis del COVID-19 como su mayor preocupación, seguida de la situación económica general, la pérdida de facturación/ventas y la evolución de su sector como ostros aspectos relevantes. Si bien la digitalización no aparece como una preocupación de las empresas, la inquietud por ella va incrementándose según aumenta el número de empleados de la empresa. Hay que destacar aquí que son las Administraciones Públicas, las que mayor pre-

Las compañías líderes digitales crecen 5 veces más rápido que sus rivales

Las empresas que han aumentado sus inversiones en tecnología durante la pandemia han crecido más que sus competidores. Así se recoge en el último estudio de Accenture: "Da el salto, ¡y lidera!", que muestra que, al intensificar las inversiones en la nube, la inteligencia artificial (IA) y otras tecnologías, las compañías denominadas "líderes" han incrementado sus ingresos cinco veces más rápido que las "rezagadas". Las empresas líderes suponen un 10% en la muestra total, y un 11% en la española, mientras que las rezagadas son el 25% a nivel global y el 36% en España.

El informe también identifica la aparición de una nueva categoría de empresas, "liebres", que han conseguido acortar en el tiempo sus transformaciones digitales mediante una estrategia tecnológica rápida y progresiva, que ha convertido los desafíos del año pasado en oportunidades de negocio y ventajas para este. Estas empresas son el 18% de la muestra total y el 14% de la española.

"La fortaleza de los sistemas, la transformación digital y un mayor foco en la innovación permiten a los líderes aumentar paulatinamente su crecimiento y diferencia sobre los rezagados", afirma Bruno Chao, managing director de Accenture Technology en España, Portugal e Israel. "Mientras tanto, las compañías liebres también están mostrando un enorme progreso, manteniendo la fortaleza de los sistemas e infundiendo innovación en toda la organización. De hecho, ahora mismo están aumentando sus ingresos cuatro veces más que los rezagados".

ocupación muestran por este aspecto, otorgándole una nota de 7,8 sobre 10.

La digitalización beneficia a las empresas aportando principalmente eficiencia en procesos y mejoras en la comunicación con clientes. En el caso de la Administración Pública, destacan también el ahorro de tiempo y dinero, junto con la mejora de la comunicación con el ciudadano. Respecto a las barreras para avanzar en la digitalización, la necesidad de contar con el talento adecuado se hace más patente y es la principal barrera para avanzar en la digitalización de las empresas y la Administración Pública.

Las organizaciones estudiadas consideran que están aún inmersas en el proceso de digitalización de sus organizaciones y solo una parte de ellas ha llegado a un nivel avanzado. En este contexto, es el segmento de las microempresas las que se perciben menos preparadas, donde un 48% reconoce estar en un nivel 'básico'. Son las grandes empresas donde se sitúa el mayor porcentaje de nivel 'avanzado', con un 42%, aunque siguen reconociendo un amplio margen de desarrollo.

Para facilitar el teletrabajo, las tecnologías que han aportado una mayor utilidad han sido las soluciones de conectividad, servicios en la nube (pública y privada), aplicaciones de videoconferencia, herramientas de colaboración, acceso remoto al puesto de trabajo y sistemas de seguridad en red o en la nube. También han tenido una gran transcendencia aquellas tecnologías que han permitido llegar de forma remota a los clientes como el marketing digital, el comercio electrónico y las aplicaciones de pago. En general, los servicios vinculados a nube o cloud y, en un segundo lugar, aquellos que tienen que ver con la conectividad son los más implantados en las empresas y Administraciones Públicas españolas. Las pequeñas empresas y autónomos disponen de 2,4 servicios frente a los 6,7 de las grandes empresas y también son quienes menos contratación de este tipo de soluciones han hecho desde que comenzara la pandemia del COVID-19.

La crisis económica derivada ha provocado una contención del gasto y de las inversiones, lo que ha tenido su reflejo en las ratios de empresas que han realizado inversión en digitalización en los últimos años, nivel que retrocede truncando así la creciente tendencia de anteriores estudios. Respecto a la presencia de planes de digitalización, aumenta ligeramente en todas las empresas, en mayor medida en las grandes organizaciones, aunque el porcentaje que asigna una partida específica para el desarrollo de este plan se estabiliza y se mantiene en un 47% en las pequeñas empresas, un 49% en las pymes, un 60% en las grandes empresas y un 57% en el caso de las Administraciones Públicas que afirman tener asignado un presupuesto para desarrollar su plan. ■

MÁS INFORMACIÓN

- 6 de cada 10 empresas españolas invertirán en digitalización para superar la crisis
- La pandemia ha impulsado la digitalización de las pequeñas empresas en España

La consolidación de una industria digital permitiría a España ser más competitiva

Siemens y PwC han presentado el informe 'Claves e inversiones estratégicas para una España 5.0', que ahonda en la oportunidad histórica que España tiene ante sí para renovar su modelo productivo y hacerlo más resiliente y sostenible, gracias al impulso que supondrán los 140.000 millones de euros que la Unión Europea (UE) inyectará a través de los distintos mecanismos contemplados en el Plan de Recuperación y Resiliencia.

Todo ese plan de actuaciones e inversiones daría lugar a lo que el estudio denomina la España 5.0, un modelo de país más sostenible y centrado en las personas, basado en una industria más digital y competitiva y apoyado en el desarrollo de infraestructuras más inteligentes y eficientes. Esta España 5.0 requeriría de nuevos modelos de negocio, una necesaria integración de diferentes tecnologías

El uso masivo de dispositivos móviles, la computación en la nube, la IA, IoT, la robótica, el 5G o el gemelo digital, entre otras nuevas tecnologías, han transformado radicalmente toda la cadena de valor del proceso productivo. La industria manufacturera mejoraría notablemente su competitividad convirtiéndose en una industria más inteligente, innovadora y sostenible.

digitales y una apuesta decidida por la creación de ecosistemas colaborativos.

En los últimos trimestres, la industria española ha sufrido de forma ostensible el impacto de la pandemia. En gran parte, debido a que el 99,4% del tejido productivo lo componen pymes y, de ellas, un 84% son microempresas. Esta realidad ha hecho que la contribución del sector al PIB se haya alejado en los últimos años del 20% marcado hace unos años por el Horizonte 2020.

TRANSFORMACIÓN DEL PROCESO PRODUCTIVO

El uso masivo de dispositivos móviles, la computación en la nube (Cloud y Edge Computing), la inteligencia artificial (IA), el Internet de las cosas (IoT), la robótica, la realidad aumentada, la impresión 3D, los drones, el 5G o el gemelo digital, por citar algunas de las nuevas tecnologías, se han convertido en realidades cada vez más habituales que han transformado radicalmente toda la cadena de valor del proceso productivo.

Gonzalo Sánchez, presidente de PwC España, resalta la importancia de "apostar de forma decidida por la digitalización, especialmente en las pymes, que constituyen el grueso de nuestra realidad económica y que pueden aprovechar esta oportunidad para ganar masa crítica y afrontar los retos de nuestra economía". Y es que la industria española adolece, en estos momentos, de un bajo consumo de bienes de equipo y maquinaria, de un elevado coste energético, de bajas tasas de inversión en I+D+i, y carece del necesario alineamiento con el sector educativo. Es necesario, por ello, que se acentúe la participación en industrias de más valor y claro potencial y minimizar la excesiva dependencia de proveedores externos.

La ejecución de estos planes aceleraría la transformación tecnológica y digital de la industria española y permitiría un crecimiento económico más sostenible, basado en la productividad del trabajo, la eficiencia y el conocimiento. La industria manufacturera mejoraría notablemente su competitividad internacional, gracias al despliegue del IoT, la robótica, el Smart Data o el 5G, convirtiéndose en una industria más inteligente, puntera, innovadora, sostenible y con una menor huella ambiental. ■

MÁS INFORMACIÓN

- La pandemia impulsa el cambio de estrategias de TI en el sector industrial
- El 70% de las empresas industriales cuenta con un plan de transformación digital

Grandes posibilidades

Esta nueva 'industria 5.0' mantendría de la anterior 4.0 la hiper conectividad, que permite llevar el dato de los sensores hasta el algoritmo de computación en la nube o en la capa Edge, donde las herramientas de predicción anticipan y permiten la toma de decisiones. Además, esta comunicación inmediata entre las máquinas y la nube se haría más sencilla, gracias al desarrollo del 5G industrial, cuyo impacto en los sectores industriales clave podría llegar a alcanzar el 0,3% del PIB en 2025 y el 1% en 2030. En definitiva, la consolidación de una industria más digital permitiría a España ser más competitiva, flexible y adaptable a los cambios, además de mejorar la seguridad y estabilidad de sus trabajadores.

El mercado de impresión ha experimentado una profunda transformación ayudando a las empresas en sus procesos de digitalización.

¡Descubra en nuestro

Centro de Recursos it User

cómo está evolucionando un sector clave en la Transformación Digital!

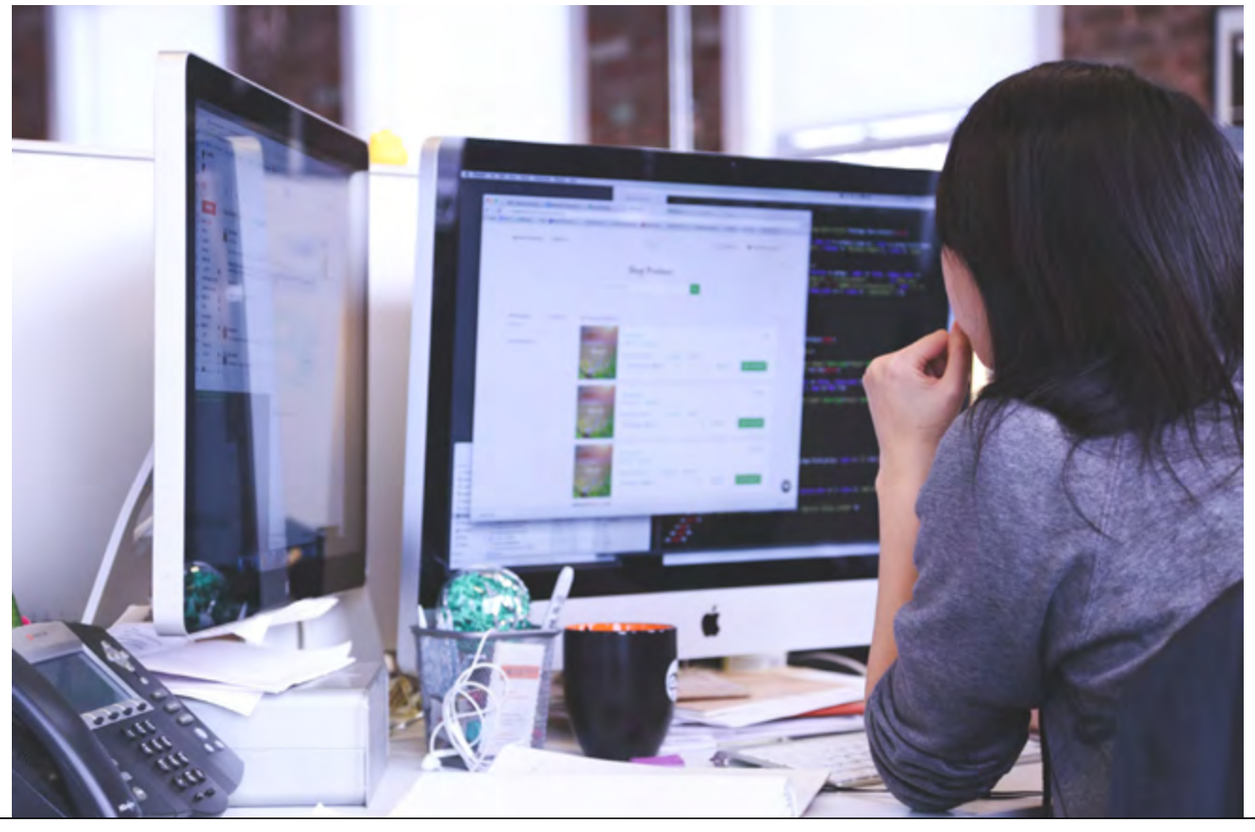
ImpresiÓN Digital

Con la colaboración de: brother

Las empresas españolas se sitúan a la cabeza en intención de gasto TI

Dynabook ha publicado los resultados del estudio 'The Hybrid Shift: Managing an increasingly remote workforce' realizado en colaboración con Walnut Unlimited, que revela que el 71% de los responsables de Tecnologías de la Información españoles prevé aumentar su gasto este año para adaptarse a las necesidades del nuevo entorno de trabajo híbrido. Las empresas españolas se sitúan así a la cabeza en intención de gasto a nivel europeo, siendo las de servicios financieros y del sector industrial las más dispuestas a elevar esta inversión, con el 76% y el 73% de las consultadas, respectivamente. Por el contrario, el comercio minorista se sitúa a la cola en aumento de gasto en TI con el 54%.

La demanda de flexibilidad laboral y la deslocalización de los equipos de trabajo son el motor de este crecimiento del gasto. En concreto, la encuesta revela que el 43% de los empleados de nuestro país trabajará desde casa o no dispondrá de un lugar fijo de trabajo tras la pandemia. En este sentido, para garantizar la productividad de esta fuerza de trabajo remota, el 54% de las empresas españolas considera prioritarias las soluciones de soporte en remoto a sus empleados. Otras herramientas fundamentales señaladas por los responsables de TI españoles son las soluciones de comunicación y colaboración (49%), equipar a los empleados con dispositivos como smartphones, tablets y portátiles (46%) o las aplicaciones de comunicación seguras (45%).



La ciberseguridad, las soluciones de trabajo colaborativo y en la nube, y los dispositivos destacan entre las prioridades de inversión en TI de las empresas españolas. El 84% señala que el portátil es el dispositivo más utilizado por sus recursos humanos para trabajar a distancia, seguido del smartphone y el PC.

ACELERANDO LA DIGITALIZACIÓN

Las empresas españolas siguen asimismo inmersas en la aceleración de su transformación digital, mediante la mejora de sus infraestructuras de TI para apoyar a la nueva fuerza de trabajo híbrida. En este sentido, el 83% de los responsables de TI considera que aumentar la inversión en ciberseguridad es más importante ahora que antes de la pandemia. A continuación, se sitúan las herramientas para trabajo colaborativo (76%), las soluciones en la nube (75%) y el equipamiento de los trabajadores con los dispositivos apropiados, concretamente, portátiles (74%).

El 66% de las empresas españolas encuestadas considera que disponer de un parque amplio de ordenadores portátiles ha cobrado mayor importancia con la crisis sanitaria, siendo este tipo de dispositivo el que más incorporarán a su infraestructura de trabajo a distancia en el próximo año. De hecho, el 84% señala que el portátil es el dispositivo más utilizado por sus recursos humanos para trabajar a distancia, seguido del smartphone (71%) y el PC (52%).

En lo que respecta a las prestaciones clave en estos dispositivos, el 81% de las empresas españolas coloca la seguridad y la conectividad al mismo nivel en el momento de valorar la compra de un portátil. Además, tienen en cuenta el rendimiento (77%), la autonomía (75%), las funciones que favorecen la colaboración (73%) y la portabilidad (69%).

"En el último año, hemos experimentado un cambio sin precedentes en la forma de trabajar, y de nuestra investigación se desprende que las empresas europeas han acelerado su transformación para garantizar que su infraestructura de TI satisface las demandas de una fuerza de trabajo híbrida. En este sentido, el papel del dispositivo está ganando importancia a medida que las organizaciones son conscientes del papel vital que desempeña el hardware -junto con el software adecuado- para garantizar la seguridad, la conectividad y la productividad de los empleados en esta nueva normalidad", asegura Damian Jaume, presidente de Dynabook Europe. ■

MÁS INFORMACIÓN

- El canal de TI español inició el año con unos sólidos ingresos de 351 millones de euros
- Los portátiles siguen registrando fuertes ventas en España en lo que va de año

Crecimiento del gasto en seguridad y gestión de riesgos

En la Encuesta 2021 CIO Agenda de Gartner, la ciberseguridad fue la principal prioridad de gasto, con el 61% de los más de 2.000 CIO encuestados que prevén aumentar la inversión en seguridad cibernética este año. De hecho, la misma consultora prevé que el gasto mundial en tecnología y servicios de seguridad de la información y gestión de riesgos crezca un 12,4% hasta alcanzar los 150.400 millones de dólares en 2021. Los analistas de Gartner, que cifran en un 6,4% el crecimiento del gasto en seguridad y gestión de riesgos en 2020, señalan que la fuerte tasa de crecimiento refleja la continua demanda de tecnologías para trabajadores remotos y seguridad en la nube.

Los servicios de seguridad, incluidos los servicios de consultoría, soporte de hardware, implementación y externalización, representan la mayor categoría de gasto en 2021, con casi 72.500 millones de dólares en todo el mundo. La tecnología integrada de gestión de riesgos (IRM) también está experimentando un crecimiento robusto de dos dígitos como resultado de los riesgos durante la crisis pandémica mundial.

El segmento de mercado más pequeño, pero de más rápido crecimiento, es la seguridad en la nube, especialmente los agentes de seguridad de acceso a la nube (CASB). "El ritmo de la investigación de los clientes indica que CASB es una opción popular para las organizaciones que utilizan la nube", afirma Pingree. "Esto se debe a la creciente popularidad del uso de dispositivos que no son de PC para interactuar con los procesos empresariales principales, lo que crea riesgos de seguridad que se pueden mitigar eficazmente con un CASB. Los CASB también permiten una interacción más segura entre aplicaciones SaaS y dispositivos no administrados."

La nube desempeña un papel fundamental para la mitad de las empresas

Microsoft ha publicado los resultados de un estudio de la Economist Intelligence Unit (EIU) sobre los retos y las oportunidades que la pandemia ha generado en las organizaciones, y la inmensa mayoría de los líderes empresariales señalan la preparación en términos de digitalización como un factor clave en su capacidad de adaptación. "La pandemia de la COVID-19 ha demostrado que las herramientas digitales son esenciales para permitir a las empresas ser ágiles a la hora de responder a las grandes adversidades", declara Michael Gold, director de la Unidad de Inteligencia de The Economist.

Los investigadores han establecido una correlación directa entre la madurez digital de las organizaciones y su capacidad para superar los efectos de una crisis sin precedentes: cuanto más avanzadas están las empresas en su transformación digital, más rápido son capaces de recuperar su actividad y preparar a sus empleados para seguir adelante.

Las empresas más avanzadas en digitalización han demostrado una mayor agilidad a la hora de facilitar el trabajo a distancia, promover la colaboración descentralizada, restablecer las cadenas de suministro e interactuar con los clientes de forma innovadora. Pero, si bien la transformación digital permitió la continuidad del negocio, el estudio también revela carencias en la capacitación, la privacidad, la seguridad y el cumplimiento normativo a medida que las organizaciones avanzan en el uso de nuevas tecnologías.

Independientemente de que estén preparadas o no, las organizaciones de todos los sectores han acelerado sus iniciativas de transformación y han comenzado a depender en mayor medida de las herramientas digitales. En este sentido, el 50% de las organizaciones afirma que la nube

Las herramientas digitales se han convertido en una plataforma indispensable en todos los sectores. Si bien la transformación digital permitió la continuidad del negocio, hay carencias en la capacitación, la privacidad, la seguridad y el cumplimiento normativo a medida que las organizaciones avanzan en el uso de nuevas tecnologías.

desempeña un papel fundamental en sus operaciones en la era COVID. Le siguen las tecnologías que permiten el trabajo en remoto (40%), la inteligencia artificial y el machine learning (33%) y la Internet de las cosas (31%).

Las herramientas digitales se han convertido en una plataforma indispensable en todos los sectores. De acuerdo con el estudio:

❖ El sector del **automóvil** es mucho más propenso a señalar el cambio climático como uno de los principales beneficiados por la transformación digital. Esta industria está invirtiendo en la automatización, la eficiencia de los procesos y la mejora de las competencias digitales de los trabajadores.

❖ Los encuestados del sector **educativo** citan el desarrollo de capacidades y la inclusión como los principales beneficios de la transformación digital, pero les preocupa que la falta de herramientas suponga un obstáculo para el progreso digital, así como la aplicación fragmentada de la tecnología en los distintos departamentos.

❖ Los **servicios financieros** han sido los más preparados digitalmente para hacer frente a los retos que suponen los cierres territoriales y las interrupciones en las cadenas de suministro. Los encuestados fueron los más propensos a estar de acuerdo en que la pandemia demostró la ventaja competitiva de las empresas avanzadas digitalmente.

Amazon y Microsoft continúan dominando el mercado de servicios en la nube

Nuevos datos de Synergy Research Group muestran que el gasto de las empresas en servicios de infraestructura en la nube en el primer trimestre superó los 39.000 millones de dólares, después de haber aumentado en más de 2.000 millones de dólares con respecto al trimestre anterior y un 37% con respecto al primer trimestre de 2020. Por tercer trimestre consecutivo, la tasa de crecimiento interanual aumentó, lo que es inusual para un mercado tan grande y de alto crecimiento.

Microsoft ha ido ganando terreno lentamente a Amazon y la brecha entre sus cuotas de mercado se ha reducido en dos puntos porcentuales en el último año. Juntos siguen representando más de la mitad de los ingresos mundiales en la nube. Más allá de Amazon y Microsoft, los proveedores cuyas tasas de crecimiento superaron el crecimiento general del mercado son Alibaba, Google, Tencent y Baidu, IBM, Salesforce, Oracle, NTT, SAP y Fujitsu, los cuales pueden considerarse proveedores de nicho en comparación con los mayores proveedores de nube.

Con la mayoría de los principales proveedores cloud que han publicado sus datos de ganancias del primer trimestre, Synergy estima que los ingresos trimestrales por servicios de infraestructura en la nube (incluyendo IaaS, PaaS y servicios alojados en la nube privada) fueron de 39.500 millones de dólares. Los servicios públicos de IaaS y PaaS, que crecieron un 39% en el primer trimestre, representan la mayor parte del mercado. El dominio de los principales proveedores de nube es aún más pronunciado en la nube pública, donde los cinco primeros controlan el 80% del mercado. Geográficamente, el mercado cloud sigue creciendo fuertemente en todas las regiones del mundo.

❖ Al **sector público** le resultó más sencillo obtener presupuesto para invertir en digitalización una vez que la pandemia se hizo patente y, en general, priorizó las herramientas que facilitaban el trabajo a distancia y la colaboración. Sin embargo, las carencias en términos de formación y habilidades, así como una posible percepción negativa asociada al despliegue de nuevas tecnologías, siguen siendo obstáculos para la transformación digital.

❖ El sector **sanitario** es el que más se ha transformado con la llegada de la pandemia, especialmente en lo que se refiere a la interacción a distancia. A la vez que se mantenía el estricto cumplimiento de la normativa sobre privacidad, los gestores y el personal sanitario ampliaron y adoptaron con rapidez capacidades virtuales. Todo ello a medida que la presión impuesta por la propia COVID obligaba a aumentar las inversiones.

❖ El sector **industrial** trabajaba ya antes de la pandemia en reducir su déficit de capacitación. La inclusión, el desarrollo de competencias y el cambio climático están entre sus principales preocupaciones, e incide en que la transformación digital puede ayudar a resolverlas.

❖ Los directivos de los **medios de comunicación** han expresado su preocupación por seguir el ritmo del progreso tecnológico y comparten su convicción de que la lucha contra la desinformación será la principal ventaja de la transformación digital en el sector.

❖ El sector **retail** y de **bienes de consumo** ha expresado su optimismo en cuanto a que la transformación digital mejorará las perspectivas de empleo. Además, es el sector más orientado a los beneficios sociales que aporta el cambio hacia modelos de trabajo descentralizados y a distancia. ■

MÁS INFORMACIÓN

- El mercado de infraestructura en la nube registra una nueva subida anual del 35%
- El gasto en servicios de nube pública superará los 332.000 millones de dólares

PaaS, IaaS y SISaaS acaparan la mitad del mercado de servicios de nube pública

El mercado mundial de servicios en la nube pública, incluyendo Infraestructura como servicio (IaaS), Software de infraestructura de sistemas como servicio (SISaaS), Plataforma como servicio (PaaS) y Software como servicio (SaaS), creció un 24,1% interanual en 2020, con unos ingresos de 312.000 millones de dólares, según IDC.

El gasto continuó consolidándose en 2020, con los ingresos combinados de los 5 principales proveedores de servicios en la nube pública (Amazon Web Services, Microsoft, Salesforce.com, Google y Oracle) representando el 38% del total mundial y creciendo un 32% interanual. Gracias a la amplia cartera de ofertas de SaaS y SISaaS, Microsoft comparte ahora la primera posición con Amazon Web Services en el mercado de servicios en la nube pública, con ambas compañías acaparando el 12,8% de los ingresos en 2020.

Si bien el mercado general de servicios en la nube pública creció un 24,1% en 2020, en consonancia con los últimos cuatro años, los segmentos de IaaS y PaaS han crecido a tasas mucho más rápidas. Esto pone de relieve la creciente dependencia de las empresas en la infraestructura en la nube, los datos definidos por software, las soluciones informáticas y de gobierno como servicio y las plataformas nativas de la nube para la implementación de aplicaciones para aplicaciones internas de TI empresariales. IDC espera que el gasto en servicios en la nube fundamentales (especialmente IaaS y PaaS) siga creciendo a un ritmo más alto que el mercado general de la nube, ya que la resiliencia, la flexibilidad y la agilidad guían las decisiones de las plataformas de TI.

La mitad de los CISO españoles se siente en riesgo de sufrir un ciberataque

El año pasado, equipos de ciberseguridad de todo el mundo se vieron ante el desafío de mejorar su estrategia de seguridad de la noche a la mañana en un entorno totalmente nuevo y cambiante. Después de haber vivido un año tan inaudito, son múltiples los retos que tienen que abordar los directores de seguridad de la información (CISOs) en 2021. De hecho, Proofpoint ha publicado el informe Voice of the CISO que revela que el 66% de los CISOs considera que su organización no está preparada para hacer frente a un ciberataque.

El panorama de amenazas está siendo implacable, de ahí que la mitad de los CISOs españoles (50%) se sienta en riesgo de sufrir un ciberataque material, es decir, que tenga impacto en su organización durante los próximos 12 meses. Sobre los tipos de ataques a los que tendrán que enfrentarse, estos señalaron el compromiso del correo electrónico corporativo o Business Email Compromise (25%), el phishing (24%) y el compromiso de cuentas cloud en Microsoft 365 o G suite (22%) como los más probables, junto con las amenazas internas y el ransomware (ambos con un 19%). No obstante, un 12% fue incapaz de predecir cuáles serán

Los ataques BEC, el phishing y el compromiso de cuentas cloud en Microsoft 365 o G suite se consideran los ataques más probables. El 58% opina que su mayor vulnerabilidad en ciberseguridad está en el error humano, y el 63% afirma que el trabajo en remoto ha hecho que su organización sea más vulnerable frente a ciberamenazas.

las mayores amenazas de ciberseguridad que se avecinan por la incertidumbre de la pandemia.

Más de un año después de que la pandemia cambiase para siempre el panorama de amenazas, el 53% de los CISOs españoles siente que su organización no está preparada para hacer frente a un ciberataque dirigido en 2021. Mientras, el riesgo en ciberseguridad va en aumento y un 62% está más preocupado por las repercusiones que pueda tener un ciberataque este año que en 2020.

EL ERROR HUMANO

Pese a que el 58% de los encuestados piensa que los empleados entienden su papel a la hora de proteger la empresa frente a ciberamenazas, el 68% de los CISOs en España sigue considerando el error humano como la mayor vulnerabilidad de su organización. La filtración de datos de forma deliberada (amenaza interna maliciosa), hacer clic en enlaces maliciosos, descargar archivos comprometidos, así como reutilizar o no cambiar contraseñas son los comportamientos que aumentan el riesgo de ataque en las organizaciones.

El 63% de los encuestados coincide en que el trabajo en remoto ha hecho que su organización sea más vulnerable frente a ciberamenazas, con un 56% afirmando haber visto un aumento de los ciberataques dirigidos en los últimos 12 meses. El 61% de los CISOs en España opina que

Las ventas de soluciones de seguridad SaaS en el canal crecen un 11%

Las ventas de productos de ciberseguridad de software como servicio (SaaS) en el canal aumentaron en los primeros tres meses de 2021, mientras que los ingresos de seguridad de redes y endpoints repuntaron a principios de abril, según los últimos datos de Context. En términos de países individuales, Francia (41%) tuvo el comienzo de año más fuerte en términos de gasto en seguridad SaaS, con el Reino Unido (14%) e Italia (11%) también con un buen desempeño, mientras que en España hubo una caída del 27%.

Mientras que las ventas de productos de seguridad para endpoints a través de la distribución cayeron un 21% y las ventas de seguridad de red cayeron un 12% interanual en el primer trimestre, el gasto en seguridad en la nube aumentó casi un 11% durante el mismo período. Esto podría deberse a la tendencia de trabajar desde casa durante el bloqueo, lo que llevaría a las empresas a invertir en ofertas de SaaS para garantizar que los empleados que trabajan a distancia y sus dispositivos permanezcan protegidos.

Dentro del mercado de seguridad en la nube, el mayor crecimiento interanual fue para el segmento de prevención de pérdida de datos (138%), seguido de la gestión de control (98%), la seguridad del correo (27%) y la seguridad de red (20%).

el cibercrimen pasará a resultar más rentable para los atacantes, aunque el 64% añade que dicha actividad podría conllevar mayores riesgos.

En general, los CISOs españoles esperan que los presupuestos de ciberseguridad aumenten un 11% o más en los próximos dos años, y dos de cada tres (65%) se ven capaces de resistir y recuperarse mejor de los ciberataques en 2023. Entre sus prioridades en este plazo está incrementar la concienciación sobre seguridad de los empleados (29%), perfeccionar también los controles de seguridad básicos (28%), así como consolidar las soluciones y controles de seguridad existentes (25%).

EL AISLAMIENTO DEL CISO

El 52% de los encuestados en España califica las expectativas en torno a sus funciones como excesivas. Según el estudio de Proofpoint, persiste asimismo entre los CISOs una sensación de falta de apoyo por parte de otros directivos, ya que solo un 22% afirma rotundamente que la junta directiva de su organización está alineada con ellos en asuntos de ciberseguridad.

Para Lucia Milica, CISO global residente de Proofpoint, "dado que el futuro laboral será cada vez más flexible, estos retos seguirán estando presentes de aquí al próximo año o incluso más. Por eso, además de proteger nuevos puntos de ataque y formar a los usuarios para el trabajo en remoto o híbrido a largo plazo, los CISOs deben infundir confianza entre clientes, stakeholders internos y el propio mercado para que vean estas opciones como factibles de manera indefinida". ■

El 75% de las pymes esperan que los ciberataques sean más frecuentes

Los ciberataques se han vuelto habituales en nuestro día a día. Sólo el pasado año el Instituto Nacional de Ciberseguridad (INCIBE) registró 130.000 incidentes graves en ciberseguridad, además de un aumento del 80% de ciberataques con casi 40.000 ataques diarios. Las previsiones indican que esta cifra seguirá aumentando, ya que los hackers están poniendo el foco en aquellas organizaciones que no están tan protegidas y que suelen responder a un perfil de pequeña o mediana empresa. Es más, de acuerdo con el "State of Website Security and Threat Report", el 75% de las pymes cree que los ataques ocurrirán con más frecuencia en 2021. Los expertos de Excem Technologies han identificado los cuatro principales riesgos que sufren las pequeñas y medianas empresas en estos entornos: ransomware, automatización de los ataques, ciberespionaje y ataques en el entorno cloud.

MÁS INFORMACIÓN

- La ciberseguridad es esencial para salvaguardar los activos y la continuidad del negocio
- La inversión en ciberseguridad superó a otros segmentos de la industria TI en 2020
- El mercado de la ciberseguridad superará en España los 1.300 millones de euros en 2021

DESCUBRE LAS **TENDENCIAS** QUE DEFINEN EL **FUTURO DIGITAL**

it TRENDS

IA e IoT
nuevas oportunidades, nuevos retos

Poco a poco, dos tendencias emergentes de los últimos años han ido conquistando espacios en el negocio. Primero, en las páginas de los medios de comunicación como tecnologías de futuro. Después, en los planes estratégicos a largo plazo de las compañías, que veían el potencial pero no acababan de tener claro la monetización de los proyectos. Por último, la Inteligencia Artificial y la Internet de las Cosas han aterrizado en las líneas de negocio y en los proyectos a poner en marcha por las compañías, y el canal de distribución no puede dejar escapar la oportunidad.

Pero antes de entrar en materia, quisimos saber si realmente en el día a día de los resellers la Inteligencia Artificial y la Internet de las Cosas son realidades palpables, con proyectos e ingresos, o líneas a desarrollar con gran potencial de crecimiento. Y, para eso, nada mejor que preguntar a las empresas que están en el mercado, que palpan a diario la realidad del canal de distribución.

En este sentido, Gabriel Maestroarena, director de la Organización de Partners en Cisco España, nos comenta que "son una realidad que sigue evolucionando. La IA, junto a otras tecnologías como Big Data e IoT, contribuyen a acelerar los procesos de transformación digital. IA es una tecnología transversal a cualquier proyecto en el que se manejen grandes cantidades de datos, mientras IoT se integra cada vez más en todo tipo de sectores. Según el último Cisco Annual Internet Report, en 2023 habrá 29.300 millones de dispositivos conectados, y la mitad serán conexiones M2M. En España habrá 350 millones de dispositivos conectados, y el 62% pertenecerán al IoT. Los sectores donde IoT crece con mayor rapidez son utilities, principalmente smart grids o redes eléctricas inteligentes; industria, por la monitorización de activos; y transporte/gestión de flotas. Y las áreas emergentes con mayor potencial son sector público, con las smart cities y los servicios ciudadanos; y atención sanitaria, con monitorización remota de pacientes mediante sensores biomédicos".

Según nos comenta Heraclio Sánchez, director general de Diode, "aún queda mucho por avanzar en este sentido. La gran mayoría de las empresas tienen intención de incorporar IoT en sus nuevos proyectos, pero aún son pocas las que se animan a evaluarlo. En GTI-Diode, como mayorista consolidado en Identificación Automática, Comunicaciones e IoT, y recientemente parte de V-Valley, área de Advanced Solutions de Esprinet, podemos acometer exitosamente proyectos de cualquier tamaño en diferentes mercados verticales lo que nos permite acercarnos a clientes de múltiples sectores".

En palabras de Anselmo Trejo, director de marketing y comunicación de D-Link Iberia, su compañía "ya ha lanzado en el canal soluciones completas de IoT, como la plataforma D-Link Edge Cloud Solutions, un avanzado ecosistema para gestionar redes interiores o exteriores con nuestros routers 4G industriales M2M (Machine to Machine) específicos para la comunicación por datos móviles entre dispositivos de IA e IoT, tales como sensores, cámaras, robots, sistemas de control de accesos...".

Para Alberto Pérez Cuesta, business development director de Exclusive Networks Iberia, "quizá por posicionamiento histórico y por ser especialmente fuertes en el mundo de la ciberseguridad, percibimos ambas revoluciones desde una perspectiva: la protección, que suele llegar tarde a este tipo de innovaciones, tanto en el ámbito de las infraestructuras Cloud e hiperconvergentes, soluciones naturalmente óptimas y muy

beneficiosas para ambos entornos, como en lo referente a infraestructuras web scale o 'edge clusters'. Sin embargo, sí empiezan a surgir múltiples soluciones que hacen uso de la IA como motor interno, con sus innatas ventajas, y de soluciones que se han adaptado a los matices y complejidades de la diversidad de dispositivos y protocolos del ámbito IoT".

También la seguridad es el hilo conductor de las palabras de José Antonio Morcillo, director de canal de Kaspersky Iberia, que apunta que "distintos informes apuntan a que el número de proyectos de IoT sigue creciendo a un ritmo imparable. Pero un informe realizado por Kaspersky dejó en evidencia que, pese a este mayor interés, no todas las organizaciones se sienten preparadas para hacer frente a las amenazas en este campo. De hecho, solo el 18% de las empresas europeas ha implantado una vigilancia activa de la red y el tráfico, y únicamente el 16% ha introducido la detección de anomalías en la red, ambas son soluciones que permiten a los equipos de seguridad rastrear las anomalías o la actividad maliciosa en los sistemas IoT".

Finaliza esta primera ronda de opiniones Fernando Feliu, director de global customer solutions, V-Valley, que lo resume diciendo que es "más de lo que parece y menos de lo que debería". Ya se están implementando muchos proyectos donde la IA se incluye a la vez que IoT. Un ejemplo son sectores como industria, donde tenemos casos de cárnicas con secaderos ya inteligentes o el tratamiento de calidad del agua; agricultura, con regadíos inteligentes o bodegas donde la IA y el IoT están implementados; el sector farmacéutico o en hospitales; o las Smart Cities, con regulación de iluminación o control de la contaminación acústica y de calidad del aire por ejemplo... Pero, indiscutiblemente, queda mucho por hacer y sólo una pequeña parte del canal se ha implicado en el desarrollo de proyectos".

> La **IA**, junto a otras tecnologías como **Big Data** e **IoT**, contribuyen a acelerar los procesos de **transformación digital**
>
> Gabriel Maestroarena, director de la Organización de Partners en **Cisco** España

EL ROL DEL CANAL

La pregunta que nos hacemos en este punto es, ¿Cuál debe ser el papel del canal en estos proyectos? ¿Cómo pueden ayudar en la aceleración de estos? Tal y como nos explica José Antonio Morcillo, "es un hecho

que, a medida que crecen los proyectos de digitalización, aumenta la conciencia de los riesgos asociados. Desde el punto de vista de la ciberseguridad, el papel a desempeñar por el canal es siempre de asesoramiento experto y de propuesta de las soluciones y herramientas que ayuden a asegurar esos proyectos ajustándose al máximo a las necesidades de cada cliente. De acuerdo con el mismo informe antes señalado, para más de un tercio de las empresas europeas (35%), los ataques IoT se han convertido en una de sus principales preocupaciones en materia de ciberseguridad, superando a amenazas tan graves como las brechas de datos (10%) o los ataques a la cadena de suministro (20%). Y para hacerles frente se requiere cada vez más la participación de profesionales de la seguridad, no sólo de los equipos de TI. Es aquí donde un canal formado y capacitado resulta esencial para colaborar con sus clientes y apoyarles en este camino".

También es consciente del protagonismo del canal Anselmo Trejo, que apunta que, "sin duda, el integrador o el proveedor de servicios juega un papel clave, puesto que muchas veces desarrollan plataformas o software de integración de soluciones con IA y gestión de dispositivos IoT con las que consiguen captar la atención de muchas entidades, tanto públicas como privadas".

Para Fernando Feliu, "el canal debe informarse de las posibilidades que abre este campo de desarrollo para el futuro, ya que promete una implementación rápida y duradera. Además las ayudas de NextGeneration UE y el rápido retorno de la inversión, hacen que sean proyectos muy interesantes, siempre y cuando haya un cambio de mentalidad en la implementación de los mismo. La mayoría de los fabricantes están trabajando en aportar soluciones hacia el Edge y cómo securizar la información aportada, pero también en cómo poner de una forma sencilla las herramientas necesarias para los proyectos en un entorno consistente".

En opinión de Alberto Pérez, "inicialmente, se requiere inversión en la formación de ingenieros multidisciplinares que, con una base sólida de conocimientos de ciberseguridad, sean capaces de entender los nuevos entornos y sus vulnerabilidades, para encontrar y diseñar las estrategias de protección más idóneas. Después, es muy importante la búsqueda de soluciones más innovadoras que realmente nazcan con un enfoque adecuado. Y, por último, para lograr economizar sus propuestas, es muy probable que convenga una cierta industrialización de estos servicios, con la definición de SLA completos que permitan llegar a los clientes de manera más fácilmente consumible y adecuada a sus necesidades".

Para Heraclio Sánchez, "el elemento más importante es la labor pedagógica. Los clientes aún no saben cómo incorporar IoT en sus proyectos y qué retorno pueden obtener de estas soluciones. Los proyectos en IoT deben orientarse mucho más desde las posibilidades de negocio que abren, y no sólo eficiencias en procesos, como solía ser el caso en los proyectos tecnológicos".

Concluye esta ronda de opiniones Gabriel Maestroarena, señalando que, "en el caso de Cisco, tanto nuestros mayoristas como resellers, integradores y SP, con grandes capacidades para construir soluciones personalizadas y para segmentos verticales, tienen una gran oportunidad para ayudar a las organizaciones a provechar las ventajas de IA y del IoT, eliminando la complejidad y respondiendo a los retos de escalabilidad, flexibilidad y seguridad".

CAMINO POR RECORRER

A la vista de sus opiniones, parece que el canal ya ha iniciado el camino, pero toda-

"El elemento más importante es la **labor pedagógica.** Los clientes aún no saben **cómo incorporar IoT en sus proyectos** y **qué retorno** pueden obtener de estas soluciones"

Heraclio Sánchez, director general de **Diode**

vía queda mucho por recorrer. Pero ¿cuándo podremos decir que estos proyectos son fuentes de negocio claras y constantes para el canal?

Gabriel Maestroarena apunta que "desde nuestra experiencia, las organizaciones con mayor éxito en IA e IoT son las que se apoyan en el ecosistema de partners en cada fase del proyecto, contemplando desde la planificación estratégica hasta la entrada en producción. Los servicios son fundamentales, y nuestros partners con la especialización Customer Experience (CX), diseñada para dar soporte a los clientes finales a través de todo el ciclo de vida, tienen una gran oportunidad en estos segmentos de mercado. A través de Digitaliza, el programa de aceleración digital de Cisco para España, y de nuestros Laboratorios de Innovación, hemos impulsado diversos proyectos colaborativos de IA y de IoT. Por ejemplo, hace dos años en Sevilla probamos, en colaboración con el Ayuntamiento de Sevilla, Bosch y Ferrovial y otros partners, un innovador sistema IoT de control de afluencia de personas y de iluminación inteligente en la ciudad. Y en Granada nos apoyamos en el IoT, junto al Ayuntamiento, Ferrovial Servicios y otros partners, para optimizar la recogida de residuos mediante analítica de datos en tiempo real. En el sector industrial también estamos trabajando en proyectos de IA donde convergen las TO con las TI. Y es que en el caso de IA, hemos anunciado recientemente junto a Intel un proyecto basado en Federated Learning para que tres hospitales de referencia, Ramón y Cajal, 12 de Octubre y Sant Pau, puedan compartir conocimiento y

> El integrador o el **proveedor de servicios** juega un **papel clave**, puesto que muchas veces **desarrollan plataformas o software de integración de soluciones con IA** y **gestión de dispositivos IoT** con las que consiguen captar la atención de muchas entidades
>
> Anselmo Trejo, director de marketing y comunicación **D-Link** Iberia

dar soporte al diagnóstico de Covid-19 respetando la privacidad de los pacientes. En el proyecto colaboran también Capgemini Engineering, Vodafone España y Gilead".

"Además", continúa, "hay muchas otras áreas donde IA/ML es parte fundamental de la solución. Cisco la integra en toda su oferta, incluyendo Webex. Nuestras redes basadas en la intención (IBN) también utilizan IA/ML para adelantarse a las necesidades de los usuarios y optimizar la aplicación de políticas, mientras en ciber-seguridad Cisco StealthWatch se apoya en esta tecnología para detectar ataques, incluyendo los ocultos en tráfico cifrado".

Desde el punto de vista de Alberto Pérez, "realmente son avances importantes en el ámbito de la manida transformación digital, y serán claves en nuevos modelos de negocio que aún siquiera podemos imaginar. Es por ello por lo que el sector tecnológico habrá de evolucionar más hacia un modelo de ingeniería, similar al del sector industrial, para poder sacar el máximo provecho y rendimiento de negocio".

En palabras de Fernando Feliu, "el punto de inflexión llegará cuando el canal conozca las soluciones de los diferentes fabricantes y de le den un contexto de implementación a sus clientes. Es una gran oportunidad de up-selling en clientes, de búsqueda de nuevas oportunidades y de diferenciación respecto a la competencia, que al final son conceptos que los resellers están buscando. Lo que está claro es que la implementación de 5G será un paso definitivo en la compartición de tanta información como se generará en el futuro".

Más optimista es Anselmo Trejo, que comenta que "ya lo estamos viendo actualmente con algunos casos de éxito que hemos transformado en beneficios reales, como la integración de nuestros routers 4G M2M, los DWM-312, en los vagones de trenes de Metrovalencia FGV para las comunicaciones del sistema de control de aforo, CappaCV, desarrollado e implantado por nuestro partner Dioxinet. Gracias a este sistema se ha dotado a Metrovalencia de un sistema inteligente de control de aforo y la demanda de esos sistemas no ha hecho más que empezar, porque, con o sin pandemia, dotar de sistemas de aforo o de analítica de tráfico será cada vez más esencial".

En palabras de Heraclio Sánchez, "todo cambiará cuando entiendan que los pro-

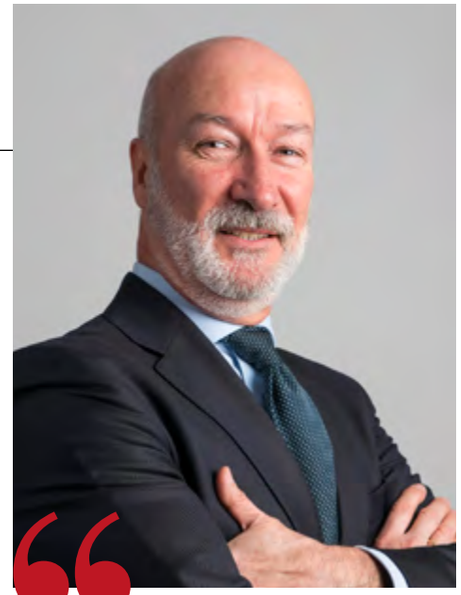
> "Empiezan a surgir **múltiples soluciones que hacen uso de la IA como motor interno**, con sus innatas ventajas, y de **soluciones que se han adaptado** a los matices y complejidades de la diversidad de **dispositivos y protocolos del ámbito IoT**"
>
> Alberto Pérez Cuesta, business development director de **Exclusive Networks** Iberia

yectos de IoT no se evalúan de la manera tradicional de cualquier proyecto tecnológico anterior. Los impulsores de estos proyectos deben localizarse más en áreas de marketing o desarrollo de negocio de las empresas, más allá de TI".

Según José Antonio Morcillo, "en Kaspersky llevamos muchos años defendiendo que la solución para que los proyectos de IoT sean una apuesta decidida por parte de las empresas, pasa porque la mayoría de los dispositivos IoT cuenten con seguridad desde el primer momento. Hasta la fecha eso no ocurre y son susceptibles de ser atacados y convertirse en vectores de entrada para el malware. Por este motivo, el concepto de ciber inmunidad de Kaspersky es realmente clave. Con ciber inmunidad nos referimos a construir diversas soluciones tecnológicas teniendo la seguridad en cuenta desde su concepción y diseño. Las soluciones ciber inmunes son capaces de resistir la inmensa mayoría de los ciberataques. En este sentido, recientemente hemos presentado nuestro primer producto ciber inmune, Kaspersky IoT Secure Gateway 100, en Hannover Messe 2021. Muy pronto habrá más productos ciber inmunes basados en KasperskyOS, el sistema operativo ciber inmune desarrollado por Kaspersky para dispositivos de red, sistemas de control industrial e Internet de las Cosas, que traerán un cambio de paradigma al mercado".

