facebook
twitter
newsbook.es

>> La revista del distribuidor informático

Newsbook

Tai editorial

Año XXVI Nº 271 Mayo 2020 0,01 Euros

Procesador Intel® Core™ i7 vPro®

EliteBook x360 1040 G6

Expectativas elevadas.

Diseño para gente en movimiento.

El magnífico y ultrafino HP EliteBook x360 1040 ofrece una versatilidad de 360° y unas imágenes sorprendentes de un extremo al otro, sobre una pantalla de 14 pulgadas.

Privacidad cuando más la necesita.

Controle lo que el mundo ve y ayude a proteger sus datos con funciones integradas de seguridad y privacidad. Deslice el obturador de la cámara de privacidad HP[1] para bloquear la visión de la cámara.

Como encontrarse cara a cara.

La cámara FHD, el audio de Bang & Olufsen y la cancelación de ruido HP hacen que sus llamadas sean claras y personales, facilitando una colaboración inspirada con vídeos y audios realistas.

esprinet INGRAM MICRO TechData VINZEO

© Copyright 2020 HP Development Company, L.P. La información que contiene este documento está sujeta a cambios sin aviso previo. [1] La cámara de privacidad de HP solo está disponible en los ordenadores equipados con la cámara HD o IR y debe instalarse de fábrica. Copyright © Intel Corporation. Reservados todos los derechos. Intel y el logo de Intel vPro son marcas registradas de Intel Corporation o de sus filiales en Estados Unidos y en otros países.

#Gracias

#JuntosPodemos

Para el Grupo Tai lo principal es la seguridad de nuestro equipo humano, lectores y clientes; por eso seguimos trabajando en remoto. Podrás contactar con nosotros para lo que necesites en cualquiera de nuestros teléfonos o vía email.

taieditorial.es | tuwebsoluciones.com | servixmedia.es

» La revista del distribuidor informático

Newsbook

Tai editorial

Año XXVI Nº 271 Mayo 2020 0,01 Euros

La implantación del trabajo en el hogar ha salvado la actividad de muchas empresas

La empresa española descubre las ventajas del teletrabajo

Mantener la actividad durante el estado de alarma decretado por la pandemia del Covid-19 ha sido uno de los principales retos que han tenido que afrontar las empresas españolas. Las herramientas tecnológicas actuales permiten realizar el trabajo en cualquier lugar, aunque esta fórmula del teletrabajo apenas era utilizada en nuestro país, que tiene una cultura presencial muy arraigada. La necesidad y la urgencia han impulsado esta opción en las empresas de todos los tamaños; aunque para algunas ha sido la primera vez que utilizaban este sistema. A pesar de las dificultades, el teletrabajo ha puesto de manifiesto que la actividad laboral no está vinculada a los espacios corporativos y que aporta ventajas como la reducción de los desplazamientos y la conciliación familiar. Ahora la cuestión que se plantea es si el teletrabajo se consolidará en la empresa. Las principales empresas TIC consideran que se ha dado un gran paso para que sea considerado una opción más.

Sigue en pág. 16

Mantiene sus planes de crecimiento para este ejercicio

DMI Computer celebra sus 30 años en el mercado

DMI es una compañía veterana en el sector de la distribución que ha asistido a los cambios que se han producido en el mercado en las últimas tres décadas. Ahora celebra sus 30 años con el foco puesto en el segmento profesional, sin olvidar la vocación de servicio a sus distribuidores que ha permitido mantenerse durante tanto tiempo en el mercado. Emilio Sánchez-Clemente, director general de DMI, comenta que el balance de estas tres décadas es positivo y un motivo de orgullo para todo su equipo. Su intención es continuar con la misma línea de trabajo para seguir creciendo, a pesar de las dificultades provocadas por la crisis del Covid-19. "Nuestro plan es continuista y seguir creciendo en todo lo que tenga que ver con el segmento profesional".

Sigue en pág. 13

El *backup*, blindaje obligatorio contra el *ransomware*

Sin variar sus técnicas, los *hackers* han intensificado sus ataques de *ransomware*, aprovechándose de la situación creada por la expansión de la pandemia del Covid-19. El uso intensivo del teletrabajo y el aumento del consumo de aplicaciones y servicios en la nube expandieron la superficie de ataque, lo que puso en jaque a muchas empresas españolas que no contaban con suficiente protección. El *backup* se ha convertido en un perfecto blindaje contra estos ataques.

Sigue en pág. 26

El Covid-19 conciencia sobre la importancia de la seguridad

La crisis sanitaria del Covid-19 ha provocado una mayor concienciación sobre la importancia de la seguridad en las organizaciones. Con la implantación del teletrabajo numerosas empresas han sido conscientes de sus carencias en esta materia. Asimismo, han valorado la necesidad de invertir en fuertes medidas que protejan los datos que manejan. Al mismo tiempo, los *hackers*, conscientes de los beneficios que pueden obtener de una situación como la actual, han centrado sus esfuerzos en sortear esta seguridad.

Sigue en pág. 32

#Gracias #JuntosPodemos

No, no hemos repetido el editorial del pasado número de abril por error. Seguimos necesitando dar las **#Gracias**. Al menos, un mes más. Porque lo más básico es lo más importante. Antes, ahora y siempre. No dejemos de valorarlo nunca.

#Graciasalos**médicos** #Graciasalas**enfermeras** #Graciasalos**auxiliares**

#Graciasalos**celadores**

#Graciasatodoslosque**formanpartedelasplantillasdeloshospitalesyloscentrosdesalud**

#Graciasalos**farmaceúticos** #Graciasalos**investigadores**

#Graciasala**industriaquímicayfarmaceútica**

#Graciasalos**supermercados** #Graciasalas**tiendasdebarrio**

#Graciasalas**cajeras** #Graciasalos**reponedores**

#Graciasalos**agricultores** #Graciasalos**ganaderos** #Graciasalos**pescadores**

#Graciasalos**transportistas** #Graciasal**personaldelosmediosdetransporte**

#Graciasalos**camioneros**

#Graciasa**todoslostaxistasquehanpuestosusvehículosadisposicióndelosenfermos**

#Graciasatodoslos**profesionalesquetrabajanenlalimpieza**

#Graciasalos**cuidadoresdemayores**

#Graciasalos**profesionalesquesehanquedadoenlasresidenciasdeancianos**

#Graciasatodoslas**personasquesehanofrecidoahacerlacompraalosmásnecesitados**

#Graciasal**ejército** #Graciasala**UME**

#Graciasatodosycadaunodelos**cuerposyfuerzasdeseguridaddelEstado**

#Graciasalos**políticosquehanpuestoelinteréscomúnporencimadetodo**

#Graciasalos**bomberos**

#Graciasalos**periodistas** #Graciasalos**kiosqueros**

#Graciasalos**fabricantesdeequipostecnológicosydecomunicaciones**

#Graciasatodala**cadenalogística**

#Graciasatodaslas**empresasquesehanpuestoafabricarmaterialesdeprotección**

#Graciasalos**quehandonadodineroparacomprarmaterial**

#Graciasalos**quehanvoladoparatraeralagenteacasa**

#Graciasalas**operadorasdecomunicaciones**

#Graciasalas**ONG** #Graciasa**Cáritas** #Graciasala**Iglesia**

#Graciasalos**quesehanquedadoencasa**

#Graciasalos**quesalendecasaporquesutrabajoesesencial**

#Graciasalos**autónomosyalaspymesquevanasacrificarseenposdelasaluddetodos**

En definitiva

#Graciasatodos #Juntospodemos

No está permitida su reproducción o distribución sin la autorización expresa de Técnicos y Asesores Informáticos Editorial, S.A. Le informamos que sus datos personales y dirección de correo electrónico serán tratados por Técnicos y Asesores Informáticos Editorial, S.A., como responsables del tratamiento, con la finalidad de llevar a cabo una gestión de carácter comercial, y para el envío de nuestra publicación y también de comunicaciones comerciales sobre nuestros productos y servicios, así como de terceros que consideramos puedan resultar de su interés. Los datos serán cedidos a Tu web soluciones, compañía de posicionamiento y análisis, S.L. y Cía. para la Empresa Servixmedia S.L., empresas colaboradoras del responsable que tratarán los datos con las mismas finalidades. Siendo conservados mientras no manifieste su oposición a seguir recibiendo el servicio solicitado. Puede usted ejercer los derechos de acceso, rectificación o supresión de sus datos, dirigiéndose a arco@taieditorial.es para más información al respecto, puede consultar nuestra Política de Privacidad en https://taieditorial.es/politica/

En Primera Persona

DMI Computer

Emilio Sánchez-Clemente, director general

En portada

Teletrabajo

Da un salto en la empresa española por la pandemia

En portada

Seguridad

Los *hackers* aprovechan el Covid-19 para intensificar sus ataques

Canal

Arrow se suma al canal de Alibaba **Pág. 5**

Pure Storage incrementa su canal mayorista en España con Ingram Micro **Pág. 7**

Esprinet elevó sus beneficios un 66 % en 2019 **Pág. 8**

Actualidad

Betchle crece por encima del 20 % en España **Pág. 10**

En portada

Backup **Pág. 26**

El *backup*, blindaje efectivo contra el *ransomware*

En profundidad

V-Valley Vinzeo y HPE **Pág. 21**

Un tándem con más de dos décadas de historia

Tecnología 3D **Pág. 22**

Las marcas se suman a la lucha contra el Covid-19

Esprinet **Pág. 24**

El mayorista blinda a su plantilla y mantiene su actividad

NFON **Pág. 25**

Mejora la colaboración empresarial con Nvoice para Microsoft Teams

Intel **Pág. 31**

Estreno de un procesador portátil para jugones

Esprinet y Midway **Pág. 37**

Una alianza para la transformación digital de la empresa

Patronales ante el Covid-19 **Pág. 38**

Las asociaciones empresariales analizan su papel en la pandemia y la recuperación

Dell **Pág. 41**

Formación y soporte financiero: armas para que los *partners* sigan haciendo negocio

IBM **Pág. 42**

El gigante azul define medidas para que su canal mantenga el negocio

Check Point **Pág. 44**

La marca, al asalto de los ataques

Newsbook

Síguenos en @newsbook_tai

DIRECTORA
Marilés de Pedro • mariles@taieditorial.es

REDACCIÓN Y COLABORADORES
Rosa Martín • rmartin@taieditorial.es
Inma Elizalde • inma@taieditorial.es
Olga Romero • olga@taieditorial.es

PUBLICIDAD
David Rico • david@taieditorial.es

PRODUCCIÓN
Marta Arias • marta@taieditorial.es

OTRAS PUBLICACIONES
directorTIC · tpvnews · PYMES · Negocios en informática

EDITA
T.A.I. Editorial, S.A.
(Técnicos Asesores Informáticos Editorial, S.A.)
www.taieditorial.es

Avda. Fuencarral, 68
28108 ALCOBENDAS (Madrid)
tel. +34 91 661 61 02
e-mail: correo@taieditorial.es

MIEMBRO DE
AEEPP · FIPP Federación Internacional de la Prensa Periódica

DISTRIBUCIÓN Publidist Publicidad Directa, S.A.
C/ Fundidores, 53 (Pol. Ind. Los Ángeles)
28906 Getafe – Madrid
Telf. 91 683 76 92

DEPÓSITO LEGAL M-20480-2002
ISSN 1696-6147

Impreso en papel ecológico

Nutanix ha lanzado un nuevo programa de financiación para *partners*

Nutanix ha presentado un programa de financiación para ayudar a sus *partners* a superar la actual situación. El Programa Especial de Asistencia Financiera (Nutanix Special Financial Assistance Program, NSFAP, en inglés) ofrece la posibilidad de ampliar los términos de pago para tener más flexibilidad en su negocio. Y, además, a través de la división Nutanix Financial Solutions (NFS) pone a disposición de sus socios del canal otras opciones para apoyar la continuidad de sus negocios.

El programa, que estará disponible hasta el próximo 31 de mayo, ofrece la ampliación en los términos de pago sin costes adicionales y con efecto inmediato. Y esta extensión la pueden trasladar a sus clientes.

Los *business partners* de Nutanix también pueden aprovechar las nuevas soluciones de financiación lanzadas desde la división Nutanix Financial Solutions (NFS) como las que permiten el pago en 180 días o las que ofrecen planes de pago personalizables.

Por otra parte, Nutanix está invirtiendo en formación y en el desarrollo de sus *partners* poniendo a disposición de sus socios exámenes gratuitos de certificación hasta el próximo 31 de julio. Esta propuesta se apoya también en cursos y recursos gratuitos en el portal de socios de Nutanix.

Chris Kaddaras, *executive vice president worldwide sales* de Nutanix, comentó que su "compromiso con toda la comunidad de socios y clientes nunca ha sido más fuerte y continuaremos evaluando sus necesidades para asegurarnos de que tengan los recursos que necesitan para tener éxito en la situación actual".

Nutanix
Tel.: 91 123 12 33

Arrow se alía con Alibaba Cloud en la región de EMEA

Alexis Brabant, vicepresidente de ventas del negocio de soluciones informáticas empresariales de **Arrow** en EMEA

Arrow ha firmado un acuerdo de distribución con Alibaba Cloud con el fin de comercializar sus soluciones en la nube en toda la región de EMEA. Esta alianza le permite al mayorista ampliar su oferta con la plataforma en la nube de Alibaba Group, que ofrece desde computación elástica hasta almacenamiento, bases de datos relacionales, recuperación ante desastres, seguridad o redes de entrega de contenidos, entre otras.

Alibaba Cloud es el proveedor de soluciones de nube pública más grande de China. Opera en 61 zonas, lo que le otorga cobertura en 20 regiones diferentes en todo el mundo, entre los que se incluyen los centros de datos en China continental, Alemania y el Reino Unido.

Alexis Brabant, vicepresidente de ventas del negocio de soluciones informáticas empresariales de Arrow en EMEA, destacó que Alibaba Cloud es uno de los mayores proveedores de nube pública del mundo. "Nuestro acuerdo brindará, sobre todo a los *players* del canal pequeños y medianos, la oportunidad de trabajar con Alibaba Cloud en el mercado de EMEA".

Max Tao, gerente senior de alianzas en Alibaba Cloud International, explicó que trabajará con Arrow para "ayudar a más compañías, tanto regionales como locales, a que comiencen su viaje hacia la nube y al *data intelligence*".

"A medida que avanzamos hacia un mundo *multicloud*, nuestros clientes pueden ahora elegir entre una gama aún más amplia de soluciones y servicios. Con Alibaba Cloud, Arrow continúa desarrollando su *portfolio* de soluciones en la nube para ofrecer aplicaciones de análisis, *blockchain*, inteligencia artificial, IoT y de seguridad a las empresas", añadió Brabant.

Arrow
Tel.: 91 761 21 51

El mercado ibérico acelera el crecimiento de Exclusive Networks en Europa

Exclusive Networks ha logrado crecer en el sur de Europa un 20 % en 2019, sobre todo por el buen comportamiento del mercado ibérico, que es el de mayor desarrollo en Europa para el mayorista en la actualidad. Estos datos se desprenden de los resultados financieros del ejercicio 2019, que acaba de presentar la compañía, que muestran un incremento de sus ingresos del 17 % hasta situarse en los 2.400 millones de euros.

Las carteras de ciberseguridad y la migración al *cloud* han sido los motores de este incremento que se ha visto acompañado por el auge del modelo de suscripción que ya representa un 10 % del negocio.

El mayorista ha logrado crecer en todas las regiones, destacando el incremento de Oriente Medio (44 %), Pacífico (18 %), DACH (17 %) y UK&I (16 %). "Hemos registrado otro fuerte año de generación de oportunidades para nuestros socios y de crecimiento orgánico por encima de las tasas de crecimiento del mercado", afirma Andy Travers, vicepresidente ejecutivo de ventas y marketing mundial de Exclusive Networks.

En los resultados de 2019 también destacó el incremento de la oferta de Managed Security Services Distributor (MSSD) que ha permitido que se incrementara en dos dígitos los ingresos en el área de servicios.

Significativo también ha sido el incremento de un 20 % de los tres principales proveedores de la compañía y un incremento de casi un 40 % en los otros tres, lo que suma seis marcas: Proofpoint, Rubrik, SentinelOne, Infoblox, Nutanix y Gigamon.

Por otra parte, la compañía ha comunicado que sigue activo su plan de negocio trazado para responder a la situación de pandemia provocada por el Covid-19. Además, está preparando el lanzamiento de un paquete de medidas de apoyo que permitirá a estos *partners* continuar desarrollando su negocio.

Exclusive Networks
Tel.: 902 108 872

MCR Pro amplía su oferta con las soluciones profesionales de Sony

Las soluciones profesionales de Sony se han sumado al catálogo de MCR Pro, gracias al acuerdo alcanzado entre el mayorista y el fabricante. La división de soluciones profesionales de MCR añade una nueva marca a su *portfolio* y refuerza su propuesta con productos que cuentan con una trayectoria en el mercado de más de 50 años.

La gama de soluciones incluye proyectores diseñados para diversas aplicaciones y sectores como el educativo, el cine digital, el *home cinema,* simulaciones en museos, atracciones o instalaciones.

MCR Pro también comercializará la gama de monitores profesionales que abarca modelos Full HD y 4K para *broadcasting,* incluyendo también los de la marca Sony Bravia.

En el *portfolio* se incluye la oferta de cámaras de red, con modelos de PTZ con calidad 4K, y otra serie de soluciones de integración para entornos de negocio, entornos educativos y aplicaciones como UbiCast, un sistema automatizado para crear y compartir contenidos de vídeo y realizar grabaciones desde múltiples ubicaciones.

Serge Garnero, *sales manager* de la división de *corporate* y educación de Sony Professional Solutions para el sur de Europa, resaltó que este acuerdo les permitirá impulsar "la distribución de nuestros productos y ponerlos más cerca de los profesionales y empresas españolas".