LO QUE EL CANAL NECESITA

Como para todas las oportunidades que se van presentando en el mercado, los resellers deben estar preparados. Tal y como nos explica Fernando Feliu, "crear nuevas oportunidades de negocio implica dar un enfoque diferente y creativo al que daríamos tradicionalmente. Esto nunca ha sido más real que con el tema que tratamos hoy. El cambio de mentalidad en la presentación de proyectos de IA con IoT supone una "revolución" a la forma de trabajo tradicional, con los que se puede optimizar los recursos existentes y conseguir estabilizar los procesos de una forma realmente impresionante con una inversión que tiene asegurada su retorno. Una vez que se tiene esto, lo que se necesita es poder acceder de forma sencilla a la información y a la formación de las necesidades de este tipo de proyectos. Esta es una labor que el mayorista debe hacer, y en el caso de V-Valley lo estamos ya realizando para poder abrir los ojos a como desarrollar y plantear a los clientes este tipo de negocios".



> "Distintos informes apuntan a que el número de **proyectos de IoT sigue creciendo** a un ritmo imparable"
>
> José Antonio Morcillo, director de canal de **Kaspersky** Iberia

Para Alberto Pérez, "hasta el momento, ambas corrientes son tan sumamente abiertas y poco definidas, que es difícil trazar una hoja de ruta de formación y capacitación. Conviene empezar por la asunción de los principales estándares y protocolos, con las opciones de despliegue Open Source más abiertas y sus integraciones más habituales, con el ánimo de disponer de una buena base de conocimientos, con solidez suficiente como para ir adoptando las nuevas tendencias de las soluciones que vayan surgiendo y transformando cada uno de ellos. Y, a partir de ahí, la máxima inmersión posible en los proyectos internacionales que se publiquen, con el ánimo de extrapolar a nuestro mercado y ser capaces de ir dotando del máximo nivel de funcionalidad, incluyendo la protección de los proyectos que surjan".

En palabras de Heraclio Sánchez, "existen dos vías fundamentales en las que centrarse: por un lado, el apartado tecnológico y, por otro lado, la parte de negocio. La exitosa implementación de soluciones IoT exige a los resellers desarrollar sus capacidades en áreas tecnológicas muy distintas: la sensorización, las comunicaciones, el software y la seguridad. Pero, no podemos olvidar que en paralelo los integradores han de ser capaces de encontrar la monetización de esos proyectos y construir propuestas atractivas para los clientes".

En opinión de José Antonio Morcillo, "evidentemente, lo primero que tiene que hacer el partner para consolidar este tipo de proyectos como una línea de negocio fuerte y con proyección de futuro es formarse. Los clientes necesitan confiar en un canal formado, especialista en ciberseguridad y que sea autónomo a la hora de ofrecer la mejor solución posible. Por eso, y con el objetivo de que los clientes reciban siempre las mejores soluciones y servicios por parte de nuestros partners, hemos diseñado el Programa de Capacitación para el Canal (PCC), para facilitar formación personalizada a cada tipo de partner, mostrarles cómo ir aumentando su nivel de conocimiento paso a paso y, en consecuencia, mantener un contacto constante con ellos y generar lealtad hacia la marca".

Explica Anselmo Trejo que "deben contar con ingenieros especialistas en redes IoT y, en especial, en la tecnología M2M y protocolos tales como SNMP, TR069, TR098, CPE/ACS, MQTT, GPX metadata… todos ellos indispensables a la hora de crear un proyecto de IA o IoT, tanto en un entorno de Smart City como en cualquier otro proyecto".

Desde la perspectiva de Gabriel Maestroarena, "Cisco ha creado un ecosistema de partners de IoT y de IA bien estructurados, mediante completos programas de certificación, formación y especialización, para que se conviertan en asesores de confianza en los proyectos. También contamos con un amplio ecosistema de partners tecnológicos, ISV y proveedores de servicios para optimizar los proyectos de para organizaciones de múltiples sectores como fabricación, transporte, energía, comercio minorista o administraciones públicas". ■

MÁS INFORMACIÓN

- The State of Industrial Cybersecurity in the Era of Digitalization
- Cisco Annual Internet Report

"Crear nuevas oportunidades de negocio implica dar un enfoque diferente y creativo, y esto **nunca ha sido más real que con la IA e IoT"**

Fernando Feliu, director de global customer solutions, **V-Valley**

Fondos Europeos para los Planes de Digitalización

https://hub.gti.es/AyudaFondosEuropeos/

Los fondos europeos para los planes de digitalización de PYMES, Administraciones Públicas y Competencias Digitales van a estar disponibles a partir del segundo semestre de 2021. Es el momento de que prepares todo lo necesario para poder aprovechar esta oportunidad de negocio sin precedentes.

Prepárate para sacar partido a las ayudas #NextGenerationEU

INFORMACIÓN | SESIONES ONLINE | DOCUMENTACIÓN

FORMACIÓN EN TECNOLOGÍA | GESTIÓN DE AYUDAS

Acronis · Hewlett Packard Enterprise · IBM · Microsoft · Microsoft Surface · poly · Red Hat · ribbon · TREND MICRO · VERITAS · WatchGuard · vmware

V-Valley the Value of exprinet · GTI Software & Networking · DIODE

Ahora más que nunca, como partner, tienes una posición estratégica y privilegiada en la recuperación de nuestra economía. Nosotros vamos a ayudarte: *https://hub.gti.es/AyudaFondosEuropeos/*

DEBATES IT:

Oportunidades para el canal de TI en torno a los Fondos Europeos de Recuperación

Según un reciente estudio de KPMG, en colaboración con la CEOE, el 45% de las empresas españolas quiere optar a los Fondos del Plan Europeo de Recuperación Next Generation EU, dotado con 750.000 millones de euros, de los que 140.000 han sido asignados a España. Sin embargo, existe un gran desconocimiento sobre cómo funcionan y cómo se pueden presentar los proyectos, lo que abre una ventana de oportunidad al canal de distribución, como vehículo transmisor entre las empresas y estos fondos.

Por este motivo, de la mano de GTI V-VALLEY, hemos querido debatir sobre las principales oportunidades de negocio que se le van a abrir al canal tecnológico en España, gracias a estos Fondos Europeos de Recuperación y, para ello, hemos organizado dos #DebatesIT centrados en esta temática con los portavoces de destacadas empresas en el panorama tecnológico español.

En el caso del primer debate, contamos con la participación de Roberto Alonso, Cloud & Business Director de GTI V-VALLEY; Santi Oller Jiménez, Spain Partner Business Development Director, Microsoft Ibérica; Juan Carlos Gentou, DAM Iberia and Italy, Poly; Miguel Ángel Díaz, BDM Openshift & Application Services, Red Hat; Rafael Vicent, Senior Channel Account Manager, Ribbon; Alberto Fernández, Manager Channel Sales - Southern EMEA & UK, TeamViewer; y Carlos Vieira, Country Manager, Watchguard, con quienes debatimos sobre las oportunidades que se le abren a los resellers alrededor de estos fondos.

El mismo foco pusimos en el segundo de los DebatesIT, en esta ocasión de la mano de Roberto Alonso, Cloud & Business Director de GTI V-VALLEY; Rafael Pestaña, Director del área HPE Centric de V-Valley; Alessandro Perotti, Channel Manager, Italy & Iberia, Acronis; Francisco López, HPE Greenlake Southern Europe Service Providers Lead; Fernando Suárez León, IBM Partner Ecosystem Leader; Carolina Castillo, Director One Commercial Partner Organization and Small, Medium, Corporate Business at Microsoft; Alexandre Tovar, Channel Account Manager, Trend Micro; y Jorge Sáez, Distribution Success Manager Iberia, Veritas.

Oportunidades para el canal de TI en torno a los Fondos Europeos de Recuperación (I)

Para hablar de esta realidad, contamos con la participación de Roberto Alonso, Cloud & Business Director de GTI V-Valley; Santi Oller Jiménez, Spain Partner Business Development Director, Microsoft Ibérica; Juan Carlos Gentou, DAM Iberia and Italy, Poly; Miguel Ángel Díaz, BDM Openshift & Application Services, Red Hat; Rafael Vicent, Senior Channel Account Manager, Ribbon; Alberto Fernández, Manager Channel Sales - Southern EMEA & UK, TeamViewer; y Carlos Vieira, Country Manager, Watchguard, con quienes debatimos sobre las oportunidades que se le abren a los resellers alrededor de estos fondos.

UNA GRAN OPORTUNIDAD

En primer lugar, quisimos conocer las valoraciones de Roberto Alonso sobre estas oportunidades y retos que se abren para el canal de distribución tecnológico español. Tal y como destacaba este responsable, "desde el grupo Esprinet/V-Valley, al que pertenecemos como parte de valor, pensamos que nos acercamos a un hito en el sector. Es cierto que si pensamos cómo nos ha afectado la pandemia, hablamos mucho de cómo ha respondido el canal ante esta movilización y digitalización para que todo el mundo pueda trabajar desde casa, pero ahora nos enfrentamos a otra situación que también incorpora cierta responsabilidad, porque hay algo de lo que hablamos mucho, la digitalización de la PYME, y ahí pensamos que el canal es clave. Porque el canal es clave y responsable de que el tejido empresarial sea más competitivo e innovador, y aproveche todas las ventajas de la tecnología. Nosotros, desde GTI V-Valley, queremos acompañar y dar el soporte que damos siempre a todos nuestros partners, dividiéndolo en tres fases: dar a conocer cómo funcionan las ayudas para

DEBATE IT: Oportunidades para el canal de TI en torno a los Fondos Europeos de Recuperación (I)

Los Fondos Europeos de Recuperación abren una gran oportunidad para que el canal de distribución tecnológico aproveche un negocio significativo pero, además, para poder estar más cerca de sus clientes ayudándoles a desarrollar proyectos y acciones encaminadas a avanzar en sus procesos de digitalización e innovación.

que los interesados puedan estar preparados, capacitar a nuestros partners en nuevas tecnologías y soluciones que requieren estos conocimientos, y el soporte, que va un paso más allá de lo tradicional, porque se necesita conocer la metodología de estas ayudas que, además, se prolongarán en el tiempo". "En definitiva", concluye Roberto Alonso, "es una gran oportunidad que tenemos que aprovechar todos como canal de distribución".

DIGITALIZACIÓN DE LA PYME Y LA ADMINISTRACIÓN PÚBLICA ESPAÑOLA

Partiendo del entorno en que van a llegar estos fondos europeos, quisimos saber, en primer lugar, qué valoración hacían los diferentes portavoces en este DebateIT del nivel de digitalización de la PYME y la Administración Pública en España y cuál esperan que sea la evolución en los próximos trimestres.

Tal y como comenta Santi Oller, de Microsoft, "han pasado muchas cosas en los últimos meses, pero intentaría destacar dos momentos. En febrero de 2020 veía un informe de CEPYME en el que se señalaba que solo el 19% de la PYME española contaba con comercio electrónico, lo que me llevó a preocuparme un par de meses después con la capacidad de supervivencia de los que no podían ofrecer sus productos y servicios de forma on-line. Pero esto era solo un ejemplo. Antes de la pandemia nos faltaban áreas a desarrollar en la digitalización. Quizá las partes más básicas estaban superadas, pero lo importante era ver el grado de digitalización. Pero en estos meses hemos vivido un empujón para que muchas empresas se digitalizasen sí o sí. Bien para que los trabajadores se fueran a casa a trabajar o bien para que muchas empresas tuvieran en escaparate al mercado a través del comercio electrónico. Se han hecho muchas cosas, algunas de forma acelerada, pero la consciencia de la necesidad se ha visto reforzada y ya no hay dudas con respecto a la digitalización. De todas formas, hay sectores que están más digitalizados y otros lo están menos. Algunos se han visto muy impactados y han hecho mucho en poco tiempo, aunque todavía no han acabado, y otros que todavía tienen que madurar su propia digitalización".

Para Juan Gentou, de Poly, "en estos meses ha habido una aceleración de la Transformación Digital. Lo que se esperaba en dos o tres años se ha tenido que hacer en uno. Hemos avanzado en una forma un tanto atropellada, pero ahora estamos en un punto en que las empresas y los empleados sabemos lo que necesitamos. Muchas empresas han adquirido soluciones sin la formación necesaria, de ahí que hayamos tenido que ayudarles mucho en este aspecto, de la mano del canal. Pero a día de hoy, alrededor del 90% de las empresas ya tienen parte de su personal trabajando en remoto, muchos de ellos seguirán, lo que abre una oportunidad importante, pero hay mucha labor de ase-

> El **canal** es clave y responsable de que el **tejido empresarial sea más competitivo** e innovador, y aproveche todas las **ventajas de la tecnología**
>
> Roberto Alonso,
> Cloud & Business Director de **GTI V-Valley**

soramiento por realizar, además de cierta adaptación de las soluciones".

Según Miguel Ángel Díaz, de Red Hat, "Vodafone ha presentado un informe recientemente sobre el nivel de digitalización del Sector Público y las PYMES, y la verdad es que no aprueban. Cierto es que, con la pandemia, ha habido una aceleración, y alrededor del 84% de las empresas y entidades públicas están abordando ahora esos proyectos. Hay que diferenciar dos ejes, por una parte, que las empresas y las entidades públicas accedan a entornos remotos, pero, por otra, y ahí pensamos que hay más retraso, si bien es donde estos fondos europeos vienen a ayudar, es en la Transformación Digital. No es que utilices tecnología, sino usarla para mejorar procesos y ser más eficiente. Y en este viaje, según el citado informe, el 47% dice que tiene un freno: la falta de capacitación tecnológica. Notamos que hay mucha falta de formación, y en esa línea estamos trabajando, para llevar esta capacitación a las pequeñas y medianas empresas. Así que entre el empujón que ha supuesto la pandemia, los fondos europeos y la concienciación de la necesidad de digitalización, pensamos que la Transformación Digital va a despegar en los próximos meses. Somos optimistas al respecto".

Rafael Vicent, de Ribbon, añade que "todos los años hacemos una encuesta sobre la realidad de las empresas en torno a su grado de adopción de tecnologías, y estas encuestas corroboran lo que ya sabemos todos, y es que esta crisis ha forzado la adopción más rápida de estas estrategias digitales. En estas encuestas vemos que las grandes empresas ya tenían definidas estrategias de transformación, pero la pandemia ha abierto una gran oportunidad para nosotros y nuestro canal para ayudar a los clientes a que puedan adoptar este tipo de soluciones".

Apunta Alberto Fernández, de TeamViewer, que "en el último año hemos visto que muchos han avanzado muy rápido, pero no siempre con cabeza. Posiblemente las PYMES más pequeñas han reaccionado mejor, porque sus necesidades básicas eran menores, pero las de tamaño medio y las Administraciones Públicas de menor tamaño no han adoptado realmente lo que necesitaban, lo que abre un período de consolidación, más que digitalización, de una transformación bien hecha, en la que deben tener en cuenta aspectos como la seguridad y todo lo relacionado con la forma de crecer de forma competitiva. Todas las tecnologías están ayudando, pero las empresas ahora deben saber cómo van a afectarles los fondos y cómo pueden aprovecharlos, y creo que nos encaminamos hacia un modelo MSP donde el canal debe ser un facilitador para sus clientes. Hace algunos años hubo algunos fondos europeos asociados al networking y muchos se perdieron porque no se asesoró bien a los pequeños ayuntamientos para solicitarlos y aprovecharlos. Y esto es en lo que también podemos ayudar, en esta información y guía, y ahí debemos enfocarnos".

> **"Se han hecho muchas cosas, algunas de forma acelerada, pero la consciencia de la necesidad se ha visto reforzada y ya no hay dudas con respecto a la digitalización"**
>
> Santi Oller Jiménez, Spain Partner Business Development Director, **Microsoft** Ibérica

Finalizamos con el área de seguridad y, en este sentido, Carlos Vieira, de WatchGuard, comenta que "desde marzo hasta verano, todas las empresas han intentado securizar los entornos para que los trabajadores pudieran conectarse desde su casa. Fue un primer paso de digitalización de muchas empresas, haciendo en semanas lo que no se había hecho en años. Gracias a este esfuerzo, muchas empresas han podido seguir trabajando y ahora siguen desarrollando su labor. Tras este primer empujón, se ha avanzado de una manera un tanto más ordenada. De cara al futuro, creo que queda mucho por hacer y hay que trabajar para llevar estos fondos a las empresas más pequeñas y las Administraciones Públicas. Ambas tienen mucho camino por delante. Pero no podemos olvidar que algunos de estos proyectos se están retrasando a la espera de los fondos europeos, lo que puede afectar a la velocidad de esta transformación. En resumen, mucho trabajo por hacer y, sobre todo, conseguir que los fondos lleguen y se aprovechen correctamente".

¿ESTÁ EL CANAL DE DISTRIBUCIÓN PREPARADO PARA ESTE RETO?

El canal de distribución TIC se ha tenido que adaptar, de forma sucesiva, a muchas situaciones y realidades, y ahora tiene ante sí un reto significativo: ayudar a los clientes con proyectos que se articularán a través del Plan Nacional de Digitalización de las PYMES. La pregunta es, ¿está preparado?

Según Carlos Vieira, "es posible que surjan empresas especializadas en este terreno, pero el canal debe aprovechar esta oportunidad de ayudar a nuestras empresas a aprovechar estos fondos para recuperarse de la situación que hemos vivido. El canal va a ayudar a transmitir este mensaje, y debe estar capacitado para poder transmitir a sus clientes la necesidad de esta transformación, tanto en el área de la ciberseguridad como en otras áreas del negocio. Va a ser necesaria la colaboración de todos los agentes implicados, y el canal va a tener que estar preparado para transmitir este mensaje a sus clientes".

Para Miguel Ángel Díaz, "el canal es un ente de gran tamaño, así que hablaré del canal con el que interactuamos en Red Hat, y, dentro de éste, hay dos grupos: los grandes integradores de sistemas, que tienen los conocimientos y las capacidades, y ya se están preparando; y el resto, las empresas medianas, necesitan todavía cierta preparación, y se apoyan mucho más en nosotros. Y ahí sí hay trabajo por hacer, para prepararlos y llevar esto después a las empresas".

> "En estos meses ha habido una **aceleración de la Transformación Digital**. Lo que se esperaba en dos o tres años se ha tenido que hacer en uno"
>
> Juan Carlos Gentou, DAM Iberia and Italy, **Poly**

Se muestra de acuerdo Rafael Vicent, que apunta que el canal es muy variado "y donde, quizá, más trabajo tenemos que hacer es en la pequeña y mediana empresa, y quizá el partner que se centra en las pequeñas empresas es el que necesita un mayor grado de preparación, desde el punto de vista tecnológico, por lo que los fabricantes tenemos que hacer

un gran esfuerzo proporcionándoles herramientas en diferentes formatos para facilitarles su labor".

Sin embargo, Santi Oller pone el foco en las PYMES, "asegurándonos de entender qué necesita, cuál es la tecnología adecuada. El canal ha demostrado que está preparado y tiene ganas, conocimiento y mucha flexibilidad, y lo hemos visto en estos meses, con la aceleración y adaptación de los proyectos de sus clientes. Por tanto, la capacidad existe. Quizá llega el momento de hacer las cosas de otra manera, con menos tensión. En los próximos meses me gustaría ver una fórmula diferente de trabajo entre el canal y el cliente, saber qué necesita la PYME, ayudarles a adaptar la tecnología y, por parte del cliente, asegurar ese conocimiento de las soluciones, reduciendo el diferencial de conocimiento, algo que hay que abordar desde diferentes puntos de vista. En estos meses hemos puesto en marcha alguna iniciativa con partners como GTI V-Valley, por ejemplo, y la respuesta ha sido magnífica. El interés es palpable. Y siempre nos gusta destacar la flexibilidad que ha demostrado el canal para adaptarse a las necesidades de las PYMES".

Coincide Alberto Fernández, que añade que "los canales están capacitados. Conocen al cliente, saben lo que necesitan en cada momento y comprenden las soluciones tecnológicas que mejor se adaptan a ellos. Si conseguimos darles la información de cómo el ayudar a su cliente a acceder a estos fondos para complementar su conocimiento tecnológico, es lo que más van a necesitar y agradecer. Una de las patas del plan es que las empresas consigan adquirir las capacidades tecnológicas necesarias, y ahí el canal también puede ayudar. A partir de ahí solo quedará darles las herramientas para que puedan llevar su mensaje más allá".

EL ROL DE LOS FABRICANTES

Al hilo de lo comentado en este #DebateIT, queda por analizar cuál debe ser el papel de los fabricantes en este engranaje. En este sentido, Juan Carlos Gentou comenta que "hay que destacar dos cosas. La primera, en la que ya llevamos meses trabajando, es la formación a nivel de soluciones. En nuestro caso, es el cliente el que usa la tecnología, pero llegamos a ellos a través del canal. Tenemos que seguir trabajando en esa línea pero, por otra parte, está el acceso a los fondos. Todavía no está clara toda la información y no han llegado los fondos todavía. Hay que darles la información de cómo acceder a los fondos para ayudar a nuestros partners.

> Entre el empujón de la pandemia, los fondos europeos y la concienciación de la necesidad de digitalización, **la Transformación Digital va a despegar en los próximos meses**
>
> Miguel Ángel Díaz, BDM Openshift & Application Services, **Red Hat**

Una vez que esto esté claro, seguiremos asesorando sobre la mejor solución en cada caso y en cada segmento de actividad".

En palabras de Carlos Vieira, "estamos llevando a cabo algunas sesiones formativas, de momento virtuales, para explicar


Rafael Vicent, Ribbon

> La **pandemia** ha abierto una **gran oportunidad** para nosotros y nuestro canal para ayudar a los clientes para que puedan adoptar **este tipo de soluciones**
>
> Rafael Vicent, Senior Channel Account Manager, **Ribbon**

cómo acceder a estos fondos. Nos falta cierta información de cómo llegar, qué requisitos existen, a quién se dirigen exactamente… y hemos de trabajar en ello, porque para que esto funcione el Gobierno deberá apoyarse en todos, desde asociaciones empresariales al canal, entre otros, para ayudar a que España coja el tren de la Transformación Digital. Seguiremos trabajando en esta línea formativa para que las empresas puedan dar los pasos que necesitan".

Según Alberto Fernández, "estamos a la espera de tener clara la oferta total de los fondos, ya sean europeos, a través del Gobierno, las comunidades autónomas… para, cuando todo esté definido, ayudar en la formación y el uso de los fondos, a través de GTI V-Valley, allí donde podamos ayudar. Normalmente, veremos una parte del negocio en formato MSP orientada a pequeña y mediana empresa, a quienes se les podrán ofrecer muchos servicios y soluciones de diferentes proveedores, y otra parte, más orientada a los partners que trabajan con empresas más pequeñas que tienen que trabajar para llevarles estas soluciones. Si miramos a la Administración Pública, llevan unos meses comprando lo justo a la espera de estos fondos, y tendremos que esperar a que lleguen para poder darles la mejor solución ajustada a las necesidades propias de la Administración".


Alberto Fernández, TeamViewer

> **El canal conoce al cliente**, sabe lo que necesita en cada momento y **conoce las soluciones tecnológicas** que mejor se adaptan a ellos
>
> Alberto Fernández, Manager Channel Sales - Southern EMEA & UK, **TeamViewer**

En la misma línea se expresa Rafael Vicent, al indicar que llevan un tiempo "preparando al canal para que puedan aprovechar los fondos para ayudar a los clientes. Pensando en las empresas más

pequeñas, estamos trabajando en una oferta de soluciones como servicios gestionados para que sus clientes puedan adoptar la tecnología de una forma muy sencilla".

Apunta Miguel ángel Díaz que "el 75% de nuestros ingresos vienen del canal, de ahí que sea vital para nosotros trabajar bien con ellos. Y en esta relación hay dos partes: la relación entre el fabricante y el canal, y la relación entre el canal y su cliente. En esta segunda parte, confiamos en el trabajo de GTI V-Valley, y ponemos el foco en la primera parte. Por eso estamos lanzando iniciativas y una de ellas, que, precisamente hemos lanzado recientemente, busca habilitar a una serie de partners para poder acudir a las operaciones de manera conjunta. Además, estamos cambiando internamente y compensando más las operaciones que se realicen a través del canal. En definitiva, seguiremos empujando para fortalecer esta relación entre el fabricante y el canal, y confiando en GTI para la relación entre el canal y su cliente".

Recalca Santiago Oller que, "centrándonos en lo que ya sabemos y podemos controlar, hemos desarrollado un plan de formación muy amplio y ese plan va a continuar. Y, por otro lado, queremos estar preparados con una oferta muy concreta y específica para las áreas que se entienden como digitalización en los planes del Gobierno, como pueden ser seguridad, trabajo en remoto, e-commerce… áreas muy concretas donde va a haber una necesidad. Nosotros estamos trabajando, en colaboración con el canal, para que exista esta oferta cuando llegue el momento, y marcar la diferencia en el nivel de digitalización de las empresas. A todo esto se añade un elemento más, transmitir positivismo de cara a abordar esta Transformación. Tenemos las herramientas, las ganas, la predisposición de todos… y tenemos que transmitir a las PYMES que es posible y que vamos a acompañarlos en su proceso de digitalización".

CONCLUSIONES

Concluye el #DebateIT Roberto Alonso señalando que "hemos visto el momento en el que estamos, el nivel de la digitalización que tenemos. Hemos pasado un primer impulso, pero todos tenemos claro que queda mucho por hacer, y estos fondos europeos nos tienen que ayudar a realizar todo lo que resta. Tal y como lo vemos desde GTI V-Valley, queremos apoya al canal en dos cosas. Primero, dar a cada empresa lo que necesita, ayudando a cada partner a definir su propuesta de valor, combinando soluciones diferentes e integrando distintos modelos de consumo, a la par que les damos la capacitación necesaria y les ayudamos en el proceso de comercialización. Por otra parte, ayudar a aquellas empresas no tan acostumbradas a estas metodologías y terminologías tecnológicas, acompañando y dando soporte al canal para ampliar esta digitalización a todo el tejido empresarial". ■

> Queda mucho por hacer y hay que trabajar para **llevar estos fondos a las empresas más pequeñas y las Administraciones Públicas**
>
> Carlos J Pinheiro Vieira, Country Manager, **Watchguard**

Oportunidades para el canal de TI en torno a los Fondos Europeos de Recuperación (II)

Para hablar de esta oportunidad, contamos en este segundo debate con la participación de Roberto Alonso, Cloud & Business Director de GTI V-Valley; Rafael Pestaña, Director del área HPE Centric de V-Valley; Alessandro Perotti, Channel Manager, Italy & Iberia, Acronis; Paco López, HPE GreenLake Southern Europe Service Providers Lead; Fernando Suárez León, IBM Partner Ecosystem Leader; Carolina Castillo, Director One Commercial Partner Organization and Small, Medium, Corporate Business at Microsoft; Alexandre Tovar, Channel Account Manager, Trend Micro; y Jorge Sáez, Distribution Success Manager Iberia, Veritas.

UN NUEVO HORIZONTE PARA EL CANAL TI

En primer lugar, quisimos conocer la visión del mayorista, en las personas de Roberto Alonso y Rafael Pestaña, sobre las oportunidades y los retos para el canal de distribución de estos Fondos Europeos de Recuperación. Tal y como señalaba Roberto Alonso, de GTI V-Valley, "estos fondos son importantes, y nosotros lo vemos así no solo como GTI V-Valley, sino como parte del Grupo Esprinet, porque hasta ahora hemos vivido una transformación forzada por la pandemia, aunque todos coincidimos que se ha acelerado mucho, pero queda mucho por hacer. Creemos que estos fondos europeos pueden marcar un hito para el sector. Y pensamos que el canal es fundamental, porque hablamos de cuestiones como la digitalización de la PYME o acercar al ciudadano la tecnología por la Administración Pública, y para eso el canal es una pieza clave. Para aprovechar estos fondos, estamos trabajando en tres líneas. Primero, dar a conocer la llegada de estos fondos

DEBATE IT: Oportunidades para el canal de TI en torno a los Fondos Europeos de Recuperación (II)

Buena parte de las empresas españolas pretende optar a los Fondos del Plan Europeo de Recuperación Next Generation EU, dotado con 750.000 millones de euros, de los que 140.000 han sido asignados a España. Sin embargo, existe un gran desconocimiento sobre cómo funcionan y cómo se pueden presentar los proyectos, lo que abre una ventana de oportunidad al canal de distribución, como vehículo transmisor entre las empresas y estos fondos.

a todos los clientes para, en una segunda etapa, estar preparados. Creemos que es importante que nuestros partners creen su propia propuesta de valor y estén preparados para acometer la digitalización de las empresas. Y una tercera etapa, la del soporte, visto como algo convencional en la labor del mayorista, pero, en este caso, hablamos de empresas que no están acostumbradas a este tipo de ayuda y nosotros podemos ayudarlas a acceder a ellas con la mayor facilidad".

Complementa esta visión del mayorista Rafael Pestaña, de V-Valley, ahondando en el mensaje. "GTI V-Valley nos aporta una capacidad de soluciones híbridas", apunta, "que se une a nuestra propuesta de la mano de HPE GreenLake, un modelo de tecnología como servicio (XaaS). Según Gartner, el 75% de las empresas medianas y pequeñas van a adoptar un modelo de cloud híbrido en este año. Esto, asociado a los fondos europeos, que nos van a ayudar a desarrollar la Transformación Digital de las compañías, hace ineludible este camino. El canal lleva un tiempo transformándose; hay un nuevo modelo de negocio, y nuestro papel consiste en apoyar, formar, enseñar, impulsar y poner de acuerdo a todos los actores ayudando al canal para que utilice la potencia de todos".

LA REALIDAD DE LA DIGITALIZACIÓN DE LA PYME

El nivel de digitalización actual de la pequeña y mediana empresa y la Administración Pública es el punto de arranque para el debate, que inicia Alessandro Perotti, de Acronis, señalando que "la llegada de estos fondos es un paso muy importante para un cambio tecnológico, para la Transformación Digital. Lo que antes era un objetivo para muchas empresas, con su propia capacidad económica, es ahora una realidad, la posibilidad de renovarse, relanzar su organización y su gestión, sobre todo en este escenario posterior a la pandemia. Muchas empresas y sectores se han visto muy afectados por la pandemia, como el Turismo y parte del sector Industrial o la Sanidad, y algunos eran, incluso, más vulnerables porque ya tenían ciertos elementos de retraso en la digitalización. De hecho, los datos de la UE nos dicen que en España hay una gran diferencia entre la inversión en infraestructuras en grandes organizaciones, frente a las PYMES, que están más retrasadas y solo el 17% de las PYMES han integrado tecnologías de Transformación Digital en su negocio, algo que en las grandes empresas se sitúa en el 50%. Por tanto, es una gran oportunidad para que muchas empresas puedan cambiar, y para ello necesitarán tecnologías que se lo permitan. Y en este

> "Creemos que estos **fondos europeos pueden marcar un hito para el sector**, y pensamos que el canal es fundamental"
>
> Roberto Alonso, Cloud & Business Director de **GTI** V-Valley

proceso el canal va a tener un papel fundamental, porque es el primer consultor de los clientes finales. El canal podrá renovarse y digitalizarse con nuevas tecnologías, como el cloud híbrido, que le permitirá mejorar su atención a los clientes. Por tanto, el canal será el primer actor que pueda beneficiarse y transmitir, a la vez, la tecnología a los clientes finales, tanto a las PYMES como a la Administración Pública. En resumen, una oportunidad que nos permita recuperar el retraso que existía".

Para Paco López, de HPE GreenLake, "hay mucho por hacer. Son dos escenarios, la PYME y la Administración Pública, que tienen poco en común. Es verdad que las grandes empresas han adoptado los modelos digitales y están digitalizando sus procesos, pero sigue siendo un debe de gran parte de la Administración y de muchas PYMES. Esta lluvia de fondos va a ser transversal a todos los segmentos, y es posible que en unos años tengamos una realidad muy diferente a la actual y a la que hemos sufrido durante la pandemia, porque esto va a acelerar la digitalización y va a impactar a muchos sectores y muchas empresas. Hay mucho trabajo por hacer y tenemos que estar preparados para abordarlo de forma correcta. Y es ahí donde creemos que tenemos que crear ciertas propuestas de valor para

ponerlas en el mercado y que el canal las aproveche. Hablamos de plataformas híbridas, adaptables y flexibles, como, en nuestro caso, GreenLake, permitiendo, a partir de estándares, que las plataformas puedan asumir las cargas de trabajo que se van a ir creando, tanto desde el centro de datos como desde la nube e, incluso, en el extremo, algo que nos va a forzar a llevar capacidad para la toma de decisiones, el proceso y el almacenamiento en el extremo. Vamos a tener mucha capacidad de digitalización en procesos que, todavía, son muy analógicos. Pero todos estos escenarios presentan una gran impredictibilidad, así que lo que hay que hacer es estar preparado para, según evolucionen, ser flexibles y capaces de interactuar con estas cargas de trabajo. En el caso de la Administración, tiene que vernos como clientes, y todavía ahí hay también mucho trabajo por hacer".

En opinión de Fernando Suárez, de IBM, "todavía queda mucho trabajo por hacer en la digitalización de las PYMES. En uno de los informes del DESI, se decía que las PYMES españolas están muy por detrás de la media europea y que tienen mucho que hacer para explotar la oportunidad que existe. Estamos por detrás en el uso de servicios en la nube y también, por ejemplo, en la implementación de soluciones de Big Data. Queda mucho por migrar a la nube, porque solo el 20%, según un estudio de IBM, de las cargas de trabajo están en la nube, y todavía

> Hay un **nuevo modelo de negocio**, y nuestro papel consiste en **apoyar, formar, impulsar y poner de acuerdo a todos los actores** ayudando al canal para que utilice la potencia de todos
>
> Rafael Pestaña, Director del área HPE Centric de **V-Valley**

quedan por mover las cargas críticas. Nosotros pensamos que con nuestra tecnología de IA y de nube híbrida abierta, tenemos la tecnología adecuada para ayudar a las PYMES y la Administración Pública. Es cierto que con la pandemia ha habido un efecto en las empresas y los modelos de consumo están cambiando, y esta aceleración supone una gran oportunidad para todos. Con la tecnología en mente, podemos ayudar a las PYMES, aportándoles, además, nuestra experiencia como empresas. En el caso de la Administración, quizá no es una respuesta única, ni por administración ni por verticales, pero estos fondos suponen una gran oportunidad para acercar la Administración a la ciudadanía. Es cierto que, a día de hoy, la mayoría de los ciudadanos interactuamos con la Administración de forma transaccional y esporádica, pero no nos sentimos tratados como exigimos a las empresas que traten a sus clientes. Por eso estamos trabajando en diversos proyectos que están siendo bien valorados por la ciudadanía. Hay una gran oportunidad para todo el ecosistema para la modificación de la Administración o de la PYME".

Se muestra optimista Carolina Castillo, de Microsoft, que afirma que "el momento es ahora, y sí estamos a tiempo, pero hay que recalcar que los informes de la UE nos sitúan como el undécimo país en el ranking. Pero estamos a tiempo de escalar posiciones y quizá un año tan duro como el pasado nos ha servido para acelerar y perder el miedo a afrontar este gran proceso de transformación, de reimaginación de los negocios, desde las pequeñas y medianas empresas hasta la Administración Pública, sin olvidar las grandes, para poder apalancarnos en la innovación que ofrecen los servicios de cloud, la digitalización y, en definitiva, la tecnología. Un dato que habla por sí solo es el del volumen de las PYMES en comercio electrónico, que tenía un dato de partida del 9% y, a raíz de la pandemia, se ha disparado en más de un 40%, por lo que este 9% inicial se tiene que convertir como mínimo en un 25%, y todas las PYMES tienen a su alcance esta posibilidad de reinventarse y de acceder a esta nueva forma de generar negocio. Otro dato era el 16% de adopción de tecnología cloud, algo que también se ha acelerado y, con los datos que maneja Microsoft, en dos meses se ha avanzado lo que estaba previsto avanzar en dos años. La PYME, con estos fondos, tiene la oportunidad de dar este tipo de saltos, potenciando el valor de la tecnología; independientemente del tamaño, puede acceder a la misma tecnología que las grandes empresas, habilitando con ello la venta y el marketing digital, habilitar sistemas de explotación de la in-

> "La llegada de estos fondos es un **paso muy importante para un cambio tecnológico**, para la Transformación Digital"
>
> Alessandro Perotti, Channel Manager, Italy & Iberia, **Acronis**

formación en beneficio del negocio, y, por supuesto, el trabajo colaborativo, en remoto, y productivo, algo en que hemos visto cómo se ha adoptado la tecnología de un nivel del 12% a un 84%. En resumen, sí se puede, pero el momento es ahora con los recursos que llegarán de Europa".

Pone el foco en la seguridad Alexandre Tovar, de Trend Micro, que explica que "las PYMES se están viendo forzadas a una transición a lo digital en un contexto en el que no tienen las herramientas, las ayudas, las capacidades ni los conocimientos para estar compitiendo. Hay que alinear la tecnología y las personas, incidir en la capacitación, en la reorientación laboral. Al final, no podemos tener una foto clara en la PYME de cómo vamos avanzando, porque hay muchos desequilibrios, al igual que en la Administración Pública. Hay diferentes velocidades, diferentes niveles en la externalización de servicios… y, en consecuencia, hay diferencias en la percepción del ciudadano en función del servicio que necesita de la Administración. Y esto es especialmente importante cuando hablamos de ciberseguridad. Los fondos son una gran oportunidad, pero la ciberseguridad va a ser clave en la rapidez de la adopción de estos servicios digitales. Sin la confianza del cliente, del usuario, es muy difícil poder avanzar en la adopción de nuevas tecnologías y plataformas. El paso a lo digital, con el retraso que hay frente a otros países, y con un menor nivel de usabilidad del que reclaman los clientes o los ciudadanos, es complicado, y más todavía si no hay una ciberseguridad desde el diseño".

Concluye esta primera ronda de intervenciones Jorge Sáez, de Veritas, que indica que nos encontramos "en una situación en la que vivimos un incremento exponencial del dato, unido a dos grandes retos: por un lado, la complejidad, que aumenta en nuestro entorno, y, segundo, la velocidad de la transformación, porque los clientes han tenido que asumir un proyecto en tres meses cuando lo tenían previsto a tres años. Es imprescindible simplificar esta complejidad y acelerar el ritmo de la transformación. Sobre los fondos, estamos ante una oportunidad histórica y la responsabilidad de los fabricantes es aportar soluciones válidas, sencillas y que permitan la escalabilidad necesaria. El peso de la responsabilidad lo tenemos nosotros, y tenemos que poner las soluciones encima de la mesa a través del canal; sin la formación, la capacidad y la sencillez con la que el canal nos permite llevar nuestro mensaje y soluciones a los clientes, es imposible que coincidamos en momento, en tiempo y en oportunidad".

> "Las grandes **empresas** están **digitalizando sus procesos**, pero sigue siendo un **debe** de gran parte de la **Administración Pública** y de muchas **PYMES**"
>
> Paco López, **HPE** GreenLake Southern Europe Service Providers Lead

UN CANAL PLENAMENTE CAPACITADO

Continúa Jorge Sáez afirmando que "quizá nunca es suficiente, por la velocidad a la que se trasforma todo, pero creo que el canal es lo suficientemente profesional para adoptar estas soluciones en tiempo, tanto a nivel mayorista, y GTI V-Valley es un ejemplo, como a nivel del resto de partners. La preparación está, pero hace falta que diseñemos planes sencillos donde seamos capaces de llevar estas tecnologías y los fondos asociados a la transformación de la PYME, que es donde está la complejidad".

Se muestra de acuerdo Carolina Castillo, que añade que ·deben ayudar a ofrecer a todos, a escala, ese conocimiento para la adopción de las herramientas tecnológicas, permitiendo que se sientan cómodos innovando a través de la tecnología. Nosotros tenemos esta visión: todas las empresas, independientemente del tamaño, se van a convertir en empresas de software. Es fundamental reformar el talento para ayudar a las personas de todos los negocios a adoptar la tecnología para poder sacar el mayor provecho de las herramientas. Hay que hacerlo sencillo, no solo vender las soluciones, las herramientas, sino ir más allá para capacitar al mayor número de personas para aprovechar la tecnología".

En palabras de Fernando Suárez, "tenemos un canal capacitado para apoyar a las PYMES y son ellos los que nos permiten llegar a los clientes, son ellos los que están democratizando la tecnología. De hecho, ya tenemos ejemplos de uso de la IA en sectores como la agricultura, la cadena de suministro alimentaria, o en logística utilizando Blockchain. Pero la formación y la capacitación debe ser continua. Y, como muestra de la madurez de nuestro ecosistema, un partner español es uno de los más avanzados del mundo y ha obtenido un reconocimiento que IBM solo da a 15 compañías a nivel mundial. Por nuestra parte, hemos hecho un anuncio que nos va a ayudar a que los partners identifiquen y nos comuniquen casos de uso, con una inversión de más de 1.000 millones de dólares a nivel mundial, para ayudar a co-crear soluciones que puedan ser consumidas y optar a estos fondos. Tenemos la tecnología, los medios, el canal capacitado y los fondos, con lo que, como decía Carolina Castillo, el momento es ahora. Y no podemos olvidar el papel de un mayorista como GTI V-Valley, que nos permite llegar mejor preparados a esta situación".

Apostilla Paco López que el canal "está preparado, pero sobre todo para aprender y transformarse para los requerimientos que tenemos por delante. La crisis de 2008 sirvió para preparar al canal ante

> "Con la tecnología en mente, podemos **ayudar a las PYMES**, **aportándoles**, además, nuestra **experiencia como empresas**"
>
> Fernando Suárez León, **IBM** Partner Ecosystem Leader

situaciones difíciles, y sobrevivieron y crecieron aquellos que se apoyaron más en la tecnología, aquellos que miraron más allá de las fronteras, y ayudaron a las empresas a crecer a partir de la tecnología. Nuestro canal se ha sabido adaptar a todas las transformaciones, pero lo que nos viene ahora va a suponer otra transformación de nuestro canal. Va a haber muchas pruebas, hay que estar preparado para fallar y apoyar a los que mejor funcionen. Creo que tenemos un canal que se adapta muy bien a los entornos, pero los entornos que tienen que venir en el futuro distan mucho de los actuales, y por eso es tan importante la capacitación, la formación, la preparación… Nosotros tenemos que poner a su disposición nuestra propiedad intelectual y ellos deben ser capaces de adaptarse a eso. Y no olvidemos que la identificación de los casos de éxito va a ser muy importante, porque van a ser las puntas de lanza de los avances del futuro".

En palabras de Alexandre Tovar, "el canal ofrece muchas ventajas competitivas, y contar con distribuidores formados es muy importante para ofrecer la flexibilidad que demandan las empresas, con modelos de pago por uso y con soluciones adaptadas. Y esta cobertura de 360 grados a la PYME es la que ofrece el partner. Por eso llevamos


Carolina Castillo, Microsoft

años trabajando con el canal con herramientas de formación y de concienciación sobre la seguridad".

En la misma línea se muestra Alessandro Perotti, que comenta que "el canal está preparado para esta oportunidad, pero dentro del mismo canal podemos ver diferentes realidades, con partners que ya han hecho la transformación, por ejemplo los nativos cloud, pero hay otro canal que está capacitado pero todavía necesita herramientas y trabajar en las personas. Nuestra labor, junto con GTI V-Valley, es ayudar a este canal que trabaja mucho por la PYME, a que le pueda ofrecer una tecnología más avanzada: formación de las personas en ciberseguridad, cómo utilizar herramientas para proteger los datos e introducir cambios en la gestión".

PASOS QUE DESARROLLAR PARA APROVECHAR ESTA OPORTUNIDAD

Para cerrar el debate, quisimos conocer qué pasos, herramientas o actividades están poniéndose en marcha para ayudar al canal a aprovechar esta oportunidad. Tal y como nos explica Alessandro Perotti, "nosotros ya tenemos una plataforma de ciberprotección cloud. Integra diferentes herramientas y tecnologías en una única plataforma de gestión remota, lo que es muy bien recibido por los partners porque les permite escalabilidad, flexibilidad, una gestión más efectiva con menores costes, mejorando su rentabilidad".

> "Las **PYMES** tienen a su alcance la **posibilidad de reinventarse** y de acceder a **nuevas formas de generar negocio**"
>
> Carolina Castillo, Director One Commercial Partner Organization and Small, Medium, Corporate Business at **Microsoft**

OPORTUNIDADES Y RETOS DE LOS FONDOS DE RECUPERACIÓN EUROPEO

Apunta Paco López que "estamos habilitando las plataformas de interconexión con modelos que permitan las nubes híbridas para gestionar las cargas de trabajo a través de nuestro canal, y desarrollar todos los productos y servicios para poder garantizar todas las peticiones que se están haciendo con esta Transformación Digital. Seguimos avanzando en estas tecnologías para dar cabida a las nuevas plataformas".

En palabras de Fernando Suárez, "el concepto clave para los fondos es ecosistema, porque estos fondos lo que quieren generar es una mejora económica. Por eso para nosotros es fundamental apalancarnos en clusters o en comunidades que puedan desarrollar estas soluciones. Además, tenemos a disposición del ecosistema tres recursos: los recursos, económicos y técnicos, para la co-creación de soluciones; la tecnología, que puede ser la base de la arquitectura para la obtención de los fondos; y nuestra experiencia, y ya hemos demostrado que podemos ser un excelente compañero de viaje para acompañar a nuestro ecosistema".

Desde el punto de vista de Carolina Castillo, "el ecosistema es fundamental, dado que hablamos de más de 3 millones de PYMES, que tienen el derecho y la oportunidad de digitalizarse. Nosotros ofrecemos la plataforma para que este ecosistema pueda hacer una solución adaptada a las necesidades de cada una de las empresas, que están muy dispersas por todo el territorio, lo que implica una capilaridad que solo aporta el canal. En cuanto a las soluciones y las herramientas, hablamos de soluciones de productividad, de integración del dato, de securización, de negocio, de gestión y factura… el abanico es infinito, y la oportunidad de que cada uno desarrolle su propia área de negocio es inmensa. Invito, de hecho, a reflexionar al canal sobre la posibilidad de desarrollar su propia oferta por vertical, porque hay oportunidades en todos los entornos".


Alexandre Tovar, Trend Micro

Según Alexandre Tovar, "como fabricantes de seguridad, nuestra labor es que nadie se quede atrás, sobre todo, por no saber acceder a las subvenciones o los fondos. Trabajamos con nuestro canal para paliar este problema, porque, al final, los atacantes aprovecha el eslabón más débil, y no podemos dejar atrás a las PYMES porque forman parte de la cadena de suministro de muchísimas empresas de este país. Un ataque a una PYME puede significar un ataque en cadena si no lo frenamos en origen. Trabajamos mucho en las labores de formación, concienciación y con soluciones integrales para que no quede abierto ningún hueco, siendo flexibles para brindar una oferta multi cloud, multi plataforma y multi entorno, para que el punto de partida de la PYME no sea un problema o que pueda cambiar de proveedor o de tecnología

> "**Sin** la **confianza** del cliente, del usuario, es muy **difícil** poder **avanzar en la adopción de nuevas tecnologías** y plataformas"
>
> Alexandre Tovar, Channel Account Manager, **Trend Micro**

en cualquier momento sin problema, reforzando, asimismo, los servicios gestionados para poder dar servicios a muchas PYMES".