Por su parte, Enrique Hernández, director de MCR Pro, resaltó que "Sony lleva más de 50 años colaborando con el mundo de los profesionales, aportando tecnología y una amplia experiencia en este sector para permitir a empresas de numerosos sectores sacar adelante sus ideas".

MCR
Tel.: 91 440 07 00

Tai editorial
www.taieditorial.es

PUBLICACIONES

Para profesionales del canal de distribución TIC
Newsbook
Negocios en informática

Para los gerentes de la pyme
PYMES

Para C-Level de mediana y gran empresa
directorTIC

Para empresas y canal especializado en POS, captura de datos y *retail*
tpvnews

El crecimiento del canal TI europeo desciende por primera vez durante la crisis del Covid19

El crecimiento del canal TI en Europa ha experimentado un descenso. Es la primera vez que ocurre desde el inicio de la crisis sanitaria del Covid19. Así se desprende de los últimos análisis realizados por la consultora Context. Razones como el teletrabajo y los niños estudiando en casa impulsaron el crecimiento de los ingresos que provocaron el magnífico rendimiento de las primeras semanas. El pico de este período se alcanzó en la duodécima semana (que arrancó el pasado 16 de marzo), momento en el que hubo un crecimiento del 10 %.

Durante las cuatro semanas analizadas por la consultora, se puede observar que el crecimiento comenzó a disminuir en la semana siguiente (la que arrancó el lunes 23 de marzo), con un ascenso del 9,2 %. El crecimiento siguió ralentizándose, primero al 0,5 %, en la semana del 30 de marzo; y luego al 7,4 %, en la posterior. En comparación con 2019 el crecimiento en la semana 15 fue del 8,1 %. Esta tendencia ha sido impulsada por Europa Occidental, donde se registró una caída del 8,9 % en dicho periodo mientras que el año anterior hubo un crecimiento del 9,4 %. En cambio, Europa del Este ha crecido el doble que en 2019.

Sin embargo, a pesar de la disminución general, las mismas categorías de teletrabajo que han experimentado fuertes crecimientos lo siguen consolidando. Es el caso de las cámaras web (102 %), el software de virtualización (48 %), los portátiles (29 %), los auriculares y micrófonos (27 %), las estaciones de trabajo (27 %), los cartuchos de tinta (19 %) y los multifunción de tinta (18 %).

Los grandes motores del canal de distribución han sufrido descensos en la semana número 15. Según los datos de Context el negocio dirigido a la pyme ha perdido un 9 %, mientras que los distribuidores corporativos han visto reducido su negocio un 10 %. Por el contrario, los e-*tailers* que se dirigen al consumo han experimentado un crecimiento del 14 %.

Sobre estos últimos datos de la consultora ha hablado Adam Simon, director ejecutivo global de Context. "La escasez de oferta en ciertos productos de consumo, combinada con una desaceleración en la actividad empresarial, provocó esta bajada", ha comenzado. "Sin embargo, todavía hay una gran demanda en Europa en muchas categorías para el teletrabajo. Por lo tanto, los distribuidores pueden esperar un mejor crecimiento", ha matizado.

Context
Tel.: 91 441 24 96

Ingram Micro, nuevo mayorista de Pure Storage para España

Ingram Micro se ha convertido en el nuevo mayorista de Pure Storage para España, gracias al acuerdo firmado entre ambas compañías. Esta alianza tiene por objetivo expandir, vender y dar soporte a las soluciones de la marca. El trabajo conjunto se centrará en acercar las soluciones a los clientes aprovechando la cobertura geográfica y los servicios de valor del mayorista.

A la hora de firmar esta alianza, Ingram Micro ha tenido en cuenta la innovación de Pure Storage que le ha permitido afianzarse en el mercado y aportar soluciones de almacenamiento flash sencillas y eficientes.

"Las soluciones de almacenamiento Flash de Pure Storage son una pieza clave dentro de nuestra estrategia de distribución. Pure Storage supone un soplo de aire fresco, al tratarse de soluciones 100 % flash nativo", destacó Martín Trullas, director de la división de Advanced Solutions de Ingram Micro.

Por su parte, Matthieu Brignone, responsable de canal y alianzas de EMEA de Pure Storage, añadió que "los servicios de distribución de Ingram Micro respaldarán y mejorarán la oferta de Pure Storage en España. Las soluciones financieras de Ingram Micro brindan a los socios y clientes múltiples formas de trabajar juntos".

Ingram Micro
Tel.: 902 506 210

Los beneficios del grupo Esprinet crecieron un 66 % en 2019

El grupo Esprinet ha cerrado el año 2019 con un incremento de sus beneficios netos del 66 %, situándose en 23 millones de euros, según reflejan los resultados anuales correspondientes al año pasado que acaba de aprobar su consejo directivo.

"Cerramos 2019 con unos excelentes resultados económicos y una sólida estructura financiera. El grupo ha mantenido la continuidad de su negocio durante el periodo de cierre gracias a los procedimientos de *smartworking* que comenzamos hace dos años y a los fuertes controles tecnológicos y operativos desarrollados a lo largo de tiempo", resaltó Alessandro Cattani, CEO de Esprinet.

El grupo logró unas ventas de 3.945,4 millones en 2019, lo que supone un incremento del 10 % en comparación con los 3.571,2 millones de 2018. En Italia logró un crecimiento del 13 %, cifrándose sus ventas en 2.494,7, mientras que en España crecieron un 6 % alcanzando los 1.378 millones. En Portugal registró un incremento del 27 %, situándose las ventas en 38,5 millones. En el resto de países de la Unión Europa vendió un 15 % más y en los países extracomunitarios un 64 %.

Los resultados conseguidos durante 2019 en Italia y España le otorgan una cuota del mercado que supera el 26 %, lo que le consolida como el principal mayorista del sur de Europa.

En los resultados del ejercicio también destaca el incremento alcanzado en sus principales áreas de negocio. En el apartado de IT Clients ha logrado un crecimiento del 10 %, obteniendo 2.036 millones de euros; mientras que en el ámbito de Soluciones Avanzadas o Advanced Solutions ha logrado un crecimiento más moderado, del 1 %. En el terreno del consumo las ventas se han cifrado en 1.393,3 millones, lo que representa un crecimiento del 15 %.

Por tipo de clientes destaca el incremento del 16 % en la tipología de los *retailers* y *e-tailers* con unas ventas de 1.930,8 millones de euros. Y sus ventas a los *resellers TI* se cifraron en 2.059,5 millones de euros, lo que supone un crecimiento del 5 % respecto al año anterior.

"El año se cerró con un beneficio neto de 23.6 millones de euros, un incremento del 66 % respecto de 2018; después de 20 años consecutivos generando beneficios y distribuyendo dividendos, prudentemente proponemos la asignación de las ganancias del año a las reservas de capital y, mientras tanto, cerramos los programas de recompra".

Esprinet
Tel.: 902 201 146

Ireo, nuevo mayorista de Bitglass en España y Portugal

Ireo se ha convertido en el nuevo mayorista de Bitglass en España y Portugal, según recoge el acuerdo alcanzado entre ambas compañías. Esta nueva alianza amplía el catálogo de soluciones de Ireo con los productos CASB (Cloud Access and Security Broker) de Bitglass, que ofrecen protección de datos en tiempo real, visibilidad y control profundo; y una completa seguridad contra las amenazas en todas las aplicaciones de SaaS, IaaS y nube privada en cualquier dispositivo, gestionado o no.

La tecnología Zero-Day Core que tienen sus soluciones bloquea las rutas de fugas de datos que se explotan por primera vez e identifican las amenazas previamente desconocidas.

La gestión de las soluciones se realiza desde una consola de administración unificada y, además, ofrece seguridad móvil sin agentes para los entornos BYOD, lo que preserva la privacidad de los empleados.

Valentin Jangwa, *regional sales director* de Bitglass para el sur de Europa, comentó que la alianza con Ireo le permitirá aumentar el "valor que Bitglass proporciona a todos sus clientes y socios".

Por su parte, Chuck Cohen, director general de Ireo, señaló que "las soluciones CASB se tornan fundamentales para los negocios de todos los tamaños; lo que unido a unos excelentes márgenes y a un gran apoyo al distribuidor, tanto en formación como en recursos, por parte de Ireo y Bitglass, representa una gran oportunidad para nuestros socios".

Ireo
Tel.: 902 321 122

La solución Virtual Cloud Network de VMware supera los 15.000 clientes

La solución Virtual Cloud Network ya ha superado los 15.000 clientes. Así lo ha anunciado VMware, que ha explicado que dicha herramienta ha experimentado un crecimiento de un 50 % de media cada año desde 2018. Se trata de un componente integral de VMware Cloud Foundation que ofrecen proveedores de servicios *cloud* como AWS, Azure, Alibaba Cloud, Google Cloud, IBM Cloud y Oracle Cloud.

Virtual Cloud Network permite a VMware ofrecer nubes privadas con los mismos niveles de agilidad y eficiencia de las nubes públicas. Además de garantizar el apoyo para garantizar la continuidad del negocio. Asimismo, la compañía ha aprovechado para anunciar innovaciones en materia de redes y seguridad para que las empresas sean capaces de ofrecer la experiencia de nube pública en sus instalaciones privadas. Gracias al empleo de sus soluciones VMware NSX-T3.0 y VMware vRealize Network Insight 5.2 las organizaciones consiguen simplificar las redes, la seguridad de la nube y los contenedores para ofrecer mayor agilidad y disponibilidad.

Tom Gillis, vicepresidente ejecutivo y director general de la unidad de negocio de redes y seguridad de VMware, ha explicado cómo sus clientes, gracias al empleo de Virtual Cloud Network, pueden ofrecer una experiencia de nube pública en sus propias instalaciones "sin necesidad de los ineficientes *tickets* de TI ni de tiempos de espera prolongados para los cambios de redes y seguridad".

El directivo ha añadido que "en redes públicas, privadas y de telecomunicaciones, del centro de datos a la oficina y la sucursal, Virtual Cloud Network permite simplificar las funciones de red y ahorrar con ello tiempo y dinero". Gillis ha matizado, "los clientes pueden reducir hasta en un 59 % los CAPEX y hasta en un 55 % los OPEX en comparación con el uso de soluciones de red tradicionales".

Las innovaciones

Desde VMware se han anunciado innovaciones para su solución Virtual Cloud Network con el objetivo de facilitar la experiencia de nube pública *on-premises*. Estas novedades son la experiencia de nube pública con la que conseguir mayor agilidad de red en centros de datos. La seguridad intrínseca, funciones de redes para aplicaciones modernas, analítica y visibilidad de extremo a extremo, funciones de red para nubes de telecomunicaciones y 5G de nueva generación. Y, por último, funciones de red de nube virtual para zonas Edge de Azure.

VMware
Tel.: 91 412 50 00

Las empresas de EMEA apuestan por los entornos *multicloud*

Las empresas de EMEA están a la cabeza de la adopción de los entornos *multicloud,* según se refleja en el estudio "Estado de los Servicios de Aplicación (SOAS)" elaborado por F5 Networks. El informe revela que el 88 % de las organizaciones encuestadas en EMEA afirma estar sacando partido a los entornos *multicloud* o multinube. Este porcentaje es superior al de las empresas del continente americano (87 %) y al de la región APCJ (86 %).

El 27 % de las empresas de EMEA asegura que a finales de este año tendrá más de la mitad de sus aplicaciones en la nube. Y un 54 % indica que la nube será la principal tendencia estratégica durante el próximo lustro. Cuando trasladan sus aplicaciones a la nube las empresas de EMEA optan por un modelo caso a caso (43 %) en vez de uno genérico del tipo *"one-size-fits-all"*. El 70 % cree que es muy importante implementar las mismas políticas de seguridad tanto *on-premise* como en la nube.

En cuanto a los retos que tienen que afrontar las empresas en este proceso. El principal es el relativo al cumplimiento normativo (33 %), fundamentado por la necesidad de cumplir con el GDPR, le sigue la aplicación de políticas de seguridad consistentes en todas las aplicaciones (30 %), la protección contra amenazas emergentes (28 %) y la migración de aplicaciones entre nubes y centros de datos (28 %).

La diversidad de arquitecturas existentes dificulta la aplicación de políticas de seguridad en todos los entornos. En este sentido, el informe refleja que el 34 % de las aplicaciones se mueve en una arquitectura cliente-servidor, un 26 % son aplicaciones web, las nuevas arquitecturas móviles representan el 14 %, los microservicios y aplicaciones nativas *cloud* un 15 % y los entornos *mainframe* aún representan el 11 % .

F5 Networks
Tel.: 91 119 05 00

Nutanix comparte su estrategia con 500 profesionales españoles en su primera cumbre virtual

Nutanix reunió a 500 profesionales españoles en el evento virtual Nutanix Now, organizado por la compañía en nuestro país. En esta cumbre, la primera que celebra totalmente digital, ha reunido a los principales ejecutivos de la compañía como Dheeraj Pandey, fundador y CEO de Nutanix; Tarkan Maner, Chief Commercial Officer; o Wendy Pfeiffer, Chief Information Officer, entre otros, junto con el equipo local que dirige Iván Menéndez.

La jornada, titulada *"Bringing the cloud inside"*, comenzó con la presentación de Dheeraj Pandey, fundador, CEO y presidente de Nutanix, quien explicó el objetivo del encuentro y resaltó las fortalezas que tiene la compañía para afrontar la situación actual y las ventajas que ofrece a las empresas. "Podemos ofrecer tanto las mejores experiencias de usuario final como las mejores experiencias de tecnología para ayudar a trabajar de forma remota. Podemos poner en marcha soluciones de recuperación de desastres y continuidad de negocio con sólo unos pocos clics. Y juntos, podemos afrontar los nuevos retos de seguridad que nos exigirán las cambiantes circunstancias mundiales", subrayó.

Por su parte, Iván Menéndez, director general de Nutanix Iberia, repasó los puntos clave de la estrategia de la compañía y señaló que "el futuro es híbrido y *multicloud*". El directivo explicó las ventajas de su propuesta tecnológica que es capaz de unir lo mejor de los dos mundos, el *cloud* y el centro de datos, en una plataforma sencilla y segura. Destacó también la flexibilidad que ofrece a través del modelo de suscripción.

Tarkan Maner, *chief commercial officer* de Nutanix, profundizó en el enfoque *multicloud* de Nutanix, destacando el papel que juegan las alianzas y resaltando la oportunidad de negocio que representa para sus socios del canal, mientras que Wendy M. Pfeiffer, *chief information officer* de Nutanix, recalcó la preparación que tiene la compañía para afrontar la situación actual que atraviesa el mercado por la pandemia del coronavirus. "Muchos de nosotros nos hemos visto afectados por el coronavirus y ya hay muchas empresas tecnológicas que han enviado a todos sus empleados a trabajar desde casa. ¡Qué gran cambio social! Pero, me doy cuenta de que de alguna manera nos hemos estado formando para esto toda nuestra vida", reiteró.

Nutanix
Tel.: 91 123 12 33

Bechtle creció un 21 % en España en 2019

Bechtle ha comunicado que ha incrementado sus ingresos un 21 % en España en su año fiscal 2019, alcanzando los 61,2 millones de euros. Este incremento se ha basado en el refuerzo de recursos efectuado en el área de soluciones y servicios en *managed workplace*, software, infraestructuras híbridas y MPS. Además, el segmento del comercio electrónico ha representado un 46 % de los pedidos de la compañía y un 11% de la facturación, debido a la intensificación de la automatización de los procesos de compra.

Juan José Moneo, director general de Bechtle España, explicó que "este nuevo crecimiento de doble dígito, con unos parámetros muy por encima de la media del mercado, indican la gran aceptación y confianza de los clientes en nuestro modelo de negocio".

Desde el punto de vista global, Bechtle ha logrado un incremento del 24,3 % de sus ingresos, que ascendieron a 5.374,5 millones de euros. Sus beneficios antes de impuestos se cifraron en 236,3 millones de euros, lo que supone un incremento del 22,3 %. Además, su plantilla también creció un 14,8 %, lo que la sitúa en 11.487 empleados.

La compañía ha logrado un incremento a doble dígito en todas las regiones, sobre todo por las adquisiciones que ha efectuado. Así ha generado en el extranjero más de 2.000 millones de euros en este año fiscal. El crecimiento orgánico del grupo ascendió al 15,2 %.

Durante el año fiscal destacó el incremento de los ingresos del segmento IT System House & Managed Services, que se cifró en un 19,9 %, alcanzando los 3.485 millones de euros. Además, el crecimiento orgánico se situó en un 16,8 %.

En el ámbito del comercio electrónico, los ingresos crecieron un 33,3 % hasta alcanzar los 1.889,4 millones de euros, fruto en parte de adquisiciones como la de Inmac WStore en Francia. Desde el punto de vista orgánico el crecimiento de los ingresos alcanzó el 11,8 %.

Bechtle
Tel.: 91 364 02 34

La inversión en tecnología de las Administraciones Públicas sube un 7 % en 2019

La inversión en tecnología de las Administraciones Públicas en 2019 alcanzó los 3.375,29 millones de euros, lo que se traduce en un 7 % más que en el año anterior. Así se desprende del Barómetro de la Inversión TIC en las Administraciones Públicas en España, que ha sido realizado por AdjudicacionesTIC.

"El último trimestre del año fue espectacular, con importantes incrementos en todas las categorías, destacando la variación de hardware", ha afirmado Carlos Canitrot, director de AdjudicacionesTIC. La inversión en tecnología durante dicho período alcanzó los 1.023,79 millones de euros, lo que supone un 43,54 % más que en el tercer trimestre y un 30 % del total anual. Otras categorías que también han experimentado un crecimiento son "la inversión de servidores, con un crecimiento del 170 %, de sistemas de almacenamiento, con un crecimiento del 133 %: o los PC y portátiles, con un crecimiento del 107 %", ha explicado. Según los datos del estudio hubo un total de 13.328 adjudicaciones, las cuales estuvieron repartidas en 10.308 licitaciones y 3.020 contratos derivados de los acuerdos marco de la DGRCC. En el último trimestre de 2019 se publicaron las adjudicaciones de 4.793 contratos.