Finaliza Jorge Sáez destacando que tienen un doble compromiso con la sociedad, "por un lado, en cómo reducir la brecha de la velocidad de la tecnología, y, por otro, en simplificar la complejidad. Nuestra aportación es desarrollar soluciones sencillas y transversales a la gestión del dato que ayuden a los clientes en lo que nos demandan hoy en día. Un 43% nos dice que lo que más les preocupa son las amenazas externas y, en segundo lugar, el compromiso regulatorio. Por eso, queremos aportar soluciones para que tengan los datos accesibles, visibles y protegidos para definir las estrategias más adecuadas".

CONCLUSIONES

Finaliza el debate con las valoraciones de Roberto Alonso y Rafael Pestaña sobre el papel a asumir por el mayorista ante esta oportunidad. Para Roberto Alonso, "estamos en un entorno de oportunidad, de responsabilidad, muy cambiante… pero con un canal que ha demostrado cómo se adapta. Nosotros le ofrecemos el acompañamiento necesario. Es cierto que hay conceptos de cambio, como el pago por uso, el consumo como servicio, la nueva realidad de la seguridad y del dato… que hace que el partner necesite alguien que le ayude en este proceso, que, al final, es lo que busca también el cliente en el partner. Nosotros queremos trabajar y ser el socio de confianza del partner para que pueda desarrollar su oferta para aprovechar estos fondos".

Para complementar, indica Rafael Pestaña que, "tenemos la capacidad de ayudar a los partners con la gestión de los fondos europeos, con ejemplos de cómo aplicar la tecnología a casos concretos. Hablamos de tecnología y de fondos, pero no es sencillo y hay que aterrizar todas estas cuestiones. Somos la clave integradora de diferentes tecnologías y la vía para llevarlas al canal, un ecosistema de empresas muy diferentes y con diferentes capacitaciones, con lo que tendremos que ayudar más a los que más lo necesiten. Y, por último, no podemos olvidar que, tras un buen momento, tenemos la solvencia y la capacidad financiera para poder ayudar a los partners a abordar proyectos de diferentes tamaños". ■

MÁS INFORMACIÓN

Los países europeos invertirán gran parte de los fondos NextGen EU en TIC

> Hace falta que seamos **capaces de convertir estas tecnologías y los fondos asociados en transformación de la PYME**, que es donde está la complejidad
>
> Jorge Sáez, Distribution Success Manager Iberia, **Veritas**

18
JUNIO
11:00 CET

REGISTRO

El fenómeno del Device as a Service y las oportunidades para el canal TI

24
JUNIO
11:00 CET

Mejorando la experiencia del trabajador remoto

REGISTRO

29
JUNIO
11:00 CET

Entendiendo la Era del dato: tecnologías y propuestas para gestionar la “datificación”

REGISTRO

#ITWEBINARS

Nuevos retos de seguridad en entornos financieros

Su impacto en el modelo de negocio

El sector financiero ante el reto de la ciberseguridad:

la digitalización abre la puerta a nuevas amenazas

Los riesgos de las TIC representan un enorme desafío para las entidades financieras y subrayan la importancia de implementar una adecuada estrategia de seguridad que abarque, desde la protección de infraestructuras hasta la seguridad de datos y usuarios. La formación y concienciación del usuario son también clave, a fin de que este se convierta en un eslabón más de la cadena en la protección.

NUEVOS RETOS DE SEGURIDAD EN ENTORNOS FINANCIEROS

A lo largo de la última década, las entidades financieras, principalmente los bancos, han acometido un importante cambio en su modelo de negocio, apostando claramente por la digitalización como motor de innovación y puntal clave en su relación con el cliente. Así las cosas, este sector ha ido avanzando desde una huella digital básica hasta un entorno basado en la omnicanalidad, con el desarrollo de nuevos productos y servicios y un mejor y mayor aprovechamiento de tecnologías disruptivas, como la inteligencia artificial, el blockchain, la analítica y las tecnologías basadas en la nube.

Sin duda, esta creciente digitalización ha favorecido importantes beneficios: el customer centric es una realidad cada vez más consolidada, pero también ha generado significativos retos y riesgos no financieros, como la dependencia de proveedores y nuevos jugadores y la proliferación de ciberataques y amenazas online, exposiciones que se han multiplicado por el aumento de dispositivos electrónicos, la migración a la nube y la apertura de puertas y ventanas que han terminado por diluir el perímetro de la red. En este sentido, datos facilitados por el Fondo Monetario Internacional (FMI) apuntan que el número de ciberataques se ha triplicado en la última década, convirtiéndose en una amenaza para la estabilidad financiera. Según esta organización, en 2020 se produjeron 1.500 casos, frente a los 400 de 2012.

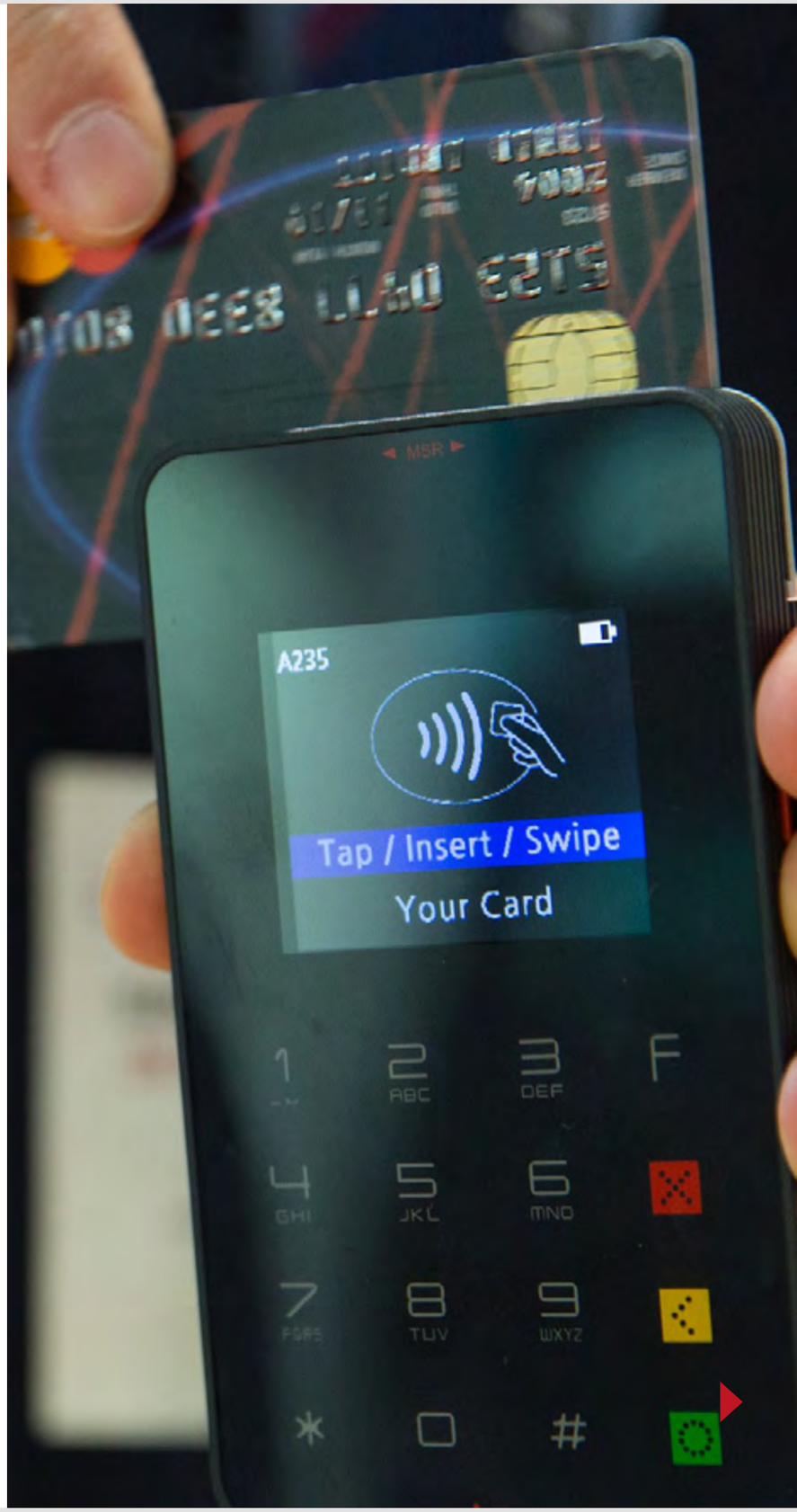
Del mismo modo, la aceleración de los planes de digitalización de estas compañías y, sobre todo, la generalización del teletrabajo a causa de la Covid-19, ha dilatado el nivel de riesgo, al abrirse nuevas vías de ataques que los ciberciminales han sabido aprovechar.

Así, este nicho ha experimentado la segunda mayor proporción de ciberataques relacionados con COVID-19, solo por detrás del sector de la salud, con un coste promedio por brecha de datos de 5.85 millones de dólares en 2020, frente a los 3.86 millones de dólares del promedio mundial, según datos de la última edición del informe anual Cost of a Data Breach Report de IBM.

EL DESAFÍO DE LA CIBERSEGURIDAD

La banca se enfrenta, por tanto, a un panorama difícil en materia de ciberseguridad, con ataques cada vez más complejos, muchos de los cuales se dirigen contra el usuario, el eslabón más débil, contra la propia infraestructura o hacia proveedores externos (ataques a la cadena de suministro). Así, a ofensivas de relleno de credenciales, fraude de apropiación de cuentas, correos electrónicos de phishing o malware (troyanos), se unen otras amenazas como el ransomware, que incluye vectores de doble extorsión y factor humano, junto con la creciente demanda de desencriptación de datos, y los ataques DDoS.

Detrás de estos ataques se esconden no solo criminales cada vez más osados, sino también estados y atacantes patrocinados por estados



que saben que por la sensibilidad de los datos que custodian, los bancos son un blanco fácil. Tanto es así, que, hoy por hoy, el ciber riesgo se encuentra en tercer lugar en el ranking de riesgos de entidades financieras, después de los lucros cesantes y el riesgo pandémico, según el 10º Barómetro de Riesgos de Allianz 2021.

Afortunadamente, y por los activos que gestionan (dinero, datos sensibles y reputación) en el sector financiero siempre ha existido una gran concienciación sobre la seguridad, tanto en la vertiente física como lógica. Se trata de un factor de confianza. Así, las entidades financieras destinaron en 2020 el 10,9% de su presupuesto a ciberseguridad, frente al 10,1% del año anterior. En términos de gasto por empleado, esto supone alrededor de 2.700 dólares, según una encuesta de Deloitte y FS-ISAC.

Ahora bien, es necesario que esta seguridad evolucione al mismo ritmo que lo hacen las tecnologías, los servicios provistos y la regulación (PSD2, Mifid2, CRD2...), sin olvidar, por supuesto, como lo hacen también la tecnología de ataque y los hackers, alumnos aventajados.

Por ello, y además de proteger infraestructuras como los ATMs, es necesario apostar por soluciones centradas en el resguardo del endpoint, la red, email, servidores o workloads en la nube, como antivirus, plataformas EDR, XDR o con capacidades de aprendizaje automático. Asimismo, estas entidades deben avanzar hacia un enfoque proactivo, que dé prioridad a la prevención, para interrumpir los ataques antes de que el malware o la amenaza maliciosa -sin archivos- pueda siquiera comenzar a ejecutarse. También, la monitorización y gestión de lo que ocurre en redes botnets o en la Deep Web ayudará a prevenir y a mejorar la seguridad, con planes de respuesta. Esto incluye la formación de los empleados en materia de concienciación sobre la seguridad, la limitación de los privilegios de los administradores y una estrategia de confianza cero que abarque la gestión de la identidad y el acceso, así como la seguridad de la red. Importante igualmente es la colaboración entre entidades y con terceros, a fin de garantizar la resiliencia operativa digital.

EL RIESGO DE LA BANCA MÓVIL

Adicionalmente, la expansión de los servicios basados en dispositivos móviles (banca móvil) y la mayor dependencia de los clientes de las aplicaciones de banca electrónica ha ampliado su vulnerabilidad, convirtiéndose estos usuarios en blancos potenciales para los actores maliciosos, que utilizan una variedad de técnicas, incluidos troyanos bancarios basados en aplicaciones bancarias falsas, para atacarles. Así, la actividad de los troyanos bancarios se ha intensificado un 15%, según un estudio de Check Point, y estos se orientan, sobre todo, a atacar el segundo factor

de autenticación, principalmente SMS, para además de robar datos de acceso o credenciales, hacerse con otros más personales.

Ante esta situación y para protegerse, los bancos deben integrar metodologías o tecnologías que ayuden a asegurar las transacciones electrónicas, como la criptografía, o que faciliten la autenticación del usuario para evitar la suplantación de identidad, como los sistemas de tokenización. Igualmente, y de cara a ser más precisos, es fundamental securizar y custodiar las claves que protegen esa información (claves de cifrado) y la gestión de su ciclo de vida, sobre todo ahora, cuando se está produciendo una clara orientación a los servicios en la nube. En este sentido, los HSMs, capaces de almacenar y proteger claves criptográficas en consonancia con las normas más rigurosas de la industria, como la Directiva Europea de Pagos PSD2, son una opción.

PROTEGER EL DATO

La progresiva implantación de modelos comerciales, como el open banking, asentado en el intercambio de datos entre bancos y terceros (Bigtech) a través de APIs, está ocasionando distintos problemas de protección, sobre todo en el ámbito de la seguridad (de usuarios y entidades) y el análisis de datos. Según McKinsey & Company, los bancos son responsables de mitigar el riesgo de fraude y deben implementar controles, que incluyan análisis avanzados (por ejemplo, para validar el origen de las llamadas entrantes a la API), modelos de

Blockchain: riesgo u oportunidad

Los bajos tipos de interés, la reducción de márgenes, y los nuevos requerimientos regulatorios están presionando a la banca para buscar nuevas fórmulas que le permitan ganar en competitividad y rentabilidad. En este contexto, tecnologías como blockchain, suenan cada vez con más fuerza, en tanto en cuanto permiten realizar directamente entre partes, transacciones seguras con el apoyo de máquinas y algoritmos.

Asociada esta tecnología a las criptomonedas, una de las formas más populares y conocidas de usar blockchain, sus capacidades van sin embargo más allá de su almacenaje e intercambio, desde transacciones en tiempo real hasta tokenización de activos, préstamos y créditos, valores, prevención del fraude e identificación de los clientes. Además, sus capacidades de seguridad, apoyadas en la descentralización de la información, así como, en la eliminación de intermediarios, y la implementación de criptografía y firma digital para asegurar las transacciones, favorecen que estas operaciones (y sus datos) tengan la mayor seguridad, privacidad y autenticidad posible.

Sin embargo, y aunque Blockchain es una tecnología bastante segura en su diseño, su incorporación en mercados y entornos regulados, como el financiero, está produciéndose lentamente. Aún se tienen que garantizar aspectos de su seguridad, muchos de ellos relacionados con la ausencia de estándares tecnológicos, la falta de interoperabilidad entre distintas plataformas de cadenas de bloques o el uso de contratos inteligentes, que puedan ser origen de fugas de datos de carácter personal, y que hace necesario incorporar metodologías de seguridad por diseño desde las primeras fases de desarrollo, para evitar riesgos como: minado de cadenas laterales o paralelas (sidechain) o ataques DDoS, entre otros.

También y en lo que tiene que ver con el sistema de autenticación de la gestión de accesos a los sistemas blockchain, y aunque la normativa europea obliga a la banca a tener sistemas de autenticación de doble o triple factor, es necesario avanzar, sobre todo, por su relación con otros sistemas de información de la empresa.

Estos aspectos podrían solucionarse con la creación segura de claves o que el proceso de firma de cada una de las transacciones que se lanzan al bloque sea invulnerable. Es necesario validar el uso de blockchain como registro fundamentado y vinculante de evidencias digitales, definiendo en qué condiciones es válido. No hay duda de que si alguien descuida la custodia de sus claves éstas podrían acabar en manos de un atacante que podría así suplantar su identidad en la aplicación correspondiente. También hay que tener en cuenta que, debido al potencial de esta tecnología, es previsible que los ciberdelincuentes busquen oportunidades para atacar cualquier vulnerabilidad, tanto humana como técnica, en el ecosistema de blockchain.

NUEVOS RETOS DE SEGURIDAD EN ENTORNOS FINANCIEROS

autenticación segura del cliente y herramientas sólidas para detectar ataques de fraude, de acuerdo a PSD2. Estas normas también requieren que los bancos proporcionen un "sandbox" protegido a los proveedores de servicios de pago para las pruebas y el desarrollo continuo de servicios que utilizan la interfaz del banco.

Además de involucrarse en oportunidades de negocio innovadoras y potencialmente lucrativas abiertas por PSD2, el sector financiero se ha lanzado de lleno hacia una mejora real en la eficiencia, escalabilidad y flexibilidad de la mano de la Nube, para asegurar, en tiempos de pandemia, una fuerza de trabajo a distancia y garantizar la capacidad de recuperación. De este modo, y con los usuarios, dispositivos, aplicaciones y datos fuera del centro de datos empresariales y la red, la necesidad de proteger esos activos, así como de poseer una visibilidad completa del entorno se ha hecho imperativo. A este respecto, IDC Research confirma que cualquier solución de seguridad para cloud ha de incluir tres elementos: integración nativa, protección amplia y gestión y automatización. En torno a esta premisa han surgido marcos de seguridad como SASE, que esboza una convergencia de múltiples funciones de seguridad, como acceso de red Zero Trust (ZTNA), Gateway Web Seguro (SWG) de próxima generación, Agente Seguro de Acceso a la Nube (CASB), Gestión de la Postura de Seguridad Cloud (CSPM) o Firewall como Servicio (FWaaS); entregados desde la nube.

Además de la nube, la externalización de las funciones y servicios de las TIC, que ha cobrado mayor importancia durante la actual crisis sanitaria, puede plantear también retos relacionados con la gestión del riesgo de terceros, la confidencialidad y la protección de los datos de los consumidores. Igualmente, la inclusión del aprendizaje automático y de la inteligencia artificial están acrecentando esta vulnerabilidad, cuando, por ejemplo, los datos corruptos no detectados se introducen en los algoritmos y se utilizan en la toma de decisiones, según Bank for International Settlements (BIS). Por último, y en el caso de sufrir un episodio de ransomware, la recuperación de los datos, podría tornarse muy compleja, y las dudas sobre la exactitud de la información recuperada podrían hacer que el problema se prolongue durante un largo periodo de tiempo.

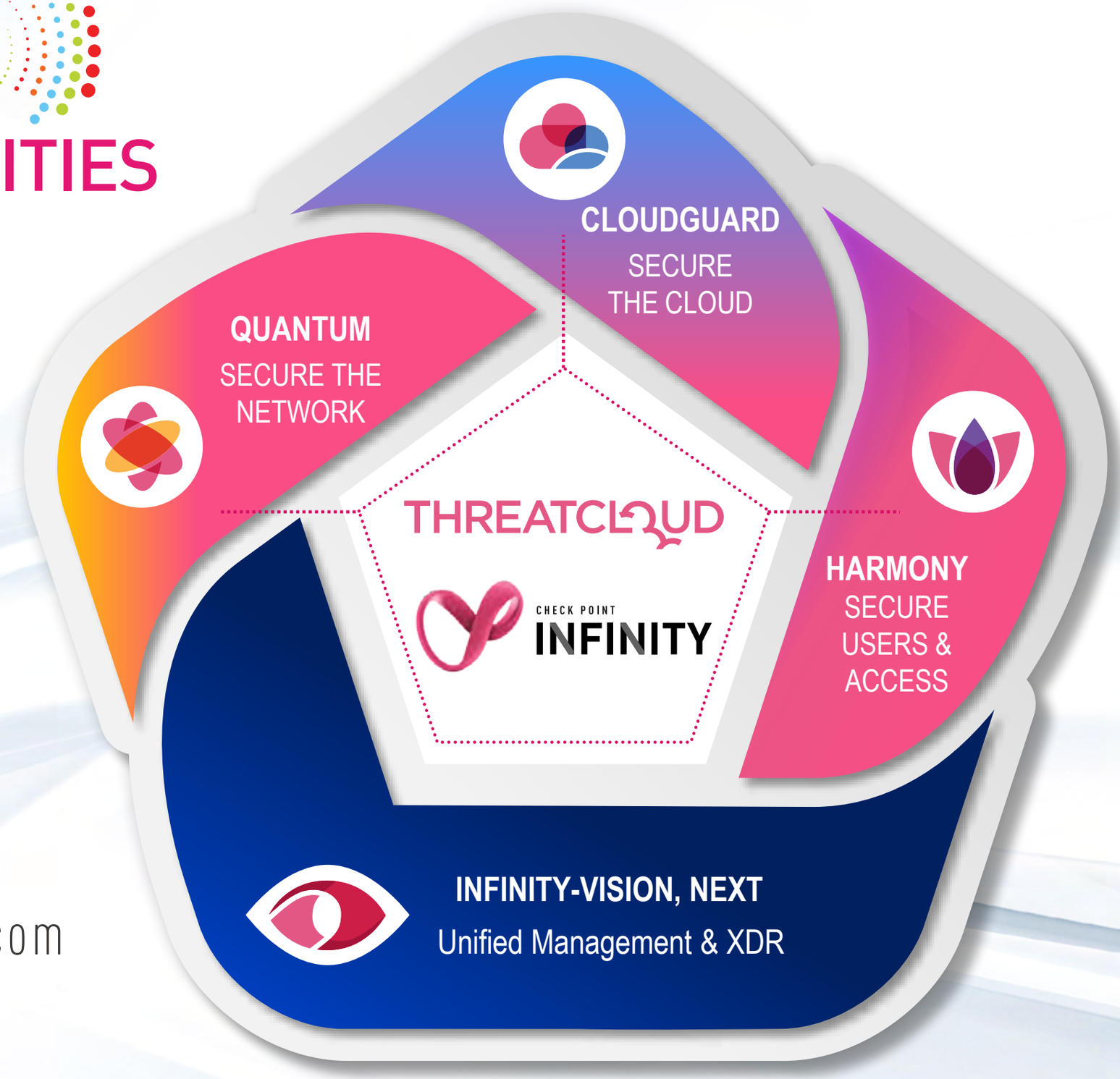
No hay duda, por tanto, que el gran volumen de datos generados por la banca requiere de la facultad de analizar y proteger dicha información, manteniendo y acatando, al mismo tiempo, las estrictas normas de la UE en materia de privacidad y protección de datos. Asimismo, el aumento de la demanda de servicios financieros en línea, y la progresiva modernización de los sistemas de pago, según el dinero en efectivo va perdiendo preponderancia, llevan a cuidar todos los aspectos de la seguridad. Cualquier incidente podría socavar la confianza del cliente, por lo que la ciberseguridad es más esencial que nunca. ■

MÁS INFORMACIÓN

- Incremento de ciberataques en la ultima década
- Ciberataques relacionados con la Covid-19
- Cost of a Data Breach Report
- 10º Barómetro de Riesgos de Allianz 2021
- Madurez en la ciberseguridad y riesgos en las instituciones financieras
- Actividad de los troyanos bancarios
- Directiva Europea de Pagos PSD2
- PSD2 y la disrupción en el open banking
- El efecto de los datos corruptos
- Bajos tipos de interés

Check Point®
SOFTWARE TECHNOLOGIES LTD

NEW WORLD
NEW OPPORTUNITIES
2021



MÁS INFORMACIÓN:

www.checkpoint.com/es

info_iberia@checkpoint.com

Nuevos retos de seguridad en entornos financieros;

su impacto en el modelo de negocio

Más tarde o más temprano las entidades financieras pueden ser víctimas de un ciberataque. Con esa idea en mente, deben prepararse para responder a las amenazas de hoy pero también a todas aquellas que van surgiendo al amparo de las nuevas tecnologías.

MESA REDONDA IT: Nuevos retos de seguridad en entornos financieros; su impacto en el modelo de negocio

El sector financiero, sobre todo la banca, lleva años sumido en una profunda transformación digital que le ha llevado a afrontar una serie de cambios, tanto en el modo de ofrecer y prestar sus servicios como en el de atender a sus clientes. Asimismo, la situación derivada de la COVID-19 ha transformado el comportamiento del consumidor, desde las preferencias de canal hasta el método de pago, y ha abierto una importante brecha en ciber-

“Las organizaciones tienen que actualizar o desarrollar sus propios sistemas de ciberseguridad según se detectan nuevos sistemas de ataque. Afortunadamente hay bastante concienciación en ciberseguridad”

EUSEBIO NIEVA,
DIRECTOR TÉCNICO DE CHECK POINT

seguridad, al incrementarse la digitalización y, por ende, la superficie de ataque. Por todo ello, ¿cuáles son los principales retos de ciberseguridad a los que se enfrentan actualmente entidades y servicios financieros? Para hablar sobre ello y conocer cómo afrontan los nuevos ataques y amenazas; su grado de concienciación al respecto de la ciberseguridad; cómo se ha adaptado este sector a tecnologías emergentes como blockchain o las nuevas normativas como PSD2; o cuál debe ser el siguiente paso en la adopción de nuevas tecnologías de seguridad, hemos contado con la participación en esta Mesa Redonda IT de Eusebio Nieva, Director Técnico de Check Point; Javier Sánchez, Territory Sales Manager de Entrust; Luis Javier Suárez, Presales Manager de Kaspersky; Jesús Rodríguez, CEO de Realsec; Igor Unanue, CTO de S21sec; Alfonso Martínez, Country Manager, Data Protection de Thales; y José de la Cruz, Director Técnico de Trend Micro Iberia.

RETOS EN CIBERSEGURIDAD

La creciente digitalización ha abierto la puerta a importantes retos en materia de ciberseguridad que, aunque extensibles a todos los verticales, en el financiero se perciben aún más. En este sector se maneja algo que todos los atacantes quieren: “dinero”, asegura Eusebio Nieva, por lo que no se debe confiar en sistemas tradicionales como protección frente a amenazas desconocidas. “Las organizaciones tienen que actualizar o desarrollar sus propios sistemas de ciberseguridad según se detectan nuevos sistemas de ataques”. Afortunadamente hay bastante concienciación en ciberseguridad.

Efectivamente, la cada vez mayor sofisticación por parte de los cibercriminales lleva a un nuevo paradigma en el que, según Luis Javier Suárez, “ya no basta con confiar en soluciones que aseguren un elevado grado de prevención, sino que se ha de plantear la hipótesis de poder estar siendo comprometido y no saberlo”. Aquí ya entra la parte de recoger ciertas métricas, telemetrías o anomalías para poder hacer un análisis y ver cómo cambian las normas del juego.

En idéntica línea, José de la Cruz recurre al planteamiento Zero Trust; “hay que asumir que

va a existir una brecha, y estar preparados para detectarla y actuar". Además, destaca dos retos que apuntan a la protección de las infraestructuras, donde hay una amalgama de tecnologías tradicionales y modernas combinadas, y a los usuarios, externos e internos. "Debemos dotarles de una seguridad que les aporte visibilidad sobre lo que ocurre en sus entornos".

Sobre estos retos, Igor Unanue considera, que, por el propio proceso de digitalización, estas organizaciones integran nuevas tecnologías, aplicaciones... que están atrayendo nuevos tipos de ataques, como los de tipo hacking, que permanecen en las redes internas largo tiempo sin ser descubiertos, causando importantes daños. "Van a seguir descubriéndose nuevas amenazas. La banca debe mantenerse alerta y estar corrigiendo para poder protegerse mejor".

UN NUEVO CONCEPTO DE BANCA

La progresiva digitalización ha marcado una senda de cambios. Se ha pasado del cliente físico al cliente móvil, de los centros de datos al cloud, ampliándose, al mismo tiempo, los vectores de ataque, lo que ha supuesto una mayor vulnerabilidad. ¿Cómo está enfocando la banca estos cambios?

Desde la perspectiva de este desarrollo, Javier Sánchez, observa que, en la actualidad, el vector de relación entre la banca y el usuario es la aplicación, por lo que hay que protegerla. "Las apps son un riesgo para los usuarios, que pueden ver comprometidos sus datos, y para los bancos, por el desprestigio para su negocio". Sobre la nube, donde cada vez residen más datos, incluso críticos, Sánchez estima que estarán seguros mientras el control de las claves que los cifran, no viaje con ellos.

Sobre este proceso de transformación, Jesús Rodríguez destaca que, a consecuencia de la pandemia, muchos desarrollos se han precipitado. "El uso del efectivo ha caído y canales que se iban a desarrollar de forma natural se han precipitado". Cada vez se hacen más operaciones utilizando dispositivos móviles y fórmulas, como el open banking, están cambiando el modo en que se utilizan los servicios bancarios. "Esto incide en la necesidad de proteger las transacciones (crip-

"Mediante la utilización de criptografía se van a proteger las transacciones, y con los sistemas de tokenización se va a autenticar a los usuarios. La suplantación de identidad es uno de los mayores riesgos para la banca"

JESÚS RODRÍGUEZ, CEO DE REALSEC

“La concienciación, incluso la formación, no dejan de ser responsabilidad del banco. El usuario tiene que ser un eslabón más de la cadena en la protección, no un habilitador de un ataque”

JOSÉ DE LA CRUZ, DIRECTOR TÉCNICO DE TREND MICRO IBERIA

tografía) y al usuario (sistemas de tokenización para evitar la suplantación de identidad).

Por su parte, Alfonso Martínez defiende la idea que con la gran evolución que ha tenido la banca en estos últimos años, esas entidades no pueden seguir protegiéndonos como hace 10 o 15 años. “Al igual que el abanico de opciones se multiplica, las amenazas también y son más sofisticadas. Los fabricantes no podemos quedarnos atrás. Tenemos que dar soluciones a las tendencias tecnológicas que van surgiendo, y ofrecer esa completa seguridad alrededor de la información”.

LA CONCIENCIACIÓN DEL USUARIO

El usuario es el centro de todo. Sin embargo, es importante encontrar un equilibrio entre la experiencia de usuario y la seguridad. ¿Cómo conseguirlo?

Para Eusebio Nieva, este equilibrio pasa porque el usuario perciba que la seguridad es útil. “Las medidas de protección pueden interferir en el usuario, en el acceso o en el dato”. Sin embargo, se debe intentar que el cliente distinga estas pautas como una ventaja, que aprecie que con estos mecanismos evita perder dinero, mientras consigue que las transacciones sean fiables y sus datos estén seguros. “A la vez que protege, la propia tecnología debe mostrar sus beneficios”.

Este componente de concienciación también es apreciado por Luis Javier Suárez, quien distingue dos desafíos para los bancos: conseguir que la experiencia del usuario no sea invasiva, mientras se recogen comportamientos y detectan anomalías que permitan tomar medidas para la detección temprana del fraude; y trabajar la concienciación, tanto dentro de la propia empresa como de cara al usuario. “Es importante trasladar las buenas costumbres adquiridas en la banca tradicional al mundo digital”.

La importancia de la concienciación, y de la formación, es destacada por José de la Cruz. “No deja de ser responsabilidad del banco proteger los activos de sus usuarios, que deben ser un eslabón más de la cadena en la protección, no un habilitador de un ataque”. Además, es clave comprender que la seguridad se ha de implementar en la fase de diseño, para que la integración sea mucho más transparente y sencilla y no interfiera en la agilidad o experiencia de usuario.

Para referirse al valor que le da el usuario a esta agilidad, Igor Unanue cita el doble factor

de autenticación, que no se implementó hasta que no fue obligatorio por ley, para no interferir en el acceso. “Es un tema de concienciación, de cultura. Cuando nos habituemos a utilizar determinadas tecnologías de seguridad también lo haremos en la banca”. No obstante, estas tecnologías han de resultar naturales para el usuario. “La seguridad debe ser cada vez más efectiva y más sencilla”.

PSD2 Y OTRAS REGULACIONES

Las entidades financieras siempre han estado a la cabeza en cuanto a modelos de transformación digital y en la adopción de medidas de seguridad, siempre han querido ir un paso por delante. Sin embargo, ha habido casos más complicados, como con la regulación PSD2. ¿Se ha logrado de una manera efectiva su adopción? Ahora, cuando ya se vislumbra el reflejo de PSD3, toca preguntarse si la banca está preparada para lo que está por venir.

Al respecto de la observancia de PSD2, Jesús Rodríguez refiere cómo las entidades se han estado preparando, primero, con el desarrollo de APIs para poner a disposición de terceros información de los clientes, y, después, con el establecimiento de un sistema de autenticación de doble factor. “En España no podemos hablar de incumplimiento, aunque la mayoría de entidades no han adoptado un sistema de tokenización; han optado por el envío de un SMS. A futuro, con la PSD3 en el horizonte, habrá que buscar otras soluciones basadas en token”.

Sobre la aceptación de estas medidas, Alfonso Martínez reconoce el gran esfuerzo realizado al abrir estas APIs para favorecer el open banking. Sin embargo, expone la importancia de implementar la seguridad desde el principio, en consonancia con PSD2, y para cumplir con otras nor-

“La seguridad debe estar habilitada desde el principio. Solo si los fabricantes ofrecemos las tecnologías adecuadas, las entidades van a poder acatar las distintas normativas y procurar los servicios (seguros) apropiados”

ALFONSO MARTÍNEZ, COUNTRY MANAGER, DATA PROTECTION DE THALES IBERIA

> "A causa de las normativas, los bancos están aplicando cada vez más niveles de seguridad sobre sus accesos a la red SWIFT. Pero hay que hacer más. Si ocurren ataques es porque detrás hay una vulnerabilidad, y los atacantes saben aprovecharlo"
>
> IGOR UNANUE, CTO DE S21SEC

mativas. En este punto el papel de los fabricantes es clave. "Debemos ofrecer las tecnologías adecuadas para que estas entidades puedan procurar los servicios (seguros) apropiados".

ATAQUES A LA RED SWIFT, UN RIESGO SISTÉMICO

Otro tema que cada vez está resultando más relevante son los ataques contra la red SWIFT, que se han multiplicado en los últimos tiempos. Ahora bien, ¿qué impacto están teniendo y en qué consisten estas ofensivas?

"Por tratarse de una red en la que fluye el negocio y circula el dinero, SWIFT es un claro objetivo para los hackers, que intentan interceptar transacciones para sacar beneficio", explica Eusebio Nieva. Para su salvaguarda, la tecnología puede ayudar muchísimo, sobre todo para el análisis de fraude y la securización de ciertos puntos que todavía son un poco débiles. "Al final se trata de aplicar la tecnología en esas transacciones. Protección y fiabilidad en todos los extremos".

Mitigar y securizar es crucial, pero antes hay que conocer cómo se producen estos ataques. En este sentido, Luis Javier Suárez, destaca que los más eficientes son los dirigidos contra la cadena de suministro. "Los atacantes manejan una cantidad abrumadora de inteligencia sobre los organismos que operan en la red SWIFT. Conocen qué vulnerabilidades pueden ser explotadas dentro de los sistemas y aprovechan esta información para saber dónde atacar y alcanzar ese objetivo".

Sobre las razones que explican los ataques a la red SWIFT, Igor Unanue revela que, por tratarse de una red externa, las medidas de seguridad son más laxas. "Sin embargo, ahora, sobre todo por las normativas, se están aplicando mayores niveles de seguridad a estos entornos, pero hay que hacer más. Si ocurren ataques es porque detrás hay una vulnerabilidad, y los atacantes la están aprovechando bien. Al final es una red de comunicación más, y como tal hay que protegerla".

La cadena de suministro es reconocida también por José de la Cruz, como el elemento más débil, y, dentro de ella, los bancos pequeños,

con medidas de seguridad menos robustas, el eslabón más frágil". No obstante, todos deben asumir que antes o después se producirá un ataque, por lo que las entidades deben dotarse de una visibilidad que les permita conocer lo que está ocurriendo, tanto en su entorno como con los flujos de información que existen con terceros.

TECNOLOGÍAS EMERGENTES

Tecnologías emergentes como blockchain, IA o IoT están empezando a impactar en los servicios financieros. ¿Cómo se están adaptando los bancos a ellas?

Sobre este punto, Javier Sánchez, expresa que "están en proceso". Los bancos custodian tanto el dinero como la confianza de sus clientes por lo que tienen que tomarse su tiempo a la hora de utilizar nuevas tecnologías y que formen parte de su proceso de negocio. En el caso de una blockchain pública no hay nadie al otro lado, por lo que los bancos no pueden comprometer su confianza con una tecnología que puede no ser segura.

Ahora mismo, la banca necesita ganar en competitividad y en rentabilidad por lo que, según Jesús Rodríguez, necesita hacer uso de tecnologías innovadoras como IA, donde están más adelantados. Otras como blockchain, muy ligada a las criptomonedas, y donde se "avanzará con una regulación", también son utilizadas para cifrar bloques o firmar smart contract, pero no cuando hablamos de claves, donde el nivel de exigencia es muy alto. Otras como IoP despegarán en un futuro.

Desde la perspectiva de representar a una empresa que fabrica tecnología que ayuda o habilita para el uso de innovaciones como blockchain, Alfonso Martínez considera que falta mucha labor de comunicación. "Estas tecnologías luego hay que aplicarlas a la vida real y, en ese sentido, falta información tanto, para los usuarios finales, que tienen que saber qué es blockchain y cómo utilizarlo como para las entidades financieras, para entender cómo lo pueden monetizar.

TECNOLOGÍAS IMPRESCINDIBLES

Ante toda esta innovación, el sector financiero no puede bajar la guardia en su seguridad. ¿Cuáles son aquellas tecnologías de seguridad que puede ser consideradas imprescindibles en la actualidad? Y ¿a futuro?

"Los bancos custodian tanto el dinero como la confianza de sus clientes. Tienen que tomarse su tiempo a la hora de utilizar nuevas tecnologías y que estas formen parte de su proceso de negocio"

JAVIER SÁNCHEZ, TERRITORY SALES MANAGER DE ENTRUST

“Cualquier organización tiene que asumir que puede ser comprometida. Este paradigma nos lleva a la gestión del incidente y al gobierno de algo que se ha impulsado desde el sector financiero: la gestión de indicadores de compromiso”

LUIS JAVIER SUÁREZ, PRESALES MANAGER DE KASPERSKY

Eusebio Nieva reconoce una alta concienciación en ciberseguridad, pero recomienda no bajar la guardia. “Estas entidades deben optar por tecnologías específicas para abordar amenazas actuales, como el ransomware, los ataques a la cadena de suministro o la protección del endpoint, pero también, por enriquecer sus sistemas con diferentes soluciones que protejan contra los peligros surgidos al calor de innovaciones, como las tecnologías cloud, y que las organizaciones financieras están convirtiendo en el core de sus servicios y de sus negocios”. Deben evolucionar y adaptarse según progresan sus tecnologías. La protección de la red o del endpoint era algo que había que hacer, y ahora hay que proteger las claves. En este sentido, Javier Sánchez respalda la importancia del cifrado, que ahora, además, es percibido tanto por otros fabricantes de seguridad como por las propias entidades del sector financiero como una solución necesaria para proteger la información. “Se ha producido una concienciación en torno a la importancia de securizar las claves, por lo que su adopción está ocurriendo de un modo natural en la banca”.

En línea con esta innovación hay un componente de concienciación importante. A este respecto, Luis Javier Suárez valora la trascendencia de que las empresas financieras desarrollen un plan de concienciación, ya sea de forma individual o con el respaldo de una empresa especializada. “También, deben asumir que su ciberseguridad puede verse comprometida, por lo que el uso de indicadores de compromiso resulta efectivo, sobre todo para compartir con terceros la información que contienen (inteligencia y patrones de ataques) y medir la afectación”. Asimismo, es esencial la explotación de inteligencia de amenazas, para ir a la par con los atacantes.

MEDIDAS PROPORCIONALES

Decidir qué solución o qué conjunto de recursos son los más adecuados para proteger las infraestructuras de las entidades financieras es complicado. “La realidad”, expresa Jesús Rodríguez, es que los riesgos están ahí, y las medidas han de ser proporcionales, así como las políticas

y los procedimientos de seguridad que se establezcan. No obstante, se deben proteger los activos de negocio, los riesgos de fraude e implantar medidas contra la suplantación de identidad o el malware. Por otro lado, el despliegue de nuevos canales de pago ha promovido un mayor uso de la criptografía, mientras que el crecimiento de los datos, precisa de medidas de protección que requieren el uso del cifrado, para cumplir con normativas como PSD2 o PCI DSS.

En la misma línea, Igor Unanue reitera que allí de donde vengan las amenazas es donde la banca más tendrá que invertir en ciberseguridad. En cuanto a futuro desafíos, señala la persistencia del malware (malware bancario) y de otros procedentes de servicios cloud, por el incremento de servicios de colaboración, que derivará en muchos riesgos. "Imperativo será también proteger el endpoint y, en general, todo aquello donde la banca perciba una amenaza".

Alfonso Martínez, coincide en que hay "mucho vector que proteger y el dato debe salvaguardarse así mismo con el cifrado". El cifrado puede ser en la nube, en máquinas virtuales, incluso en movimiento o viajando de una nube a otra. Lo importante es entender que detrás de esos sistemas tan complejos existe una inteligencia real a la que hay que ayudar para que la gestión sea sencilla y la criptografía no se convierta en un dolor de cabeza. "Debemos darles las herramientas para poder gestionarlo todo de manera centralizada y correcta".

Para José de la Cruz, la banca se enfrenta a un panorama heterogéneo, con diferentes tecnologías, proveedores y entornos, que le provocan un grado de exposición muy alto. La respuesta ante eso es visibilidad y control. "Visibilidad de lo que se protege, para conocer el origen y alcance de un ataque, y control sobre aplicaciones que no han sido diseñadas con la seguridad en mente y que hay que resguardar de un modo transparente". En lo que respecta a servicios como DevOps o cloud, un enfoque Cloud Security Posture Management ayuda a dar esa capa de visibilidad, y a identificar riesgos, para mitigarlos. ■

MÁS INFORMACIÓN

- Mesa Redonda IT: Nuevos retos de seguridad en entornos financieros; su impacto en el modelo de negocio

JOSE FRANCISCO PEREIRO, GLOBAL HEAD OF PRIVACY TECH | RISK, BNP PARIBAS

“Un equipo de profesionales de seguridad capacitado y motivado es el mejor control para mitigar los riesgos”

En una situación como la que nos está tocando vivir hay que entender que el riesgo cibernético, lejos de reducirse, ha aumentado. Estamos viendo a través de los medios de comunicación como el cibercrimen está atacando multitud de empresas privadas y administraciones públicas con ataques de tipo ransomware, incluyendo infraestructuras críticas.

¿Cuáles son los principales retos de ciberseguridad a los que se enfrentan actualmente los servicios financieros?

Uno de los principales retos es gestionar el riesgo de terceras partes, la cadena de suministro se está transformando con velocidad y creciendo en volumen. Adicionalmente a la colaboración histórica con grandes multinacionales tecnológicas, es cada vez más frecuente en el sector financiero la colaboración con startups, fintech y multitud de nuevos socios. Estas organizaciones aportan sin duda innovación y nuevos modelos de negocio, pero es necesario evaluar con detenimiento los riesgos de seguridad y ayudarles a mitigarlos antes de comenzar una iniciativa conjunta.

Otro de los retos es la evolución y sofisticación de los ataques informáticos, cada vez más dirigidos y mejor ejecutados. Contra esto, además seguir trabajando en el diseño e implementación de nuevos controles técnicos para detener los ata-

ques, es fundamental entender el factor humano, puesto que muchos de estos ataques tienen como base de entrada la ingeniería social, que intenta explotar las debilidades que todos tenemos cuando somos expuestos a una situación de falso peligro o urgencia con el objetivo de influir en nuestra conducta. Por esto, ya no es suficiente con disponer de un programa formación en ciberseguridad, sino que es necesario cubrir tres dimensiones: formación, concienciación y entrenamiento. La segunda, la concienciación, hace referencia a la capacidad de crear impacto emocional para protegernos de situaciones de peligro, como muy bien se hace por ejemplo en las campañas de tráfico. La tercera, el entrenamiento, es la más importante y consiste en simular situaciones cercanas a un ataque cibernético para desarrollar las habilidades necesarias y responder adecuadamente cuando se produzca un ataque real.

El tercer reto es la captación y retención del talento en ciberseguridad. Un equipo de profesionales de seguridad capacitado y motivado es el mejor control para mitigar los riesgos, pero es necesario competir en un mercado laboral de nicho en el que cada vez hay más empresas interesadas en reclutar este tipo de profesionales. Por eso, además de desarrollar políticas de atracción para las nuevas generaciones, es necesario darse cuenta de que, muchas veces, el talento está más cerca de lo que se piensa y que una alternativa interesante es formar en ciberseguridad a profesionales que estén trabajando en otras áreas.

¿Cómo se han adaptado los servicios financieros a tecnologías emergentes como Blockchain o IoT?

Las tecnologías emergentes, como el Blockchain, IoT, AI, Big Data, Cloud y muchas otras, ofrecen sin duda una gran oportunidad para desarrollar nuevos modelos de negocio y de relación con nuestros clientes. Las ventajas de estas tecnologías suelen ser evidentes y crean un alto nivel de interés en las áreas de negocio. Sin embargo, por tratarse de tecnologías emergentes, no siempre hay experiencia en la industria que nos permita modelizar y dimensionar los riesgos de ciberseguridad de una forma estándar.

Por ejemplo, las arquitecturas Blockchain o DLT, que son reconocidas como de las más seguras en la actualidad por su base criptográfica, tienen ya algún riesgo identificado como el asociado al compromiso del 51% de los nodos de la red. Si bien ejecutar este tipo de ataque es extremadamente difícil en aplicaciones basadas en Blockchain públicos con decenas de miles de nodos, como es el caso de la criptomoneda Bitcoin, si hablamos de una implementación privada con sólo decenas de sistemas y sistemas homogéneos, el riesgo de este tipo de ataque se incrementa, por lo que es necesario de dotarlo de medidas adicionales.

Un caso particular de tecnología emergente es la computación cuántica que, cuando ésta alcance cierta escala, pondrá en riesgo la seguridad de muchos sistemas a nivel global, al poder romper el cifrado de clave pública en el que se basan muchos algoritmos criptográficos.

Por tanto, la aproximación adecuada con las tecnologías emergentes es la basada en un análisis pormenorizado de los riesgos, mediante una aproximación consultiva, dedicando profesionales de seguridad al estudio de las posibles fallas y la definición de los controles y tecnologías de seguridad necesarios, así como la realización de pruebas exhaustivas antes de su salida a producción.

¿Qué regulaciones están afectando al sector financiero y cómo se está haciendo frente a ellas?
El sector financiero es el más regulado desde hace muchos años, teniendo que cumplir con numerosos requisitos de información y reporting a agencias y bancos centrales de todo el mundo. Esto nos ha permitido disponer de una estructura empresarial y cultura organizativa que permite asimilar nuevas regulaciones con relativa ventaja a empresas de otros sectores. Dicho esto, y con relación al tema que nos ocupa, las regulaciones de privacidad que están surgiendo a lo largo del planeta, y en particular la GDPR en la zona europea, están teniendo un impacto significativo en los sistemas de información y en las medidas de ciberseguridad asociada.

Por un lado, se ha regulado el concepto de protección de datos en el diseño de nuevas aplicaciones y servicios, que tiene inherentemente asociada un componente de ciberseguridad. De esta forma, cada vez que se desarrolle un nuevo producto que procese datos de carácter personal, este deberá tener en cuenta las necesidades regulatorias y de seguridad. Además, la GDPR, en su artículo 32, establece la obligatoriedad de implementar las medidas de seguridad necesarias para proteger los datos proporcionalmente a los riesgos a los que está expuesta. La privacidad debe ser embebida en todas las arquitecturas y soluciones IT, por ejemplo, cuando antes estábamos hablando de tecnologías emergentes, la GDPR afecta en mayor o menor media en diferentes aspectos: el derecho al olvido en Blockchain, las transferencias de datos internacionales en Cloud, las decisiones automatizadas en la Inteligencia Artificial o el tratamiento masivo de datos en el Big Data.

> "Uno de los grandes retos es la evolución y sofisticación de los ataques informáticos, cada vez más dirigidos y mejor ejecutados"

Por último, la privacidad ha tenido un efecto más sutil, pero no menos influyente en el mundo de la seguridad. Hasta ahora, si una tecnología de seguridad se consideraba como buena para mitigar riesgos, se implementaba; pero tras la llegada de las regulaciones de privacidad a diversas partes del mundo es necesario asegurar que dichas tecnologías cumplen con la regulación. Por ejemplo, las tecnologías de detección de anomalías en el comportamiento de usuarios, que permitían detectar si una cuenta de usuario había sido comprometida, ya no podrán ser implementadas si no garantizan los derechos y libertades en materia de protección de datos.

Tras un año de pandemia, ¿qué han aprendido los CISOs del sector financiero?
La enseñanza fundamental es que la seguridad no se puede poner en ERTE. En una situación como la que nos está tocando vivir hay que entender que el riesgo cibernético, lejos de reducirse, ha aumentado. Estamos viendo a través de los medios de comunicación como el cibercrimen está atacando multitud de empresas privadas y administraciones públicas con ataques de tipo ransomware, incluyendo infraestructuras críticas. Además, durante esta crisis ha sido necesario tomar decisiones transcendentes en un plazo muy breve de tiempo, como la de tener que poner centenares de miles de trabajadores españoles a teletrabajar de la noche a la mañana. Estas decisiones, necesarias para la continuidad de negocio, si no son acompañadas por medidas de ciberseguridad que mitiguen los riesgos del nuevo escenario, pueden tener efectos adversos. De igual forma, los servicios bancarios online han pasado de ser una mejora a ser una necesidad, por lo que garantizar su continuidad y fiabilidad 24 horas al día frente a ataques es una de las prioridades.

Es necesario concienciar a la sociedad sobre el peligro real que supone el cibercrimen y hasta donde está dispuesto a llegar. Hemos visto como en los peores momentos de la pandemia han sido atacados los sistemas de información de algunos hospitales.

¿Qué tecnologías de seguridad considera imprescindibles para una empresa perteneciente al sector financiero?
Todas las tecnologías de prevención de fuga de datos son esenciales para evitar la filtración ac-

"El sector financiero es el más regulado desde hace muchos años, teniendo que cumplir con numerosos requisitos de información y reporting a agencias y bancos centrales de todo el mundo"

cidental o intencionada de información sensible. Es fundamental que estas estén integradas en los canales de comunicación con el exterior para monitorizar y bloquear las transferencias de datos sospechosas. Debemos asegurar que cubren todos los canales, no solo el email sino la subida de información a través de servicios web, la extracción de información a través de los puertos del ordenador e incluso también la impresión.

Dicho esto, se debe tener en cuenta que estas tecnologías son inútiles si no se definen e implementan las políticas adecuadas de identificación y bloqueo de contenidos y, para esto, el equipo de ciberseguridad no puede trabajar de forma autónoma, necesitará de la colaboración del negocio y otras áreas. Además, hay que asegurar que se dispone de un equipo de profesionales de seguridad cualificado para analizar y responder a las alertas emitidas. Sin políticas y profesionales, la tecnología DLP tendrá las mismas capacidades de mitigación del riesgo cibernético que instalar un jarrón en nuestro centro de datos, eso sí, muy caro.

Existen muchas otras que son esenciales bajo mi punto de vista, como las tecnologías y servicios para proteger frente a ataques de denegación de servicio, la protección frente al malware, el cifrado, la protección del perímetro, y los cortafuegos de aplicación y bases de datos.

¿Qué tecnologías que todavía no están ampliamente adoptadas, cree que serán imprescindibles en los próximos años?

En los últimos tiempos han aparecido nuevas posibilidades tecnológicas para la protección de los datos que deben ser exploradas por las entidades financieras para mitigar, aún más, los ciber-riesgos asociados a estos. La información es almacenada por las organizaciones en dos formatos: de forma estructurada, como por ejemplo las bases de datos; y de forma no-estructurada, como por ejemplo las hojas de cálculo.

En lo relativo a la protección de la información estructurada, a las técnicas tradicionales de anonimización y pseudo-anonimización, ampliamente empleadas como la tokenización o el masking, se unen nuevas alternativas como el uso de la encriptación homomórfica o los datos sintéticos. Es importante disponer de un portfolio amplio y contrastado de estas técnicas, puesto que no hay ninguna de ellas que, de forma individual, pueda cubrir todos los casos de uso del negocio.

Cuando hablamos de información no estructurada la situación es todavía más compleja, puesto que existen numerosos ficheros que son intercambiados diariamente como parte de la operativa normal del negocio financiero en interacciones internas y externas. Para esto es necesario implementar tecnologías que nos permitan garantizar la seguridad de los datos durante todo su ciclo de vida, siendo especialmente importantes las tecnologías de descubrimiento de la información y clasificación de los datos. Son también muy interesantes las tecnologías denominadas genéricamente como IRM, que nos van a permitir insertar las políticas de seguridad dentro del dato (control de acceso, trazabilidad, caducidad...), disponiendo de esta forma de la capacidad de proteger la información con independencia de dónde se ubique. ■

MÁS INFORMACIÓN

BNP Paribas

Más visibilidad.
Más potencia.
Más control.

¿No pensó estar preparado/a para el EDR?
Ahora lo está.

go.kaspersky.com/es_optimum

kaspersky PREPARADOS PARA EL FUTURO

Objetivos de la ciberseguridad en las entidades financieras:

protección de clientes, dispositivos y empresa ante los ataques

EUSEBIO NIEVA,
director técnico de
Check Point Software para España y Portugal

La ciberpandemia es uno de los peligros que actualmente están amenazando a cientos de compañías. Tras los meses en los que la Covid-19 ha obligado a miles de personas a extremar las precauciones para evitar el contagio y el uso del pago por móvil o la tarjeta de crédito se han instaurado como opciones masivas. Por ello, las entidades financieras se están convirtiendo en uno de los principales objetivos de los ciberataques, sobre todo, por el rédito económico que puede llegar a reportar el atacarlas.

Desde el comienzo de la pandemia, empresas de todos los sectores se han visto obligadas a implantar el teletrabajo con el consecuente incremento de los dispositivos móviles conectados a la red, aumentando considerablemente las brechas de seguridad y mejorando las oportunidades de éxito de los cibercriminales. Los frentes para los negocios se multiplican y contar una buena defensa es la única opción.

Debido a la situación, ahora se están llevando a cabo diferentes tipos de fraude y extorsión contra la banca, para de esta forma vulnerar la privacidad de estas compañías con el objetivo de llenarse los bolsillos. Así los datos respaldan la realidad del sector, ya que según Informe Global de Amenazas DNS 2020 elaborado por IDC de la mano de EfficientIP, en el 2020 cuatro de cada cinco empresas del ámbito financiero (79%) sufrieron más de diez ciberataques DNS a lo largo del año y cada uno de ellos supuso un coste de 1,16 millones de euros de media.

Uno de los mayores desafíos que tienen que afrontar las entidades financieras es la

seguridad móvil, tanto por el lado usuario como por el de sus trabajadores. Ahora más que nunca, el acceso a redes corporativas a través de móviles no securizados es un objetivo. Para ello, Check Point Harmony Mobile protege los dispositivos móviles de los empleados de todos los vectores de ataque (aplicaciones, red y sistema operativo). Este software está diseñado para reducir los gastos generales de los administradores y aumentar la adopción del usuario, escala rápidamente, evita descargas de aplicaciones maliciosas, impide el phishing en todas las aplicaciones previene ataques Man-in-the-Middle, bloquea aparatos infectados para que no accedan a aplicaciones corporativas y detecta técnicas avanzadas de jailbreaking y rooting y vulnerabilidades del sistema operativo.

En la otra cara de la moneda encontramos cómo estas entidades financieras pueden proteger a sus clientes, sus credenciales y datos personales cuando acceden a sus apps. La mejor manera de mantenerlas a salvo de los cibercriminales es contar con una protección adecuada. Impulsado por el motor de IA contextual de Check Point CloudGuard, Check Point CloudGuard AppSec es una solución que bloquea los ciberataques contra las aplicaciones, incluyendo: la desconfiguración del sitio web, la fuga de información y el robo del inicio de sesión del usuario. Para ello, es capaz de analizar cada solicitud en su contexto y asignándole una puntuación de riesgo, para una prevención precisa, eliminando los falsos positivos y evitando los más sofisticados ataques contra una aplicación, incluidos los ataques OWASP Top 10.

> “Todas las empresas pertenecientes al sector de la banca deben contar con software de protección en el total de sus emplazamientos y en todos los dispositivos que tenga conexión a su red”

Es imprescindible señalar que la banca debe contar con un software que sea capaz de proteger a la empresa de cualquier tipo de ciberataque a sus centros de datos. Esta herramienta debe mantener a salvo todos los archivos, documentación y datos pertenecientes a la propia sociedad y también de los clientes que forman parte de la misma.

Para lograr el objetivo, en Check Point Software contamos con Check Point Quantum Maestro, una solución que posibilita a las compañías ampliar fácilmente sus gateways de seguridad bajo demanda y crear nuevos servidores y recursos informáticos en la nube pública. Además, este software permite que un solo gateway se extienda hasta alcanzar la capacidad y el rendimiento de 52 en cuestión de minutos, lo que proporciona flexibilidad dinámica y un rendimiento máximo del firewall Terabit/segundo. Esta escalabilidad casi ilimitada permite soportar la alta velocidad de datos y contar con la latencia ultra baja de las redes 5G, una red que lo va a cambiar todo desde este mismo año y que será clave para todas las entidades financieras. Asimismo, hay que destacar el hecho de que llega a proteger a los entornos más extensos y con más recursos, estableciendo nuevos estándares en la seguridad de redes a hiperescala. Finalmente, es importante especificar que Check Point Quantum Maestro tiene la habilidad de extender las capacidades de seguridad Gen V de nuestra arquitectura Check Point Infinity a los entornos de hiperescala.

Si algo ha quedado claro en este último año es que todas las empresas pertenecientes al sector de la banca deben contar con software de protección en el total de sus emplazamientos y en todos los dispositivos que tengan conexión a su red para mantener a salvo todos los datos confidenciales que manejan frente a los posibles ciberataques. ■

Salvaguardar las transacciones, proteger al usuario

El financiero es uno de los sectores más afectados por los ciberataques avanzados, ahora muy enfocados en la banca móvil. Proteger al usuario frente a estas amenazas es imperativo, pero sin descuidar otros vectores, como la red SWIFT o los cajeros. La ciberseguridad de la banca debe evolucionar en la misma medida en que lo hacen los servicios.

A causa de los desafíos ligados a la pandemia el uso de la banca móvil se ha incrementado, y con ello el aumento de las ciberamenazas dirigidas contra los dispositivos móviles. Ante esta realidad, Eusebio Nieva, director técnico de Check Point, explica la importancia que tiene para estas entidades desarrollar una estrategia de ciberseguridad que englobe también este canal, con la integración de soluciones avanzadas de ciberseguridad móvil en sus apps.

En Check Point trabajan con varias entidades bancarias a las que proporcionan sus servicios de seguridad en forma de un interfaz de programación de aplicaciones (API) o de un kit de desarrollo de software (SDK) que se pueda consumir. Con esto se consigue trasladar la seguridad al dispositivo desde el cual el usuario está accediendo a los servicios, pero en vez de instalarla en dicho terminal, se pone a disposición de las entidades bancarias, de modo que cuando ellos lancen su propia aplicación de consumo o de servicios bancarios esta estará asociada a los servicios de seguridad de Check Point.

Otra consecuencia de la evolución hacia una banca más móvil, y en general más digital, es que el uso de cajeros automáticos (ATM) ha descendido, al igual que el empleo de efectivo. Hoy en día, y a causa de la pandemia, el dispositivo ubicuo que casi todo el mundo utiliza para hacer pagos es un terminal móvil o una tarjeta de crédito o débito. Sin embargo, y aunque el uso de ATM se ha reducido, lo cierto es que aún se siguen produciendo ataques contra dichas máquinas, por lo que es necesario seguir invirtiendo en su protección. Asimismo, hay que tener en cuenta que la tecnología que integra el cajero es muy antigua, por lo que es trascendental ir actualizando los servicios proporcionados por el cajero, así como la tecnología asociada a los mismos.

Además de no descuidar la defensa de los cajeros automáticos, las instituciones financieras que utilizan el sistema de pagos SWIFT también deben permanecer vigilantes. Las ofensivas contra esta red se han multiplicado en los últimos años, por lo que los bancos están implementando no solo medidas de seguridad estándar, sino también protecciones avanzadas, tecnologías de análisis de fraude, machine learning… para disuadir a los atacantes sobre su explotación, y frenar o impedir las transacciones fraudulentas o los intentos de falsificación de esas transacciones en la red de comunicaciones financieras. Nieva distingue que la tecnología de protección de las tarjetas bancarias o de los dispositivos móviles aún no está a la par con la tecnología de ataque utilizada por los ciberdelincuentes. En este sentido, sería necesario que nuevas metodologías o herramientas entraran en funcionamiento a fin de asegurar las transacciones, sobre todo desde el punto de vista del usuario que es quien las realiza. Con ello se podrían evitarse los fraudes y los ataques a dispositivos móviles con troyanos bancarios, con troyanos de tarjeta de crédito, etc. que pueden ser utilizados contra los usuarios. Por tanto, esta evolución paralela de servicios y ciberseguridad debe ser prioritaria.

Protegeré las claves, protegeré las claves, protegeré las claves…

JAVIER SANCHEZ FUERTES,
Territory Sales Manager,
Data Protections Solutions Entrust

Las empresas de servicios financieros se enfrentan a desafíos únicos en sus esfuerzos por proteger la información sensible de los clientes y cumplir con las regulaciones en evolución. El Repositorio de Confianza es fundamental aquí. La identificación y la autorización de los dispositivos, el cifrado y la verificación de los datos y las actualizaciones del software tienen algo en común, y ese denominador común es la criptografía. Y la base de la criptografía son las claves de cifrado que se necesitan para firmar y validar los certificados de los dispositivos para su identificación y autorización.

La mayoría de la infraestructura desplegada en los servicios financieros utiliza claves para el correcto desarrollo de sus funcionalidades, y en la mayoría de los casos esas claves carecen de la protección adecuada.

Por lo tanto, asegurar estas claves es fundamental, y ahí es donde entra en juego el Repositorio de Confianza para proteger y gestionar las claves de cifrado a lo largo de su ciclo de vida, completamente separadas del resto del sistema con hardware robusto y controles duales para garantizar que ningún individuo o entidad pueda subvertir las políticas establecidas para el uso de las claves.

De esta manera nuestros Hardware Security Module (HSM) nShield forman parte de esta ecuación. ¿Cómo se traduce esto en el mundo financiero?

Los certificados digitales son la forma en que las diferentes partes del ecosistema de pagos establecen la confianza entre sí. Estos certificados suelen ser emitidos por una PKI que se apoya en un Repositorio de Confianza. En la raíz de una PKI se encuentran claves criptográficas fuertes y de confianza creadas en un Hardware Security Module o HSM. Los HSM de Entrust nShield proporcionan una garantía sólida y certificada a un despliegue de PKI al tiempo que facilitan la automatización de la renovación de certificados y firmas, manteniendo las claves criptográficas privadas en un entorno seguro. Pueden desplegarse en otras áreas del nuevo ecosistema de pagos allí donde se requieran servicios criptográficos desde un entorno seguro y de confianza.

Piense en monedas virtuales, seguros, préstamos, grandes minoristas, aplicaciones bancarias móviles, etc. Los HSM de uso general pueden realizar tareas como la protección y validación del PIN, y la gestión de claves, también se despliegan como parte de las soluciones de procesamiento de pagos y puntos de venta móviles con partners de la industria. No olvidando la protección de las claves de firma y el proceso de firma de código de las Apps, el elemento de relación principal entre cliente y entidad financiera.

> "Las empresas utilizan diariamente miles de claves en sus procesos de negocio que deben protegerse de forma conveniente y evitar que sean comprometidas"

Están surgiendo nuevos servicios de pago al realizar compras en línea o a través del teléfono móvil, especialmente en Europa. El cambio puede ser un resultado directo de la PSD2, la última Directiva de Servicios de Pago. Las organizaciones de servicios financieros se enfrentan a desafíos únicos en sus esfuerzos por proteger la información sensible de los clientes y cumplir con las normativas en evolución. Merece la pena recordar que la certificación de los HSM de nShield según NIST FIPS 140-2 y Common Criteria ofrece a los clientes la garantía de que están seleccionando un producto validado según algunas de las normas de seguridad más rigurosas.

Las organizaciones financieras también siguen adoptando tecnologías nuevas y emergentes, como la nube y los contenedores, que, si bien ofrecen posibles eficiencias y reducciones de costes, amplían la huella digital de la organización. Estas organizaciones necesitan tener el control sobre las claves de cifrado que utilizan los proveedores de nube pública y de esta manera será Entrust con el cliente quienes definan las políticas y permisos asociadas a las mismas. No es una cuestión de confianza sobre los proveedores de nube pública sino de control sobre los datos y a afrontar sus retos de seguridad en la nube.

Uno de los principales obstáculos para la adopción más amplia de Blockchain es la seguridad. A medida que las organizaciones continúan encontrando nuevos e innovadores casos de uso para Blockchain, la seguridad debe incorporarse desde el principio. Entrust ayuda a abordar los desafíos de seguridad fundamentales asociados con las implementaciones de Blockchain: creación de claves, protección del proceso de firma y protección de la lógica de consenso. Debido a que se encuentra alojado dentro de los límites seguros del HSM nShield, CodeSafe ofrece protección certificada FIPS 140-2 Nivel 3 para su código más confidencial.

En definitiva, las empresas utilizan diariamente miles de claves en sus procesos de negocio que deben protegerse de forma conveniente y evitar que sean comprometidas con los consecuentes riesgos que eso significa. ■

Proteger la clave para salvaguardar el dato

Los desafíos de la regulación y el cumplimiento de la seguridad de los datos son muy altos en el entorno financiero. Por ello y a medida que evolucionan las amenazas cibernéticas, la combinación de integración tecnológica y análisis avanzado es más necesaria nunca.

Por la naturaleza de su negocio, las compañías financieras siempre han tenido que ser pioneras en cuanto al uso de medidas de seguridad, y en concreto en lo que se refiere al uso de cifrado y de Módulos de Seguridad de Hardware (HSM). Ahora, cuando la digitalización avanza rápidamente y la información fluye por distintos entornos (local, cloud, IoT) esto es más importante que nunca. Sobre ello, Javier Sánchez Fuertes, Territory Sales Manager de Entrust, observa que esa actitud pionera sigue manteniéndose, y lejos de quedarse anclada en el medio de pago, ha ido extendiéndose a otros casos de uso dentro del mundo financiero, para, por ejemplo, la protección de la infraestructura de clave pública (PKI), de los procesos de firma electrónica o de los procesos de negocio, entre otros.

Por otro lado, se habla mucho de la seguridad de los datos de manera genérica, pero hay un aspecto específico que es la seguridad de los datos en reposo que a veces pasa desapercibida. ¿Cuál es el reto en estos casos?

Sobre su importancia, Javier Sánchez cree en las empresas en general y en las financieras en particular se realizan importantes inversiones para proteger el entorno de red o el endpoint, abandonando en muchas ocasiones al dato, que por sí mismo no puede defenderse. El desafío, por tanto, pasa por identificar cuáles son los datos críticos para una entidad financiera y, sobre ellos, aplicar medidas de cifrado y por supuesto de protección de las claves. No hay que olvidar que las políticas de cifrado son tan seguras como lo son la protección de las claves.

Parece que la tecnología de cadena de bloques, Blockchain, está llamada a transformar el mundo de la banca. Sin embargo, el despliegue de servicios financieros sobre esta tecnología presenta retos en cuanto a seguridad. A este respecto, Javier Sánchez explica que la adopción de Blockchain en el mundo de la banca debe hacerse con cuidado. Los clientes depositan su dinero en un banco porque confían en dicha entidad.

En este sentido, Javier Sánchez explica que en Blockchain cada transacción que se envía a un bloque va firmada y por ese motivo lleva asociada una clave, y como hay una clave necesariamente debería haber un Módulo de Seguridad de Hardware (HSM). Desde Entrust lo que se propone es la protección de esas claves criptográficas y de esos procesos de firma, incluso de consenso, para que se realicen de forma segura mediante el uso de HSMs.

Además de trabajar en la seguridad y privacidad de Blockchain, las organizaciones financieras deben cuidar y conservar también sus claves, que están más desamparadas. En este contexto, y a raíz del crecimiento de la banca digital y móvil, el número de transacciones a través de estos medios se ha multiplicado. Por ello, Javier Sánchez incide también en lo crucial que resulta salvaguardar la clave utilizada para firmar el código de una app bancaria. Es más, teniendo en cuenta que la aplicación es, al final, el instrumento de relación entre el banco y los clientes, extremar las medidas de seguridad para resguardar esta aplicación no es baladí. De hecho, hoy por hoy, es su principal herramienta de negocio, por lo que hay que custodiarla.

La amenaza del malware financiero

se mantiene constante en España

ALFONSO RAMÍREZ,
director general
Kaspersky Iberia

La seguridad financiera es una de las preocupaciones más comunes tanto para los usuarios finales como en el mundo empresarial. Y es que las ciberamenazas en este campo son cada vez más peligrosas, y afectan al bienestar económico de las víctimas, ya sean individuos u organizaciones.

Según señala nuestro último informe anual sobre Ciberamenazas financieras en 2020, España fue el tercer país del mundo y primer país europeo con mayor incidencia de amenazas financieras el año pasado. Los troyanos bancarios, que suelen emplear ingeniería social para engañar al usuario y que los descargue, implica que cualquiera pueda encontrarse en el buzón de entrada de su correo, su WhatsApp o su lista de SMS con mensajes maliciosos que pretenden infectarlo.

De hecho, la incidencia de los virus informáticos diseñados para robar credenciales bancarias se sitúa entre las principales amenazas que afrontan los usuarios en Internet y el correo electrónico es el vector de ataque más habitual. En el mismo los cibercriminales se hacen pasar por una empresa (banco, empresa de envíos…) o por un organismo oficial (la Agencia Tributaria, Correos, DGT…).

Otro de los enfoques habituales utilizados por los atacantes para obtener acceso a las cuentas de los usuarios incautos es asumir el papel de "rescatador", fingiendo ser expertos en seguridad. Los atacantes llaman a los clientes de los bancos haciéndose pasar por expertos de seguridad e informan de cargos o pagos sospechosos para posteriormente ofrecer su ayuda. Bajo ese disfraz, el atacante puede pedir a los clientes

“La clave reside tanto en la protección como en la concienciación, de manera que los distintos ataques a los datos financieros no lleguen a causar daños”

que verifiquen su identidad mediante un código enviado en un mensaje de texto o una notificación push, que detengan una transacción sospechosa o que transfieran dinero a una “cuenta segura”. También pueden pedir a la víctima que instale una aplicación para la gestión remota fingiendo que es necesaria para la resolución de problemas. Los estafadores suelen presentarse como empleados del mayor banco de la región de la víctima potencial y utilizan un identificador de llamadas falsificado para las llamadas entrantes para hacerse pasar por un banco real.

Un tercer caso clásico es aquel en el que los ciberdelincuentes actúan como “el inversor”. En este caso, los estafadores se hacen pasar por empleados de una empresa de inversión o por asesores de inversión de un banco. Llaman a los clientes ofreciéndoles una forma rápida de ganar dinero invirtiendo en criptomonedas o acciones directamente desde la cuenta del cliente, sin tener que personarse en una sucursal bancaria. Como requisito previo para prestar el “servicio de inversión”, el falso inversor pide a la víctima el código recibido en un mensaje de texto o en una notificación push. El objetivo final siempre es el mismo: engañar al usuario para que haga ‘clic’ y descargue el código malicioso en su equipo. A partir de ese momento, los ciberdelincuentes tienen acceso a la información.

En este tipo de ataques el objetivo principal suelen ser las credenciales bancarias, que luego se venden en la darkweb por precios realmente bajos. Datos de tarjetas de crédito, acceso a servicios bancarios y de pago electrónico son mercancía habitual en este tipo de mercados.

Ante este panorama, la clave reside tanto en la protección como en la concienciación, de manera que los distintos ataques a los datos financieros no lleguen a causar daños. Así, para ayudar a los particulares y a las empresas a estar protegidos frente a las técnicas de fraude en constante evolución, es importante adoptar una serie de medidas básicas como, por ejemplo, limitar el número de intentos para realizar una transacción, de manera que los ciberdelincuentes no pueden intentar introducir varias veces las credenciales. Otra recomendación que muchas entidades financieras ya han puesto en marcha es informar de forma periódica a sus clientes sobre los posibles trucos que pueden utilizar los ciberdelincuentes, con información para saber cómo identificar el fraude y la mejor manera de comportarse ante estas situaciones.

En cuanto a las medidas de protección, la recomendación es realizar auditorías de seguridad y pruebas de penetración anualmente con el fin de detectar problemas de seguridad en la red de la empresa, contar con un equipo de análisis de fraudes capaz de encontrar y analizar los métodos emergentes que utilizan los defraudadores, implementar la autenticación multifactor para minimizar la posibilidad del robo de cuentas e instalar una solución de prevención del fraude que pueda adaptarse rápidamente para identificar nuevos esquemas y métodos de ataque. ■

MÁS INFORMACIÓN

Todo sobre EDR y MDR

Inteligencia de amenazas para prevenir el fraude

En línea con su evolución tecnológica, el sector de los servicios financieros es un objetivo esencial para los ciberdelincuentes y soporta gran parte de sus ataques. Es por eso que las entidades financieras no deben bajar la guardia. Sobre este aspecto, Luis Javier Suárez, Presales Manager de Kaspersky Lab, destaca que se vienen observando una serie de tendencias dirigidas a integrar metodologías basadas en agile, en la constante evolución de los aplicativos, y que, aunque en ocasiones incluyen la seguridad en el punto inicial, no siempre es así. Por ello, es crucial no descuidar la protección y seguir estrategias DevSecOps que siempre tienen la seguridad en mente.

A esta problemática se unen otros asuntos como la heterogeneidad de sistemas o la persistencia de sistemas legacy, que contrastan con nuevos desarrollos y la evolución hacia otros entornos como cloud. Sobre la nube, Luis Javier Suárez cita la falta de visibilidad como un inconveniente acuciante, ya que no tener conocimiento de lo que allí ocurre puede derivar en peligros como el Shadow IT.

El ritmo de evolución de las tecnologías también tiene que ser tenido en cuenta, sobre todo, porque es bidireccional. Bajo esta premisa y para poder contrarrestar ataques cada vez más sofisticados, es importante contar con servicios o programas de inteligencia de amenazas que ayuden a identificar y analizar las ciberamenazas dirigidas contra la empresa.

Sin embargo, añadir mayor seguridad puede perjudicar la experiencia del usuario, algo que en este sector es muy importante. ¿Cómo se puede aplicar seguridad sin impactar en la experiencia de usuario?

Para Luis Javier Suárez transformar la seguridad en algo que no sea invasivo e incómodo para la experiencia del usuario es complicado, máxime cuando desde el punto de vista de gestión de proyectos se pone mucho foco en esta experiencia. En este sentido, observa que existe una tendencia en el mercado hacia la integración de plataformas o entornos que sean Secure by Design, los cuales, por otra parte, sería conveniente acompañar también de un ciclo de adopción y mantenimiento. Además, no hay que olvidar que la integración de nuevas tecnologías puede traer consigo nuevos vectores de ataque y que tanto el actual auge del comercio electrónico como la preponderancia del cliente como eje central de la experiencia (customer centric) hacen necesaria la existencia de sistemas para apoyar esa seguridad. También debe haber una capa de información (sistemas antifraude) que permita detectar posibles campañas a fin de poder actuar en la fase más temprana.

A raíz de la creciente digitalización y teniendo en cuenta la sensibilidad del activo que aquí se gestiona, el dinero, Luis Javier Suárez valora que, aunque no habrá grandes cambios en cuanto a técnicas de ataque, si se incrementarán las campañas de ransomware dirigido, ataques contra cajeros automáticos (ATMs) y otros fraudes derivados del aumento de los canales digitales. El auge del mercado cripto también traerá consigo campañas focalizadas, desde phishing a otras más sofisticadas.

Por ello, y para asegurar la protección de sus activos, Luis Javier Suárez incide en la importancia de la concienciación de empleados y usuarios, y en la resiliencia. En este contexto, recomienda la adopción de tecnologías Endpoint Detection and Response (EDR), que permiten tener una visibilidad extendida de lo que ocurre dentro del entorno, y también la implantación de un Plan de Respuesta a Incidentes para, llegado el momento, poder aplicar una serie de medidas para contrarrestar el incidente. Este plan ayudará a alcanzar un nivel mayor de resiliencia.

Pagos, transacciones y dinero digital:

una realidad que ha venido para quedarse

JESÚS RODRÍGUEZ,
CEO Realsec

Hace algo más de un año todo cambió en nuestras vidas y un claro ejemplo de ello es la diferente forma en la que hoy compramos y hacemos uso de los medios de pago, donde la transformación digital es la protagonista de esta nueva situación social y económica.

Todo esto, se evidencia en diferentes acciones como el incremento de las compras a través de los sistemas de comercio electrónico, cuyo crecimiento, durante 2020 en España, ha sido de un 67% junto con la proliferación de la banca electrónica y la banca móvil, que ha pasado de un 44% a un 57% en su ratio de uso. Así mismo, se ha multiplicado el uso de las Apps de pago sobre teléfonos móviles, lo que se conoce como Open Banking (Amazon Pay, Samsung Pay…), las tarjetas virtuales prepago, los sistemas wallets, los pagos contactless, el Internet de los Pagos (IoP) a través de dispositivos inteligentes conectados en la red de Internet de las Cosas y la tokenización de las tarjetas. Todo ello, sumado a una gran expansión de nuevos agentes financieros como las Fintechs y la consolidación de las "finanzas descentralizadas" o DeFi, donde tienen su origen las criptomonedas, los smarts contracts y las Apps construidas en tecnología Blockchain.

El número de transacciones de este nuevo ecosistema financiero digital representa un porcentaje superior a las operaciones de pago en efectivo, cuyo descenso en 2020 se cuantifica en un 45%, aunque no debemos olvidar que, para su efectividad, transparencia y confianza, es fundamental implementar una securización robusta.

“Esta nueva economía requiere avanzar hacia una situación en la convivan el dinero fiduciario y las monedas digitales en un marco regulado y ordenado por los Bancos Centrales”

El riesgo de fraude online crece, exponencialmente, asociado al crecimiento de los medios de pagos digitales; es por ello, que las entidades financieras necesitan reforzar la seguridad implementando medidas como la autenticación de doble factor en base a la Directiva PSD2 o mayor transparencia y gobernanza en el caso de utilizar tecnologías como Blockchain para realizar pagos digitales transfronterizos, operaciones de compensación bancaria o intercambio de cédulas de pago internacional. Así como en la gestión confiable de los cripto-activos o la securización de los entornos de pago asociados al Internet de las Cosas “Blockhain of Things”

Aunque hoy la tecnología disruptiva Blockchain por inmutabilidad, descentralización y transparencia puede considerarse confiable para determinados procesos de negocio, podemos robustecerla, en el ámbito financiero, con la implementación de módulos criptográficos HSM (Hardware Security Module) que fortalecen la infraestructura de la red Blockchain, ya sea ésta pública, privada o híbrida, tanto para las operaciones financieras, gestión de criptomonedas y la protección de otros procesos de negocio.

El crecimiento de los pagos digitales en más de un 30%, a nivel mundial durante el último año, junto con los nuevos canales digitales, en detrimento del uso del efectivo, sumado a la proliferación de las monedas digitales (CBDC) y criptodivisas en un mercado no regulado (salvo excepciones como el caso del e-Yuan chino, pero con anuncios y expectativas de una futura regulación por parte de muchos Bancos Centrales del mundo, como el BCE con la creación de Euro Digital) supone asumir la realidad de una nueva economía. La que muchos denominan “Cripto-economía”, puesto que aquí la criptografía desempeña un papel clave para la protección y la seguridad de los activos financieros que traerá consigo una mayor adaptación y confianza, tanto a los usuarios del nuevo espectro digital como a las entidades financieras, interesadas siempre en minimizar los riesgos de seguridad en los medios de pago, como la suplantación de la identidad o el fraude.

Sin duda, esta nueva economía requiere avanzar hacia una situación en la convivan el dinero fiduciario y las monedas digitales en un marco regulado y ordenado por los Bancos Centrales en el que las nuevas tecnología disruptivas, como el Blockchain, cumplan con los mismos o superiores niveles de exigencia, en materia de seguridad, a los exigidos por la Banca, como es el uso una criptografía robusta para proteger las transacciones financieras, avalada por un organismo acreditado internacionalmente, como la Certificación PCI HSM PTS en el ámbito de los medios de pago.

Para conocer más sobre la situación y el estado del arte de esta tecnología en España y América Latina les animamos a leer el II Informe de Blockchain de REALSEC, elaborado junto con IDC. ■

La ciberseguridad como factor de confianza

El sector financiero se enfrenta a un ambiente regulatorio estricto, con muchas normas que acatar y exigencias en cuanto a protección y seguridad muy explícitas. Tal situación, no obstante, ha favorecido que se haya convertido en uno de los nichos más avanzados en cuanto a ciberseguridad. A este respecto, Jesús Rodríguez, CEO de Realsec, destaca que, si bien antes de la pandemia la banca ya trabajaba en determinados procesos de transformación digital, el confinamiento ha acelerado extraordinariamente este desarrollo. Sin embargo, el crecimiento de la banca electrónica y móvil ha repercutido también en un incremento de los ciberataques y en un mayor riesgo de fraude, activando la demanda de soluciones y sistemas de cifrado para la protección de transacciones y de otros procesos de negocio.

No obstante, Jesús Rodríguez aclara que la banca siempre ha cuidado mucho todo lo relacionado con ciberdelincuencia. Es un factor de confianza, el mayor de todos, por lo que a medida que el nivel de ciberriesgo ha evolucionado, se han ido implantado soluciones de protección para mitigar estas amenazas. Adicionalmente, y en lo que respecta a la parte de medios o sistemas de pago, la tecnología de criptografía bancaria ha prosperado como sistema de protección, al igual que la orientada al tratamiento seguro de las transacciones electrónicas, la protección de la información y de los datos mediante el cifrado.

La usabilidad de la tecnología de blockchain también se ha extendido, y no solo para la gestión de criptoactivos, sino para otros procesos de negocio como la compensación electrónica o los pagos transfronterizos. Sin embargo, esta tecnología debe considerarse, además de por sus capacidades de eficiencia y trazabilidad, por sus características de seguridad. Los bloques pueden ser cifrados y dentro de la tecnología de blockchain se pueden utilizar contratos inteligentes (smart contract).

Aunque fue el año pasado cuando la normativa PSD2 entró en vigor, su acatamiento ha estado posponiéndose durante los últimos años a través de varias moratorias. En ese tiempo, las entidades bancarias han estado preparándose, trabajando en una doble dirección: el desarrollo de APIs, para permitir el acceso a nuevos actores en el ámbito financiero y en la autenticación de doble o triple factor para cumplir con la directiva de pagos PSD2. Al respecto de su acatamiento, y aunque no se puede decir que ningún banco español esté cumpliendo con la directiva en sí, si se puede aseverar que no todas las entidades financieras están utilizando soluciones de tokenización para su observancia. Dichas soluciones han sido reemplazadas por SMSs con una clave adjunta que el usuario utiliza para demostrar que es quién realmente dice ser durante la operación financiera.

La banca está ahora mismo viviendo una situación revuelta; una fase de adaptación. La crisis económica generada por la pandemia está obligando a sus entidades a adoptar una serie de medidas para no perder competitividad y rentabilidad. Así, y aunque los bancos llevan tiempo trabajando en la gestión de activos, en las criptomonedas, se está produciendo una tendencia creciente a cambiar activos financieros y efectivo por criptodivisas. Sobre ello, Jesús Rodríguez considera que según avance la regulación, esta realidad irá asentándose. Previsiblemente se avanzará hacia un euro digital regulado (algo en lo que está trabajando el Banco Central Europeo) y se extenderá la usabilidad del blockchain hacia otros procesos de negocio, como los arriba comentados.

Síguenos en:

SOLUCIONES DE CIBERSEGURIDAD_

- HSM de Propósito General
- HSM Financiero
- Remote Key Load
- Soluciones de Cifrado, Firma Digital y Sellado de Tiempo
- Soluciones PKI
- Ciberseguridad Blockhain&IoT

www.realsec.com

realsec
La clave para proteger su negocio

OFICINAS CENTRALES
C/ Infanta Mercedes 90. Planta 4. 28020 Madrid
Tfno.: +34 91 449 03 30 - E-mail: info@realsec.com

MÉXICO
Avda. Ejército Nacional, 1112 Despacho 404 Piso 4
Colonia Los Morales C.P. 11510. Ciudad de México
Tfno.: + 52 (55) 44 35 00 46 - E-mail: infomexico@realsec.com

USA
303 Twin Dolphin Dr Suite 600 Redwood City, CA 94065
Tfno.: +1 (650) 632 4240 - E-mail: sales@realsec.com

SINGAPUR
REALSEC Inc.12 Marina Boulevard.
MBFC Tower 3. Level 17-01. Singapore 018982
Tel. +65 6809 5001 • infoapac@realsec.com

El sector financiero, en el punto de mira de los cibercriminales

IGOR UNANUE,
CTO S21sec

La ciberdelincuencia es, desafortunadamente, un factor de riesgo para varios sectores como el sanitario, el público o el educativo, pero la industria financiera es y seguirá siendo uno de los sectores más vulnerables a los ciberataques. Desde siempre, el sector financiero ha estado expuesto al cibercrimen, ya que en el 90 por ciento de los casos la motivación de los atacantes es puramente económica. Tal y como detectamos en 2019, los ataques hacia entidades financieras aumentaron de forma notable y los cibercriminales encontraron vías muy sencillas de penetración en dichas organizaciones a través de simples ataques de ingeniería social vía correo electrónico. Desde entonces, los cibercriminales cuentan con más y mejores recursos.

Este año, además de sufrir el típico malware financiero, el sector financiero podría ser víctima de ataques de robo de información relacionada con credenciales bancarias, datos de tarjetas de crédito o sufrir ataques Zero-Day, donde los cibercriminales se aprovechan de las vulnerabilidades y utilizan códigos maliciosos para desplegar los ataques. Muchas entidades financieras ya cuentan con sus propios sistemas de protección para hacer frente a ataques recurrentes como el phishing o el envío de información falsa mediante correo electrónico. No obstante, hay muchos nuevos software maliciosos que van surgiendo y que no son tan fáciles de identificar.

En este sentido, desde S21sec nos encargamos de monitorizar la actividad de los cibercriminales y de detectar todas las nuevas

“Toda entidad financiera debería contar con un buen sistema de detección para así identificar malware, detectar movimientos laterales o cualquier otro tipo de ataque”

amenazas que puedan afectar al sector financiero. Cada día, se identifican casi 15.000 malware diarios y la clave reside en averiguar a qué tipo de entidades afectan y qué banco en concreto está siendo víctima de dicho ataque. Nos encargamos de recuperar la información robada, además de proporcionar nuestros servicios de SOC y equipos de servicios profesionales que trabajan en proyectos de integración, consultoría o en la parte de auditoría. La consultoría en entidades financieras es muy importante debido al cumplimiento normativo que les impone implantar medidas de seguridad.

Otro aspecto a tener en cuenta es que debe haber un equilibrio entre la seguridad y la experiencia del cliente; es decir, añadir mayor seguridad puede perjudicar la experiencia del cliente, y en el sector financiero, no es fácil limitar el acceso mediante seguridad porque las entidades deben seguir funcionando. Además, la pandemia ha impulsado el teletrabajo y el uso de la banca online, con lo que es complicado imponer una seguridad total en este sentido. La única solución al respecto es estar alerta y seguir controlando la seguridad en paralelo, identificando los puntos más débiles que puedan suponer un riesgo para la compañía. En S21sec consideramos que esa es la gestión del riesgo que toda entidad y compañía financiera debe realizar, ya que imponer medidas de seguridad extremas supondría entorpecer el funcionamiento de la compañía, debiendo hacer un esfuerzo por identificar correctamente el punto de entrada más vulnerable para así implantar medidas de seguridad, como por ejemplo establecer reglas de correlación, puntos de control y sistemas preventivos.

No hay que olvidar que los cibercriminales siempre llevan a cabo sus ataques aprovechando las vulnerabilidades de los grandes fabricantes y, por ello, es imprescindible mantener los sistemas parcheados y protegidos para evitar cualquier fuga de información; es algo que el sector financiero debe tener muy claro para protegerse contra los ciberataques. Asimismo, también es importante saber que muchos de los ataques recientes han sido silenciosos y difíciles de detectar porque utilizan nuevos sistemas de ataque, de manera que los ataques son lentos y no se identifican inmediatamente.

Por ello, desde S21sec recomendamos a todo el sector financiero tener un sistema de monitorización constante y estar siempre alerta ante nuevas amenazas. Toda entidad financiera debería contar con un buen sistema de detección para así identificar malware, detectar movimientos laterales o cualquier otro tipo de ataque. Además, también es recomendable que estén al tanto de todo lo que ocurre en las redes, visualizar las vulnerabilidades y tener en cuenta que las entidades financieras estarán siempre expuestas al riesgo de los ciberataques. ■

Seguridad gestionada para mitigar los riesgos

El sector financiero siempre ha estado en el punto de mira de los cibercriminales, dado que, además, en el 90% de las ocasiones estos actores se rigen por una motivación financiera. No obstante, Igor Unanue Buenetxea, CTO de S21sec, reconoce que no es el que sufre el mayor número de ataques, aunque si al que llegan los más tradicionales, como los dirigidos contra sus clientes.

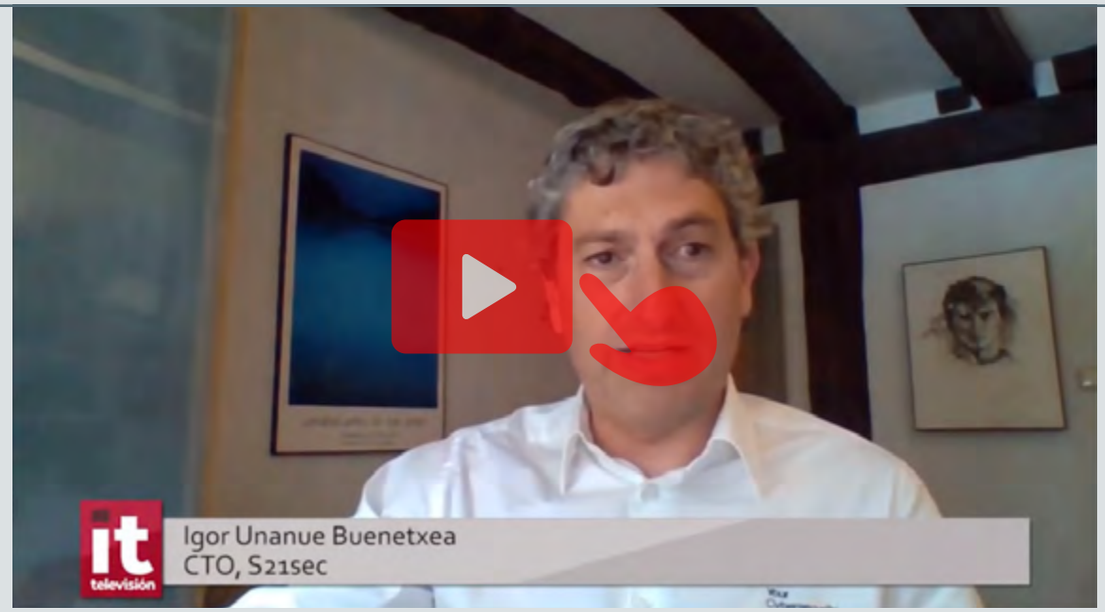
Aunque el malware financiero siempre ha existido y seguirá en activo, desde S21sec consideran que, durante 2021, tendrán mayor relevancia las vulnerabilidades Zero Day y los ataques dirigidos destinados al robo de información (credenciales, datos personales, tarjetas de crédito).

Asimismo, Unanue alerta sobre el cibercrimen bancario, el cual se está expandiendo sin pausa, y al que desde la propia empresa hacen frente a través de la monitorización de los cibercriminales, para no dejar escapar malware nuevo. En este contexto, S21sec analiza diariamente más de 15.000 muestras, lo que le permite averiguar a qué tipo de entidades afecta, incluso un banco concreto. Adicionalmente, S21sec recupera credenciales robados, monitoriza constantemente la Deep Web en busca de tarjetas de crédito e información robada a las entidades financieras (análisis en profundidad continúo). También ofrece servicios de seguridad gestionada en remoto (SOC) 24/7 y cuenta con un equipo de servicios profesionales que trabaja en proyectos de integración, auditoría y consultoría.

Sobre este último, Igor Unanue reconoce que la acción de consultoría es muy importante para este tipo de organizaciones, ya que deben implementar medidas de seguridad concretas para acatar el cumplimiento normativo. Estas, además, deben estar muy bien implantadas, ya que serán auditadas por el Banco Central Europeo (BCE).

No obstante, a veces, añadir mayor protección pueden perjudicar la experiencia del usuario; por lo que el reto está en obtener ese equilibrio para aplicar seguridad sin impactar en la experiencia de usuario

A este respecto, Igor Unanue comenta la dificultad que entraña conjugar ambos aspectos. Limitar el acceso o las comunicaciones con mecanismos de seguridad no es tan sencillo, más si cabe, ahora, con la mayor parte de las plantillas teletrabajando y los clientes operando a través de banca digital. Hay que dejar abiertas ciertas puertas para que la comunicación fluya, la economía funcione, mientras se controla la seguridad, sobre todo en los puntos de mayor riesgo. Para ello es necesario llevar a cabo una monitorización 24/7, desplegar sistemas preventivos, reglas de correlación… En definitiva, aplicar medidas de seguridad optimas sobre ese punto, para monitorizar y no siempre bloquear.



Además de desplegar una estrategia de gestión de riesgo basada en la defensa de los puntos más sensibles, desde S21sec recomiendan vigilar las vulnerabilidades Zero Day que se producen, ya que últimamente se han detectado un alto número en productos de grandes fabricantes (desplegados en organizaciones financieras). En este sentido parchear los sistemas es clave, así como mantenerlos actualizados y monitorizados. También el despliegue de un sistema de detección Endpoint Detection and Response (EDR) para poder detectar movimientos laterales, de malware y otro tipo de ataques en los puestos finales y servidores, además de monitorizar y gestionar todo lo que ocurre en las redes y que les pueda aplicar a ellos como entidades financieras. No en vano, siempre van a estar en el punto de mira de los ciberdelincuentes.