La Administración General del Estado fue la mayor inversora del año con 1.584,47 millones de euros, seguida de Cataluña con una cantidad total invertida de 633,79 millones de euros en 1.671 adjudicaciones. En tercera posición está Madrid, con 230.91 millones de euros invertidos en 951 contratos adjudicados.

En cuanto a los principales adjudicatorios fueron: Telefónica con 380 millones de euros (440 adjudicaciones). A continuación, Indra con 231 millones de euros en 267 contratos e IBM con 163 millones en 53 adjudicaciones. En lo referente a organismos inversores, la lista la encabeza el Centro de Telecomunicaciones y Tecnologías de la Información de la Generalitat de Cataluña, con una inversión superior a los 419 millones de euros en 51 contratos, seguido de la Dirección General de Racionalización y Centralización de la Contratación, con más de 185 millones de euros en 11 pliegos. En tercer lugar, la Gerencia de Informática de la Seguridad Social, con más de 121 millones de euros en 87 proyectos.

Adjudicaciones TIC
www.adjudicacionestic.com

AMETIC propone la creación de un consejo asesor para la transformación industrial

AMETIC ha anunciado que propondrá al Gobierno la creación de un consejo asesor para la reindustrialización y la transformación industrial para impulsar la recuperación económica. Este consejo tendría que estar formado por expertos en el sector industrial que participen en las distintas patronales industriales.

Dentro de esta iniciativa, AMETIC propone impulsar acciones y macroproyectos tractores en los que lleva años trabajando y que giran en torno a cuatro áreas: el sistema de salud, la movilidad en el ámbito urbano e interurbano, la industria agroalimentaria y el turismo.

La Administración Pública debería desempeñar un papel motor junto con el sector industrial, a través de planes, medidas legislativas e instrumentos de financiación adecuados para su desarrollo, así como con el impulso y buen uso de la compra pública.

AMETIC ofrece diferentes consideraciones para las áreas de la salud, la movilidad, el sector de la agroalimentación y el segmento turístico.

AMETIC
Tel.: 91 590 23 00

El Grupo Wallix lanza operaciones en España a través de Wallix Ibérica

El Grupo Wallix ha anunciado el lanzamiento de operaciones en España a través de su filial Wallix Ibérica. Esta acción está dentro del plan de expansión internacional, conocido como Plan Ambition 21. Para desarrollar este programa la compañía adquirió en 2019 dos empresas, Simarks en España y Trustelem en Francia. Además de la creación del centro de excelencia tecnológica en el país galo donde se desarrollan productos de última generación en software de ciberseguridad.

A partir de ahora los clientes españoles podrán disfrutar del catálogo de herramientas de ciberseguridad del que dispone el Grupo Wallix. El proveedor europeo está especializado en PAM con su solución Wallix Bastion y en desarrollar e implementar soluciones propias para la protección de las identidades, accesos y datos de sus clientes.

Wallix mantiene una sólida posición en el mercado europeo de la ciberseguridad con un claro objetivo en el horizonte: llegar a cubrir hasta el 80 % de este mercado en 2021. Actualmente, el proveedor proporciona herramientas de protección avanzadas así como soporte técnico permanente para cubrir los más de 1.000 clientes con los que cuenta en 88 países.

Según ha explicado Jean-Noël de Galzain, CEO de Wallix, "España es un mercado prioritario" porque las empresas españolas tienen como una de sus prioridades la ciberseguridad ya que "han visto cómo el número de ciberataques se multiplica año tras año, con un fuerte impacto en la reputación e incluso en la viabilidad de las empresas afectadas", ha comentado.

La propuesta tecnológica del proveedor es "apoyar a las empresas para alcanzar los niveles de protección adecuados en sus sistemas IT/OT, eliminado los riesgos asociados a los accesos privilegiados, robo de credenciales, exfiltración de datos, etc.", ha aclarado el directivo.

Wallix Ibérica comercializa sus productos y soluciones a través de una red de *partners*, a los que le une una estrecha relación de colaboración y a los que proporciona herramientas de gestión de clientes, apoyo de marketing, formación y una extensa biblioteca de información técnica y comercial.

El proveedor dispone de un portafolio con productos de última generación en protección PAM, como Wallix Bastion, y en EPM, como Wallix BestSafe. Todos los productos están integrados entre sí con el objetivo de ofrecer soluciones de protección escalables, perfectamente adaptables a cada negocio y transparentes para el funcionamiento del negocio.

"La aceleración de la digitalización y la generalización del acceso remoto están aumentando la superficie de ataque y deberían obligar a las compañías a protegerse mediante la implementación de soluciones de seguridad: gestión de identidades, autenticación, gestión de acceso y los derechos y privilegios de los usuarios", ha explicado Didier Lesteven, Wallix *executive vicepresident sales and marketing opertations for* DACH, España y Estados Unidos.

Wallis
www.wallix.com

TeamViewer ofrece su solución Pilot de manera gratuita para organizaciones médicas

TeamViewer Pilot, la solución para la asistencia remota con realidad aumentada de TeamViewer, estará disponible durante la pandemia del Covid-19 de manera gratuita para las organizaciones de salud de todo el mundo.

Los sanitarios pueden utilizar las conexiones individuales de TeamViewer Pilot para compartir la transmisión de vídeo interactiva y las anotaciones para resolver rápidamente los problemas cuando no pueden estar en el mismo lugar al mismo tiempo. Estas sesiones pondrá ser grabadas y compartidas con otros profesionales para explicar cómo resolver problemas similares.

TeamViewer Pilot podrá utilizarse para establecer distintas fórmulas de colaboración entre los equipos médicos a distancia. Por ejemplo, para explicar el uso de equipos o dispositivos del hospital, para formaciones o para la obtención de segundas opiniones.

TeamViewer
www.teamviewer.es

Espera alcanzar una facturación de 135 millones este año

"Nuestro plan es seguir creciendo en el segmento profesional"

Emilio Sánchez-Clemente, director general de **DMI**

DMI Computer lleva 30 años en el mercado de la distribución. Esta larga trayectoria le ha permitido asistir a los cambios y a la transformación del negocio del mayorista, que se ha convertido en una figura más global, capaz de atender a todos los actores del canal. Su experiencia, la diversificación de su negocio y su nueva apuesta por el ámbito profesional le han posicionado como uno de los mayoristas nacionales con una propuesta más completa tanto de productos como de servicios. Emilio Sánchez-Clemente, director general de DMI, confirma que el balance de estas tres décadas es positivo y confía en mantener sus planes de crecimiento para este año.

Rosa Martín

DMI celebra sus 30 años en el mercado, ¿Qué balance hacen de estas tres décadas?

El balance no puede ser nada más que positivo. Estar 30 años en un mercado tan competitivo es muy importante y bonito para todo el equipo que en algún momento ha formado parte del camino de DMI. Es un momento para sentirse muy orgulloso.

¿Cuáles han sido los hechos más destacados de su trayectoria?

En 30 años hay muchas cosas que han podido ser importantes. El primero fue fabricar clónicos, que marcó un camino. Otro fue en el año 2000, cuando adquirimos una estructura de otra compañía y nos permitió abrir cinco delegaciones y tener más capilaridad en el mercado. Crear una división de *retail*, poco tiempo después, también fue una decisión que ha tenido su trascendencia en el futuro. El cambio de nave marca un hito y lo que estamos haciendo ahora en el área de DMI Pro, que recordaremos como un buen hito en el futuro.

En este periodo, ¿cómo ha cambiado la figura del mayorista? ¿Qué características eran imprescindibles antes y cuáles son las más importantes ahora?

Al mayorista nacional antes se nos identificaba como un mayorista regional, focalizado en mercados de proximidad. Ahora somos mucho más globales. Tenemos un contacto más directo con el fabricante, que quiere que se dé un servicio más de boutique para atender a los clientes. Atendemos a todos los segmentos de clientes.

En el panorama actual, con muchos competidores en el mercado tecnológico, ¿Qué papel está desempeñando el mayorista

frente a otras figuras y por qué sigue siendo clave en la cadena de distribución?

El mayorista no deja de ser un enlace entre el fabricante y el cliente. Hace una labor logística, financiera y de prescripción a los clientes. España es un país de pymes, que está atendida por pequeños profesionales que están dando servicio a esas empresas a nivel tecnológico. Nosotros estamos atendiéndolos y nuestra figura es importante para dar este servicio, que es una parte muy importante de lo que es el mercado de las tecnologías en España; pero cada vez más somos más globales.

A su juicio, ¿continuará la concentración tanto en el canal mayorista como en la distribución?

Concentración no ha habido. Ha habido algunos movimientos, pero es imprescindible que haya concentración. Es un mercado de escalas y, sin duda, se necesitan figuras más grandes. Todavía no ha empezado, pero no tardará mucho en empezar.

¿Cómo cerró el año 2019 y cómo afrontan este año?

El año pasado crecimos por encima del 14 %, superamos la cifra de 125 millones. Fue un buen año. Planteábamos este año con un crecimiento parecido, moderado, pero queríamos estar por encima de 135 millones. El primer trimestre ha sido muy bueno, a pesar de los últimos 15 días, pero cuando miramos más allá, aunque mantenemos todos nuestros proyectos y planes, el coronavirus lo trastoca todo. Ahora es muy difícil ver más allá de una semana. Lo primero es que se resuelva la crisis sanitaria y ya llegará el tiempo de resolver la económica; pero seguimos manteniendo nuestros planes.

A lo largo de los años, DMI ha ido ampliando su negocio y diversificándolo desde el volumen hasta el valor con la división profesional o el servicio a las tiendas MR Micro. ¿Cómo se reparte su negocio en la actualidad? ¿Cuál es la línea prioritaria en este momento?

El negocio de *retail* supone un 25 %, la división de las tiendas que tenemos asociadas, MR Micro, está por encima del 10 %, la nueva división DMI Pro supone un 10 % y el resto es lo que llamaríamos *"breath"* que son pequeños negocios o cadenas de tiendas. Donde más esfuerzo estamos haciendo es en el desarrollo de DMI Pro.

Uno de los puntos fuertes de DMI es la automatización y mecanización de procesos en el apartado logístico. ¿Cómo está funcionado este apartado? ¿Tiene desarrollada toda la capacidad logística?

Está funcionando muy bien e incluso estamos dando servicios a terceros. Estamos consiguiendo un nivel de eficiencia que sin esa mecanización sería complicado alcanzar. Aún no lo tenemos desarrollado del todo. La automatización del *picking* es la parte que nos falta y la queremos tener lista para la campaña de final del año.

En el negocio tradicional, más enfocado al volumen, ¿cómo está funcionado el negocio? ¿Cuáles son los productos más vendidos?

Todo el primer trimestre ha funcionado muy bien. Estamos creciendo prácticamente en todas las áreas, aunque hemos notado un incremento muy importante en *computing* con el portátil, ya no solamente en el último mes por toda la situación, sino en los meses anteriores, desde el final del último trimestre del año pasado. Y tomando como referencia el mes de marzo casi hemos cuadriplicado las ventas.

> "El año pasado crecimos por encima del 14 %"

El negocio de ensamblaje de PC, ¿sigue siendo rentable?

Sigue siendo rentable; lo que permite el ensamblaje de equipos es una personalización que de otra manera no se tendría. Hay operaciones corporativas y otras que requieren unas especificaciones técnicas que no se consiguen en la oferta de los fabricantes tradicionales y así sí. Es un negocio que se mantiene estable en los últimos años y es un complemento más a lo que tenemos.

¿Cuántos equipos ensamblan al año?

Entre 12.000 y 15.000 ordenadores al año aproximadamente.

¿El equipo para *gaming* sigue creciendo?

El *gaming* ha venido para quedarse y sigue creciendo a buen ritmo. El ensamblaje de equipos permite hacer lo que el *gamer* necesita en ese momento. No es el gran volumen, pero cualitativamente tiene bastante importancia. Es un área de crecimiento.

DMI cuenta con la red de tiendas MR Micro, ¿cómo ha evolucionado la relación con las tiendas desde su creación?

Desde el origen hasta ahora ha cambiado muchísimo. El proyecto de MR Micro siempre fue un paraguas para nuestros clientes habituales frente a las cadenas de franquicias, que se estaban consolidando en ese momento. Se les ofreció una imagen conjunta y se les trasladó unas ofertas exclusivas de los fabricantes. Esto en esencia no ha cambiado; lo que sí que lo ha hecho es la tipología de clientes que componen MR Micro. Antes eran tiendas muy volcadas en el consumo y ahora son tiendas orientadas al servicio, que es donde estamos consiguiendo introducir el producto profesional que necesitan e intentando acompañarlas en esa estrategia.

¿Cuántas tienen en la actualidad? ¿Ha crecido la facturación que procede de las tiendas?

Tenemos más de 200 repartidas por toda la geografía nacional. La división MR Micro creció un 20 % aproximadamente. Estamos consiguiendo ese crecimiento porque hemos vendido los productos que nos estaban demandando para el segmento profesional. Esto, unido a lo que ya hacíamos, permite que consigamos estas cifras.

Hace un par de años creó una división especializada en el segmento profesional, ¿cómo ha evolucionado en este periodo?

La base ha sido tener una serie de productos que ya nos estaban demandando. En los últimos años hemos firmado solo para esta área con más de 25 fabricantes para tener una oferta competitiva. Otra fase ha sido detectar qué clientes estaban más en ese área, hacer formación y que entendieran que podíamos ayudarles a llegar a los proyectos que anteriormente no estaban llegando.

Dentro de esta división crearon el canal certificado de asesoramiento. ¿Qué tipo de ac-

ciones llevan a cabo con esta red de distribuidores?

Se están dando cursos en la central y en las delegaciones para que conozcan toda nuestra oferta y para que puedan estar preparados para dar un servicio.

Uno de los últimos acuerdos para esta división fue el que firmó con Toshiba Tec para la comercialización de sus soluciones para el punto de venta. ¿Cómo está funcionado esta alianza y qué objetivos quieren alcanzar?

Estamos muy contentos con nuestra alianza con Toshiba. Es uno de los líderes en el sector *retail* y Horeca. Estamos trabajando en proyectos importantes y se ha hecho una labor de prescripción para nuestros clientes que ya están atendiendo pequeños proyectos. Tenemos muchas expectativas puestas en este fabricante.

Estas soluciones forman parte de su oferta para el sector *retail* y Horeca. ¿Es uno de los verticales más destacados dentro de la división?

El sector Horeca es el que está más cerca de nuestros clientes; aunque hay otro vertical que está funcionando bien, que es el logístico. Ahí destacamos nuestro acuerdo con Zebra con el que estamos haciendo proyectos interesantes.

DMI cuenta con una zona para el *ecommerce* en su web. ¿Qué peso tiene en su negocio?

El 50 % de los pedidos llega a través de la web y creciendo. Cada vez es más habitual que sea así.

¿Qué tipo de servicios son los más demandados entre sus clientes?

Servicios financieros, logísticos y sobre todo nos están pidiendo formación. Ha sido una sorpresa muy agradable ver la demanda y las ganas que tienen de reciclarse y aprender de todo el entorno profesional.

La pandemia del Covid-19 ha obligado a tomar medidas para garantizar la continuidad el negocio. ¿Cómo están funcionando?

Desde el primer día el objetivo ha sido cuidar la salud de los empleados y de los clientes. Pasamos toda la plantilla a teletrabajo y ha funcionado fantásticamente. Y para las personas, que tienen que acudir de manera presencial en almacenes y servicio técnico, se han tomado las máximas medidas de seguridad para preservar su salud. Con respecto a los clientes, hicimos una campaña de promoción para que no se tuviesen que desplazar a recoger la mercancía, regalándoles los portes y llevando los productos a sus propios clientes. Esto también está funcionando bien.

> "El mayorista hace una labor logística, financiera y de prescripción a los clientes"

De cara a los próximos meses, ¿cuáles son sus planes?

El Covid-19 trastoca todo. Ahora mismo lo importante es que se acabe la crisis sanitaria y ver cómo salen de esto los clientes, que son muy importantes para nosotros. Nuestro plan es continuista, seguir creciendo en todo lo que tenga que ver con el segmento profesional. A nivel de gestión tenemos claro que queremos poner en marcha el *picking* automatizado y el servicio de web. No han cambiado los planes, la situación hará que haya cosas que se retrasen o que cambien algunas, pero no creo que nos vaya a cambiar mucho el objetivo final.

DMI
Tel.: 91 670 28 48

Durante el mes de marzo se incrementaron las ventas de herramientas para el trabajo en casa

El teletrabajo en la empresa española, ¿ha llegado para quedarse?

El teletrabajo ha sido la principal medida que, con urgencia, han tenido que implantar las empresas para continuar con su actividad, tras declararse el estado de alarma, el pasado mes de marzo, por la pandemia del Covid-19. Esta fórmula, que hasta ahora no era frecuente en las empresas, no solo ha permitido mantener los negocios abiertos sino que ha puesto de manifiesto la necesidad de cambiar la mentalidad y de transformar el puesto de trabajo que ya no está sujeto a una oficina física. Esta situación ha hecho que se pierda el miedo al trabajo en remoto y ha revelado sus ventajas sobre el medio ambiente y la conciliación familiar sin restar productividad, aunque el reto ahora es que permanezca en las empresas.

Rosa Martín

La fórmula de trabajo a distancia, que permite trabajar en cualquier lugar y evita los desplazamientos a la oficina, solo era una práctica habitual con una frecuencia de 1 ó 2 veces por semana para el 32 % de los trabajadores españoles, según se desprende del estudio "Teletrabajo: una solución puntual o el futuro de las empresas", elaborado por Citrix.

Este informe revela que el 34 % de los encuestados considera que es más productivo trabajando desde casa, un 32 % cree que lo es menos, y un 35 % siente que sus niveles de productividad son los mismos en la oficina y en casa.