Gestión de la seguridad de los datos en tiempos de crisis para las instituciones financieras

ALFONSO MARTÍNEZ,
Country Manager Iberia, Thales Digital Identity & Security

En una crisis mundial sin precedentes como la de la COVID-19, las organizaciones que han implantado nuevas tecnologías y han elaborado un enfoque coherente de su planificación de la continuidad de la actividad y de gestión de crisis, parecen salir mucho mejor paradas.

Esto es especialmente cierto para las instituciones financieras que ahora se enfrentan a nuevos retos de ciberseguridad debido a la pandemia. Según el último informe Modern Bank Heists, la pandemia de COVID-19 se ha relacionado con un aumento del 238% en los ciberataques contra bancos de todo el mundo.

Dado que una filtración de datos puede afectar significativamente a múltiples funciones dentro de una organización, la protección de los datos debe ser responsabilidad de todos los departamentos, además del equipo ejecutivo, para garantizar la continuidad del negocio sin fisuras.

Para ilustrar esto aún más, a continuación se muestra cómo las brechas de datos pueden afectar a funciones cruciales en una institución financiera:

1. FINANZAS

Según el "Informe sobre el coste de una filtración de datos en 2019" ("2019 Cost of a Data Breach Report ") realizado por el Ponemon Institute, el coste medio de una brecha de datos se cifra en 3,92 millones de dólares a nivel mundial. Esta cifra es testimonio del importante daño financiero que cualquier in-

“La mitigación de los riesgos de los datos depende de las inversiones estratégicas en tecnologías de protección de datos y de la adopción de las mejores prácticas de ciberseguridad”

cidente de brecha de datos puede causar a una organización.

2. LEGAL

La mayoría de las normativas de protección de datos, como el Reglamento General de Protección de Datos (RGPD), el Estándar de Seguridad de Datos del Sector de las Tarjetas de Pago (PCI DSS)... obligan a seguir procesos estrictos para proteger los datos sensibles y prescriben sanciones rigurosas en caso de incumplimiento. El incumplimiento de estos mandatos legales puede costar caro a una empresa, como ha experimentado recientemente el operador de telecomunicaciones italiano TIM, que ha sido sancionado con 27,8 millones de euros por la Autoridad de Protección de Datos italiana, Garante, por incumplimiento del GDPR.

3. LÍNEA DE NEGOCIO (LOB)

Las brechas de datos pueden comprometer drásticamente las aplicaciones empresariales básicas, como los sistemas de gestión de créditos, los sistemas de gestión de las relaciones con los clientes (CRM), los sistemas de bases de datos de tarjetas de crédito/débito, etc. La indisponibilidad de estas aplicaciones críticas (que a menudo son el objetivo de los piratas informáticos) puede causar una pérdida significativa de la confianza de los clientes y del negocio.

En este contexto, es fundamental que las instituciones financieras refuercen su resistencia cibernética con herramientas y soluciones adecuadas.

La mitigación de los riesgos de los datos depende de las inversiones estratégicas en tecnologías de protección de datos y de la adopción de las mejores prácticas de ciberseguridad.

A continuación, se presentan tres mejores prácticas para construir una ciberseguridad sin fisuras para una óptima protección de los datos de la empresa.

1. Cifrar los datos sensibles

Busque en los servidores de archivos, las aplicaciones, las bases de datos y las máquinas virtuales los datos en reposo, y rastree los datos en tránsito que fluyen por la red corporativa entre ubicaciones lejanas. Una vez identificados y rastreados estos datos sensibles, es crítico cifrarlos para hacerlos inútiles a los hackers en caso de un ciberataque.

2. Almacenar y gestionar de forma segura las claves de cifrado

Las claves de cifrado pasan por múltiples etapas a lo largo de su vida: generación, distribución, rotación, archivo, almacenamiento, copia de seguridad y destrucción. Gestionar estas claves en cada etapa de su ciclo de vida a través de una solución de gestión de claves centralizada, es fundamental para la protección de los datos.

3. Implantar políticas sólidas de gestión de accesos

Implemente políticas sólidas de gestión de acceso para evitar el acceso no autorizado a los datos cifrados y a las claves de cifrado. Esto es especialmente importante en condiciones de trabajo remoto, para garantizar que sólo el personal autorizado pueda acceder a los datos sensibles en función de la necesidad de conocerlos.

Thales ha estado a la vanguardia para ayudar a las organizaciones a proteger de forma cohesiva sus datos empresariales, y continuar con la actividad habitual incluso en situaciones de crisis. Las soluciones de cifrado de datos y de gestión de claves de Thales, protegen los datos sensibles en todos los dispositivos, procesos, plataformas y entornos, cumpliendo al mismo tiempo con todos los mandatos normativos. ■

Proteger las claves y la gestión de su ciclo de vida

En un mundo cada vez más digital, el uso de certificados y claves criptográficas es imprescindible y por tanto las entidades financieras tienen que poner el foco en cómo se custodian esas claves, además de en la firma digital de las transacciones.

La banca lleva años embarcada en una evolución tecnológica orientada a la provisión de nuevos servicios de valor añadido que le permitan satisfacer las demandas y mejorar la experiencia de sus clientes, además de reducir costes. El avance de los servicios digitales es palpable, está ahí. Sin embargo, Alfonso Martínez, Country Manager España & Portugal del negocio de seguridad e identidad digital de Thales, advierte que tal desarrollo lleva aparejado un incremento de la complejidad, lo que a veces impide a estas organizaciones asegurarse de que las soluciones de seguridad de la información que implementan son realmente capaces de proteger los datos sensibles, confidenciales, que entran y salen de la entidad.

Al respecto de esta protección, Alfonso Martínez explica que las empresas financieras no deben plantearse si están cifrando bien o mal sus datos, si no, más bien, si tienen desplegada una adecuada estrategia de cifrado. De nada sirve implementar una solución de cifrado muy potente o novedosa si al final las claves criptográficas están expuestas o no están protegidas de manera conveniente. Conviene separar el tesoro de la llave, más aún cuando se está produciendo una creciente orientación a servicios en la nube. En este sentido, es primordial que los bancos mantengan la custodia y la propiedad de esas claves criptográficas con las que están cifrando datos sensibles en la nube.

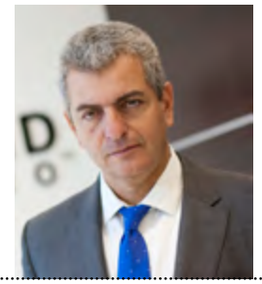
El financiero es un sector hiper-regulado, con muchas normativas a las que hacer frente: PCI DSS, P2PE, PSD2 o GDPR. Sin embargo, Alfonso Martínez explica que además de poner foco en su observancia y en la implantación de soluciones tecnológicas que, como los Módulos de Seguridad de Hardware (HSM), pueden ayudar en su cumplimiento, no hay que pasar por alto otras realidades muy en boga, como el blockchain (con las criptomonedas, los smart contract, IoT) y otras más sencillas, como las facturas electrónicas o el uso de los certificados SSL de los servidores. Al final, en este mundo digital, el uso de certificados y claves es imprescindible, por lo que es muy importante cuidar la forma en que se custodian esas claves y la firma digital de las transacciones.

Sin duda, las entidades financieras no solo se enfrentan a ciberataques, muchos problemas vienen también de las brechas de datos. Sobre ello, Alfonso Martínez especifica que se han visto casos muy cercanos de filtraciones en entidades financieras en las que no solo se han revelado datos bancarios sino también personales (nombre, DNI…). El problema aquí es claro: un número de tarjeta se puede cambiar, pero una identidad u otros datos personales asociados a una cuenta particular es imposible.

Para defender esta información, que también "viaja" a las nubes, ya sea privada, pública o híbrida, Thales propone una estrategia de seguridad que pasa primeramente por descubrir dónde reside la información sensible, por ejemplo, en qué servidores, y de qué tipo de datos se trata (una tarjeta de crédito, una dirección de correo…) para seguidamente proceder a su cifrado. No obstante, ese cifrado hay que asegurarlo poniendo el foco en la custodia de las claves criptográficas y, por supuesto, en una gestión de un ciclo de vida de esa clave para saber a quién pertenece, cuándo ha sido generada o cuando caduca. Se trata, por tanto, de proteger las claves criptográficas y la gestión de su ciclo de vida.

La industria financiera ante nuevos retos y viejas amenazas

JOSÉ BATTAT,
director general de Trend Micro Iberia



En 2020 las ciberamenazas no dieron tregua –la pandemia no ayudó–, y 2021 no está siendo diferente. El cambio de año no ha modificado las ciberamenazas de siempre, implicando que el robo de datos y el ransomware -a menudo en el mismo ataque-, así como el Business Email Compromise (BEC), los troyanos bancarios, el phishing o el malware de minado de monedas sigan copando titulares. Solo en 2020 Trend Micro detectó más de 62.600 millones de ciberamenazas, el 91% de las cuales se originaron en el email. Aunque la mayoría podrían estar vinculadas con ataques automatizados y básicos, podría decirse que son las más dirigidas y personalizadas las que suponen la mayor amenaza para los resultados y la reputación de la empresa.

Algunos sectores pueden verse más afectados que otros este año, pues los ciberdelincuentes siempre van a por el fruto más fácil: las oportunidades de generar el máximo rendimiento de los ataques. Así, aunque bancos y entidades financieras siempre han destacado que la seguridad está entre sus prioridades, el sector y sus clientes siguen estando entre los principales objetivos de los atacantes, a pesar de las nuevas normativas para reforzar aún más la ciberseguridad y la privacidad. Además de las florecientes oportunidades de negocio que han abierto las empresas de e-commerce y tecnología financiera (FinTech), la constante conectividad de los dispositivos móviles inteligentes conectados 24x7 supone para los ciberdelincuentes el acceso para estudiar y observar las lagunas de seguridad, lo que sitúa a los usuarios y a las empresas financieras como

“Los ataques online y offline amenazan constantemente al sector financiero y, a medida que el uso de la tecnología crece y se desarrolla, se presentan simultáneamente más oportunidades de negocio y de ataques”

blancos más fáciles para las transacciones fraudulentas y las brechas.

LA ESTRATEGIA DE SEGURIDAD COMIENZA AQUÍ

Si aún no lo ha hecho, evalúe los ciberriesgos para averiguar cuáles son sus puntos débiles y elabore un plan para solucionarlos.

El enfoque por adoptar dependerá de la predisposición al riesgo de la organización, del sector al que pertenezca y de la madurez de su posición actual de seguridad. Sin embargo, cualquier iniciativa debe incluir formación y concienciación de los usuarios; actividad que debe ser continua e incluir simulaciones de phishing y BEC del mundo real, y debe comunicarse regularmente al personal en pequeños fragmentos. Adapte las sesiones de formación a las últimas campañas de phishing y asegúrese de que sus herramientas ofrecen información detallada sobre las personas para centrarse en los empleados más débiles. Recuerde que todos los empleados, desde el director general hasta el último trabajador, deben asistir, incluidos los trabajadores temporales y los contratistas. Solo hace falta un clic erróneo para meter a la organización en problemas.

Otro enfoque que está ganando en popularidad es el de zero-trust. En un mundo de trabajo distribuido, dispositivos móviles y aplicaciones SaaS, la máxima de “nunca confiar, siempre verificar” se impone. Centre sus esfuerzos en la autenticación de los usuarios con herramientas multifactor (MFA), y despliegue la microsegmentación de red para restringir el acceso a recursos. Este enfoque también se relaciona muy bien con las herramientas SASE basadas en la nube para dar a los equipos de seguridad visibilidad de todo el tráfico entrante y saliente.

Los riesgos asociados a una plantilla distribuida también exigen herramientas de seguridad y gestión de endpoints basadas en la nube para obtener la máxima flexibilidad, visibilidad y control. La detección y respuesta a amenazas adquiere especial importancia, sobre todo las soluciones que incorporan IA para ayudar a los equipos de seguridad a priorizar la forma de hacer frente a los sofisticados ataques entrantes. De hecho, la IA seguirá facilitando la vida de los profesionales de la seguridad al detectar patrones sospechosos en el tráfico de red que los humanos podrían pasar por alto, detectando estilos de escritura anómalos en los emails de BEC y añadiendo automatización a la detección y repuesta.

En definitiva, los ataques online y offline amenazan constantemente al sector financiero y, a medida que el uso de la tecnología crece y se desarrolla, se presentan simultáneamente más oportunidades de negocio y de ataques. Como parte de la “vieja guardia” que se ve obligada por la tecnología a innovar y seguir desarrollándose, la concienciación en seguridad, la vigilancia, la formación y la integridad siguen siendo constantes sólidas en el sector en todo momento. ■

Protección y visibilidad de todos los vectores de ataque

Una mayor conectividad por parte de los usuarios y una evolución hacia una banca cada vez más digital han servido como reclamo para los ciberdelincuentes, que han incrementado el ritmo y la dureza de sus embestidas contra este mercado. Bajo esta situación, José de la Cruz, Director Técnico de Trend Micro, explica cómo la evolución de los ataques y amenazas contra este sector debe ser evaluada desde una doble dimensión.

Desde el punto de vista de TI, con empleados y usuarios interactuando permanentemente con aplicaciones, se aprecia cómo el ransomware ha cobrado una nueva dimensión, con campañas masivas para infectar al mayor número de compañías posible y la subasta de la información sustraída en la Dark Web. Estos ataques son cada vez más diversificados, sobre todo, en cuanto a la tecnología que utilizan para propagarse, y los vectores han cambiado. Así, y aunque el correo electrónico sigue siendo el más utilizado para iniciar un ataque, una vez emprendido este, otros vectores se involucran en el proceso, desde la comunicación a través de las distintas redes hasta la propagación desde endpoints a servidores, cloud, etc.

En lo que respecta específicamente a la banca, las amenazas se dirigen principalmente a tres elementos: infraestructuras, aplicaciones bancarias, y empresas de terceros.

Los cajeros automáticos (ATM) son las infraestructuras más atacadas, y aunque si bien es una tendencia descendente en España, no se debe bajar la guardia. Distinto es cuando se trata de aplicaciones bancarias, con ataques que se dirigen a aplicaciones de uso móvil, y donde el objetivo es el segundo factor de autenticación; y los destinados a los servicios de la entidad expuestos en Internet, aplicaciones y APIs. Por último, destacan las agresiones a la cadena de suministro, donde hay proveedores que interactúan con el banco y que, en muchos casos, no cuentan con las mismas medidas de seguridad.

Además de prepararse para luchar contra estas amenazas, la banca tiene que lidiar también con reglamentaciones como la PSD2, o incluso la futura PSD3. Sobre ello, José de la Cruz confirma que, si bien la PSD2 empezó con brío, por su orientación a fomentar la integración y el pago colaborativo, está empezando a quedarse obsoleta. Y es que, aunque los criterios de colaboración con los que fue creada sí se están cumpliendo, no se puede considerar que exista una homogenización en cuanto a estándares, APIs o modos de colaboración con terceros. En este punto, se espera que la PSD3 establezca una estandarización a nivel de API, lo que implicará además unas condiciones de seguridad más robustas.

A la luz de cómo están evolucionando los ataques y amenazas contra el sector financiero, es vital contar con una visibilidad total de la red, para luchar contra el ransomware; implementar mecanismos de control de dispositivos, de supervisión de integridad, para salvaguardar los ATMs; y optar por un segundo factor de autenticación mucho más robusto, y que no dependa de los SMS, para proteger las aplicaciones móviles.

De igual modo, sería recomendable contemplar el enforcement de políticas de seguridad, a fin de que los usuarios acaten unos requisitos mínimos cuando se conecten con el banco; proteger aplicaciones y containers; y, cuando se trate de cloud, vigilar el CSPM (Cloud Security Posture Management) para el cumplimiento de normativas. Por último, y para defender la cadena de suministro, es clave implementar mecanismos para proteger no solo a la entidad sino también a terceros.

S21 SEC

DFIR

Digital Forensics & Incident Response

¿Sabes cómo enfrentar un incidente grave de seguridad?

No serás juzgado por el incidente, sino por la velocidad en resolverlo.

¡Contáctanos ahora para obtener más información!

marketing@s21sec.com

www.s21sec.com/es/dfir-incidentes-seguridad/

Permitir la productividad en Internet con el más alto nivel de seguridad

La misión de Check Point es "proporcionar a cualquier organización la capacidad de realizar su trabajo en Internet con el más alto nivel de seguridad". Abordan las necesidades de ciberseguridad más inminentes de las organizaciones basándonos en tres principios básicos:

1. Enfoque de prevención en primer lugar: implementar protecciones de usuario preventivas para eliminar las amenazas antes de que lleguen a los usuarios.

2. Gestión Gold Standard: panel único para gestionar todo el patrimonio de seguridad.

3. Solución consolidada: obtenga una protección preventiva completa contra las amenazas más avanzadas mientras logra una mejor eficiencia operativa.

SECURE YOUR EVERYTHING CON CHECK POINT INFINITY

En esta nueva normalidad, permiten a los clientes mantener la productividad mientras permanecen protegidos en todo lo que hacen. Dondequiera que se conecte, a lo que se conecte y como quiera que se conecte: su hogar, sus dispositivos, su privacidad y los datos de su organización deben estar seguros y protegidos de cualquier amenaza cibernética. Para hacer realidad su visión, en 2021 han recalibrado su oferta de productos Infinity para enfocarlas hacia aquellas tecnologías y capacidades que brindarán seguridad sin concesiones basada en estos tres principios básicos.

Check Point consolida más de 80 productos y tecnologías y los ha organizado en tres pilares principales: Harmony, CloudGuard y Quantum, con Infinity-Vision como base.

HARMONY: EL MÁS ALTO NIVEL DE SEGURIDAD PARA USUARIOS REMOTOS

Check Point Harmony protege a los empleados remotos, los dispositivos y la conectividad a Internet de ataques maliciosos, al tiempo que garantiza un acceso remoto seguro y de confianza cero a cualquier escala y en cualquier aplicación corporativa. Check Point Harmony proporciona conectividad segura y de punto final (SASE), como una solución consolidada y unificada basada en la nube que incluye acceso remoto fácil y seguro (basado en la adquisición de Odo), navegación segura por Internet, punto final y seguridad mó-

vil y seguridad del correo electrónico. La solución ofrece la cobertura más amplia de vectores de ataque con la prevención de amenazas impulsada con Inteligencia Artificial.

Harmony presenta tecnologías que admiten entornos híbridos seguros de trabajo desde cualquier lugar (WFA). Asegurar a los empleados en el domicilio se ha convertido en una de las principales prioridades de las organizaciones de todo el mundo. La nueva familia de productos Harmony reúne más de siete categorías de productos para proporcionar una protección preventiva completa para los usuarios remotos. Incluye conectividad segura desde cualquier lugar y un entorno de trabajo seguro en cualquier dispositivo, incluidos los dispositivos móviles, personales y administrados por la empresa, tanto cliente como sin cliente.

CLOUDGUARD: NUBE SEGURA DE FORMA AUTOMÁTICA

CloudGuard optimiza la protección de las cargas de trabajo críticas en la nube, tanto públicas como privadas. Ofrece gestión de la postura en la nube, seguridad serverless y una nueva generación de firewalls de aplicaciones web con tecnología de Inteligencia Artificial contextual que protege las API, las aplicaciones web y los servidores web alojados y on-premise.

CloudGuard proporciona seguridad consolidada y prevención de amenazas en todos los entornos, activos y cargas de trabajo de la nube. Alineado con la naturaleza ágil del desarrollo y la implementación en la nube, CloudGuard ofrece una solución tanto para los profesionales de la seguridad en la nube como para las DevOps en la nube, desde la fase inicial de DevSecOps, pasando por la seguridad de la red en la nube hasta la seguridad de las aplicaciones en la nube (WAAP), así como la protección de contenedores y funciones sin servidor.

QUANTUM: SEGURIDAD DE LA RED EMPRESARIAL PARA EL PERÍMETRO Y EL DATACENTER

En 2021, la compañía seguirá aprovechando Maestro, su solución de rendimiento escalable única y disruptiva. Acelerarán la innovación en el firewall del centro de datos con la introducción de un gateway de firewall súper rápido con un rendimiento de firewall de 200 Gbps y una latencia de menos de 3 microsegundos.

Quantum refleja la solución de seguridad de red más completa para cada organización, perímetro y centro de datos, que abarca IoT Nano-Security hasta superredes Terabit y ofrece los más altos niveles de seguridad y rendimiento para administrar entornos de centros de datos.

Las puertas de enlace de seguridad de Check Point Quantum brindan una seguridad superior más allá de cualquier firewall de próxima generación (NGFW) y están diseñadas para administrar los requisitos de políticas más complejos. Con más de 60 servicios de seguridad, estos gateways previenen la quinta generación de ciberataques.

Además, tienen previsto el lanzamiento de una nueva serie de dispositivos para sucursales y oficinas dirigidos a las pequeñas y medianas empresas: Quantum SPARK.

INFINITY-VISION

Pensada para lograr una gestión de seguridad unificada y un 100% de prevención de brechas de seguridad. Permite la administración todo el patrimonio de seguridad con Check Point Infinity Portal, una gestión de seguridad como servicio (SMaaS) basada en la nube. Entregue políticas, supervisión e inteligencia unificadas desde un solo punto. Exponga, investigue y bloquee los ataques más rápido, con una precisión del 99,9% con las capacidades SOC y XDR utilizadas por Check Point Research. ■

MÁS INFORMACIÓN

- Quantum
- Harmony
- CloudGuard
- Infitiny Vision

Entrust ayuda a las empresas de servicios financieros a mejorar la seguridad de sus datos y el cumplimiento de la normativa

Empresas de servicios financieros de todo el mundo confían en Entrust para abordar sus desafíos de seguridad. Entrust cuenta con una gama de soluciones de hardware y software para ayudar a las empresas a reducir el riesgo, cumplir los distintos reglamentos y mejorar la agilidad mientras persiguen objetivos estratégicos en torno a tecnologías emergentes de pago y transacciones:

- Sólida administración de claves.
- Entorno de ejecución seguro.
- Alineación con los estándares regulatorios y de cumplimiento global en varios entornos.
- Listo para aplicaciones de Blockchain.

LA FAMILIA DE PRODUCTOS NSHIELD DE ENTRUST

Los módulos de seguridad de hardware (HSMs) nShield de Entrust son dispositivos reforzados y resistentes a manipulaciones indebidas que protegen los datos más confidenciales de su empresa. Estos módulos con certificación FIPS 140-2 realizan funciones criptográficas como la generación, administración, protección de claves y proceso de firma seguro, así como la ejecución de las funciones sensibles dentro de sus límites protegidos.

Para adecuarlos con su entorno específico, la familia de productos de HSM nShield incluye los siguientes modelos:

- **nShield Connect:** dispositivos conectados a la red
- **nShield Edge:** Módulo portatil con conexión USB
- **nShield Solo:** Tarjetas PCIe para integrar en dispositivos o servidores
- **nShield as a Service:** Solución por suscripción para acceder a HSM nShield en la nube

FUNCIONALIDADES DE LA FAMILIA DE PRODUCTOS NSHIELD DE ENTRUST

Interfaces de servicios web compatible con la nube

El nShield Web Services Option Pack optimiza la interfaz entre sus aplicaciones y HSM al ejecutar comandos a través de llamadas de servicio web.

Soporte contenerizado en instalaciones o en la nube

El nShield Container Option Pack proporciona un conjunto de scripts preempaquetados que simplifican en gran medida la integración de los HSM nShield y de esa manera proveed servicios

de criptografía a las aplicaciones desplegadas en contenedores.

*** Administración de claves para sus datos en la nube con nShield BYOK**

nShield BYOK (Bring Your Own Key) le permite generar claves robustas en el HSM nShield ubicado en las instalaciones y exportarlas de forma segura a sus aplicaciones en la nube, ya sea si utiliza Amazon Web Services, Google Cloud Platform, Microsoft Azure, o las tres.

*** Optimización de operaciones utilizando Administración y Monitorización remota**

nShield Monitor y nShield Remote Administration, disponibles para los HSM nShield Solo y Connect, le ayudan a reducir los costos operativos a la vez que se mantiene informado y en control 24x7 de sus estados de HSM.

*** Configuración remota**

Los modelos nShield Connect XC ofrecen una opción de consola en serie simplificando la instalación física del HSM para alinear, cablear y aplicar potencia. Esto facilita la implementación y la reimplementación sin necesidad de revisitar el centro de datos.

*** Arquitectura altamente flexible de Security World**

La arquitectura de Security World de nShield admite HSM nShield de Entrust mediante la creación de un entorno de administración de claves flexible y exclusivo. Con Security World de nShield, usted puede combinar diferentes modelos de HSM nShield para construir un ecosistema unificado que ofrece escalabilidad, perfecta tolerancia a fallos y balance de carga.

SOLUCIONES DE CIFRADO DE WORKLOAD, GESTIÓN DE CLAVES INTEGRADA PARA ENTORNOS MULTI-NUBE

Gestión universal de claves para workload cifrados

Entrust KeyControl es un servidor KMIP certificado por VMware, escalable y con muchas funciones, que simplifica la gestión de claves para los workload cifrados. Sirve como KMS para los clientes encriptados de VMware vSphere y vSAN, así como para otros productos compatibles con KMIP.

Cifrado de datos, gestión de claves multi-nube y seguridad del workload

Entrust DataControl asegura las workloads multi-nube a lo largo de su ciclo de vida y reduce la complejidad de proteger las cargas de trabajo a través de múltiples plataformas de nube. Funciona en las instalaciones y con las principales plataformas de nube pública, así como con soluciones de hiperconvergencia y almacenamiento. DataControl incluye el servidor de gestión de claves (KMS) de Entrust KeyControl, certificado por VMware.

ALIANZAS CON LÍDERES DE LA INDUSTRIA

Entrust a través del programa de sus socios tecnológicos, colabora para integrar los HSM nShield en una variedad de soluciones de seguridad incluyendo la creación de credenciales y PKI, seguridad de base de datos, firma de códigos, firmas administración, gestión de cuentas privilegiadas, entrega de aplicaciones, inteligencia en la nube y los big data. ■

MÁS INFORMACIÓN

- Uno de los diez bancos más importantes del mundo implementa los HSMs de Entrust para ofrecer servicios fiables y de confianza a sus clientes y colaboradores
- Protección de Blockchain
- Estudio Global de Tendencias de Cifrado 2021
- Protección de claves en entornos híbridos

cpl.thalesgroup.com

THALES
Building a future we can all trust

CipherTrust Data Security Platform

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

Localizar Proteger Controlar

Empiece a localizar, proteger y controlar sus datos hoy mismo

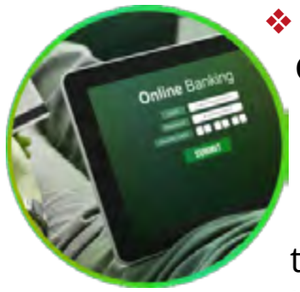
Protección para entornos financieros

RealSec dispone de una serie de soluciones de seguridad, tanto de propósito general como orientadas al segmento financiero. Aquí repasamos algunas de ellas.

SOLUCIONES DE CIBERSEGURIDAD

❖ **HSM de Propósito General/ Cryptosec LAN**

Se trata de un servidor criptográfico en red, de altas prestaciones y seguridad, diseñado para servicios de cifrado y aplicaciones de firma digital, independientemente del sistema operativo dónde éstas residan. Ofrece generación, almacenamiento y custodia de claves y certificados capaces de integrarse con aplicaciones de firma electrónica, PKI, cifrado de archivos y BBDD, blockchain...



❖ **HSM Financiero / Cryptosec Banking**

HSM financiero para pagos en red, de muy alto rendimiento, que proporciona toda la operativa y funcionalidad criptográfica específica para el ámbito de Banca, Fintech y la industria de los Medios de Pago. Cumple con todos los requerimientos y estándares definidos por el consorcio PCI (VISA, MASTERCARD...).

❖ **Remote Key Load / Cryptosec RKL**

Automatización de la carga de Claves en los ATM utilizando cifrado asimétrico, en sustitución del antiguo proceso de carga manual, tan costoso como ineficiente. Es la solución del mercado más avanzada, madura y eficiente que ofrece servicio multiempresa y está homologada por las marcas más importantes y reconocidas de ATM internacionales, cumpliendo con los requerimientos definidos por el consorcio PCI.

SOLUCIONES CIFRADO Y FIRMA DIGITAL

❖ **Servidor de firma digital/ CryptoSign Server**

Servidor Integrado de Firma Digital que incluye en un único dispositivo (hardware y software) los elementos necesarios para que, en un entorno de red, se pueda realizar cualquier proceso de firma con las mayores garantías de seguridad y gestionar los certificados digitales.

❖ **Autoridad de Sellado de Tiempo/ Cryptosec Openkey TSA**

La Firma Digital asegura quien ha realizado una determinada acción, pero no es válida para certificar que la acción se ha producido en un determinado instante de tiempo. Para ello, se requiere de una Autoridad de Sellado que afirme y certifique que los documentos electrónicos firmados han existido desde un determinado momento, y que son válidos desde ese instante.

❖ **Servidor de cifrado y firma digital de correo electrónico/ Cryptosec Mail**

Sistema centralizado de firma digital y/o cifrado del correo electrónico capaz de alma-

cenar y administrar, de forma segura, las claves de los certificados ya que está orientada a minimizar los riesgos del «Phishing» y a conseguir la total confidencialidad del contenido de los correos mediante su encriptación.

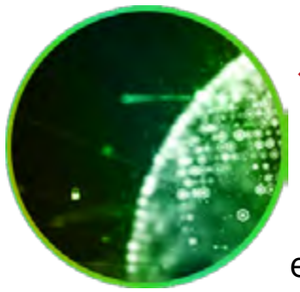
AUTORIDAD DE SOLUCIONES PKI

❖ **Certificación/ Cryptosec Openkey CA**

La Autoridad de Certificación es el elemento más importante y al que más hay que proteger en una infraestructura de clave pública (PKI). Es el componente de confianza emisor de los certificados y que determina su validez en el tiempo.

❖ **Autoridad de Registro/ Cryptosec Openkey RA**

La Autoridad de Registro es el punto de acceso de los usuarios finales a la Autoridad de Certificación. Al mismo tiempo que es el instrumento en el que se generan las solicitudes de certificación y las solicitudes de revocación.



❖ **Autoridad de Validación/ Cryptosec Openkey VA**

Con la Autoridad de Validación podemos conocer el estado de revocación de los certificados digitales emitidos bajo una determinada infraestructura. ■

MÁS INFORMACIÓN

- Segundo Informe Blockchain
- Cifrado y Firma Digital para Organizaciones Inteligentes
- Fintech y Banca. Tendencias de seguridad & HSM

Cobertura completa de riesgos de ciberseguridad en los procesos de negocio

El desarrollo de un mundo cada vez más hiperconectado, en el que las empresas enfrentan complejos procesos de transformación digital y dependen de un mayor de dispositivos conectados a Internet, resulta clave proteger los datos de las organizaciones, así como la operatividad de sus sistemas y cumplimiento con el RGPD.

S21sec es, tal y como se define a sí misma, "la compañía pure-player de ciberseguridad más grande de Iberia con una dilatada experiencia en el sector, lo que le permite ofrecer una cobertura completa de riesgos de ciberseguridad en los procesos de negocio de las organizaciones".

Una plantilla de más de 500 expertos refleja las capacidades de S21sec para investigar, detectar y prevenir amenazas; piezas clave para reaccionar con mayor rapidez ante cualquier ataque e identificar, diagnosticar y remediar eventuales incidentes en el menor tiempo posible.

Perteneciente al grupo Sonae, S21sec está entre las cinco principales compañías de ciberseguridad de Europa, con la aspiración de liderar el mercado europeo a medio plazo.

Además, cuenta con el primer SOC de España, convertido ahora en un multiSOC

global distribuido en cuatro localizaciones, garantizando la integridad de múltiples organizaciones en España, Portugal y México.

S21sec se guía por una serie de valores clave a la hora de desarrollar e implementar sus soluciones con éxito:

Una plantilla de más de 500 expertos re-fleja las capacidades de S21sec para inves-tigar, detectar y prevenir amenazas

- **Transparencia:** se pone a disposición la información necesaria para la colaboración y la toma de decisiones colectivas.
- **Excelencia:** se persigue ofrecer la más alta calidad gracias a encontrarse en un continuo proceso de aprendizaje.
- **Trabajo en equipo:** se dedica esfuerzo para encontrar la mejor forma de ayudarse entre sí, poniendo el rendimiento de la compañía por encima del rendimiento individual.
- **Innovación:** se busca la diferenciación a través de implementar cambios que mejoran su eficiencia y ventaja competitiva.
- **Confianza:** se construyen relaciones con las personas y las organizaciones basadas en la confianza y la honestidad.
- **Pasión:** se disfruta del trabajo porque siempre se busca de manera proactiva diferenciarse.

PROPUESTA DE SOLUCIONES

S21sec aúna soluciones diferentes de manera transversal y está diseñado en torno a cinco necesidades:

1. **Identificar:** análisis de riesgos y plan general de ciberseguridad, cumplimiento regulatorio, ciberseguridad en la nube y programas de transformación y Red Team.
2. **Proteger:** diseño y despliegue de arquitecturas y tecnologías, servicios de formación y concienciación, gestión de dispositivos de seguridad, seguridad de la información y seguridad ATM.

3. **Detectar:** SOC gestionado y SIEM como servicio, Unidad de Inteligencia de Ciberamenazas, EDR - Detección y respuesta End Point.
4. **Responder:** CSIRT - Gestión de incidentes de ciberseguridad 24x7, DFIR - Análisis forense digital y respuesta ante incidentes, plataforma de respuesta ante incidentes, SOAR - Automatización, Remediación y Orquestación de la Ciberseguridad y amenazas emergentes - evaluación y perfilación.
5. **Recuperar:** Continuidad de negocio y planes de respuesta ante ciber-desastres. ■

MÁS INFORMACIÓN

- Threat landscape report
- Test autoevaluación cyberGRC

Soluciones de cumplimiento y seguridad de datos para la banca y servicios financieros

Los proveedores de servicios financieros de todo tipo están ampliando sus ofertas para competir a escala global, ahorrar costes y mejorar la experiencia del cliente con servicios de valor añadido. Pero a medida que evolucionan los servicios financieros, deben asegurarse de que sus soluciones de seguridad TI sean realmente capaces de proteger los datos confidenciales que se adquieren y transmiten.

Thales ofrece soluciones integrales de gestión de acceso y protección de datos que aseguran los datos en dispositivos, procesos y plataformas in situ y en la nube. Estas soluciones ayudan a las organizaciones a cumplir con los requisitos de cumplimiento de los servicios financieros, facilitan la auditoría de seguridad, protegen a sus clientes y evitan el daño a su reputación causado por brechas de datos.

En cuanto a seguridad, el sector financiero se enfrenta a varios desafíos:

- **Cubrir los requisitos de cumplimiento de los servicios financieros.** El cumplimiento normativo puede llegar a ser abrumador para los servicios financieros. Las normativas que abarcan requisitos de seguridad de datos incluyen PCI DSS para información relacionada con tarjetas de crédito, el RGPD y PSD2 en la UE, SOX/J-SOX, leyes de notificación de brechas de datos y de residencia locales, y muchas más en todo el mundo.
- **La protección de los datos.** Para evitar multas costosas y proteger su reputación, las empresas del sector bancario y financiero y sus ejecutivos deben salvaguardar los datos financieros confidenciales contra la exposición accidental, información privilegiada deshonesta, APT y otras amenazas conocidas y desconocidas. Y no solo deben existir procedimientos para proteger los datos, sino también para identificar y alertar a la organización cuando se produce un acceso no autorizado.

¿CÓMO THALES LES PUEDE AYUDAR?

Thales cuenta con una oferta de soluciones en diferentes áreas que incluyen:

✱ **Soluciones de cifrado.** Las soluciones de protección de datos CipherTrust Transparent Encryption y CipherTrust Application Data Protection , incluídas en la solución CipherTrust Data Security Platform de Thales, proporcionan un único marco extensible para proteger los datos en reposo bajo los diversos requisitos de la industria de servicios bancarios y financieros en la más amplia gama de plataformas de sistemas operativos, bases de datos, entornos de nube e implementaciones de Big Data. El resultado es un bajo costo total de propiedad, así como una implementación y operación simples y eficientes.

✱ **Administración de claves robusta.** Las soluciones de administración de claves de Thales, permiten la gestión centralizada de claves de cifrado para otros entornos y dispositivos, incluido el hardware compatible con KMIP, claves maestras TDE de Oracle, SQL Server...

✱ **Protección de datos de pago.** Las soluciones de Thales están diseñadas específicamente para aplicaciones de pago. El módulo payShield 10K, la quinta generación de HSM de pago de Thales, ofrece un conjunto de funciones de seguridad de pagos comprobadas en entornos críticos y que incluyen el procesamiento de transacciones, protección de datos confidenciales, emisión de credenciales de pago, aceptación de tarjetas móviles y tokenización de pagos. payShield 10K de Thales atiende lo último en requisitos de seguridad obligatorios y en mejores prácticas para una amplia gama de organizaciones que incluyen EMVCo, PCI SSC, GlobalPlatform, Multos, ANSI, así como las varias marcas y redes de pago globales y regionales.

Por otro lado, CipherTrust Tokenization with Dynamic Data Masking permite a los administradores establecer políticas para devolver un campo completo tokenizado o enmascarar dinámicamente partes de un campo. Con las capacidades de tokenización de la solución que preservan el formato, los administradores pueden restringir el acceso a activos confidenciales y, al mismo tiempo, formatear los datos protegidos de una manera que les permita a muchos usuarios hacer su trabajo.

VENTAJAS DE LAS SOLUCIONES THALES

Las soluciones de Thales ofrecen:

❖ **Cumplir las obligaciones reglamentarias.** Con sus productos de Data Security, la industria bancaria puede cumplir con los estándares regulatorios y de seguridad de datos en reposo mientras protege la información de brechas de datos en toda la empresa, en la nube y en entornos de Big Data.

❖ **Rápida de instalar.** Thales puede instalar las soluciones de seguridad de datos CipherTrust en semanas en lugar de meses. Las soluciones de Thales funcionan con la mayoría de los principales sistemas operativos, incluidos los servidores Linux, UNIX y Windows en entornos físicos, virtuales, en entornos de datos de titulares de tarjetas (CDE) de la nube y Big Data.

❖ **Fácil de usar.** Su oferta CipherTrust Data Security Platform simplifica la resolución de problemas de seguridad y cumplimiento al proteger simultáneamente los datos en bases de datos, archivos y nodos de Big Data, en nubes públicas, privadas, híbridas e infraestructuras tradicionales. La administración centralizada de toda la plataforma de seguridad de datos, facilita la ampliación de la protección de seguridad de los datos, y la satisfacción de los requisitos de cumplimiento en toda la empresa, creciendo según sea necesario, sin agregar nuevo hardware ni aumentar las cargas operativas. ■

MÁS INFORMACIÓN

- Cifrado Total
- The Key Pillars for Protecting Sensitive Data
- payShield Brochure

Soluciones más robustas gracias a la inteligencia de amenazas compartida

Trend Micro trabaja para ayudar a que el mundo sea seguro para el intercambio de información digital. Aprovechando los más de 30 años de experiencia en seguridad, investigación de amenazas globales e innovación continua, la firma permite la resiliencia de las empresas, gobiernos y consumidores con soluciones conectadas a través de cargas de trabajo en la nube, endpoints, correo electrónico, IIoT y redes.

Su estrategia de seguridad XGen impulsa sus soluciones con una combinación intergeneracional de técnicas de defensa frente a amenazas que están optimizadas para los entornos clave y aprovecha la inteligencia de amenazas compartida para una mejor y más rápida protección.

SOLUCIONES Y PRODUCTOS

Trend Micro ha innovado para adaptar su oferta a la evolución de las amenazas y a las necesidades de empresas y usuarios. Cuentan con un amplio catálogo de productos que permiten ofrecer protección en cualquier entorno, ya sea físico, virtual, en la nube y en contenedores.

El catálogo de Trend Micro ofrece una mayor cobertura, pues busca cubrir todos los vectores de ataque posibles (endpoint, cloud, navegación, email, entornos colaborativos, redes privadas/cloud, OT...), y por tecnología, ya que combinan tecnología de última generación junto con la experiencia que les aporta su trayectoria en el mercado.

Un ejemplo de esta evolución es la Tecnología XDR, introducida en el mercado por Trend Micro, que aprovecha la información recabada por los distintos vectores (endpoint, servidores, correo, red...). XDR extiende las capacidades del EDR tradicional aportando contexto a los ya citados ataques multivector, permitiendo a los clientes identificarlos y bloquearlos de manera prematura.

Por otro lado, Trend Micro estructura su oferta en torno a los siguientes ejes:

❖ **Solución Hybrid Cloud Security:** agrupa seguridad cloud simplificada gracias a la plataforma de servicios Trend Micro Cloud One. Protege entornos físicos, virtuales, en la nube y en contenedores con control y visibilidad centralizados; proporciona un conjunto completo de prestaciones de seguridad; reduce el número de herramientas de seguridad necesarias para proteger entornos híbridos y satisfacer los requisitos de cumplimiento; ahorra recursos y reduce los costes con una seguridad optimizada del entorno y políticas automatizadas. Disponible como software, como servicio, o en los marketplaces de AWS y Microsoft Azure, cuenta con tecnología de seguridad XGen, que ofrece un conjunto intergeneracional de controles de seguridad optimizados para entornos líderes.

❖ **Network Defense Solution:** área desde el que ofrece protección contra amenazas conocidas, desconocidas y ocultas, es decir, aquellas vulnerabilidades de las que no se tiene visibilidad y que residen en la red. Mediante la integración de las soluciones de Intrusion Prevention (IPS) y Advanced Threat Protection (incluido sandboxing), Trend Micro proporciona una combinación de técnicas intergeneracionales y de detección de defensas avanzadas para aumentar al máximo la protección e ir más allá de lo conocido y desconocido, ofreciendo protección más inteligente, logrando tiempos de reacción más rápido, mayor rendimiento y protección automatizada que se adapta a entornos híbridos.

❖ **User Protection Solution:** brinda protección avanzada e inteligente a los usuarios con la técnica adecuada en el momento adecuado, en cualquier dispositivo, aplicación y lugar. Se trata de una seguridad conectada y que utiliza varias capas para detener las amenazas emergentes y reducir los gastos de gestión. Seguridad optimizada para funcionar en su entorno por un proveedor de confianza y con visión de futuro que siempre trabaja en una nueva generación de seguridad. Gracias a Smart Protection Suite, son capaces de proteger a los usuarios desde el gateway hasta el endpoint.

Este catálogo de soluciones, que también abarca el segmento de la pyme, se ve complementado con servicios de soporte al cliente para garantizar un funcionamiento sin problemas y una asistencia superior. ■

MÁS INFORMACIÓN

- The Banking and Finance Industry Under Cybercriminal Siege: An Overview
- Banks Under Attack
- Mobile Banking Trojan

THE ART OF CYBERSECURITY

Trend Micro Vision One™

Mayor visibilidad para una respuesta más rápida

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

Más información en:
www.trendmicro.com

CONTENIDOS↓

Tecnología para tu Empresa

CENTRO DE RECURSOS

it

La pyme pone rumbo al mundo digital

KIO Networks · NetApp · NFON Cloud Telephone System · SAMSUNG · servicenow

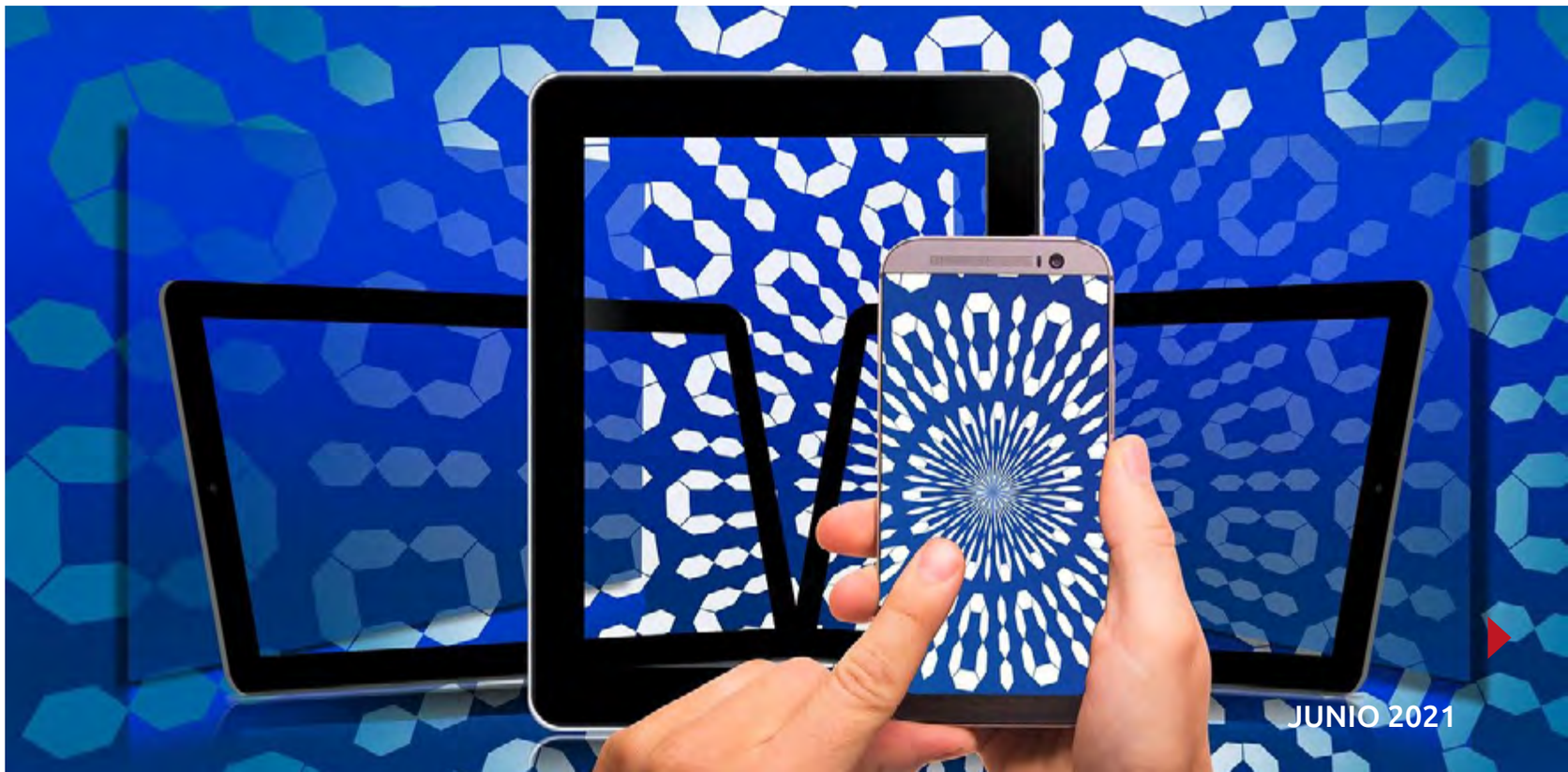
La pyme pone rumbo al mundo digital

2020 supuso una dura prueba para los pequeños negocios y autónomos que, en muchos casos, habían postergado su decisión de digitalizarse. Sin embargo, con la irrupción de la pandemia, han tenido que empezar este proceso, que está continuando este año tratando de impulsar más el comercio electrónico y el marketing digital, y prestando atención a la seguridad de los datos.

GoDaddy ha presentado los resultados de su observatorio "Estado actual de la digitalización las pequeñas empresas y autónomos españoles 2021" en el que destaca que, aunque estos meses han sido tremendamente complicados, está claro que han sabido adaptarse a la situación para superar las dificultades de los cierres y restricciones derivadas de la pandemia poniendo en el centro de su actividad la digitalización y sus herramientas.

Estos negocios están abiertos a la innovación y a la mejora y, contra todo pronóstico, han logrado hacer frente a esta crisis sin precedentes, pues muchas se han beneficiado de la digitalización y de la venta de sus productos y servicios online. La tecnología se ha convertido en protagonista y única salvación para un significativo número de pequeños empresarios españoles. Tanto es así que uno de cada cuatro ha llegado a ampliar sus áreas de negocio en estos meses y un 12% ha iniciado o expandido su tienda online.

"Esta ha sido una crisis sin precedentes, nadie ha visto, ni vivido, nada parecido y esa es la principal razón por la cual esto ha sido tan complicado, porque nadie contaba con una experiencia similar en la que basarse. Pero si algo ha logrado salvar el negocio de la gran mayoría de estos pequeños empresarios españoles ha sido la digitalización y sus herramientas, ya que el comercio electrónico se ha convertido en su principal canal de venta", señala Gianluca Stamerra, director regional de GoDaddy para España, Italia y Francia.



Aunque son muchas las dificultades con las que se están encontrando este tipo de negocios desde que comenzaron las restricciones, más del 48% de las pequeñas empresas esperan resurgir con más fuerza que antes de la COVID-19. Además, destaca la manera en la que están aclimatándose a los nuevos canales digitales para aumentar las ventas y continuar: el 52% dice utilizar la página web de su empresa, para el 39% lo son las redes sociales y un 20% manifiesta que utiliza su propia tienda online.

Las pequeñas empresas españolas encuestadas afirmaron que los principales retos a los que se enfrentaron durante la pandemia de la COVID-19 fueron mantener el negocio (32%), aumentar el número de nuevos clientes (20%) e incrementar la fidelidad de los clientes (13%). Y, para enfrentar estos desafíos, destacan que se han dedicado parte de sus recursos a contabilidad/finanzas y RRHH e informática (35%), ventas y marketing (36%) y en atención al cliente (15%). Para el 71% de los pequeños empresarios es importante ampliar los conocimientos tecnológicos y soluciones digitales.

LA EMPRESA ESPAÑOLA ESTÁ LISTA PARA UNA DIGITALIZACIÓN EXITOSA

LA IMPORTANCIA DE LA TECNOLOGÍA

El IV Estudio sobre el estado de digitalización de las empresas y administraciones públicas españolas de Vodafone, muestra el creciente protagonismo que ha desempeñado el teletrabajo durante los meses de la pandemia. En el caso de las grandes empresas la implantación del teletrabajo asciende al 94%, mientras que el teletrabajo en microempresas se ha duplicado hasta alcanzar un 30% durante los meses de pandemia.

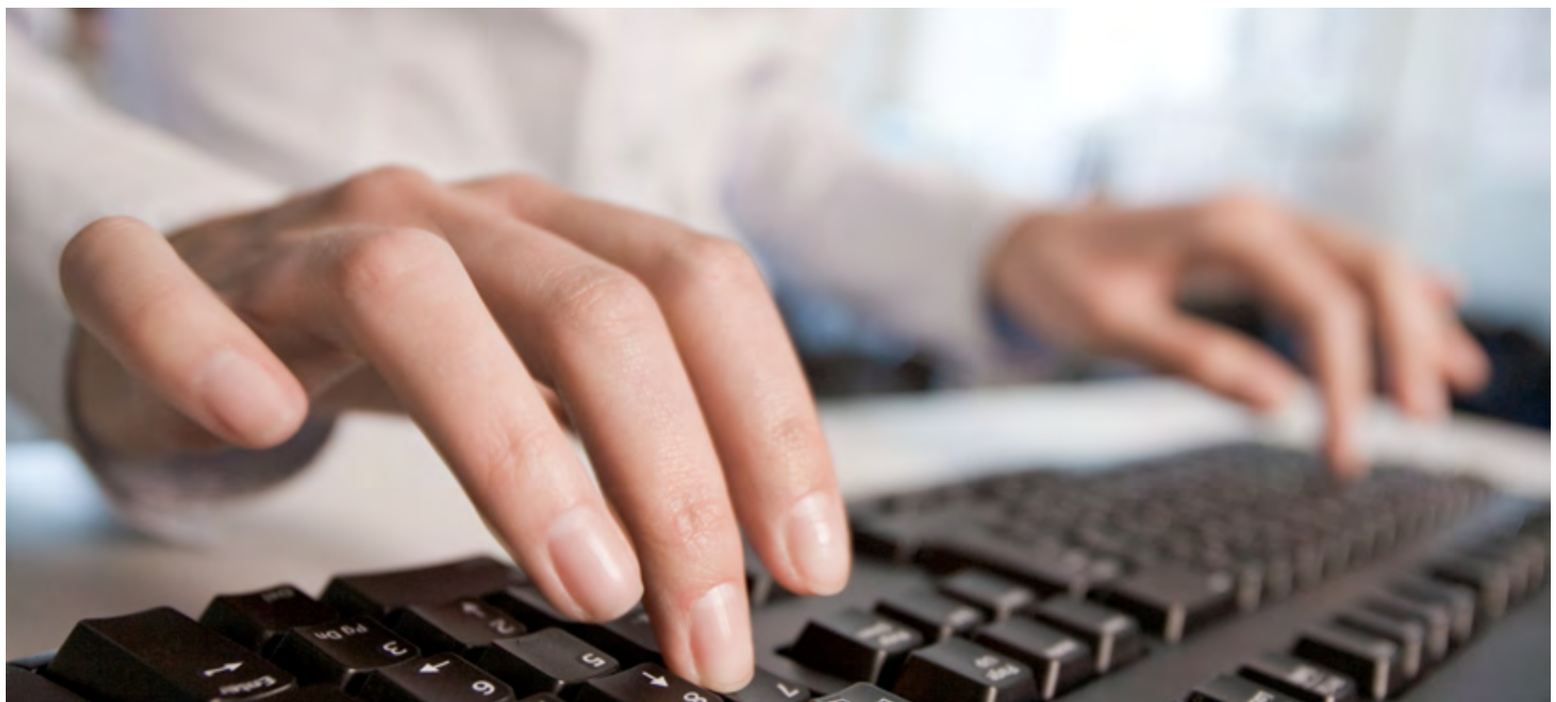
Las empresas españolas consideran que contaban con las soluciones necesarias para la implementación del teletrabajo en la pandemia. De hecho, la mayoría de las empresas se autopercibe como “preparada”, siendo el segmento de las grandes empresas y las pymes donde esta percepción obtiene sus mayores porcentajes (87% y 84% respectivamente).

Para facilitar el teletrabajo, las tecnologías que han aportado una mayor utilidad han sido las soluciones de conectividad, servicios en la nube (pública y privada), aplicaciones de videoconferencia, herramientas de colaboración, acceso remoto al puesto de trabajo y sistemas de seguridad en

red o en la nube. También han tenido una gran transcendencia aquellas tecnologías que han permitido llegar de forma remota a los clientes como el marketing digital, el comercio electrónico y las aplicaciones de pago. En general, los servicios vinculados a nube o cloud y, en un segundo lugar, aquellos que tienen que ver con la conectividad son los más implantados en las empresas y Administraciones Públicas españolas. Las pequeñas empresas y autónomos disponen de 2,4 servicios frente a los 6,7 de las grandes empresas y también son quienes menos contratación de este tipo de soluciones han hecho desde que comenzara la pandemia del Covid-19.

En el futuro todas las organizaciones planean reducir el teletrabajo, pero las empresas de todos los tamaños continuarán en niveles ligeramente superiores a la situación previa a la pandemia. Sin embargo, en el caso de las Administraciones Públicas el porcentaje de teletrabajo podría mantenerse en un 55%, previéndose así un incremento notable respecto a la situación previa.

A mayor tamaño de la empresa se incrementa la importancia atribuida a las nuevas tecnologías para un futuro inmediato. Consideran estas como muy importantes o bastante importantes un 57% de las microempresas, un 68% de las pymes, un 82% en el caso de las grandes empresas y para el 84% de las AAPP.



Todos los tipos de empresas coinciden en citar la crisis del Covid-19 como su mayor preocupación, seguida de la preocupación por la situación económica general y la pérdida de facturación/ventas y la evolución de su sector como otros aspectos relevantes. Si bien la digitalización no aparece como una preocupación de las empresas, la inquietud por la ella va incrementándose según aumenta el número de empleados de la empresa. Hay que destacar aquí que son las Administraciones Públicas, las que mayor preocupación muestran por este aspecto, otorgándole una nota de 7,8 sobre 10.

La digitalización beneficia a las empresas aportando principalmente eficiencia en procesos y mejoras en la comunicación con clientes. Las organizaciones estudiadas consideran que están aún inmersas en el proceso de digitalización de sus organizaciones y solo una parte de ellas ha llegado a un nivel avanzado. En este contexto, es el segmento de las microempresas las que se perciben menos preparadas, donde un 48% reconoce estar en un nivel 'básico'. Son las grandes empresas donde se sitúa el mayor porcentaje de nivel 'avanzado', con un 42%, aunque siguen reconociendo una amplia margen de desarrollo. Respecto a las barreras para avanzar en la digitalización, la necesidad de contar con el talento adecuado se hace más patente.

Respecto a la presencia de planes de digitalización, aumenta ligeramente en todas las empresas, en mayor medida en las grandes organizaciones, aunque el porcentaje que asigna una partida específica para el desarrollo de este plan se estabiliza y se mantiene en un 47% en las pequeñas empresas, un 49% en las pymes, un 60% en las grandes empresas y un 57% en el caso de las Administraciones Públicas que afirman tener asignado un presupuesto para desarrollar su plan.

TRES IMPRESCINDIBLES PARA LA PYME

Del análisis de las respuestas a una encuesta llevada a cabo por GoDaddy se desprende que la digitalización es más importante ahora que hace un año, tras la irrupción de la pandemia. Un 56% de los encuestados está convencido de que la digitalización es importante para el porvenir de su negocio, y a la pregunta de cuáles son esas tecnologías que consideran más relevantes para este 2021, los autónomos y las pequeñas empresas españolas han destacado las siguientes:

❖ **Tienda online:** hasta hace poco eran muchas las empresas que no tenían siquiera en mente la idea de implantar una tienda online en su página web y, hasta antes de la pandemia, solo el 7% contaba con un e-commerce propio. Pero ahora la situación ha cambiado de manera radical y el 22% de las pequeñas empresas y autónomos que han participado en el estudio declaran que les habría gustado contar con un canal de venta propio o marketplace creado antes de la llegada del coronavirus para haber mantenido abiertas otras vías de negocio. En 2021 contar con una tienda online puede suponer la diferencia entre continuar con el negocio o cerrar las puertas definitivamente.

❖ **Diseño web 'responsive':** contar con una página web para una pequeña empresa se está convirtiendo en una herramienta básica para una mayor visibilidad en la web, mantener la actividad y hacer crecer el negocio hoy en día. Pero dado que el acceso a la información, las compras online, etc. se realiza a través de múltiples dispositivos diferentes, es fundamental que la página web de una empresa esté diseñada para adaptarse a cualquier pantalla.

❖ **Certificado SSL:** son muchos los usuarios que evitan realizar alguna transacción en una web sin garantías, lo cual indica la importancia que le dan los clientes a contar con todas las medidas de seguridad a la hora realizar una compra online. El protocolo HTTPs o certificado SSL ofrece la máxima seguridad web, permitiendo que el intercambio de información sea completamente seguro, protegiendo la transferencia de datos personales desde el sitio web al servidor. Además, tener un certificado SSL instalado en un sitio web, proporciona un plus de profesionalidad a una página, mejora el posicionamiento SEO y aumenta, de manera significativa, la confianza de los clientes.

MÁS INFORMACIÓN

- Toda la información sobre las tendencias tecnológicas en las empresas
- Cómo está evolucionando la cloud
- El mercado de las comunicaciones unificadas crece
- El mercado de almacenamiento SMB se transforma
- ¿Cómo serán los nuevos espacios de trabajo?
- Cuál es la propuesta de KIO Networks para el mercado cloud
- Cuál es la propuesta de NFON para el mercado de la telefonía en la nube
- Cuál es la propuesta de Samsung para el almacenamiento SMB
- Cuál es la propuesta de ServiceNow para el nuevo entorno laboral

¿SABES CUÁNTO PERDERÍA TU EMPRESA SI SE PARASEN LOS ENTORNOS DE IT CRÍTICOS?

Garantiza la Continuidad de Negocio con la nube de **KIO** y las soluciones de **NetApp**, expertos en la gestión de datos en el **Cloud**.

KIO NetApp

“LA CLOUD AYUDA A LAS EMPRESAS A SER MÁS COMPETITIVAS”

JAVIER JARILLA, DIRECTOR GENERAL DE KIO NETWORKS SPAIN

Que los sistemas y aplicaciones de una compañía garanticen sus operaciones y aseguren la continuidad de negocio siempre ha sido algo prioritario. ¿Una economía digital como la actual amplía los desafíos empresariales en este campo?

El nivel de exigencia sobre los sistemas informáticos de organizaciones y consumidores se ha elevado exponencialmente, los problemas informáticos, de toda índole, se han convertido en noticias de primera página por la repercusión económica que tienen.

Las empresas se han dado cuenta de que no pueden enfrentarse solas al reto que ha traído la transformación digital y empiezan reparar en que es mejor concentrar los esfuerzos en las áreas funcionales y buscar servicios que les garanticen la alta disponibilidad de sus Sistemas de Información.

Este escenario ha abierto una puerta a crear servicios que sostengan y garanticen la economía digital. El cloud computing ya es una fórmula aceptada y adoptada por muchas empresas, pero ahora ya se exige que sean servicios de altísima disponibilidad, ese es el gran desafío empresarial, unido a la seguridad.

¿Cómo han evolucionado el mercado de data centers para adaptarse a la nueva realidad?

El mercado de data centers sigue creciendo y poniendo a disposición de las empresas una cantidad im-

"LA CLOUD AYUDA A LAS EMPRESAS A SER MÁS COMPETITIVAS"

portante de metros cuadrados, sin embargo, llama la atención que las certificaciones de alta disponibilidad sigan siendo las mismas de hace 7 años. Creo que la verdadera evolución del centro de datos llegará cuando estas instalaciones se especialicen por tipos de servicio y cliente; no tiene las mismas necesidades a nivel de centro de datos un cloud provider que un cloud privado. En nuestro caso, concebimos nuestro cpd como centro de dato exclusivo como nube.

La informática en la nube avanza como parte fundamental de la transformación digital que están llevando a cabo la mayoría de las organizaciones, ¿cómo está afectando al mercado de centros de datos en general el auge de la nube pública?

Entendiendo la pregunta como una comparación entre servicios cloud y housing de sistemas o colocation, está claro que cuando un cliente opta por servicios de cloud computing como IaaS, por ejemplo, deja de necesitar espacio o racks en un centro de datos para pasar a consumir recursos de una nube que también está alojada en un centro de datos. Una empresa que opta por subirse a la nube reduce drásticamente sus necesidades de espacio en un centro de datos.

Toda la información sobre la situación TI de las empresas españolas en @TIyEmpresa_ITDM

No obstante, los proveedores de centros de datos de máximo nivel están teniendo un importante papel en el suministro de clouds privadas. ¿Qué ventajas ofrecen frente a otras alternativas?

Un ejemplo de cloud privado es trasladar la infraestructura que tiene la empresa en sus instalaciones a un centro de datos. Salvo por razones estrictas de certificación existentes en algunos sectores, como el financiero (pci/dss) o alguno más, creo que no le aporta ventajas a la empresa porque sigue teniendo los problemas derivados de la infraestructura pero lejos de sus instalaciones. Para mí, la elección no es cloud privado frente a cloud público, la verdadera elección debe estar basada en cuestiones como disponibilidad, seguridad y facilidad. Creo que lo que demandan las empresas es dejar atrás los problemas derivados de la infraestructura y centrarse en la parte funcional que es donde se encuentra la verdadera transformación.

¿Cuáles son las consecuencias a las que se enfrentan las empresas que no dispongan de un plan de continuidad de negocio?

Hay voces que dicen que la empresa que no disponga de un plan de continuidad se enfrenta a la desaparición y creo que no andan desencaminadas. Cuando los procesos de la compañía dependen de los sistemas de información es imposible operar sin ellos y el valor de las caídas anuales se cifra en cientos de miles de euros de pérdidas para las empresas.

Lamentablemente, hemos visto demasiados casos en el último mes con elevado impacto para los que los han sufrido.

¿Cuáles son los factores críticos que cualquier organización debe tener en cuenta a la hora de ase-

gurar la alta disponibilidad de los sistemas y la continuidad de negocio?

Son muchos; la energía, la climatización, las comunicaciones, el hardware, el software, las ubicaciones, la seguridad y la operación de todos ellos vista como un factor crítico. A estos hay que añadirles los problemas derivados de la seguridad física, riesgos de catástrofes, etc.

Cualquiera de ellos es capaz de poner en jaque la continuidad de negocio. Cuando diseñas un servicio de alta disponibilidad para ofrecerlo a tus clientes te das cuenta de la cantidad de disciplinas que se deben contemplar, que por ellas mismas no aportan valor, y que cualquiera de ellas te puede producir un problema de disponibilidad.

Como hemos mencionado con anterioridad, en un escenario de incertidumbre cobra especial importancia disponer de un plan integral que garantice la continuidad del negocio. ¿Cuál es la propuesta de KIO Networks en este sentido?

Kio es un proveedor de infraestructura como servicio (IaaS). Entre los servicios que presta se encuentra VDC+ que es una infraestructura que incluye replica síncrona de la información del cliente en dos centros de datos separados 200Kms. Ello permite que ante una incidencia en una de las ubicaciones el sistema arranque de manera automática con un RPO= cero, es decir sin pérdida de datos, y con un RTO (tiempo que tarda en recuperarse el sistema) inferior a cuatro minutos. Este servicio permite a las empresas adoptarlo de manera inmediata y en régimen de pago por uso. Además de la réplica de la información, proporciona la réplica del backup y la configuración automática de las comunicaciones. Se trata de alta disponibilidad geográfica totalmente automatizada. ■

MÁS INFORMACIÓN

- Toda la información sobre Tecnología para tu Empresa
- ¿Cómo está evolucionando el modelo cloud?
- Toda la información sobre la propuesta de KIO Networks

LO QUE FALTABA... ¡LOS NÚMEROS SALEN!

Me sorprendió el éxito de uso que tuvieron las iniciativas de bicicletas compartidas; para alguien criado en la cultura de la propiedad ver que había público encantado de pagar por usar un servicio como la bicicleta fue revelador. El pago por uso se ha convertido en la clave económica de la revolución digital.

Según Wikipedia, la computación en la nube (del inglés cloud computing), conocida también como servicios en la nube, es un modelo que permite ofrecer servicios de computación a través de una red, que normalmente suele ser internet.

Entre los servicios de cloud computing que podemos contratar el primero que encontramos es el IaaS (infraestructura como servicio, en inglés). Consiste en dejar de comprar servidores, licencias de sistemas operativos, cabinas de discos y elementos de red, entre otros elementos, para pasar a contratar un servicio a cambio de una cuota mensual. Si este servicio permite aumentar o reducir las cantidades de los elementos que lo componen, actualizando su precio en función de las variaciones, se considera que estás pagando por el uso.

JAVIER JARILLA, director general de KIO Networks

Puedes leer la tribuna de opinión completa en este enlace.

CONTENIDOS↓

cloudya

¡Pruébalo gratis!

Tu negocio siempre conectado en la “nueva” normalidad.

Más información en **nfon.com**

La nueva libertad en la comunicación empresarial.

Con Cloudya, NFON ofrece una solución de centralita cloud que permite teletrabajar con una sencilla y rápida configuración. Como solución 100% en la nube, puedes llamar a través de IP o GSM, sin importar desde dónde estés trabajando: desde tu oficina en casa o de forma remota usando la aplicación en el móvil o en el ordenador, usando teléfonos de sobremesa o auriculares. Usa el mismo número desde todos tus dispositivos. Más de 40.000 empresas en Europa ya lo están usando. ¡Pídenos tu prueba gratis! **nfon.com**

910 616 600

partners.iberia@nfon.com

NFON
Cloud Telephone System

"LA VERSIÓN 2.0 DEL SERVICIO DE SIP TRUNK PRESENTA NOVEDADES SIGNIFICATIVAS EN FLEXIBILIDAD Y CONTINUIDAD DE NEGOCIO"

La telefonía IP ha ido ganando cada vez más popularidad, y son cada vez más las empresas que emplean una combinación de sistemas de telefonía convencional e IP. ¿Cuáles son los motivos que están llevando a realizar esta transición en sus comunicaciones?

La telefonía IP lleva entre nosotros más de un cuarto de siglo. La tendencia previa a la pandemia en la que la conciliación laboral/familiar, el ahorro de costes en dietas y la sostenibilidad a la hora de reducir la huella de CO2, reduciendo los viajes innecesarios, sentaban unas bases para que la migración hacia una solución de comunicaciones "todo IP" permitiese esa flexibilidad del empleado a la hora de utilizarla. Pero es cierto que la situación generada por la pandemia ha reactualizado, dado mayor visibilidad y relanzado este mercado, en el que algunos proveedores llevamos ya hace muchos años. Por eso, todo tipo de empresas, pequeñas, medianas o grandes, están buscando esa transición.

Un sistema SIP Trunk sirve de intermediario entre los sistemas de telefonía convencionales y los de VoIP. ¿Qué requisitos tiene que cumplir una empresa para poder adoptar este sistema?

Los enlaces SIP Trunk presentan requisitos tanto hacia el operador que lo proporciona como hacia la PBX con la que se conecta.

❖ Por un lado, hacia el operador que lo presta, se debe disponer del

DAVID TAJUELO, country manager de nfon Iberia

ALBERTO DOMARCO, Director de Operaciones y Preventa de nfon Iberia

ancho de banda necesario para soportar el número de canales, o conversaciones simultáneas, que deban proveerse. Este ancho de banda dependerá también del códec empleado para el transporte de la voz. Algunos minimizan este consumo a costa de reducir la calidad de la voz, pero con los anchos de banda disponibles en la actualidad es preferible, en general, dedicar uno mayor y no perder calidad en la voz.

❖ Por otro lado, y hacia el sistema PBX, se precisa que este soporte la tecnología SIP trunk tal como hacen la mayoría de sistemas actuales. En los casos en que no lo soportan, se puede continuar usando la tecnología de SIP trunk mediante la instalación de un sistema Gateway intermedio, capaz de "hablar" SIP trunk hacia el exterior y típicamente RDSI hacia la PBX.

"LA PANDEMIA HA ACELERADO LA ADOPCIÓN DEL SIP TRUNK", David Tajuelo, NFON Iberia

NFON acaba de presentar Nconnect Voice 2.0, la nueva versión de SIP Trunk, que proporciona una transición fluida hacia comunicaciones IP flexibles y escalables. ¿Cuáles son las principales novedades que ha incorporado NFON a esta nueva versión?

La nueva versión 2.0 del servicio de SIP trunk presenta novedades significativas en lo referente a la flexibilidad y a la continuidad de negocio principalmente. Por destacar algunas novedades:

❖ Respecto a la flexibilidad, permitimos la asignación de números y rangos de numeración internacionales a los trunks, de cualquiera de los países en los que prestamos servicios.

❖ En lo referente a la continuidad de negocio, permitimos la definición de múltiples PBXs asociadas a un trunk, de modo que en caso de indisponibilidad de alguna PBX las llamadas continúen entregándose en una PBX alternativa del cliente. Incluso en caso de indisponibilidad total de todas las PBXs, continuamos pudiendo entregar las llamadas en números públicos alternativos, fuera de nuestra propia red.

❖ Por añadir una novedad más, soportamos también la integración de nuestros trunks en la plataforma Teams de Microsoft, de modo que somos una pasarela entre la misma y los servicios públicos de telefonía.

¿Cuáles son los elementos diferenciales de Nconnect Voice 2.0 en comparación con otras soluciones que están en el mercado?

Respecto a la competencia, y además de las funcionalidades ya mencionadas que en muchos casos otros proveedores no proporcionan, ofrecemos una solución basada en infraestructura cloud altamente redundada para garantizar la disponibilidad del servicio. Valoramos igualmente la calidad de la voz que transportamos, por lo que usamos siempre códec G711 sin compresión. Además, soportamos el cifrado total de las comunicaciones mediante el uso de TLS y SRTP.

Entre los beneficios que obtienen las empresas que eligen un sistema SIP Trunk se encuentran el ahorro en cuotas, llamadas más económicas y mayor movilidad. ¿Qué perfil de empresa es el que más partido puede sacar a este tipo de solución?

En realidad cualquier empresa puede sacarle partido a estas características y a la mayor flexibilidad del modelo de conexión respecto a los modelos tradicionales, pero evidentemente será mayor el beneficio para aquellas que usen las funcionalidades diferenciales ya presentadas: Empresas con varias PBXs entre las que balancear el tráfico de voz, con necesidades de numeración internacional, o con necesidad de integrar MS Teams son candidatas ideales ya que sacarán partido a todas estas funcionalidades.

Con el lanzamiento de Nconnect Voice 2.0 ¿van a lanzar algún tipo de acción concreta para su canal de distribución?

Por supuesto, estamos tan seguros de que nuestra solución renovada, y ya probada durante muchos años en el exigente mercado alemán, será del gusto de nuestros partners y clientes que vamos a poner en marcha una promoción, tanto en canales como en tráfico, de 2 meses gratis. Sabemos que después de este tiempo, nuestros clientes seguirán confiando en nosotros. Tenemos la menor tasa de churn de todo el mercado europeo, y eso hace que sepamos que el que prueba NFON, se queda con nosotros.

Nconnect Voice 2.0, ¿puede ser comercializado por cualquier reseller de NFON o está orientado a un tipo concreto de partner?

Por cualquiera de nuestros partners, pero lógicamente está pensado para aquellos partners y clientes que quieran hacer una transición "suave" al "todo IP". Trabajando con NConnect Voice 2.0 se podrá acercar al mundo IP prácticamente toda la base instalada de centralitas tradicionales. Y de esta manera, enseñando al cliente /partner todas las posibilidades que una plataforma de comunicaciones, o simplemente una centralita, en la nube pone a la disposición de nuestros futuros clientes y partners.

¿Cuáles son las principales ventajas que podrán obtener los clientes de su canal de distribución?

Como decía, cualquier partner puede ofrecer y revender nuestros nuevos SIP Trunks. Es un mercado realmente en auge y abre múltiples posibilidades de generar beneficios para el partner. Lógicamente hablamos de comisiones recurrentes, tanto para los canales de voz que se quieran activar, como para el tráfico generado, y con las características técnicas más avanzadas para este tipo de soluciones. Pero también hablamos de la posibilidad de integrarlos con las licencias de Microsoft Teams que sus clientes ya tengan, generando valor añadido tanto para la venta de servicios adicionales, como de las posibles licencias de Microsoft necesarias para que el sistema corra sin ningún tipo de sobresalto. ■

MÁS INFORMACIÓN

- Toda la información sobre las tendencias tecnológicas en las empresas
- El mercado de la telefonía en la nube crece
- Cuál es la propuesta de NFON para el mercado de la telefonía en la nube

SAMSUNG

NVMe SSD 980 PRO

Unstoppable speed

PCIe 4.0

WORLD'S
No.1
FLASH MEMORY
SINCE 2003
SAMSUNG

* Source: 2003-2019 IHS Markit data:
NAND suppliers' revenue market share

“EL ALMACENAMIENTO SSD ES UN PRODUCTO MÁS SEGURO, MÁS RÁPIDO, Y MÁS VIABLE”

EUGENIO JIMÉNEZ CARRASCO, BRANDED MEMORY BUSINESS HEAD EN SAMSUNG STORAGE IBERIA

Según los últimos datos de las consultoras, el mercado SSD crecerá en torno a un 15% anual hasta 2026. ¿cuáles son los motivos que están llevando a los usuarios a adquirir este tipo de almacenamiento?

Las previsiones de las principales consultoras es que este mercado crecerá notablemente en los próximos años y esto se debe a varios motivos.

Los crecimientos esperados en SSD siguen basándose en la renovación del parque antiguo de portátiles y equipos de sobremesa cuyo almacenamiento siguen dependiendo del histórico HDD. Los ciclos de compra de un portátil/PC suele estar en torno a los 6-7 años, por lo que muchos consumidores prefieren darle un lavado de cara a sus equipos sustituyendo el HDD por el SSD y no comprando un equipo nuevo, afectando tanto al canal profesional como al de consumo.

No obstante, el abaratamiento que se ha producido está hacien-

do que muchos usuarios decidan adquirir nuevas soluciones.

Además, otro de los motivos es que existen usuarios que están renovando el parque de SSD de la primera generación.

Nos hemos encontrado con una demanda cada vez más creciente. Este mercado está creciendo a doble dígito en todos los segmentos y prevemos que vaya a continuar en los próximos años.

Poco a poco, el SSD está reemplazando el uso de otros soportes más convencionales. ¿Por qué es mejor adquirir almacenamiento SSD en vez de otro tipo de soporte?

Las ventajas del almacenamiento SSD frente a otros soportes más convencionales son múltiple.

El almacenamiento SSSD es un producto más seguro, más rápido, y más viable. Las garantías son bastante amplias y de cara al usuario todo son ventajas, ya que se aumenta la productividad, la eficiencia de los equipos, el consumo de batería de los portátiles, la seguridad de los dispositivos al contar con tecnología de cifrado, la velocidad de acceso a determinados programas, la velocidad de arranque de los propios equipos...

Esta transición supone un incremento de la demanda de componentes. ¿Cómo va a afectar esto a la hora de comprar un SSD? ¿Se espera un incremento de precios?

Lo que estamos comprobando en Samsung es que, en el mercado de almacenamiento, en la primera mitad del año va a haber cierta escasez, no de los componentes en general, sino de la parte de controladoras.

Esta realidad está afectando al mercado, pero a Samsung en menor medida. ¿El motivo? Samsung fabrica el 100% de sus componentes. Esto nos lleva a ofrecer un producto de mayor garantía y terminado, mientras que otros fabricantes lo que hacen es recurrir a un mercado de terceros y es precisamente este mercado de terceros el que está teniendo escasez de producto.

Desconocemos si esta situación va a llevar a un encarecimiento de productos. Por lo menos, nuestra política está siendo mantener los precios.

Samsung dispone de un amplio abanico de soluciones tanto para entornos empresariales como de consumo para el mercado SSD. ¿Cuáles son las principales diferencias de esta propuesta frente a la de sus principales competidores?

En SSD, la propuesta de valor de Samsung radica en la fiabilidad de sus productos. Samsung se preocupa por entregar la mejor calidad en sus productos. En este sentido, hemos de destacar tan-

Toda la información sobre la situación TI de las empresas españolas en @TIyEmpresa_ITDM

"DE CARA AL USUARIO, EL ALMACENAMIENTO SSD SOLO OFRECE VENTAJAS"

to las velocidades ofrecidas dada nuestra fuerte apuesta por los SSD con tecnología NVMe como las amplias garantías de nuestros SSD, permitiendo un ciclo de vida de nuestros productos más alargado y sostenido en el tiempo.

El último lanzamiento de Samsung es el modelo 870 EVO. ¿Cuáles son las principales características de esta solución?
El 870 EVO es nuestro caballo de batalla, al ser el disco más vendido del mercado. En este sentido, hemos mantenido el listón de la anterior generación en cuanto a garantías, velocidad o fiabilidad. Además, hemos actualizado el software de gestión. La demanda está siendo muy alta.

¿Qué ventajas son las que ofrece Samsung frente a la competencia?
Samsung dispone de una variedad de producto lo suficientemente amplía para poder adaptarse a cualquier escenario y satisfacer las demandas más exigentes de los clientes tanto en el mercado de consumo como en el profesional. ■

UN SSD QUE ACELERA LAS TAREAS INFORMÁTICAS DIARIAS

El SSD 870 EVO une rendimiento, fiabilidad y compatibilidad para los usuarios ocasionales de ordenadores portátiles y de escritorio, pero también para aquellos usuarios de almacenamiento conectado a la red (NAS). La unidad ofrece una mejora de casi un 38% en la velocidad de lectura aleatoria con respecto al modelo 860 anterior, lo que mejora la experiencia de usuario mediante la realización de múltiples tareas, como navegar por la web o simplemente arrancar un PC. EL SSD está disponible con 4TB, 2TB, 1TB, 500GB y 250GB de capacidad.

La solución SATA posee el último controlador y tecnología V-NAND 3-bit MLC (TLC) de la compañía, lo que le permite alcanzar velocidades máximas de lectura y escritura secuencial de 560 y 530 MB/s, respectivamente. Al utilizar un búfer SLC variable, la tecnología Intelligent TurboWrite de la unidad mantiene sus niveles máximos de rendimiento.

Samsung diseña todos los componentes de SSD internamente para garantizar que todas las partes funcionen de manera unificada, lo que permite que 870 EVO ofrezca alrededor de un 30% de mejora en el rendimiento sostenido con respecto a 860 EVO, así como una clasificación de terabytes escritos (TBW) líder en su categoría, de 2.400 TB, o una garantía limitada de 5 años, para su modelo de 4 TB.

Al ofrecer una amplia compatibilidad con muchos dispositivos informáticos, así como con las funciones de PC más actualizadas, la unidad se puede utilizar con todos los dispositivos que tengan una conexión de interfaz SATA de 2,5 pulgadas. Además, con su modo de suspensión de ahorro de energía, 870 EVO es compatible con dispositivos que admiten la función Modern Standby de Windows, lo que ofrece una mayor comodidad a los usuarios de PC.

MÁS INFORMACIÓN

- Toda la información sobre las tendencias tecnológicas en las empresas
- El mercado de almacenamiento SMB crece
- Cuál es la propuesta de Samsung para el mercado de almacenamiento SMB

SERVICENOW MUESTRA EL PODER TRANSFORMADOR DE LOS FLUJOS DE TRABAJO EN KNOWLEDGE 2021

Imaginar ser capaz de resolver cualquier problema al que tu negocio se enfrente. En Knowledge, ServiceNow mostró el poder transformador de los flujos de trabajo, los cuales pueden hacer crecer a las empresas más resilientes y remodelar industrias.

El pasado 11 de mayo arrancó una nueva edición de Knowledge, el evento estrella de ServiceNow, una experiencia digital donde los visitantes pudieron descubrir como la Now Platform ofrece experiencias modernas a clientes y empleados que aceleran el valor y la innovación.

Durante el evento, los asistentes pudieron descubrir cómo las empresas más innovadoras hacen que el mundo del trabajo funcione mejor para las personas a través de las charlas de líderes digitales, socios y expertos. Entre los ponentes destacan Bill McDermott, presidente y CEO de ServiceNow; Dave Wright, director de Innovación de ServiceNow; Chirantan 'CJ'Desai, director de producto de ServiceNow; Kimberly Quan, jefa global de eDiscovery & Digital Forensics de Juniper Networks; Dave Hellman, director de ITSM de Levi Strauss; y Amedeo Guarraci, vicepresidente de PepsiCo.

PALABRAS DE BILL MCDERMOTT

"ServiceNow se encuentra en el centro de la revolución del flujo de trabajo", aseguró Bill McDermott, quien recordó que, gracias a su propuesta, las empresas pueden desarrollar negocios digitales del Siglo XXI. "Quere-

mos que éstas faciliten grandes experiencias a las personas".

Bill McDermott también tuvo palabras para la pandemia. Ésta ha provocado toda una revolución en la forma en la que trabajan, y viven, las personas y tras un periodo en el que el teletrabajo se impuso, ahora su compañía está facilitando "la vuelta segura a las oficinas".

En su opinión, "la plataforma Now está haciendo fluir soluciones que hacen que el trabajo y la vida sean mejores para las personas. El mundo trabaja con ServiceNow".

UN PROGRAMA COMPLETO

En Knowledge 2021 los más de 40.000 registrados pudieron elegir entre cientos de sesiones en las que descubrieron cómo otros clientes y socios utilizan flujos de trabajo para transformar su negocio, y aprender de expertos de la industria y líderes de ServiceNow a abordar temas centrados en el futuro.

Asimismo, también pudieron maximizar sus habilidades en Now Platform con discusiones interactivas y profundas de 30 minutos con expertos de ServiceNow, y acelerar la innovación, aumentar la agilidad y mejorar la productividad con la versión Now Platform Quebec.

Los patrocinadores premier de Knowledge 2021 fueron Accenture, Deloitte, DXC Technology, EY, KPMG y Microsoft.

UN ALUVIÓN DE LANZAMIENTOS

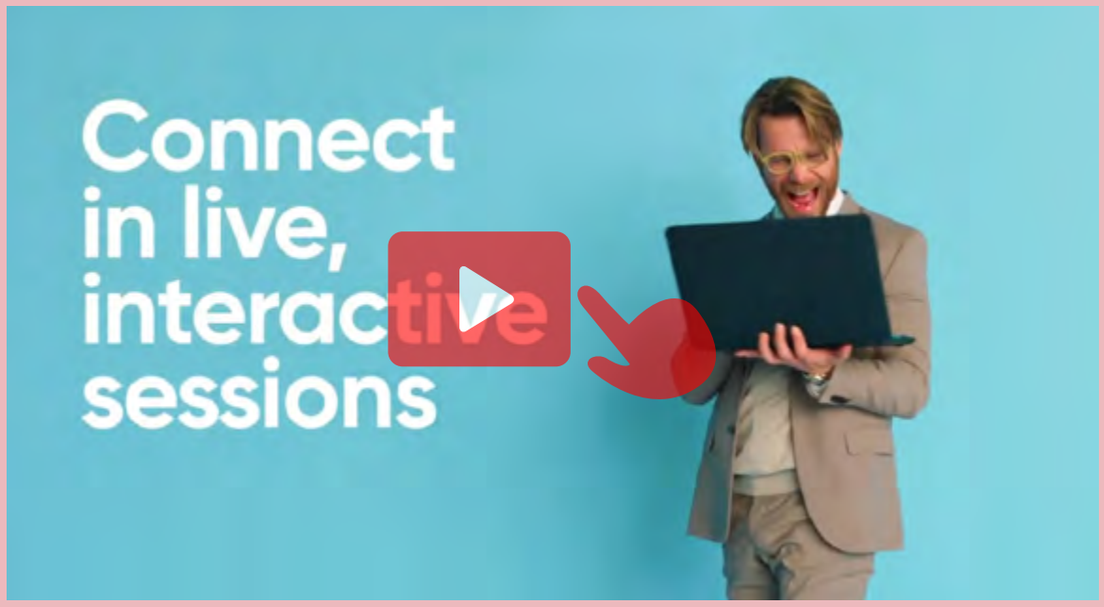
Durante la celebración de Knowledge 2021 ServiceNow anunció nuevas soluciones, innovaciones y movimientos estratégicos que tienen el fin de extender el potencial transformador de los flujos de trabajo para afrontar los grandes cambios a los que se enfrentan tanto los negocios como las personas.

Y es que, para ofrecer una experiencia de servicio al cliente óptima, se debe tener en cuenta todas las personas, los procesos y las herramientas que participan en ka organización. Para ServiceNow debes implementar flujos de trabajo digitales inteligentes que conecten tu front office con los equipos de middle y back office, y los equipos de servicios de campo.

Entre las novedades destacan aquellas orientadas a las industrias de fabricación, salud y "ciencias de la vida", como Operational Management (que ayuda a las empresas de fabricación a hacer que las operaciones sean más eficientes y seguras a la par que mejora la experiencia de los empleados), o Healthcare and Life Sciences Service Management (simplifica las gestiones para mejorar la experiencia del paciente); las que impulsan los esfuerzos que se están realizando en la vacunación (se han anunciado nuevas capacidades en la solución de Gestión y Administración de Vacunas (VAM) de ServiceNow).

Con las nuevas funciones que se han añadido a la solución Workplace Service Delivery y Safe

Toda la información sobre la situación TI de las empresas españolas en @TIyEmpresa_ITDM



ÚNETE A KNOWLEDGE 2021

SERVICENOW ANUNCIA LA COMPRA DE LIGHTSTEP

Consolidando aún más su posición como la plataforma preferida para las empresas digitales, ServiceNow ha anunciado la adquisición de Lightstep, una compañía emergente centrada en la monitorización y observabilidad de aplicaciones de última generación. ServiceNow espera completar la adquisición en el segundo trimestre de 2021.

En un mundo basado en la nube y en DevOps, el software que impulsa a las empresas de hoy en día es cada vez más complejo. Sin embargo, se prevé que las empresas aumentarán su innovación y velocidad sin sacrificar la fiabilidad y el rendimiento. En este sentido, la combinación de ServiceNow y Lightstep ofrecerá una visión operativa exhaustiva para que las empresas puedan utilizar de forma más eficaz las pilas de la tecnología moderna.

"Las empresas están apostando por digitalizarse para prosperar en el siglo XXI, pero la transición a menudo es difícil de afrontar", explica Pablo Stern, SVP & GM, IT Workflow Products, ServiceNow. "Con Lightstep, ServiceNow transformará la forma en que se entregan las soluciones de software a los clientes. Esto, en última instancia, facilitará a los clientes la innovación rápida. Ahora serán capaces de construir y operar su software más rápido que nunca y afrontar la nueva era del trabajo con confianza".

La solución de Lightstep analiza las métricas de todo el sistema y los datos de seguimiento en tiempo real para comprender la causa y los efectos de los cambios en el rendimiento, la fiabilidad y la velocidad de desarrollo de las aplicaciones. Now Platform coordina la respuesta técnica y del equipo, vinculando los conocimientos con las acciones necesarias para impulsar la transformación digital. De esta forma, los clientes podrán supervisar y responder más fácilmente a las alertas e indicadores de criticidad sobre el estado del software aprovechando las capacidades de Lightstep junto con las soluciones de flujos de trabajo de TI de ServiceNow para conectar elementos dispares en una estructura digital sin fisuras. Ello confiere a las empresas la confianza y la claridad necesarias para impulsar una innovación más rápida y mejorar los resultados en el ámbito de la experiencia digital.

Fundada en San Francisco en 2015, Lightstep fue cofundada por el consejero delegado, Ben Sigelman, el director de operaciones, Ben Cronin, y el arquitecto jefe, Daniel Spoonhower, quienes ayudaron a definir la observabilidad moderna con su trabajo previo en materia de rastreo y monitorización de métricas en Google.

"Hoy en día, la observabilidad beneficia principalmente a los equipos de DevOps que crean y despliegan aplicaciones de misión crítica", afirma Ben Sigelman, CEO y cofundador de Lightstep. "Siempre hemos creído que el valor de la observabilidad debería extenderse a toda la empresa, proporcionando una mayor claridad y confianza a todos los equipos involucrados en estos negocios modernos y digitales. Al unirnos a ServiceNow, juntos haremos realidad esa visión para nuestros clientes y ayudaremos a transformar el mundo del trabajo en el proceso, y no podríamos estar más entusiasmados con ello".

Workplace Suite de ServiceNow, las empresas facilitarán la vuelta segura al trabajo de sus empleados. En Knowledge 2021 también se pudo ver la nueva herramienta de planificación Safe Workplace Dashboard, así como se habló de la última adquisición de la firma: Lightstep. ■

MÁS INFORMACIÓN

- Toda la información sobre las tendencias tecnológicas en las empresas
- ¿Cómo está evolucionando el puesto de trabajo?
- Cuál es la propuesta de ServiceNow para ayudar en la transformación del puesto de trabajo

¿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 Centro de Recursos itUser

Tecnología para tu Empresa

KIO Networks

NetApp

NFON Cloud Telephone System

SAMSUNG

servicenow

REPORTAJE

El contact center se alza como el salvavidas de muchas empresas en la pandemia

El sector de la atención al cliente lleva años centrándose en la experiencia de usuario, y el contact center se ha convertido en uno de los puntos de interacción más importantes para el cliente, por lo que hay un claro crecimiento en este segmento. Lógicamente, el año 2020 aceleró la demanda de soluciones que permitieran mejorar la experiencia del cliente y la eficiencia operativa como necesidades urgentes, a lo que se ha sumado el desafío de gestionar operaciones de manera remota y perfeccionar el teletrabajo, haciendo que la gran tendencia actual sea la irrupción del contact center en la nube con mucha analítica y automatización de procesos. De la influencia de la pandemia en este mercado, de la evolución tecnológica del contact center y de lo que representa para el negocio del canal de distribución hemos hablado con Ingram Micro, LCRcom, masvoz, Mitel, NFON, Ringover y Snom.

Las expectativas de atención al cliente ya estaban aumentando antes de la COVID-19 y muchas compañías ya se estaban apuntando a desarrollar su estrategia de contact center para satisfacer las necesidades de los clientes. Así que la pandemia solo ha acelerado la velocidad de esta tendencia. Como apunta David Tajuelo, director general de NFON Iberia, "las tendencias del mercado de contact center ya apuntaban a la transformación digital, y el año 2020 aceleró ese proceso. La demanda ha crecido mucho el pasado año, y este sigue una misma tendencia".

ADAPTACIÓN AL COVID-19

La COVID-19 ha sido, como para todo sector, un gran desafío. La forma en que los clientes se relacionan con las marcas se ha transformado, haciendo que el escenario de la respuesta al cliente, o la emisión de llamadas, haya dado un vuelco.

La pandemia ha hecho que los clientes hayan incrementado el número de operaciones con los servicios de atención de las empresas en general, y con los contact center en particular, al reducirse e incluso llegar a desaparecer en algunos momentos el contacto directo y personal tradicional por las limitaciones y el distanciamiento social.

Según un estudio reciente de Mitel sobre la experiencia del cliente, en el que participaron más de 4.000 consumidores, el 60% percibe una mejora en la experiencia del cliente desde la pandemia, lo que indicaría que las empresas reconocen su importancia en la estrategia de relación con el cliente y están actuando en consecuencia adoptando soluciones de contact center. "En Mitel no solo hemos notado un aumento de la demanda de este tipo de soluciones, sino que hemos recibido peticiones de muchas empresas que no identifican en primera instancia que necesitan un contact center, pero que buscan las capacidades de este tipo de solución. Al final, todas las empresas tienen clientes y deben brindarles la mejor atención posible", asegura Eva Arroyo, Marketing Manager, Mitel Iberia & Italia.

"La aparición del Covid-19 aceleró los planes de las empresas para conseguir que sus centros de contacto pudieran trabajar a distancia, y tuvieron que hacerlo de la noche a la mañana. Por este motivo, y en muchos casos, la calidad de las llamadas no se ha podido mantener de forma continuada, ya que los agentes no siempre tienen una buena conexión a Internet y/o su red local puede no ser lo suficientemente buena como para proporcionar una buena calidad de llamada, y este es el mayor problema para un centro de llamadas remoto", comenta Renaud Charvet, Cofundador y CEO de Ringover.

Por su parte, José María Barranco, PRO AV & UCC SALES MANAGER en Ingram Micro Iberia, cree que "la COVID-19 ha revolucionado el mercado, produciendo un verdadero cambio de paradigma que entendemos que ha venido para quedarse. Realmente siempre hubo empresas que ya contaban con planes y tecnología para deslocalizar el trabajo de un centro físico a uno remoto. Para otras fue un reto de una envergadura inicial muy incierta que finalmente supieron llevar a buen puerto".