Estos datos revelan que el trabajo en remoto ha producido un cambio muy rápido tanto en la empresa como en el profesional, que han tenido que adaptarse en un tiempo récord a una situación nueva para la que en muchos casos no estaban preparados.

A juicio de Santiago Campuzano, *Iberia regional director* de Citrix, la clave para una correcta respuesta al desafío que suponía cambiar de modelo de trabajo ha sido la existencia de un plan definido para ello dentro de la empresa. "Entre las grandes organizaciones, muchas de ellas tenían modelos ya preparados de continuidad donde, aún sin tener el teletrabajo implementado de forma generalizada, tenían estructuras y procesos preparados", comenta.

Esta preparación ha permitido que muchos de sus clientes como empresas energéticas, operadoras, financieras o aseguradoras tuvieran planes para continuar con su negocio. En el

caso de las que no tenían un plan establecido han tenido que buscar soluciones, aunque fueran más sencillas para poder teletrabajar.

En ambos casos, la opinión mayoritaria de los proveedores es que las empresas españolas han reaccionado de manera rápida para poder trabajar desde casa.

Alberto Fernández, director de desarrollo de negocio de TeamViewer en España, resalta que "en general, las compañías no estaban preparadas para afrontar un cambio tan radical en tan poco tiempo". Considera que no es lo mismo trabajar de manera puntual desde casa que diariamente y que lo haga toda la empresa a la vez. A pesar de estas dificultades, señala que si antes "el teletrabajo era más bien una moda, ahora es una obligación para que las empresas puedan seguir funcionando".

Esta necesidad ha exigido que las empresas españolas hagan un esfuerzo considerable para adaptar su modelo al teletrabajo como reflejan los índices que miden su implantación. Según Eurostat, antes de la crisis en España teletrabajaba el 4,3 % de los empleados, frente al 13,3 % de Finlandia. Este porcentaje nos sitúa por delante de Italia, pero nos deja por detrás de los países nórdicos e incluso Portugal (6,1 %). La media europea estaría en torno al 17 % con los países nórdicos a la cabeza, según datos de la OIT (Organización Internacional del Trabajo), lo que nos aleja de los países avanzados en este terreno.

> "Las compañías no estaban preparadas para afrontar un cambio tan radical en tan poco tiempo"

A pesar de esta situación, las grandes empresas y las *startups* con modelos digitales nativos ya tenían sistemas de trabajo remoto lo que ha permitido que "hayan podido extender esta fórmula al resto de los empleados, porque ya disponían de los canales y recursos digitales necesarios para implementarla", destaca Carolina Moreno, vicepresidenta de ventas de Liferay EMEA y directora general para el sur de Europa.

Alberto Sagredo Castro, *pre-sales engineer* de Snom Technology Iberia, cree que las herramientas tecnológicas para teletrajabar ya estaban disponibles, pero en muchos casos no se utilizaban. "La situación actual de confinamiento ha obligado a poner en práctica lo que teníamos al alcance de nuestra mano, pero que por nuestra cultura de "lo presencial", o bien apenas hacíamos uso de ellas o, incluso, las rehusábamos".

Esta necesidad y el uso de las herramientas ha supuesto un cambio en el modelo y se espera que impacte en los modelos productivos. "No todas las empresas estaban preparadas para pasar de un modelo plenamente presencial, a un modelo a distancia, pero esta situación va a hacer que muchas empresas se replanteen su anterior modelo productivo" señala Javier García Garzón, director de canal de HP.

Patricia Núñez, directora del canal comercial de Lenovo, explica que aunque las empresas más grandes están mejor preparada para afrontar esta crisis, las pymes y los emprendedores pueden readaptarse a los nuevos retos y adoptar "los nuevos entornos de trabajo de forma rápida".

Soluciones más demandadas

El auge del teletrabajo ha impulsado las ventas de las soluciones que hacen posible el trabajo en el hogar. Según datos de Context, en los primeros países europeos en los que se decretó el confinamiento como España e Italia se disparó la venta de equipos portátiles para las empresas durante el primer trimestre del año y, especialmente, en el mes de marzo. En nuestro país, el incremento registrado en esta categoría alcanzó el 143 %. Al mismo tiempo, se registró un incremento de las ventas de cámaras web, auriculares, soluciones para la administración de base de datos, virtualización y de las herramientas para el desarrollo y la seguridad.

Este crecimiento lo han notado la mayoría de proveedores. Samsung señala que las tabletas han jugado un papel muy destacado para que los niños pudieran seguir sus estudios en casa. David Alonso, director del negocio B2B de Samsung, señala que en el terreno de la empresa el reto principal es asegurar la productividad y pone como ejemplo su solución DeX. "Con Samsung DeX, cualquier habitación se puede transformar en una zona de trabajo, incluso cuando no tenemos un portátil. Tan sólo hay que conectar un *smartphone* o *tablet* directamente a un monitor y un teclado, y Samsung DeX se iniciará automáticamente como si fuera un PC".

Por su parte, Luis Casero, director de marketing y administración de ventas de Vertiv, resalta que su misión durante esta situación ha sido dar servicio y garantizar el funcionamiento de las infraestructuras porque "ahora es más es necesario mantener el seguimiento de los datos y de las personas conectadas".

Microsoft ha comprobado el incremento en sus plataformas *cloud* como Azure y sus herramientas de colaboración y productividad como es Microsoft 365 y Teams.

Las soluciones para videoconferencia que facilitan la comunicación de los empleados también han crecido en este periodo de confinamiento. Cisco ha comprobado que Webex ha superado los 300 millones de usuarios y los 14.000 millones de minutos en reuniones.

Ricoh también ha comprobado el crecimiento del uso de su solución para videoconferencia UCS Advanced. "En marzo España era el segundo país con mayor incremento de las llamadas en remoto después de Polonia, en el mes de abril ya somos los primeros en el uso de esta solución por delante de otros países europeos como Italia, Suecia o Polonia", destaca el director de marketing de Ricoh España y Portugal.

Las soluciones para la virtualización de aplicaciones en modo *on premise* o *cloud* han sido de las más demandadas de Citrix.

SentinelOne también ha visto cómo se ha incrementado la demanda de sus solución de protección del *endpoint;* mientras que TeamViewer ha comprobado cómo se han triplicado las conexiones a sus soluciones de acceso en horas de trabajo y cómo ha crecido el uso de su solución de realidad aumentada TeamViewer Pilot.

En VMware ha crecido la demanda de sus soluciones para facilitar la continuidad del negocio como VMware Cloud on AWS y VMware Cloud Solutions on Azure.

Positivo

A la hora de implantar el teletrabajo, los proveedores señalan la rapidez y la flexibilidad como lo más positivo del proceso de implantación del teletrabajo. Para Xavier Moreno, director de marketing de Ricoh España y Portugal, "el éxito para hacer frente a la imposición del teletrabajo ha dependido en gran medida del nivel de madurez digital de las empresas". Roberto Moral, director de arquitecturas en Cisco España, añade que en el lado de lo positivo también figura el esfuerzo efectuado por la Administración Pública.

VMware, como indica Margarita Sanz, directora de canal de esta compañía, considera que la adopción de las herramientas para el trabajo en remoto ha funcionado bien y ha permitido incrementar la productividad en esta situación. El papel que han jugado las personas también ha sido decisivo para adaptarse a esta situación. "Ha funcionado bien la reacción de los equipos, su entrega y su nivel de compromiso", apunta Tomás Font, *general manager* de Wolters Kluwer Tax & Accounting.

Carencias y retos

A pesar del esfuerzo por adaptarse a la nueva situación y ampliar sus recursos tecnológicos para implantar el teletrabajo, se han observado carencias en este proceso provocadas por la prisa al elegir soluciones sin tener en cuenta un aspecto tan importante como la seguridad. En este sentido, Ovanes Mikhaylov, *regional sales manager* de SentinelOne Iberia, avisa que por la urgencia en algunos casos los empleados han optado por utilizar sus dispositivos personales y este uso ha dejado desprotegida la información corporativa. "La información y otros recursos corporativos que antes se gestionaban en un terreno acotado y protegido por *firewalls*, soluciones de seguridad de correo electrónico y otras han pasado a administrarse en una ubicación alejada e independiente, carente en muchos casos de medidas básicas de protección como un antivirus actualizado", recalca.

Mantener la seguridad es uno de los retos que tienen las empresas en esta situación. "La protección de los usuarios debe reforzarse con cuatro soluciones clave: conexión VPN, mecanismos de verificación multi-factor, seguridad *cloud* y DNS y protección de cualquier dispositivo o terminal", aconseja el director de arquitecturas de Cisco España. Además, es de "suma importancia contar con una buena política de seguridad informática que blinde la organización", apunta el director de canal de HP.

> "Esta situación va a hacer que muchas empresas se replanteen su anterior modelo productivo"

Una opinión similar muestra Miguel Ángel Cervera, director de la unidad de negocio de *modern workplace* de Microsofft, quien apunta que "los CISO y los administradores de TI deben examinar con urgencia nuevos escenarios y vectores de amenazas a medida que sus organizaciones se convierten en "dis-

La Red pasa la prueba

El teletrabajo masivo ha puesto a prueba la capacidad de la Red en España. El uso intenso en los hogares para el trabajo y para el ocio ha supuesto un nuevo reto para los operadores de telecomunicaciones y los especialistas en conectividad.