> La **pandemia** ha sido el **último empujón** que necesitaba el mercado de **contact center en la nube**
>
> Pablo Romero, Responsable de Soluciones Cloud en **LCRcom**

LA MODALIDAD CLOUD Y AS-A-SERVICE GANA PESO

Para compatibilizar la atención al cliente con el trabajo en remoto, las empresas han tenido que adoptar soluciones de contact center con capacidades sólidas para agentes remotos, que garanticen que los teletrabajadores pueden proporcionar la misma experiencia que podrían ofrecer en un entorno de oficina, impulsando la irrupción de soluciones en la nube.

A juicio de Pablo Romero, Responsable de Soluciones Cloud en LCRcom, "la pandemia ha sido el último empujón que necesitaba el mercado de contact center en la nube. Hasta los más escépticos frente a este tipo de tecnologías se han visto obligados a contratar estos servicios ya que los modelos on premise no eran lo suficientemente ágiles para la nueva situación de teletrabajo".

De la misma opinión es Nacho Ginés, Product Manager en masvoz, para quien "el futuro de las infraestructuras de comunicación estará inevitablemente vinculado al cloud. Los sistemas de telefonía en la nube son una opción más rentable para las empresas que el mantenimiento de redes fijas tradicionales, además de ser una alternativa idónea para garantizar la movilidad que ahora se antoja tan necesaria".

En términos generales, los sistemas de comunicación ofrecidos como servicio o basados en un modelo de suscripción están siendo muy bien acogidos, y cada vez más demandados por los clientes. La escalabilidad y migración al ritmo del cliente que ofrecen las soluciones de contact center como servicio (CCaaS) son clave tanto para optimizar las comunicaciones como para proteger las inversiones.

A este respecto Eva Arroyo, de Mitel, señala que, "en el ámbito del contact center, las empresas deben adaptarse a una nueva generación de consumidores siempre conectados que esperan un servicio ultrapersonalizado y una disponibilidad inmediata. Con una solución de CCaaS, dispondrán de las herramientas para construir relaciones positivas con sus clientes y, al mismo tiempo, tendrán la garantía de que invierten únicamente en las capacidades que necesitan en cada momento".

> Las soluciones de contact center siguen creciendo en el ecosistema de las **comunicaciones unificadas**
>
> Miguel Anillo, Channel Manager Iberia de **Snom**

UNA SOLUCIÓN MULTISECTORIAL

El contact center se encuentra en un momento de importante crecimiento, al ser las empresas más conscientes de que facilitar la mejor experiencia al cliente es una acción que consigue aumentar la fidelización de estos, así como un incremento de las ventas. La demanda de este tipo de soluciones proviene pues de todos los sectores, incluida la Administración Pública, para la que es un imperativo para mejorar la atención y los servicios que ofrece al ciudadano.

"Todo el mundo quiere no perder llamadas y quiere poder ofrecer la mejor experiencia posible a sus clientes, partners y proveedores", explica David Tajuelo, de NFON, destacando que "el sector de las telecomunicaciones y los medios se mantienen como los principales demandantes para las empresas de contact centers".

Nacho Ginés, de masvoz, ha notado que "en sectores más afectados por la pandemia, como es el sector de la salud, teléfonos de atención psicológica, gestión de citas, etc. han contado con una mayor demanda. Por otra parte, aquellos servicios y empresas relacionadas con el e-commerce, los cuales han tenido un mayor incremento del tráfico en su negocio se han visto en la necesidad de implementar también soluciones de webchat y asistentes virtuales".

José María Barranco, de Ingram Micro, por su parte, recalca que "decenas de servicios de cualquier industria pasaron de la noche a la mañana a gestionarse a través de un contact center, como la telemedicina, seguimientos a contagiados, etc.".

Por otro lado, muchas veces se asocia una solución de contact center a empresas grandes, pero cualquier negocio, por pequeño que sea, tiene clientes y necesita una estrategia que mejore la experiencia al interactuar con ellos. En este sentido, Miguel Anillo, Channel Manager Iberia de Snom, afirma que "lo bueno es que ahora las pymes también pueden operar en igualdad de condiciones contratando este tipo de servicios para un periodo concreto, como una promoción o una feria profesional".

"Los contact centers solían ser principalmente para las empresas, debido a la inversión inicial y a los costes de funcionamiento. Incluso el software estaba diseñado para equipos grandes. Pero el paso a la nube cambió por completo la situación. Ya no hay enormes inversiones iniciales, y es económicamente posible conseguir un contact center para unos pocos agentes, e incluso para uno solo", puntualiza Renaud Charvet, de Ringover.

INNOVACIÓN CONSTANTE

La experiencia de cliente se ha posicionado como una parte esencial dentro de los

> Los clientes demandan **omnicanalidad,** y un ejemplo de ello es la utilización del **chatbot**
>
> David Tajuelo, director general de **NFON** Iberia

> La utilización de la **Inteligencia Artificial** y los **asistentes virtuales** es ya una realidad
>
> Nacho Ginés, Product Manager en **masvoz**

contact center, donde la tecnología está siendo clave para mejorar día a día esta experiencia, convirtiéndose en el centro de toda la innovación y desarrollo. Una de las capacidades más demandadas para satisfacer el 'customer journey' del consumidor digital de hoy es la omnicanalidad.

Así lo cree que David Tajuelo, de NFON, para quien, "en general, los clientes demandan omnicanalidad, y un ejemplo de ello es la utilización del chatbot, una práctica cada vez más extendida entre las empresas. Durante el año 2019, el 67% de los usuarios se comunicaron con atención al cliente a través de un canal de este tipo, así que las cifras señalan un auge del papel de los chatbots en los contact center como vehículo de comunicación. Pero no solo hablamos de ellos, sino también de utilizar canales como teléfono, WhatsApp, chat online o redes sociales".

Asimismo, en el contexto actual, tecnologías como la inteligencia artificial (IA) y las funciones que tienen que ver con opciones de autoservicio y automatización están viendo un incremento notable. Muchas empresas han debido adaptarse a plantillas más pequeñas por lo que son soluciones muy demandadas para aliviar a los agentes del contact center de tareas rutinarias, permitiéndoles centrarse en aquellas interacciones de valor añadido.

"La utilización de la Inteligencia Artificial y los asistentes virtuales es ya una realidad y durante estos meses veremos continuos avances en el procesamiento del lenguaje que, entre otras cosas, harán que estos asistentes sean aún más inteligentes y puedan responder a preguntas más complejas de los usuarios", apunta Nacho Ginés, de masvoz.

Eva Arroyo, de Mitel, también cree que "la inteligencia artificial se aplicará más ampliamente. Más allá del enrutamiento de llamadas o del uso de agentes virtuales, la IA estará cada vez más integrada en las interacciones con los clientes, ayudará a desarrollar más opciones de autoservicio y se profundizará más en el análisis predictivo para ayudar a optimizar las experiencias e incluso guiar a los clientes a través de su 'buying journey'".

También ganarán cada vez más peso las herramientas de análisis para convertir datos, como grabaciones de llamadas y pantallas, chats, mensajes SMS y más,

"Las empresas deben adaptarse a una nueva generación de **consumidores siempre conectados**"

Eva Arroyo, Marketing Manager, **Mitel** Iberia & Italia

en información realmente útil para los agentes y para crear los dashboards con las métricas que afectan al negocio y tomar decisiones basadas en datos.

Por último, las integraciones con soluciones de terceros de colaboración, vídeo o CRM, por ejemplo, son muy demandadas para brindar una experiencia superior tanto a clientes como a empleados. "La integración con las herramientas empresariales es la característica clave que la mayoría de los clientes exigen, Una herramienta de contact center debe estar integrada con el CRM y/o el helpdesk del cliente", ratifica Renaud Charvet, de Ringover.

EL CANAL COMO GUÍA

Está claro que las empresas tienen un importante aliado en las soluciones de contact center a la hora de trabajar para mejorar la experiencia del cliente, pero, por atractivas que parezcan tecnologías como la IA o los chatbots, antes de crear una solución se necesita comprender la hoja de ruta del cliente. Es ahí donde el canal tiene una gran oportunidad para realizar el acompañamiento al cliente en su viaje.

"El canal debe ayudar a definir la mejor estrategia en función del grado de madurez de los clientes", declara Eva Arroyo, de Mitel, añadiendo que "el gran peso de los servicios profesionales en todas las fases de un proyecto de contact center hace imprescindible que los operadores trabajen con fabricantes y partners capaces de suministrar una solución integral".

En lo que todos coinciden es que el mercado de Contact Center representa una oportunidad de negocio real para el canal. "Están apareciendo nuevas oportunidades de servicios para ellos en empresas que hasta hace poco no los tenían en su radar de ventas. Los partners tienen todo el conocimiento y herramientas para dar cobertura a esta demanda", reconoce Pablo Romero, de LCRcom.

"Es un mercado muy competido, pero a la vez muy dinámico, y eso hace que represente una verdadera oportunidad de negocio para todo el ecosistema", argumenta José María Barranco, de Ingram Micro. "La clave de la rentabilidad reside en el valor añadido total que se ofrezca desde el canal a los clientes, donde el peso de la parte de servicios en muchos casos es determinante".

Los partners pueden aportar valor con su capacidad para ayudar a los clientes a encontrar la solución adecuada y qué tipo

> Una herramienta de contact center debe estar **integrada con el CRM y/o el helpdesk del cliente**
>
> Renaud Charvet, Cofundador y CEO de **Ringover**

> La clave de la **rentabilidad** reside en el **valor añadido** total que se ofrezca desde el canal a los clientes
>
> José María Barranco, PRO AV & UCC SALES MANAGER en **Ingram Micro** Iberia

de integraciones necesitan. Además, tras la venta, brindar servicios de valor añadido como mantenimiento, soporte técnico e integraciones personalizadas pueden abrir un mundo completamente nuevo de oportunidades.

"Estamos viendo que las empresas de canal siguen aumentando su influencia en este espacio a medida que las soluciones de contact center siguen creciendo en el ecosistema de las comunicaciones unificadas", comenta Miguel Anillo, de Snom. "Los márgenes en el sector de las comunicaciones se han resentido en los últimos 20 años, y los servicios de valor añadido, como las nuevas soluciones de contact center, combinadas con terminales y dispositivos de gama alta, están revertiendo esta tendencia".

David Tajuelo, de NFON, concluye señalando que "nuestros partners se encuentran con demandas por parte de pymes cada vez más pequeñas que necesitan proporcionar a sus clientes una atención profesional. La solución puede ir desde una simple gestión de colas de llamadas hasta la integración con herramientas tipo ERP o CRM. Todos esos servicios y soluciones, proporcionados habitualmente por nuestros partners, son una excelente oportunidad para el crecimiento de negocio transversal". ■

MÁS INFORMACIÓN

- El mercado de software de contact center crecerá cada año más de un 20% hasta 2026
- La mitad de las empresas españolas migraría su contact center a la nube
- Así está cambiando la atención al cliente: la evolución del contact center
- El contact center ha sido el canal más empleado por los clientes durante la crisis
- Así evoluciona el empleo en el sector del contact center
- Las ventajas de cloud llegan también al contact center

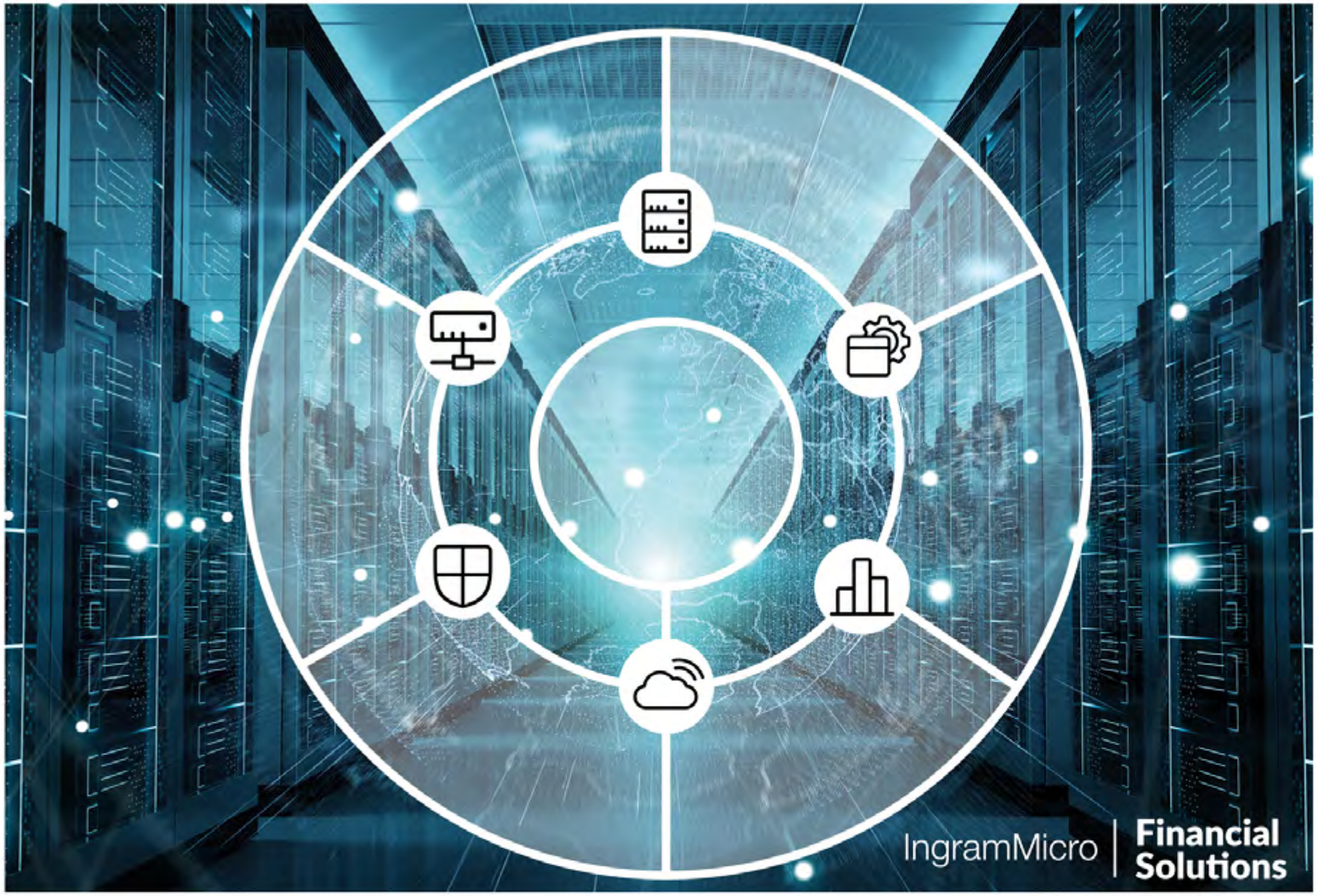
Externalización vs contact center interno

Aunque hay organizaciones que prefieren disponer de su propio contact center, la subcontratación de este tipo de servicios a empresas especializadas es una tendencia en alza desde hace tiempo. De hecho, hay muchas empresas que ofrecen servicios de contact center por días o también por horas, todo ello debido a la idea de servicio 24/7.

Preguntado por si está habiendo más demanda de soluciones de contact center por parte de las empresas clientes o por parte de empresas que prestan estos servicios, David Tajuelo, de NFON, afirma que "las empresas que prestan los servicios, por la pandemia, ha tenido que adaptarse muy rápidamente y poner encima de la mesa soluciones para que los empleados puedan trabajar desde casa de la misma manera que lo hacían en su centro de trabajo; lógicamente hablamos de grandes sistemas para dar respuesta no solo a un cliente, sino a varios, o muchos, cada uno con unas necesidades. Por otro lado, las empresas han sufrido un crecimiento generalizado del número de llamadas entrantes y necesitan poder gestionarlas, porque una llamada perdida puede ser un gran negocio perdido".

Pablo Romero, de LCRcom, opina que "la demanda de soluciones es mayor por parte de las empresas que prestan servicios de contact Center. Este servicio es muy específico por lo que las grandes empresas prefieren contratar servicios especializados en estos casos. Ahora bien, también se están dando casos en los que empresas y clientes han visto que estas soluciones tienen una fácil implantación, y tanto su mantenimiento como su configuración son sencillas de acometer, y están apostando en integrarlo dentro de sus servicios para tener aún más cerca y controlada la atención a sus clientes".

Renaud Charvet, de Ringover, añade que "hoy en día es posible que una empresa tradicional tenga acceso a soluciones profesionales de contact center a una fracción del coste que solía tener y sin una instalación dolorosa, ya que no hay hardware, todo está en la nube, y es accesible para los agentes estén donde estén. Esto es una verdadera revolución".



INGRAM MICRO®
Advanced Solutions

Advanced Solutions

Advanced Solutions, la División de Valor de Ingram Micro para ntegradores especializados en tecnologías de Datacenter. Servidores, almacenamiento, ciberseguridad, networking, virtualización y software empresarial.

- HPE DIVISION
- CISCO DIVISION
- SERVERS & STORAGE
- VIRTUALIZATION & MOBILITY
- NETWORKING & SECURITY
- POWER & COOLING

Life Is On APC by Schneider Electric · aruba a Hewlett Packard Enterprise company · Barracuda · cisco Partner Distribution Partner · cisco Meraki · citrix · DATACORE · EATON Powering Business Worldwide · flexxible IT Leading a revolution in digital transformation · FUJITSU · Hewlett Packard Enterprise · McAfee · Praim Transforming Enterprise Computing · PURE STORAGE · riello ups · RSA · SONICWALL · SOPHOS · VERTIV

Para más información: 902 902 750 - www.ingrammicro.es - comercial@ingrammicro.es

Inteligencia y analítica de datos como oportunidad para el canal, a debate

De éstas y otras cuestiones debatimos junto a Javier Grande, business solutions and transformation manager en Arrow ECS España; David Fernández, customer success director en Inbenta España; Alberto Pascual, director ejecutivo de Ingram Micro España; y Moisés Martínez, responsable de Inteligencia Artificial en Paradigma Digital.

La información es uno de los activos principales de las empresas, pero es evidente que hay que transformar esta información en valor para el negocio. Tal y como apunta Javier Grande, "la información está ahí, pero hay que sacar el valor de estos datos, y por eso empresas como las que estamos en este debate estamos ayudando al canal para que lo traslade al cliente. Llevamos años recopilando datos, pero ha llegado el momento de sacarle el jugo a todos ellos y transformarlos en acciones que puedan aportarnos valor".

Para David Fernández, "todas las empresas quieren conocer más y mejor a los clientes, y necesitan el dato como vehículo para ello. Pero lo que realmente quieren es ofrecerles un mejor servicio y que la tecnología les ayude en el día a día para ser más productivos. Esto es lo que va a conseguir que las empresas tengan un posicionamiento más competitivo. Para nosotros, en el análisis de la información, el dato es fundamental, pero lo analizamos desde el punto de vista del significado, porque un dato puede tener diferentes significados dependiendo del con-

INTELIGENCIA Y ANALÍTICA DE DATOS COMO OPORTUNIDAD PARA EL CANAL, A DEBATE

De la capacidad de extraer valor de los datos dependerá el posicionamiento competitivo de las organizaciones en el nuevo orden digital. De ahí que la inteligencia artificial y la analítica deban ayudar a manejar de manera eficiente la gran cantidad de información existente para transformar el Big Data de volumen en valor. ¿De qué manera se está adentrando el canal en un sector tradicionalmente ajeno a su foco de actuación, pero que le puede proporcionar un abanico ingente de oportunidades?

texto, y con herramientas para poder mejorar la interpretación del dato". En palabras de Alberto Pascual, "estamos convencidos de que estamos en una Cuarta Revolución Industrial. Si bien en las anteriores había una tecnología que era la locomotora del avance, en el caso actual hay una convergencia de tecnologías emergentes que están facilitando la transformación. Pero sí hay un hilo conductor, la IA, que es el motor ahora mismo. Como con otras tecnologías emergentes, el canal necesita un período de inmersión en la tecnología y de inversión en recursos, y somos los mayoristas los que damos el primer paso para que el canal pudiera acceder a estos recursos y servicios. Para ello, hemos creado un centro de IA como servicio, con orientación regional. Además, vemos un gran potencial en la IA para detectar amenazas, y para ello hemos creado un segundo centro experto, donde hemos desarrollado dos herramientas. Y, en tercer lugar, hemos creado un centro en España para aportar inteligencia de mercado a fabricantes y resellers y donde hemos creado una herramienta para hacer análisis de digitalización de PYMES. En la parte de la distribución pura, tenemos algunas soluciones, pero pensamos que ahora nuestra labor debe ser la de evangelizar".

En opinión de Moisés Martínez, "nosotros ofrecemos estas posibles aplicaciones en las que la IA es una realidad. Entendemos el uso de la IA como una herramienta para ofrecer mejores soluciones, y pensamos que ahora hay una gran oportunidad por la gran cantidad de datos y tecnología. Todo esto, eso sí, desde una perspectiva ética y explicable. Intentamos que las compañías y los usuarios sepan exactamente por qué sus productos hacen lo que hacen. Y esto es algo en lo que no muchas compañías se centran, algo que cambiará, y, de hecho, las autoridades europeas ya están preparando una legislación al respecto".

Apunta David Fernández que hay tecnologías "que parten de un análisis desconocido para el usuario. Nosotros partimos de soluciones que explica cómo el sistema funciona para darte una respuesta. Esto permite que el cliente no solo conozca lo que está pasando, sino que pueda adaptarlo a su negocio".

DATOS INTELIGENTES, DECISIONES ÁGILES

Según IDC, para 2022, el 75% de las organizaciones van a incorporar la automatización inteligente en el desarrollo de sus procesos, apoyándose en la IA para descubrir ideas que puedan desarrollar, permitiendo un crecimiento, en España, del negocio de la IA en España genere 650 millones de euros en un año, con un crecimiento interanual del 30%.

Al hilo de estos datos, Moisés Martínez señala que son "extremadamente optimistas. Uno de los problemas que tenemos en España con la IA es la falta de profesionales con la capacitación necesaria. En los últimos años, hemos visto la democratización de tecnologías que se apoyan en la IA, como el Machine Learning o el Deep Learning, pero estas soluciones se hacen sin un conocimiento real de cómo funcionan estas técnicas, lo que provocará que se queden obsoletas con el paso de los años. Y esto se debe a la falta de personal y perfiles expertos para llevar la IA al siguiente nivel. De ahí que, en el caso de España, necesitemos más tiempo para conseguir resultados. Y más, sobre todo, si se empiezan a aplicar las nuevas normas de la UE que complicarán, para bien, eso sí, el desarrollo de estas soluciones, lo que demandará nuevos profesionales capacitados para ello".

Añade Alberto Pascual que estamos viviendo un desarrollo de la IA en dos velocidades. "Por un lado", explica, "está China, que cuenta con grandes fuentes de datos internas que permiten el desarrollo acelerado de la IA. Además, son menos restrictivos en cuanto al uso de los datos. El resto de los países vamos a otra velocidad. Se han

> La información está ahí, pero **hay que sacar el valor de estos datos**
>
> Javier Grande, business solutions and transformation manager en **Arrow** ECS España

democratizado muchas herramientas automatizadas, pero lo importante es cómo se utilizan estas herramientas y vemos que hay falta de profesionales que aprovechen estas capacidades. De ahí la apuesta por agrupar el talento en torno a estos centros que comentaba anteriormente, para que el canal pueda aprovecharlo como servicio. Ahora mismo hay un déficit de profesionales capacitados, y será un reto a solucionar. Precisamente, llegan ahora los Fondos Europeos de Recuperación y la formación en entornos digitales es uno de sus ámbitos".

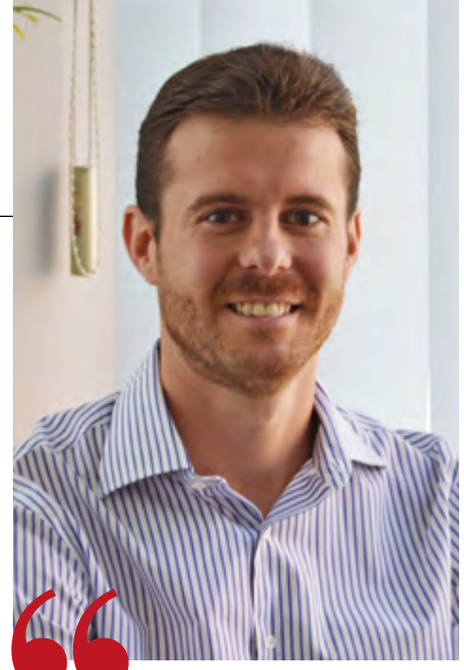
Para Javier Grande, "los números de IDC pueden ser acertados o no, dependiendo de lo que entendamos por soluciones de IA. Debido a la falta de conocimiento que hay en el mercado, los grandes fabricantes están democratizando la IA para que se consuma en el día a día. Vemos muchos ejemplos a diario, como las recomendaciones en los e-commerce o el auto-completado de frases cuando escribes. Son ejemplos de productos que incorporan IA embebida para facilitar su consumo. Si entendemos que proyectos de IA son los creados específicamente sobre la base de la inteligencia artificial, no creo que lleguemos a las cifras que comenta IDC, pero si unimos estas soluciones que incorporan la IA en los ejemplos anteriores, posiblemente superemos esos datos".

Asimismo, añade que "la IA es una realidad porque cada día tenemos más datos y más capacidad de computación, pero hay que intentar que las soluciones ofrezcan los resultados más éticos y claros posibles".

Según David Fernández, "cada día va a ser más difícil separar tecnología e Inteligencia Artificial porque cualquier desarrollo que se haga incluirá algo de IA. Es muy complicado acertar con las cifras, pero se estima que en diez o quince años la mayoría de las empresas van a estar utilizando alguna de las grandes soluciones de Inteligencia Artificial: visión artificial, asistentes virtuales… Esto es muy esperanzador, y también va a proporcionar a las empresas unos beneficios muy importantes".

SECTORES MÁS AVANZADOS

En estos meses hemos visto ejemplos de aplicación de IA en soluciones en el sector



"Todas las empresas quieren **conocer más y mejor a los clientes**, y necesitan el **dato como vehículo** para ello"

David Fernández, customer success director en **Inbenta** España

"Se han **democratizado muchas herramientas automatizadas**, pero lo importante es cómo se utilizan estas herramientas y vemos que hay **falta de profesionales** que aprovechen estas capacidades"

Alberto Pascual, director ejecutivo de **Ingram Micro** España

sanitario, que se unen a otros, como el Retail, el transporte… Así que quisimos saber qué sectores verticales pueden apostar por este tipo de tecnologías a corto plazo.

En palabras de Alberto Pascual, "hay que hacer dos consideraciones. Por un lado, las empresas deben mirar qué han hecho bien esos unicornios que han conseguido crecimientos exponenciales. Hay que extraer lecciones de cómo han empleado la tecnología y de cómo han aprovechado los datos para mejorar la atención a sus clientes, algo en lo que la IA juega un papel esencial. Y en esta línea veo un crecimiento rápido en un segmento como el Retail, que emplea la IA para ofrecer una experiencia de cliente idónea. Otro ejemplo es la seguridad física, donde la cámara IP ha dejado de ser un elemento para monitorizar lo que sucede, para pasar a ser un sensor que recoge datos que pueden ser analizados por herramientas de IA. Y este es un segmento muy interesante para el canal. El segundo vector a analizar es la lista de sectores que hemos visto que necesitan un mayor esfuerzo transformador, y ahí vemos otros dos, el sector sanitario, donde hay una gran oportunidad para mejorar la atención al paciente al liberar a los profesionales de tareas repetitivas; y la educación, donde hemos visto la diferencia entre la realidad de la sociedad digital y de sus infraestructuras, lo que abre otro espacio de oportunidad prioritaria. El resto, se irán incorporando paulatinamente".

En una línea similar se coloca David Fernández, que añade que "ambos sectores han quedado en evidencia por la excepcionalidad de la situación generada por la pandemia, que desbordó las infraestructuras y nos cambió a todos el paso. Estos sectores, Sanidad, Educación y Retail, se enfrentaron a un reto para el que no estaban preparados. Viéndolo con perspectiva, hemos conseguido pasarlo con nota, pero estos tres sectores tienen un gran recorrido por delante, porque han visto que la tecnología es clave para su supervivencia. Otros sectores, que tenía cubierta esta primera capa de tecnología, se han adaptado mejor".

Discrepa Moisés Martínez con ellos no porque estos sectores no necesiten estos desarrollos, sino porque se van a enfrentar a lo que se ha enfrentado otro segmento que lleva tiempo apostando por la IA, como es la Banca. Tal y como comenta, "la Banca se ha dado cuenta de que aplicar la IA por el mero hecho de aplicarla, no tiene ningún sentido e, incluso, puede suponer un problema, porque estás sesgando a determinados usuarios. Por eso creo que el desarrollo de la IA será más rápido en segmentos donde su uso no tenga una implicación discriminatoria sobre los seres unamos. Un ejemplo puede ser el Retail, donde aplicar la IA será sencillo. También lo vemos en el sector Agrario, para automatizar determinadas tareas. Pero en sectores como la Medicina tardará más, como pasa con la Banca, por la falta de confianza en si la respuesta de la IA es la más ética y equitativa".

Añade Javier Grande que, primero, "hay que digitalizar esos sectores. Una vez que lo estén, y que tengas muchos datos recogidos, es cuando puedes aplicar algoritmos a esa información. En Banca y Sanidad, los tienes; en Agricultura, no los tienes, pero puedes obtenerlos con el uso de sensores".

Pero hay ejemplos que necesitan menos datos, apunta Moisés Martínez. "Hay áreas de desarrollo que empiezan a aplicarse ahora, y no necesitas grandes datos para ello".

En todo caso, responde Javier Grande, "sigues necesitando datos, ya sean más o sean menos. Pero quizá donde se va a utilizar más la IA es en el sector de la ciberseguridad, donde el uso de información compartida puede aportar una mayor respuesta a las amenazas. Vemos los beneficios de la IA sin ver realmente todo lo que ha por detrás".

Apunta Alberto Pascual que, efectivamente, "podríamos estar tentados de hacer en un sector como el sanitario lo mismo que se ha hecho en otros, como la Banca, crear

> "Uno de los **problemas** que tenemos en España **con la IA** es la **falta de profesionales** con la capacitación necesaria"
>
> Moisés Martínez, responsable de Inteligencia Artificial en **Paradigma Digital**

un entorno sandbox para poder experimentar sin riesgos. Pero en Sanidad ya se está haciendo, con aquellas personas que, voluntariamente aportan unos datos personales protegidos por las leyes, y que luego se benefician de los desarrollos obtenidos".

Sanidad es un ejemplo claro, para Moisés Martínez, de este riesgo de parón, "tanto por la legislación como por la reticencia a ceder determinados datos, mientras que en otros sectores será posible tener un acceso más sencillo a la información para ver evolucionar estas técnicas".

NUEVAS FIGURAS EN EL MERCADO...

¿Cuál debe ser el papel de partner en el desarrollo de esta área? En opinión de David Fernández, "en la realidad actual, hay empresas, como la nuestra, que aparecen creando un modelo disruptivo en el mercado, lo que fuerza a las empresas grandes a mantener la agilidad para seguir siendo relevantes. Nosotros tenemos la responsabilidad de seguir evolucionando la plataforma en dos líneas, rentabilidad y sostenibilidad".

Para Moisés Martínez, "hay una gran cantidad de tecnologías en las que aparecen startups muy pequeñas y ágiles y grandes empresas que pueden seguir evolucionando sus productos para conseguir una evolución del mercado que dé cabida a redes de empresas que trabajen para adaptar las soluciones a segmentos verticales o a modelos más disruptivos".

Se muestra de acuerdo Javier Grande, que añade que la tecnología está ahí y hay empresas "que deciden aplicarla de una manera que nadie ha hecho antes y consiguen crecer de manera exponencial. La clave está en la idea, en cómo monetizar la tecnología, y es donde diferenciarse es esencial. Lo básico es lo que haces con la tecnología y cómo la aplicas".

...Y NUEVOS ROLES PARA LAS TRADICIONALES

Aparecen nuevas figuras, pero se mantienen otras más tradicionales, como los mayoristas, Tal y como explica Alberto Pascual, "las startups han demostrado su capacidad innovadora, pero hay que ver cómo escalar estos modelos. Hablamos de verticalización, de especialización, de capilaridad, de personalización… algo que está en manos del canal TI, que es el que está cerca del cliente y lo conoce. Pero este canal va todavía lento con estas tecnologías, quizá porque le está yendo bien con otras tecnologías. Mientras tanto, los dinamizadores tenemos que ser nosotros que, por tamaño y escala, tenemos capacidad para invertir y favorecer el desarrollo de estas tecnologías. Y una forma es la creación de centros expertos para desarrollar y llevar estas soluciones al canal de una forma eficiente".

Para Javier Grande, "en los últimos años estamos viendo un cambio de paradigma entre la distribución clásica y un modelo en el que el cliente está en medio y el consumo se realiza como servicio. El mayorista tiene que aportar nuevas plataformas para facilitar al partner el go-to-market, inyectando nuevas formas de tecnología. En el caso de la IA, nosotros la incorporamos a nuestra plataforma, ArrowSphere, para ofrecer capacidades predictivas a los partner. Por otra parte, ayudamos a empresas que están creando sus propios algoritmos para dar una mejor respuesta a sus clientes exprimiendo los datos para aplicar valor".

"Aportar valor en una plataforma integradora es el camino adecuado", apunta David Fernández, que añade que "porque la solución concentra lo mejor de cada elemento. Además, nosotros ayudamos a las empresas a conocer mejor a sus clientes, porque los datos no sirven si no puedes aprovecharlos".

La clave, recalca Moisés Martínez, es "ofrecer soluciones que sean aplicables a empresas de cualquier sector. La gran ventaja de la IA es que se podrá aplicar de forma sencilla en todos los entornos, independientemente del nivel de digitalización de cada uno". ■

MÁS INFORMACIÓN

- Inteligencia y analítica de datos como oportunidad para el canal, a debate
- El 18% de las grandes empresas españolas apuesta por la inteligencia artificial

Data Intelligence

Ponemos los datos al servicio de la empresa, para obtener mejores resultados

arrow.com/ecs/es

GEORGE CHEN, DIRECTOR GENERAL DE NEWLINE EMEA

“El trabajo semipresencial es la tendencia que más se va a consolidar”

Según Future Source, Newline vendió 3.000 monitores interactivos en España en 2020, lo que le permitió hacerse con el 16% del mercado y ser el fabricante con mayor crecimiento del sector. Son varias las claves que explican tamaño rendimiento, pero todas giran en torno a las denominadas 3S: Seguridad, Servicio y Sencillez. Entrevistamos a George Chen, director general de Newline EMEA, que entre otras muchas cuestiones nos explica por qué este fabricante decidió situar en España su sede central en EMEA.

Pablo García Reales

¿Cuáles son las principales tendencias, según Newline, que se están produciendo en el ámbito de la colaboración empresarial y las comunicaciones unificadas en los sectores corporate y educativo?

En el ámbito empresarial vemos que cerca del 60% de los trabajadores desarrolla su tarea profesional parcial o completamente desde casa. El desafío de las corporaciones está en alcanzar el mayor grado de colaboración no solo en el cara a cara, sino también en condiciones remotas cumpliendo con el protocolo anti-COVID.

Si antes de la pandemia, centros educativos y empresas podían avanzar lentamente en su proceso de digitalización, sin prisa pero sin pausa, conteniendo la inversión en equipamiento

audiovisual, desde marzo de 2020, como sabemos, la situación giró 180º y obligó a la compra de herramientas como portátiles, monitores, headsets y micrófonos, etc. De la mano vino un cambio en la cultura del trabajo y de la enseñanza, descubriendo retos y oportunidades para los que el mercado debía estar preparado.

Es importante destacar que son muchos quienes creen que el equipamiento cámara + micrófonos ya responde a una solución unificada, pero lo cierto es que para que esa solución cumpla con las necesidades reales se deben incorporar datos. La fórmula quedaría así: audio, vídeo y datos = interacción real presencial y remota.

Según Future Source, Newline vendió 3.000 monitores interactivos en España en 2020, lo que supuso hacerse con el 16% del mercado y ser el fabricante con mayor crecimiento del sector. ¿Cuáles son las claves de este rendimiento?

Hay 4 pilares que justifican el crecimiento de Newline: en primer lugar, servicio in situ. Por otro lado, ofrecemos un equilibrio entre calidad, funcionalidad y precio. Con nuestra amplia gama de productos satisfacemos las diferentes necesidades de los clientes, tanto del sector empresarial como del educativo. En

tercer lugar, las formaciones (showroom en Madrid, formación en línea para los usuarios finales o nuestros distribuidores) que muestran el funcionamiento de los productos y su encaje como respuesta a las necesidades de los clientes. Y, por último, que cuidamos a nuestros partners ofreciéndoles apoyo y protegiéndolos en los proyectos.

¿Cómo ha tratado de adaptarse Newline tecnológicamente hablando al nuevo escenario que ha dibujado la pandemia?

Se puede explicar este tema en dos sentidos, por un lado en relación con nuestra estructura y por otro, con nuestro producto-servicio. Respecto al primero, la estructura, hemos incorporado Sales Force (Sistema CRM), Predictive Index (Sistema HR), Team/Zoom (videoconferencia), Fresh Desk (sistema del servicio posventa) y un portal de marca Newline, que es un espacio de marketing para que nuestros partners puedan acceder a información y material nuestros desde cualquier parte, aportando rapidez a los procesos de trabajo.

Respecto a nuestros productos, hemos introducido las gamas de producto MIRA y Newline Flex. La primera está compuesta por una pantalla interactiva de gran formato con 65-75-86 pulgadas que incorpora micrófonos y cámaras. Una solución todo en uno ideal para afrontar la nueva era del trabajo híbrido. La segunda, Newline Flex, está formada por un monitor táctil de 27 pulgadas, también con la cámara 4K y matriz de micrófonos. Cuenta con tecnología capacitiva y es compatible con Windows Ink, lo que la convierte en una solución única para el espacio de trabajo, sea cual sea y esté donde esté.

Tras la explosión del teletrabajo experimentada con motivo de la pandemia, ¿se mantendrá este modelo remoto o híbrido, o volveremos al trabajo eminentemente presencial?

Desde nuestro punto de vista, el trabajo semipresencial es la tendencia que más se va a consolidar. Si bien la modalidad presencial va a seguir ahí porque la colaboración y la conversación cara a cara

España, sede de Newline en EMEA

España, como sede de Newline EMEA, fue una apuesta personal de George Chen y su socio, Carlos Velasco. Cuando llegó el momento de elegir destino "valoramos cuestiones como el coste financiero del espacio de oficinas, el clima, el talento y la actitud de los empleados... España fue el país que mayor equilibrio presentaba entre productividad y gasto", reconoce el directivo.

Si bien las oficinas de la sede están en España, el almacén de sus productos para la región de EMEA se ubica en Holanda, dado que por su localización en el centro del continente le permite abastecer de forma ágil y eficaz a los países de la zona.

ENTREVISTA

> La mayoría de los **centros educativos**, según nuestra opinión, **no estaban preparados para las clases a distancia**. Pero la **tecnología está cada vez más ligada a la educación** y ofrece evidentes beneficios tanto a los estudiantes como a los docentes

es la más efectiva, cada vez será más habitual encontrar personas desarrollando sus tareas profesionales de manera remota. El resultado es una tendencia hacia el trabajo híbrido.

Creemos, además, que según aumente el número de vacunados, la colaboración presencial experimentará un repunte. Volverán los cara a cara en los negocios y, también en el ámbito académico donde el contacto con los compañeros y los profesores es quizás más importante que en el empresarial. En cualquier caso, la vuelta a la normalidad no supondrá, como avanzamos, una renuncia a la modalidad remota. Simplemente impulsará la semipresencialidad.

¿Qué están buscando los centros educativos a la hora de incorporar tecnología interactiva a las aulas?

En primer lugar, buscan una herramienta sencilla e intuitiva de utilizar. En segundo lugar, priorizan la garantía. Por último, el precio es un aspecto determinante a la hora de tomar la decisión de qué modelo interactivo adquirir. Cada vez se invierte más en la digitalización de las aulas, un proceso imparable que abarca a las aulas de todos los niveles educativos. La tecnología está cada vez más ligada a la educación y ofrece evidentes beneficios tanto a los estudiantes como a los docentes.

¿Estaban los centros educativos preparados para afrontar las clases en remoto? ¿Y las empresas?

La mayoría de los centros educativos, según nuestra observación, no estaban preparados para las clases a distancia. Mantener la atención de los alumnos nunca ha resultado sencillo y la enseñanza remota no facilita la tarea, pero creemos que las herramientas digitales se convierten en aliados y están impactando directamente en la forma de dar clase. La transformación digital que necesariamente están llevando a cabo los centros educativos

permite a los profesores aprovechar las ventajas que las nuevas tecnologías tienen para impulsar el aprendizaje de los estudiantes.

Por su parte, las empresas estaban mejor preparadas, sobre todas las empresas internacionales o mutiprovinciales. Muchas ya tienen más o menos instalados equipamientos de videoconferencia para trabajar remotamente.

¿Qué rol busca ocupar Newline en los ámbitos de negocio en los que está presente?

La impresión de Newline que queremos dar al sector y a los clientes del sector corporativo es: Seguridad, Servicio y Sencillez (3S). Somos conscientes de que el 90% de las empresas utiliza el sistema operativo Microsoft Windows o la suite Microsoft Office. Por esa razón, desarrollamos la gama de productos interactivos NAOS IP con tecnología capacitiva y un diseño sencillo y elegante. Lo característico de estas soluciones para empresas es que no interfieren con la seguridad gracias a la eliminación del sistema operativo Android.

Los empleados traen sus propios dispositivos (móviles o portátiles) y los conectan al monitor táctil de NEWLINE a través del código QR o código de acceso. Con estos sencillos pasos pueden compartir su presentación, datos, cálculos o diseños con los clientes o colegas a través del monitor, e interactuar con ellos. Con la oferta de producto NAOS IP o Newline FLEX, la seguridad está garantizada y cumple el concepto BYOD (bring your own device). Además, la garantía de la gama corporate de Newline es de 5 años.

¿Qué importancia le otorga Newline a la investigación y al desarrollo?

Sin duda es fundamental. Destinamos mucho tiempo y recursos a conocer las necesidades de los usuarios para, como fabricantes, esforzamos en darles respuesta. Nuestros productos buscan diferenciarse como herramientas interactivas capaces de maximizar la colaboración y la eficiencia en cualquier espacio de trabajo de la manera más sencilla posible. Newline cuenta con 4 centros de desarrollo, 625 ingenieros, y 418 patentes tecnológicas que dan muestra de nuestro compromiso con el I+D.

A través de nuestros distribuidores conseguimos entender qué quiere el usuario final, qué necesita y para qué pretende usar los productos Newline. Esta información se transmite a nuestros expertos del centro de investigación, dando como resultado una amplia gama de soluciones para empresas y centros educativos cuya calidad nos permite ganar presencia y cuota de mercado en EMEA.

¿Cuál es el modelo de ventas de Newline? ¿Qué importancia juega el canal de distribución?

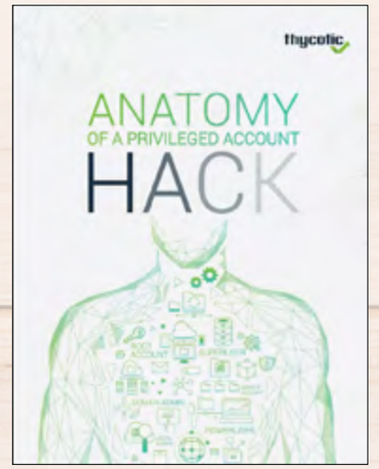
Newline trabaja con mayoristas, a través de quienes factura. Con el canal, es decir los distribuidores, fomentamos una relación de apoyo y formación continuada que busca ofrecerles las herramientas necesarias sobre el uso y las características de nuestra gama de productos. Cuidamos mucho la relación con los distribuidores porque somos conscientes de su papel como embajadores de la marca Newline. Les consideramos socios y como tal les brindamos el máximo apoyo para que crezcan y se posicionen en el mercado. Es un win win, si ellos ganan nosotros también. Newline EMEA tiene delegaciones en cada país en el que está presente. Allí los empleados dan soporte local para asegurar la mejor dinámica de trabajo y relación con el canal. El objetivo es claro: la mejor calidad en la atención y en los productos. ■

MÁS INFORMACIÓN

- Newline es premiada por la calidad de diseño de su monitor Newline Flex
- Newline se hace con el 16% del mercado de monitores interactivos en España
- Newline apoya la transformación del espacio de trabajo con Flex

La documentación TIC, a un solo clic

Anatomía del ataque a una cuenta privilegiada



Este documento técnico realizado por Thycotic describe un ataque a una cuenta privilegiada; explica cómo los atacantes externos o los internos malintencionados pueden explotar las vulnerabilidades utilizando ejemplos como la contraseña de una cuenta de correo electrónico comprometida que se convierte en una violación total de la seguridad de la red.

7 consejos para proteger los datos de tu empresa y vencer al ransomware

La pérdida de datos no es una broma. Los ataques de ransomware y malware van en aumento, pero ése no es el único riesgo. Con demasiada frecuencia, las empresas piensan que sus datos están bien respaldados, pero en realidad no lo están. Este documento de Commvault muestra siete razones comunes por las que las empresas pierden datos, a menudo porque nunca estuvieron realmente protegidos, junto con consejos para ayudarte a evitar que te ocurra lo mismo.

Cloud Migration: Apuesta por el futuro de tu organización en la nube

En tiempos de incertidumbre, la migración a cloud supone una ventaja organizacional al obtener una mayor funcionalidad, escalabilidad y flexibilidad, además de accesibilidad en cualquier momento y lugar. Este documento de Making Science recoge las principales ventajas de la migración a la nube, ejemplos de migración y las capacidades que ofrece Google Cloud a las organizaciones.

Guía para implementar una CDN moderna

Este documento de Fastly señala la evolución de la relación de los desarrolladores con la CDN (Red de Distribución de Contenidos) y explica por qué las CDNs tradicionales están obsoletas. El texto también detalla los beneficios que pueden aportar las CDNs modernas, que van desde una mejor visibilidad de los patrones de tráfico hasta el diseño de APIs que potencian una experiencia de usuario personalizada.

¿Qué me aporta una herramienta RMM?

Las soluciones RMM (Remote Monitoring and Management) ofrecen supervisión y gestión a distancia, es decir, gestión TI de manera remota. Estas tecnologías están diseñadas para ayudar a los proveedores de servicios gestionados (MSP) o a los administradores de TI a supervisar, de manera remota, dispositivos de TI, una supervisión que incluye el mantenimiento proactivo para mejorar la fiabilidad y la productividad en entornos TIC.

Las tecnologías RMM incluyen funcionalidades básicas para cualquier empresa, tales como configuración de ordenadores, gestión de acceso remoto, copia de seguridad y recuperación a distancia, gestión de implementación de parches,

Las soluciones de gestión y monitorización remota (RMM, por su denominación en inglés, Remote Monitoring and Management) son una opción muy interesante para que cualquier reseller las incluya en la oferta tecnológica a los clientes. Descubre en estas líneas cuáles son sus principales ventajas.

Las **soluciones RMM**, Remote Monitoring and Management, ofrecen **supervisión y gestión a distancia**, es decir, **gestión TI de manera remota**

actualización y mantenimiento de soluciones de seguridad, o control de riesgos ante filtraciones de datos, entre otras, lo que capacita a un reseller para ofrecer toda una gama de servicios en remoto a sus clientes sin que por ello se incremente de manera proporcional su necesidad de personal especializado, o, en otras palabras, se incrementen sus costes.

Con una solución RMM, un reseller podrá gestionar, asegurar y mantener el entorno TI de sus clientes, estén estos donde estén y con el nivel de dispersión que tengan en sus infraestructuras TI, lo que favorece la flexibilidad y la productividad de las empresas.

Los resellers pueden hacerse cargo también de tareas rutinarias de mantenimiento durante el tiempo de inactividad de los usuarios, reduciendo al mínimo las interrupciones, sin que para ello sea necesario el desplazamiento de su personal técnico, y pudiendo gestionar, en paralelo, a múltiples clientes desde una única ubicación central. Además, la gestión remota de la seguridad de sus clientes por parte del reseller permite a las empresas centrarse en su negocio sin necesidad de contar con personal con las capacidades necesarias para afrontar los retos de seguridad y gestión imprescindibles, sobre todo en un momento en que se incrementan mucho los entornos de TI dispersos en las empresas.

Asimismo, la creciente proliferación de dispositivos más allá del PC, hace muy valiosa la administración remota por parte de los resellers, lo que permite a sus clientes mantener todos estos dispositivos en funcionamiento, e incrementa su productividad.

N-ABLE RMM

Una de estas soluciones RMM de las que el reseller puede obtener valor para su negocio y sus clientes es N-Able RMM. Se trata de una solución que permite administrar, supervisar y asegurar la red desde una consola basada en web unificada. Esta herramienta RMM proporciona una oferta completa de servicios para asegurar, mantener y mejorar de manera eficiente las TI desde un solo panel, sin necesidad de que los clientes tengan que instalar aplicaciones on-premise. ■

MÁS INFORMACIÓN

- Diez cosas que debe buscar en una solución RMM

NO SOLO it

PANEL DE EXPERTOS

TECNOLOGÍA Y NEGOCIO

Verdades y falacias del estado real de la digitalización empresarial y transformación digital en España

Jorge Díaz-Cardiel,
Socio director general de
Advice Strategic Consultants

ENCUENTROS Y DESENCUENTROS CON LA COMUNICACIÓN

Los seis sombreros en la comunicación

Manuel López,
Asesor de comunicación

REFLEXIONES éTICas

Un café con el Homo Virtualis

Màrius Albert Gómez
Experto en digitalización
e Innovación y humanista
por convicción

CIBERSEGURIDAD 4.0

El Amanecer de la Humanidad Digital

Mario Velarde Bleichner,
Gurú en CiberSeguridad

MARKETING Y CONSUMO

Neurociencia y medios de pago

José Manuel Navarro,
CMO MOMO Group

NO SOLO it Tecnología y negocio

Verdades y falacias del estado real de la digitalización empresarial y transformación digital en España

Jorge Díaz-Cardiel

Socio director general de Advice Strategic Consultants

Economista, sociólogo, abogado, historiador, filósofo y periodista. Autor de más de veinte mil de artículos de economía y relaciones internacionales, ha publicado más de una veintena de libros, cinco sobre Digitalización. Ha sido director de Intel, Ipsos Public Affairs, Porter Novelli International, Brodeur Worldwide y Shandwick Consultants.

"La digitalización ha avanzado en los últimos meses 4, 6 o 10 años en España durante la pandemia", afirmaba un ejecutivo de CEPYME, patronal de las pymes españolas, en la presentación de la cuarta edición del Observatorio de la Empresa de Vodafone, mediante encuesta personal a 3.500 personas en el último cuatrimestre de 2020. El universo de análisis (y sus muestras correspondientes) fue el de grandes empresas, pymes, autónomos y administraciones públicas.

Las conclusiones de la encuesta no podían ser más positivas… para quienes han hecho el estudio, aunque obviaran al resto del sector tecnológico o se refirieran a él en genérico arrogándose el mérito de lo que han hecho otros: "hemos hecho un gran esfuerzo en el despliegue de redes, de fibra". Cierto, pero lo ha hecho Telefónica, Orange...

En ninguna ocasión en la presentación del estudio se habló de la crisis económica, sa-

nitaria y social que vive España, ni que tenemos una tasa de paro del 16,1% (versus el 6% de Estados Unidos) o que el PIB cayó en 2020 un 11% y la renta per cápita un 11,6%. Es como si alguien hubiera dicho que "ya está bien de penas, vamos a contar un mensaje optimista". El problema de un análisis hecho desde premisas que no son reales es que las conclusiones del estudio acaban siendo igualmente sesgadas. Es como aquello de "tienes muchas razones, pero no tienes razón". O cuando alguien escribe un libro de historia conocida por todos y orienta sus datos para obtener una conclusión premeditada: "todos los datos que cita son ciertos, pero la historia no es verdad".

Al decir de un directivo de Google y una directiva que representa en España al MIT Harvard Review, España es un paraíso de la digitalización. Desde su punto de vista esa utopía es cierta porque, para ellos, el teletrabajo es lo normal ("su normalidad", ignorando que "su" realidad no es la de todos los trabajadores de España. Un buen análisis sociodemográfico y socioeconómico empezaría por reconocer que España tiene 11 millones de personas mayores que, en su gran mayoría, están alejados de la transformación digital. O que en España hay cuatro millones de parados y más de medio millón en ERTE, cuya prioridad tampoco es la digitalización. Y que si los 19 millones de asalariados tuviesen todos un "smartphone", tampoco eso equivaldría a una mayor digitalización de la fuerza laboral. Pero algunos, torticeramente, lo equiparan.

Sí, en Google trabajan con ordenador y utilizan herramientas colaborativas como Zoom y Teams, pero ellos son una minoría comparada con toda la fuerza laboral del país. Supongo que es lógico que quieran vender las bondades del producto que ofrecen, como el vendedor de manzanas dice que sus manzanas son las mejores del mundo, aunque no tenga por qué ser necesariamente cierto.

Según el estudio, la crisis económica no ha afectado a los proyectos de digitalización en marcha en ninguno de los segmentos de mercado empresarial analizados. Es más, según dicen, en administraciones públicas y en microempresas han aumentado. Las pymes afirman disponer de un presupuesto "del 60% para digitalización", como si les sobrara el dinero.

Los datos del Instituto Nacional de Estadística que hace públicos ONTSI-Red. es sobre la penetración de las TIC y la digitalización en las empresas son de todo el ejercicio 2019, por tanto, antes de la pandemia. Luego no admiten comparación con el cuarto trimestre de 2020, cuando se hizo esta encuesta y, desgraciadamente, se produjo la mayor caída del PIB español y el menor gasto en tecnología por parte de las empresas, excepto en la compra de ordenadores, como anticipamos en IT User, con datos reales, en noviembre pasado.

Pero, ni siquiera el INE, cuyo rigor estadístico está fuera de toda duda, se atreve a afirmar que las pymes españolas (que en 2020 hay tenido una única misión: la supervivencia) destinen 60% de presupuesto a proyectos digitales. Simplemente, no es creíble.

Como tampoco lo es la vieja táctica de poner un ejemplo concreto como exponente de un fenómeno generalizado: una anciana que pide a su nieta le ayude a bajarse la app de la Seguridad Social (¿los once millones de

ancianos españoles han hecho eso mismo?); los hijos de una directiva de redes de la operadora "que han tenido formación online durante la pandemia, como antes, pero frente al ordenador" (¿es el caso de todos los niños de España? No. La escuela pública, 14 meses después, aún está en mantilla, según datos del ministerio que dirige la ministra Celaá y la educación privada y la concertada tardaron una media de seis meses en "ponerse las pilas" y 12 en completar el proceso de digitalización: when on earth are you coming from, you people?); "una escuela de negocios que pasa al online a la mitad de los chavales que no lo estaban" (la mayor parte de las escuelas de negocios del mundo tardaron mucho tiempo en acomodarse porque, precisamente, "la gracia" de Harvard, Stanford o Yale es el prestigio del profesorado y no la conexión a Internet y, por eso y no por otro motivo, se resistieron al cambio, pero no porque no tuviesen medios económicos o tecnológicos).

Y poner un ejemplo del campo y otro de la industria para ilustrar, con condescendencia, que también esos sectores se digitalizan…; por Dios, el INE y Eurostat niegan la mayor.

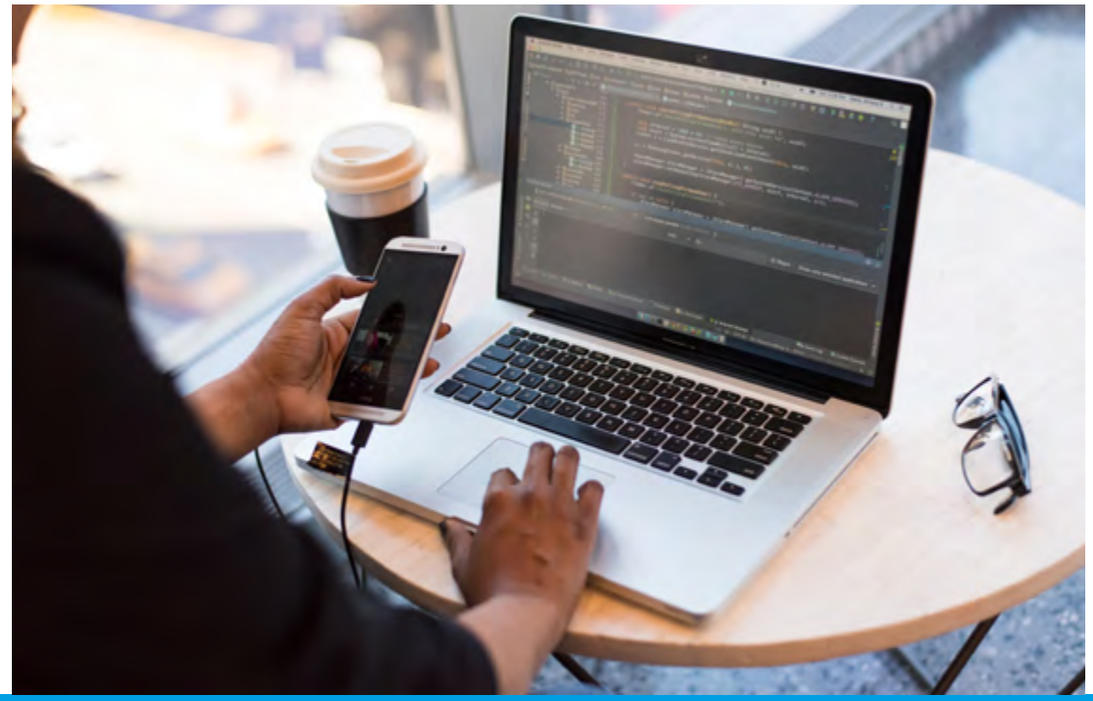
Pintar un escenario en que, en España, reina 5G, el teletrabajo, la inteligencia artificial, big data, Internet de las Cosas, Cloud Computing, centralita virtual y 24 horas como herramientas de digitalización que ya están ampliamente extendidas es una falacia, o no, y todos vivimos en 1) Matrix, 2) Charlie y la fábrica de chocolate con Johnny Depp.

Lo que sí es verdad es que de 19 millones de cotizantes a la Seguridad Social, 400.000 trabajan en el sector tecnológico (TIC, Telecomunicaciones, Contenidos, Digital) y, esos sí, viven en una burbuja digital: la suya, pero que no es la de todos los asalariados ni de los 3,4 millones de autónomos (54% de los cuales son autónomos sin asalariados, según datos de la Seguridad Social de marzo de 2021).

¿Hay que recordar a los autores del estudio que la economía más digitalizada del mundo, la norteamericana, lo está en un 30% de su PIB, ergo le falta el restante 70%? Si eso es así en la única economía que mide el impacto de la digitalización en su PIB desde 2013 a día de hoy y con carácter retroactivo desde 1939 hasta hoy… ¿qué porcentaje del PIB español es digital? Los autores del estudio no lo dijeron (no lo saben). Y, si ellos no lo dijeron, yo tampoco se lo diré, aunque sí lo sé, que no en vano he publicado cinco libros sobre digitalización, realizado 600 informes y estudios y más de 730 proyectos de consultoría en digitalización.

Hay extensa literatura reciente de 2016 al primer trimestre de 2021 que explica pormenorizadamente el estado real de la transformación digital en los países más ricos del mundo, que pertenecen a la OCDE. Y hay cientos de estudios bien hechos, como los realizados por los premios nobeles de economía Robert Solow, Michael Spence y Paul Romer, que se reirían si leyeran este estudio. O Klaus Schwab, fundador del World Economic Forum, orientado a la transformación digital en los últimos cinco años, autor de dos libros sobre la Cuarta Revolución Industrial y de cientos de estudios sobre digitalización. ¿Qué le cuesta a la gente formarse un poquito, estudiar? Si algo (entre otras muchas cosas) logró Juan Soto Serrano (primer presidente de Hewlett-Packard) en España es que "los trabaja-

La realidad de la digitalización en España es un "work in progress", con datos objetivos y reales



dores de HP no fueran vendedores de coches de segunda mano". Y la misma política de elevación han seguido Helena Herrero en HP y José María de la Torres en HPE.

Decir que estamos digitalizados, al mismo tiempo que nuestro Producto Interior Bruto cae un 11% y la tasa de paro real es del 20% (Datos EPA, 16,1% + empleados en ERTE, 4% de la fuerza laboral) es como decir que tenemos autopistas maravillosas, las mejores del mundo…, pero ignoramos que están todas en quiebra, porque nadie las utiliza. Esto último tampoco es una opinión, sino un dato.

¿Saben cuál es la realidad? Que España ha avanzado en digitalización, sí, especialmente entre las grandes empresas y el sector público, aunque ambos sectores luchan por sobrevivir, las primeras por su elevada deuda corporativa (que no tienen Big Tech en EEUU: Google, Amazon, Apple, Microsoft, Facebook) y por la falta de demanda; el Estado se nutre de impuestos y, un concepto que ignoran los autores del estudio, "la presión fiscal en España es del 43%". Y nuestra deuda pública supera el 122% sobre el PIB. Cruzando ambos datos, la resultante es que muy difícilmente es sostenible el sistema actual de AAPP en España, porque no genera, sino que recibe. Y recibe del sector privado, del cual sabemos que el Turismo ha perdido 81.000 millones de euros; el Retail y la Distribución no alimentaria está en crisis, junto a HORECA, que tiene medio millón de pymes al borde de la quiebra y 1 millón de trabajadores en ERTE. Para las cadenas hoteleras es aún peor, pues no dejan de cerrar hoteles y despedir empleados, con 800.000 trabajadores en ERTE. La industria… ¿qué industria? Cuando no cierra Abengoa lo hace Alcoa y ojo a Duro Felguera… ¿ilustran estos ejemplos la situación de la industria? Sí, cito a FUNCAS (20 servicios de estudios económicos):

"La caída más intensa del PIB se observó, como cabía esperar, en los sectores más afectados por las restricciones impuestas para controlar la extensión de la pandemia, es decir, en las ramas de comercio, transporte y hostelería, cuyo VAB descendió un 40,4%, y en actividades artísticas, recreativas y culturales, con una caída del 33,9%.

La contracción de la actividad ha sido una de las más acusadas de Europa. El resultado se debe, en parte, al peso del turismo y de otros servicios especialmente afectados por la pandemia. Estos sectores representan el 28% del PIB, más que el total de la industria, la construcción y el sector primario".

Nuestro objetivo no es sacar los colores a nadie, sino decir la realidad de la digitalización en España, que es un "work in progress", con datos objetivos y reales. La pandemia ha cambiado las prioridades de las empresas, especialmente de la mayoría: el 99,88% de pymes españolas, cuya prioridad no es digitalizarse, sino sobrevivir, debido a los cierres, confinamientos y falta de demanda. ¿Tan difícil es de entender? Los fondos de reconstrucción europeos, cuando lleguen, podrán ayudar a levantar la economía española y, cuando esto suceda, podremos hablar del cambio de nuestro modelo productivo hacia la economía del conocimiento.

Y, entonces, como Estados Unidos ahora, podremos hablar de que la digitalización es la fuerza motriz del crecimiento económico, el empleo y la digitalización.

Hasta que llegue ese momento, por favor, seriedad intelectual, trabajo esforzado, rigor en las fuentes y trabajar para mejorar España y el nivel de vida de los españoles, también con la digitalización, pero no como un valor absoluto, sino como un componente motriz más de la generación de riqueza en España. ■

MÁS INFORMACIÓN

- España en la era post-COVID: TI para transformar el negocio
- Producto Interior Bruto español en el primer trimestre de 2021
- Previsiones sobre la economía española y mundial
- IT Trends 2021. Asimilando la aceleración digital
- Previsión del PIB en España para 2021 y 2022
- Funcas: previsiones para la economía española para 2021 y 2022

NO SOLO it Encuentros y desencuentros con la Comunicación

Se intuye el final del túnel de la pandemia, ¿y ahora qué?

Los seis sombreros en la comunicación

Manuel López

Asesor de Comunicación

Madrileño de nacimiento, horchano de adopción, informático de profesión, con más de 35 años de experiencia en el sector de TI, ha desarrollado la mayor parte de su carrera profesional en Hewlett-Packard, donde ocupó cargos de responsabilidad en diferentes áreas como consultoría, desarrollo de negocio, marketing, comunicación corporativa o PR. Actualmente dedica la mayor parte de su tiempo a asesorar a starups en temas relativos a la comunicación, desde su posición de partner en la plataforma de profesionales goXnext.

Parece que por fin estamos viendo un poco de luz al final del túnel o al menos vemos unas pequeñas luces que nos indican el camino de salida. Incluso podemos distinguir a lo lejos gente que está ya cerca de la luz.

Después de mucho tiempo en las tinieblas y con pocas ganas de mirar atrás (está muy oscuro), llega el momento de pensar en que pronto podremos estar en una situación similar a la de la prepandemia, en la que debemos olvidarnos de los malos tiempos y mirar al futuro con ilusión y con la convicción de que la situación económica repuntará.

Pensando en cómo deberíamos afrontar esta situación desde el punto de vista de la comunicación, me vino a la cabeza una teoría de hace muchos años (queda un poco extraño decir que es del "siglo pasado") que yo descubrí en el libro del gran escritor y psicólogo Edward de Bono, "El pensamiento creativo". La teoría se llama "Los seis sombreros para pensar". Yo la he utilizado en múltiples ocasiones en mi vida profesional y aunque está orientada para desarrollar un pensamiento creativo, creo que es muy adecuada para reflexionar sobre lo que se nos viene encima desde el punto de vista de la comunicación en el mundo post-COVID.

Dice Edward en su libro que "el método de los seis sombreros es extremadamente simple, pero esa simplicidad resulta poderosa". Yo creo que la simplicidad y la comunicación forman la mejor pareja para afrontar la crisis que nos amenaza en el mundo post-COVID.

Voy a describir brevemente el método y después lo utilizaremos como ayuda para la situación actual. Obviamente, buscamos como usar este método para tener un "Encuentro con la Comunicación", siguiendo con el leitmotiv de esta serie de artículos que bajo el paraguas de "Encuentros y Desencuentros con la Comunicación" llevo ya tiempo publicando en este medio.

El método básicamente describe como afrontar problemas e indica la función a

ejecutar en función del color del sombrero que nos pongamos.

Sombrero blanco: Datos e información. Objetividad. Analizar hechos, cifras e información de forma lo más neutral posible.

Sombrero rojo: Emoción sentimiento y pasión. Analizar la situación desde la intuición, buscar el aspecto emocional sin necesidad de justificarlo.

Sombrero negro: Miedo, pesimismo y negatividad. Actuar como "abogado del diablo", juzgar con opinión crítica, explicar por qué no va a funcionar algo.

Sombrero amarillo: Sueños, optimismo e ilusión. Enfocarse en el optimismo, en por qué va a salir bien, enfoque constructivo, buscando la oportunidad.

Sombrero verde: Ideas, imaginación y creatividad.

Buscar el punto de vista original, diferencial, provocativo incluso.

Sombrero azul: Gestión, control y visión panorámica. Organizar, sacar conclusiones y planes de acción.

Normalmente es una metodología pensada para el trabajo en equipo, pero también es útil para el trabajo individual de creación de soluciones. Cuando afrontamos un problema es importante que nos pongamos todos los sombreros y que nos cambiemos de sombrero a lo largo del proceso.

Bien, pues pongámonos los distintos sombreros para describir un punto de vista singular acerca de lo que se supone que nos vamos a encontrar al final del túnel. Salgamos del túnel con cada uno de los sombreros puestos y describamos la visión.

Si nos ponemos el sombrero blanco, tenemos una situación difícil. Los datos económicos no son nada positivos y parece que encontraremos dificultades para recuperar la economía. Da la impresión de que fuera del túnel hay tormenta y nos vamos a mojar. También es cierto que la llegada de fondos europeos de recuperación, abren la puerta al desarrollo de la economía en un horizonte próximo.

Si nos ponemos el sombrero rojo, llevamos más de un año de contención, de desesperación, incluso, y tenemos unas ganas tremendas de trabajar, de aportar y de desarrollar nuestro negocio. Con el sombrero rojo no nos importa la lluvia, ni mojarnos al salir, queremos salir y comernos el mundo.

Con el sombreo negro puesto, parece que no es buena idea salir del túnel, donde bajo un ERTE o similar se está más o menos calentito y no parece lo mejor salir, mojarse y quizá hasta pillar un catarro.

Si nos ponemos el sombrero amarillo, solo nos concentraremos en la luz, en las tremendas oportunidades que nos esperan ahí fuera, con un mercado ansioso por consumir nuestros productos y servicios y con cierta capacidad adquisitiva que no ha sido posible emplear durante la pandemia.

Siguiendo con la luz, nos ponemos el sombrero verde y lo que empieza a bullir en nuestra cabeza son nuevas formas de comunicar, nuevos clientes objetivo, ideas para conseguir un rápido crecimiento y ganar cuota de mercado. Y por qué no, ¿qué tal si vendemos paraguas para la lluvia?

Por último, nos ponemos el sombrero azul y evaluamos las posibilidades que tenemos de ejecutar las ideas, de soportar el crecimiento, de gestionar los recursos necesarios para conseguir el éxito.

Así pues, y volviendo al principio, el final del túnel parece que está al alcance de nuestra mano, las oportunidades están afuera, esperándonos, pero antes de salir y exponernos a la tormenta, pongámonos los sombreros y salgamos lo más protegidos posible.

Y en esto es en lo que estamos: Encuentros con la comunicación, para evitar desencuentros y frustraciones con la comunicación. ■

La simplicidad y la comunicación forman la mejor pareja para afrontar la crisis que nos amenaza en el mundo post-COVID

MÁS INFORMACIÓN

Ser creativo: Seis sombreros para pensar

NO SOLO it Reflexiones éTICas

Un café con el Homo Virtualis

Màrius Albert Gómez

Experto en digitalización e Innovación y humanista por convicción

Marius Gómez en su columna éTICa, sintetiza la voluntad de compartir unas reflexiones que nos ayuden a entender un mundo digital caracterizado con esos grandes "trending topics" actuales como son el Big Data, la Inteligencia Artificial, la IOT o la computación en general, y que son vistos desde un marco de consideraciones éticas, humanistas y sociales. Dichas reflexiones se realizan desde la actitud y el desempeño multidisciplinar, tanto individual como empresarial, y tienen el objeto de contribuir a "aportar un pequeño granito de arena en el proceso de repensar el papel que las TIC deben jugar en la vida de nuestros hijos, en su formación, en su trabajo, en su día a día... con un punto de vista que supere el meramente tecnológico".

Reflexionaba recientemente de la mano de L. Floridi, en cuanto a la evolución social y humana respecto las TIC, con un planteamiento que establece tres grandes fases: la prehistoria, la historia y la hiperhistoria. En la prehistoria no hay TIC. En la historia hay TIC, simplificadamente caracterizada por sistemas de información que gestionan y procesan datos. En la hiperhistoria hay TIC que gestiona y procesa datos de forma cada vez más ubicua, automatizada, autónoma e inteligente, estableciendo en el día a día de las personas, una dependencia inherentemente tecnológica en su relación social y laboral. Y es que realmente parece que vamos progresivamente a una realidad que cada día más se conforma como una suma combinada e indistinguible de realidad física y virtual. Es más, seguramente la componente virtual ya podría ser dominante en muchos casos por su facilidad y rapidez de "consumo", aventajando un proceso reflexivo mucho más "lento", de mayor transcendencia y producción intelectual.

Y es que, dentro de la red, en la infoesfera virtual, la tecnología no contiene ética ni inteligencia en sí misma, la adopta de nosotros. Construimos sistemas automatizados de decisión, redes sociales, apps móviles, bots, sistemas biométricos, integramos en IOT nuestro día a día, híper conectamos sistemas... y en ellos volcamos cada día más una parte que nos define, de nuestro conocimiento, de nuestras relaciones, de nuestro aprendizaje. Fácilmente, espontáneamente, sin cuestionarnos nada. Pero ¿ocurre lo mismo con nuestros valores éticos? Nadie se debería extrañar si en unos años un artículo rompedor nos estremece con el titular "¿dónde o cuándo perdimos parte de nuestra humanidad en la red?". Está claro que la digitalización nos ofrece muchas oportunidades como sociedad: eficiencia, sostenibilidad, resiliencia, equidad, nuevos modelos productivos... pero siempre y cuando el talento

Reflexionemos por un modelo inherentemente definido por talento digital sí, en un mundo virtual y físico muy imbricados sí, pero también diseñado por talento ético organizativo y social

que "consume" las TIC y que "produce" con las TIC, lo haga desde una vertiente mucho más humana, ética e intelectualmente comprometida para que forme parte del proceso de transformación digital.

Necesitamos en estos momentos y para los nuevos retos de digitalización mucho talento, sí, y más aún si cabe en el contexto de los nuevos fondos de recuperación, transformación y resiliencia. Sí, necesitamos talento STEM, ingenieros, científicos y matemáticos y nuevas fórmulas de colaboración conjunta entre todos los actores (sector público, privado, universidades…). Pero necesitamos también invertir en capacitación ética y humanidades, filosofía y cultura. Necesitamos más capacidades Homo en la constitución del Homo Virtualis. Si cogemos perspectiva y pensamos en la transformación del sector productivo que pretendemos, ¡reflexionemos un instante sobre el modelo social y económico que queremos! Reflexionemos por un modelo inherentemente definido por talento digital sí, en un mundo virtual y físico muy imbricados sí, pero también diseñado por talento ético organizativo y social.

Daniel Kahneman, autor americano-israelí y premio Nobel, analizando los procesos de toma de decisiones en situaciones de alta incertidumbre, donde tanto los beneficios como las pérdidas son inciertas, nos aporta un nuevo punto de vista basado en lo que se denomina ya la teoría de las perspectivas. Según esta teoría, en dichos momentos de alta incertidumbre nos alejamos de la racionalidad a la hora de tomar decisiones y tomamos lo que se denomina atajos heurísticos. Uno de los criterios de los atajos heurísticos, por ejemplo, es la aversión a la pérdida, aunque, en el fondo, todos estos atajos podríamos entenderlos bajo una perspectiva de que al final nos domina la parte intuitiva, lo simplificamos a lo binario, sin considerar alternativas. En este sentido, por tanto, resulta fundamental afrontar una reingeniería de nuestras propias ideas reconociendo tal carencia, rechazando la facilidad de adoptar en muchos casos los atajos heurísticos, y promoviendo nuevas decisiones y soluciones que nos ayuden con el reto digital. Debemos dotarnos de unas herramientas y un talento holístico que nos permita visualizar y definir una transformación digital, con optimismo ético y digital.

El café siempre ha sido una piedra angular de la cultura social y empresarial, de su bienestar, de la reflexión, de la relación con nuestros colaboradores, de establecer nuevas relaciones, de la escucha activa de nuevos puntos de vista… Quizá necesitemos unas buenas dosis de café con el Homo Virtualis en los nuevos puestos de trabajo híbridos del futuro para poder crear una hiperhistoria digital y virtual, ética, e intrínsicamente humana por definición en sus valores. ■

MÁS INFORMACIÓN

- The Onlife Manifesto - Being Human in a Hyperconnected Era, L. Floridi
- ¿Por qué decides lo que decides? Así afectan los sesgos cognitivos a nuestro pensamiento racional

it Digital Security

Todo lo que necesitas saber de Ciberseguridad está a un clic

Una propuesta informativa compuesta por una publicación digital, una página web para profesionales de la seguridad, así como Dialogos ITDS, Webinars o desayunos de trabajo con los principales referentes del sector.... ¡¡¡Y no te pierdas nuestras entrevistas!!!

NO SOLO it Ciberseguridad 4.0

El Amanecer de la Humanidad Digital

Mario Velarde Bleichner

Gurú en CiberSeguridad

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

Estamos viviendo el amanecer de la Humanidad Digital, pero no quiere esto decir que los seres humanos estén sufriendo mutaciones que los estén convirtiendo en individuos diferentes a los que han vivido en previamente al advenimiento de la nueva Humanidad Digital.

Este amanecer es más bien fruto del trabajo y esfuerzo de todas las generaciones anteriores que han ido evolucionando desde sus primeros individuos, que, al adquirir conciencia de sí mismos, han iniciado un camino que nos ha traído hasta este maravilloso momento en el que vislumbramos los primeros rayos del nuevo sol de la Digitalización como catalizador de avances en la evolución humana que trascienden de los puros logros materiales que traen estas tecnologías.

Veremos, por ejemplo, como, por primera vez desde la aparición del lenguaje, toda la humanidad se podrá comunicar en un único lenguaje digital; esto no quiere decir que perdamos nuestros idiomas nativos, que ganaran todos en hacerse universales. Cada persona comunicará en su idioma y cada persona recibirá esa comunicación en su propio lenguaje nativo mediante dispositivos digitales que realizaran la traducción instantáneamente con el apoyo de la Inteligencia Artificial que realizará un trabajo impecable.

La nueva Humanidad Digital podrá por fin superar por fin el mito de la Torre de Babel y la confusión de los pueblos con idiomas distintos que tanto daño ha hecho hasta ahora dividiendo y enfrentando a la humanidad.

Podemos pensar, sin pecar de un optimismo exagerado, que el hecho de que toda la humanidad se pueda ya comunicar libremente sin la limitación idiomática mejore el entendimiento entre los pue-

blos y, siendo optimistas, nos permita dar los primeros pasos hacia una única Humanidad Digital Global nueva que evolucione a partir esa premisa.

Hay agoreros que dirán que esta tecnología digital eliminará miles o tal vez millones de puestos de trabajo de traductores, cuando en realidad lo que hará será dar a todos los seres humanos la libertad de comunicarse con cualquier otro ser humano, que ahora es un privilegio reservado a las elites que disfrutan de "esclavos" humanos que traducen sus muy importantes comunicaciones. En fin, cambiará el paradigma de la comunicación humana en un sentido que jamás habíamos imaginado.

Veremos, por ejemplo, un gran salto en la sanidad y, aun cuando los avances en la curación de enfermedades malditas como el cáncer irán mucho más rápido con la utilización de las tecnologías digitales, el gran avance de la Humanidad Digital estará en la Medicina Preventiva, que podrá ser realmente Universal con la llegada de dispositivos digitales de bajo coste que hagan un seguimiento continuo de parámetros médicos a todos los humanos digitales del futuro. Esta inmensa cantidad de datos, analizada por nuevos y mejores algoritmos de Inteligencia Artificial permitirán conocer y hacer previsiones del estado de salud de toda la población del planeta sin perder de vista la situación sanitaria de cada individuo de esta nueva Humanidad Digital.

¿Cómo podemos ser tan optimistas cuando en la actualidad tantos niños mueren todos los días de desnutrición o de enfermedades comunes? Porque en un futuro no muy lejano las Tecnologías Digitales de micro y nano sensores unidos a los avances de las comunicación digital inalámbrica llegarán, sin duda, a una plataforma capaz de cubrir todos los puntos del planeta con un ancho de banda inimaginable capaz de proveer a todos los habitantes de Medicina Preventiva apoyada por sistemas de Inteligencia Artificial que puedan atender a cada individuo y, al mismo tiempo, evaluar continuamente el estado sanitario de todas las poblaciones del planeta e, incluso, tener una visión clara del estado sanitario de todo el planeta como una unidad.

Solo estos dos rayos de luz en el amanecer de la Humanidad Digital, lenguaje de comunicación universal y sanidad preventiva universal, son suficientes para

El gran avance de la Humanidad Digital estará en la Medicina Preventiva, que podrá ser realmente Universal con la llegada de dispositivos digitales de bajo coste que hagan un seguimiento continuo de parámetros médicos a todos los humanos digitales del futuro

tener la esperanza en una evolución exponencial de la especie humana. Imaginad cuando todo el potencial de la tecnología Digital esté a disposición de los futuros ciudadanos digitales hasta dónde puede llegar esta nueva fase evolutiva de la Especie Humana.

Pero este amanecer, como todos los amaneceres de cada día en nuestro bello planeta, viene con nubarrones que, sin duda, provocaran lluvias o tormentas que pueden entorpecer, retrasar o incluso terminar con este maravilloso viaje de la Especie Humana Digital.

No olvidemos esa terrorífica herencia que nos ha dejado la era industrial, que, en su faceta nuclear, habiéndonos traído avances como la medicina o la energía eléctrica de origen nuclear, nos deja un arsenal de bombas y misiles con capacidad de aniquilar todo tipo de vida en nuestro precioso planeta. Este horrible Armagedón debe ser eliminado por la Humanidad Digital si quiere tener un futuro.

Otro regalo de las revoluciones industriales son los desastres ecológicos, con el calentamiento global como el más peligroso de todos ellos. Estoy seguro de que, según avance la Humanidad Digital, estos problemas serán corregidos y volveremos a un equilibrio con nuestro entorno.

A pesar de ser estos dos nubarrones graves problemas en el amanecer de nuestra Humanidad Digital, podemos decir sin ánimo de culpar de todo al pasado que, a pesar de todo, ha sido necesarios para que Tecnologías Digitales nacieran y fueran madurando hasta llevarnos a este nuevo amanecer y es un peaje que sabremos llevar para eliminar estas amenazas tan graves a toda la humanidad.

Hay un nubarrón que no proviene de los avances tecnológicos necesarios en el pasado y es la mala utilización de la comunicación digital en las plataformas de redes sociales donde los Ciudadanos Digitales encontraron por fin un espacio donde comunicarse directamente, hacer visible su opinión y crear tendencias sin la tutela de los grandes medios de comunicación ni siquiera de los medios de comunicación públicos al servicio de los gobernantes de turno.

> Cada persona comunicará en su idioma y cada persona recibirá esa comunicación en su propio lenguaje nativo mediante dispositivos digitales que realizaran la traducción instantáneamente con el apoyo de la Inteligencia Artificial

La mala utilización de la comunicación digital, en particular en las redes sociales, la protagonizan los ciberdelincuentes que, aprovechando la buena fe de los ciudadanos digitales les roban dinero, secuestran sus perfiles y les llegan a someter a chantajes para recuperar sus datos, en fin delitos típicos de delincuentes comunes.

Más grave es la mala utilización de la comunicación digital, en particular en las redes sociales, la que protagonizan los gobiernos de unos países en contra de otros intentando, y a veces consiguiendo, manipular procesos electorales usando noticias falsas, creando falsas historias que son compartidas masivamente por ejércitos de usuarios fantasmas manipulados desde organizaciones paragubernamentales para eludir su responsabilidad ante el mundo; vemos que son mucho peores que los ciberdelincuentes comunes.

Todavía más grave aún es la mala utilización de la comunicación digital, especialmente en redes sociales la que perpetran los partidos políticos ya no solo en dictaduras declaradas sino incluso en las democracias consolidadas incluso en aquellas con tradiciones democráticas de varios siglos. Todos los partidos políticos sin excepción hacen sin ninguna vergüenza lo que los gobiernos tratan de ocultar, crean falsas historias, insultos de grueso calibre e incluso amenazas de todo tipo, todo lo que sea necesario para desacreditar a sus adversarios democráticos, que han pasado a ser enemigos en un ejercicio indigno que ensucia y pervierte la política y deshumaniza esta actividad humana.

Menos mal que con el paso de cada día los Ciudadanos Digitales vamos aprendiendo y reconociendo el peligro de los ciberdelincuentes, gobiernos delincuentes digitales y políticos delincuentes digitales y nos vamos inmunizando de tanta delincuencia como si nos vacunaran del peor virus pandémico.

La Humanidad Digital solo evolucionará por nuevos y más potentes avances de las tecnologías, que de manera aún más acelerada que lo que hemos visto hasta ahora irán afectando, cambiando y estableciendo nuevos paradigmas en todas y cada una de las actividades de la especie.

Estos cambios de paradigmas, provocarán indudablemente un gran cambio en los nuevos ciudadanos digitales, en su forma de relacionarse, en los valores individuales y colectivos, avanzando, como ha pasado con todos los cambios tecnológicos del pasado desde la invención de la rueda o el descubrimiento del fuego, hacia sociedades más complejas pero también más respetuosas con la propia especie humana.

Hay que tener confianza en que los nubarrones que estamos viendo en este amanecer sean superados por la nueva Humanidad Digital y de la misma manera tener confianza en que dificultades mayores y aún desconocidas que seguramente aparecerán en un futuro serán superadas hasta llegar a un brillante futuro de la especie humana en su fase digital. ■

MÁS INFORMACIÓN

- Traducciones en tiempo real con Android
- Una salud orientada a la prevención

NO SOLO it Marketing y consumo

Neurociencia y medios de pago

José Manuel Navarro
CMO MOMO Group

José Manuel Navarro Llena es experto en Marketing, Durante más de treinta años ha dedicado su vida profesional al sector financiero donde ha desempeñado funciones como técnico de procesos y, fundamentalmente, como directivo de las áreas de publicidad, imagen corporativa, calidad y marketing. Desde hace diez años, basándose en su formación como biólogo, ha investigado en la disciplina del neuromarketing aplicado, lo que le ha permitido dirigir, coordinar e impartir formación en diferentes masters de neuromarketing en escuelas privadas y en universidades públicas. Es Socio fundador de la agencia de viajes alternativos Otros Caminos, y de la entidad de dinero electrónico con licencia bancaria otorgada por el Banco de España SEFIDE EDE de la que en la actualidad es director de Marketing. Autor de "El Principito y la Gestión Empresarial" y "The Marketing, stupid", además de colaborador semanal desde 2006 en el suplemento de economía Expectativas del diario Ideal (Grupo Vocento).

2020 ha sido el año en el que los medios de pago electrónicos han tenido la oportunidad de consolidar su posicionamiento y asentar las bases para un futuro cercano sin dinero físico o, al menos, con un volumen de transacciones reducido a la mínima expresión. El miedo al contagio y el cierre temporal de establecimientos calificados como "no esenciales" ha determinado, por un lado, un menor uso de dinero en metálico y de lectores de banda o chip de tarjetas para TPV y ATM y, por otra parte, ha impulsado la utilización de EMV/NFC tanto de tarjetas como de billeteras móviles, a pesar del crecimiento que han tenido sistemas emergentes como los pagos P2P (en el que ha tomado especial relevancia el modelo Bizum) y con código QR.

Las predicciones que hicieron el año pasado Research and Markets y el gabinete de estudios de Deutsche Bank situaban a las billeteras móviles y al efectivo como los principales medios de pago a final de la actual década, pero recientes informes de Payments, Cards & Mobile vaticinan otro escenario en el que las tarjetas de crédito y de débito mantendrán su liderazgo a nivel global avaladas por la costumbre y la confianza del usuario que, en tiempos de pandemia, ha preferido su uso (en su versión contactless) como recurso seguro ante el contagio y ante el incremento del fraude en canales digitales.

A esta situación también está ayudando la contracción de las redes de sucursales y de cajeros automáticos (y de casi un 30% de entidades financieras en el período 2008-2019), ya que cada día se reducen los puntos para obtener efectivo y, por otro lado, desde estas instituciones se recomienda insistentemente a los clientes el uso de los canales de banca digital, las tarjetas de débito para compras y las tarjetas de crédito como alternativa a la financiación del consumo (aunque éstas están mostrando una clara desventaja respecto a las múltiples alternativas de aplazamiento del pago ofrecidas por muchos proveedores de bienes y servicios y empresas de crédito rápido para bajo importe y elevados tipos de interés). De hecho, Anne Boden, directora de Starling Bank, predice la desaparición del efectivo en 2030 ya que este hecho podría acarrear más beneficios que perjuicios si se proporciona a toda la población las herramientas y la formación digital necesarias para que se produzca una adopción completa de los sistemas financieros electrónicos.

NO SOLO it Marketing y consumo

No obstante, esta visión, para hacerla más consistente, habría que completarla con lo que diversos estudios de psicología aplicada al consumo nos desvelan acerca del comportamiento de los usuarios cuando se enfrentan a la decisión de compra utilizando uno u otro medio de pago. Son conocidos los que apuntan que con el efectivo se controla más el gasto que con las tarjetas y, dentro de éstas, más con las de débito que con las de crédito. Ello es debido a que con el efectivo vemos disminuir directamente nuestro dinero y con las tarjetas de débito nuestro saldo en cuenta en el momento del pago. En cambio, con las de crédito, aplazamos la disminución de nuestra tesorería, descontando el tiempo de "dolor" hasta el momento del cargo en cuenta.

Estudios de neuropsicología han analizado las reacciones que, a nivel fisiológico, se producen en nuestro cerebro cuando realizamos un pago con efectivo o con tarjeta. Las áreas que intervienen son diferentes y ello implica que las decisiones de gasto también sean distintas; mientras que cuando pagamos en efectivo se activan los núcleos relacionados con la aversión a la pérdida (amígdala, ínsula, hipotálamo y locus coruleus), cuando lo hacemos con tarjeta se implican los relacionados con el sistema de recompensa (córtex prefrontal y núcleo accumbens). Por ello, es más fácil caer en la tentación de comprar más y gastar más dinero con tarjeta que con dinero efectivo. Esto ya lo saben muchas empresas, por lo que estimulan el uso de tarjeta, sobre todo para artículos de importe bajo, ya que no ponen en marcha los circuitos de anticipación a la pérdida futura.

Este hecho lo corroboran varios autores en el artículo "Mecanismos neuronales del gasto con tarjeta de crédito", en el que exponen las evidencias de que este medio de pago aprovecha los sesgos cognitivos y otros mecanismos psicológicos por los que los consumidores sobreestiman su capacidad futura de reembolso, aunque luego se sorprenden por el cargo con elevados intereses en el momento del vencimiento. Añaden que los estudios empíricos muestran que los compradores con tarjetas de crédito están dispuestos a comprar más y más caro, al tiempo que se centran más en los beneficios que obtienen del producto que en su coste. Por ello, toman decisiones de compra más indulgentes e impulsivas.

Otro estudio realizado por varios autores, "Efectivo, tarjeta o teléfono inteligente: los correlatos neuronales de los métodos de pago", confirma lo expuesto en la investigación anterior, pero además tiene en cuenta el mecanismo de autorregulación que dispara el pago en efectivo, por lo que para la administración pública puede ser una herramienta para ayudar a los ciudadanos a controlar las compras compulsivas y la ludopatía.

¿Y qué sucede en el entorno digital? A.K. Kar ha identificado que los determinantes de la satisfacción en el uso de los sistemas de pago móviles eran el costo, la utilidad, la confianza, la influencia social, la credibilidad, la privacidad de la información y la capacidad de respuesta ante incidencias. Estos atributos, alejados de los instrumentales dominados por justificaciones racionales, son los que las empresas proveedoras de servicios de pago móviles deberían tener en cuenta para incentivar e incrementar la

NO SOLO it Marketing y consumo

Estudios de neuropsicología han analizado las reacciones que, a nivel fisiológico, se producen en nuestro cerebro cuando realizamos un pago con efectivo o con tarjeta

adopción de sus sistemas, valorando también cómo manejar la ventaja que les puede aportar el estímulo de los mecanismos de recompensa que se activan en el caso de uso de las tarjetas para crear acciones promocionales y de fidelización orientadas a potenciar este efecto.

Aunque la tecnología ayuda a mejorar la experiencia de usuario, es necesario tener en cuenta otras consideraciones que pueden parecernos banales o que la intuición nos indica que pueden facilitar el proceso de pago móvil y que, en realidad, lo que pueden hacer es activar la aversión a la pérdida como en el pago en efectivo. Es el caso de la vibración háptica en el proceso de compra con el móvil, la cual reduce la disposición a gastar de los participantes en el estudio llevado a cabo varios autores, en comparación con un grupo de control que no recibía ninguna retroalimentación mediante la vibración del móvil.

Estos detalles de diseño que, aparentemente, mejoran la experiencia de usuario pueden volverse en contra si no se tiene en cuenta la reacción inconsciente que provoca. Algo parecido sucede en el comercio electrónico y la percepción de seguridad durante el proceso de pago, como han analizado J. Sánchez Fernández y otros en un reciente estudio en el que han concluido que los pagos con tarjeta que se realizan en plataformas que se perciben como no seguras activan las áreas cerebrales relacionadas con el procesamiento emocional negativo (aversión a la pérdida). En cambio, en las que se perciben como seguras se involucran las áreas que procesan las emociones positivas (anticipación de recompensa). Y en el caso de PayPal, en el que el usuario no aporta los datos de su tarjeta, se produjo además una activación mucho mayor del cerebelo, lo que se puede traducir como una valoración más positiva y correlacionada con una mayor intención de uso.

Aunque las tendencias del mercado y las predicciones sobre la evolución de la tecnología a corto plazo apuntan hacia la "omnidigitalización", con especial intervención de los sistemas soportados por inteligencia artificial, realidad aumentada, virtual y mixta, internet de las cosas, bots de soporte… es necesario tener en cuenta, como señala KPMG en su reciente informe sobre la nueva realidad de las experiencia de cliente, que el consumidor en este último año se ha vuelto más reflexivo y selectivo en su toma de decisiones, valorando más la integridad y la confianza como atributos esenciales para elegir la empresa a la que adquirir sus productos. Factores como la marca, el propósito y la reputación se están incorporando en el proceso de toma de decisiones en igualdad de condiciones con la seguridad, la garantía, la conveniencia y la certidumbre.

Al conocimiento de estos factores, todos ellos en el marco de las emociones, nos podremos acercar con métodos de investigación convencionales vía test y focus group, pero será la neurociencia las que nos aporte la información más relevante sobre la respuesta neuronal que realmente condicionará la decisión de un individuo acerca de la compra de un producto o servicio a una empresa en concreto y del medio de pago con el que lo va a adquirir. ■

MÁS INFORMACIÓN

- Predicciones Research and Markets
- El futuro de los pagos, Deutsche Bank
- Payments, Cards & Mobile
- Desaparición efectivo en 2030
- Mecanismos neuronales del gasto con tarjeta de crédito
- Efectivo, tarjeta o teléfono inteligente: los correlatos neuronales de los métodos de pago
- A.K. Kar
- Vibración háptica en el proceso de compra con el móvil y su efecto en el gasto
- Comercio electrónico y la percepción de seguridad durante el proceso de pago
- Nueva realidad en la experiencia del cliente

it User
TECH & BUSINESS

Cada mes en la revista, cada día en la web.