Anselmo Trejo, director de marketing y comunicación de D-Link, resalta que "nos hemos enfrentado a un gran desafío, pero en términos generales no estamos notando grandes problemas".

Los datos del tráfico registrado dan una idea de la tensión que han tenido que soportar. Se ha registrado un incremento del 150 %, según datos de los operadores, y en los domicilios se han multiplicado los dispositivos conectados, pasando de cuatro de media a 12 o más. Al mismo tiempo, el *"prime time"* se ha alargado lo que ha obligado a algunas de la plataformas de contenidos a rebajar las definiciones.

Las llamadas de teléfonos móviles también han crecido un 50 % y el uso de los datos móviles un 25 %. El director de arquitecturas en Cisco España comenta que el vídeo es uno de los mayores responsables del incremento del tráfico IP. "Ya representa el 70 % del tráfico de Internet en España y en 2022 supondrá el 80 %".

En este contexto de uso intenso y masivo se ha notado la diferencia entre los entornos urbanos con despliegues de fibra y los rurales, aunque los especialistas destacan el buen trabajo realizado por los operadores regionales. En este sentido, Javier Gómez, director de Iberia y la zona del Mediterráneo de Cambium Networks, recalca que el papel de los operadores inalámbricos o WISP regionales "ha sido clave ya que han sido capaces de ofrecer un servicio de élite ante tal avalancha".

Javier Giménez, director general de Extreme Networks, cree que el buen comportamiento que ha tenido la Red ha sido posible por las inversiones en infraestructura que las grandes operadoras de telecomunicaciones han hecho en los últimos años.

Esta situación ha permitido ver la fortaleza de los proveedores de servicios que han sido muy rápidos para incrementar los recursos internos para ajustarse a la demanda, pero también ha dejado ver que la calidad ofertada no se ajustaba a lo contratado. Álvaro Ausín, director de ventas y canal de TP-Link, se muestra crítico al indicar que "la gran mayoría de los ISP, a pesar de años ofertando acceso a Internet de 300/600 y hasta 1000 mbps, no cumplen lo prometido".

A pesar de que los anchos de banda no sean los contratados, Gómez matiza que "un hogar conectado no requiere mas de 10 o máximo 15 Mbps para trabajar a la perfección. España está a la cabeza mundial en la oferta real de ancho de banda por servicio (105 Mbps de media), es decir, tenemos margen".

Ante esta situación todos han puesto en marcha medidas para ayudar a sus clientes y socios a enfrentarse a esta nueva situación.

D-Link ha detectado que muchos clientes no tenían en su red las medidas necesarias de seguridad, por lo que ha optado por reforzar todo lo relacionado con los productos y tecnologías de red necesarias para garantizar el acceso securizado remoto a la red local y a los servidores mediante VPN y *firewall*.

Extreme Networks ha lanzado una oferta específica y paquetizada, que Giménez califica como de "primeros auxilios" que permite a las empresas tener conectividad rápida y segura para las oficinas o entornos de trabajo remotos. A la vez, ha facilitado la adquisición de productos y ha puesto en marcha otras medidas de formación y certificación para sus *partners*.

TP-Link ha incrementado el soporte técnico y está ayudando a las pymes a incrementar sus recursos internos para asegurar los accesos a Internet.

Cisco también está poniendo diferentes recursos gratuitos para facilitar el teletrabajo en las empresas.

tribuidas" de un día para otro, con menos tiempo para hacer planes detallados o ejecutar pilotos".

Al mismo tiempo, las empresas tienen que cuidar otros recursos que están sometidos a un mayor estrés en este momento como las redes o la continuidad de los servicios.

Una modalidad para el futuro

El incremento del teletrabajo por obligación ha abierto el debate sobre si esta modalidad tendrá más peso en el futuro y se quedará en la empresa como una opción habitual. Los proveedores coinciden en señalar que este cambio ha servido para demostrar que se puede trabajar en cualquier lugar y acelerará la transformación del puesto de trabajo en las empresas. "Nada volverá a ser como era. El teletrabajo existe desde hace años, aunque muchas organizaciones no habían dado un paso firme para implantarlo. El Covid-19 ha forzado esa decisión, no ha dado otra opción, y ha puesto de manifiesto que para muchos negocios es totalmente viable y mucho más eficiente, ahorrando viajes y tiempos de desplazamientos", explica Tomás Font, de Wolters Kluwer.

Una opinión similar mantiene García Garzón, de HP, quien explica que esta conyuntura es una oportunidad para las empresas que eran reacias a esta fórmula. "Supondrá un antes y un después especialmente para las pequeñas y medianas empresas que deberán afrontar una digitalización completa en su negocio para poder sobrevivir en la economía actual".

"Ha funcionado bien la reacción de los equipos, su entrega y su nivel de compromiso"

El director de marketing de Ricoh de España y Portugal cree que ya no hay marcha atrás, aunque matiza que para que tenga continuidad es totalmente necesario que las empresas gestionen la adopción de esta nueva forma de trabajar y la digitalización que conlleva. Esta es, sin duda, la gran asignatura pendiente de cara al futuro".

El aprendizaje de los empleados de esta situación y su capacidad de adaptación a esta fórmula será una de las ventajas que pueden aprovechar los empresarios para que sea más fácil teletrabajar. Carolina Moreno, de Liferay, cree que"las empresas que han implementado este modelo con mucha probabilidad, querrán y podrán aprovecharlo en un futuro próximo, cuando esta situación llegue a su fin".

Alberto Sagredo, de Snom, considera que para que se generalice esta opción será necesario un "cambio de mentalidad por parte del empresario, y que a partir de ahora considere que tenerte delante, no significa que estés trabajando a pleno rendimiento".

Margarita Sanz, de VMware, cree que esta situación permite acabar con los miedos al teletrabajo por parte de algunas empresas y se consolidará por las ventajas medioambientales que aporta "y, ademas, las empresas que opten por este cambio lograrán captar y retener talento".

Los profesionales también apuestan por el teletrabajo como una opción habitual, como se refleja en la encuesta de Citrix, que revela que el 71 % de los encuestados cree que esta fórmula será más frecuente. El responsable de esta compañía añade que "hay que entender que el trabajo es lo que se hace, no dónde se hace".

Transformación del espacio de trabajo

La transformación de los espacios de trabajo implican una serie de fases y de condiciones para que el funcionamiento sea óptimo. Liferay apunta cuatro fases en este proceso: intranets tradicionales, intranets avanzadas, espacios de trabajo digital básicos y espacios de trabajo digital avanzados.

En nuestro país, la mayor parte de las empresas está en la fase de Intranets avanzadas, lo que significa que disponen de herramientas que facilitan la colaboración departamental y entre departamentos a través de bases de conocimiento, *Blogs* y gestión de documentos. Los empleados no realizan todo su trabajo en la intranet, pero sí utilizan su funcionalidad para colaborar.

Carolina Moreno, de Liferay, señala que para avanzar habría que disponer de soluciones que aporten capacidades de integración para unificar las herramientas digitales a través de una única capa para que la plantilla trabaje de forma cohesionada. Esto ayudaría a dar el paso para habilitar verdaderos espacios de trabajo digital.

Junto a este aspecto, también es necesario que se den otras condiciones para que sea efectivo el teletrabajo. Patricia Núñez, de Lenovo, señala que "son muchas las condiciones que han de verificarse para que el entorno sea satisfactorio para el teletrabajo. Y no solo las tecnológicas; también me refiero a condiciones ambientales, ergonómicas y emocionales que permitan al trabajador en remoto lograr un buen desempeño".

En cuanto a los beneficios, García Garzón, de HP, explica que "el hecho de que una persona se libere del tiempo invertido en los desplazamientos diarios y del encorsetamiento del puesto físico puede disparar su creatividad y eficiencia y contagiar su motivación al resto del equipo".

Más del 90 % del negocio de valor de V-Valley Vinzeo procede de HPE

HPE y V-Valley Vinzeo: tándem de canal

HPE es el pilar que sustenta, casi en exclusividad, la oferta de V-Valley Vinzeo. Una marca que le ha convertido en su mayorista de referencia tras más de dos décadas de una estrecha relación que ha evolucionado al ritmo que lo hacía tanto el mercado como el propio fabricante. Ahora, con la oferta de HPE perfectamente definida hacía 3 áreas (el desarrollo de la *cloud* híbrida, el *edge* y los servicios bajo un modelo gestionado), el objetivo del mayorista no ha variado un ápice: seguir trasladando al canal la innovación de la marca, aportando el soporte y la formación necesaria para asegurar su adecuada implantación.

Marilés de Pedro

Rafael Pestaña, director del área de valor de V-Valley Vinzeo, incide en que la relación está basada en la profesionalidad. "Se trata de aportar un valor a nuestros clientes, los distribuidores, que complemente al fabricante y seguir trabajando en mantener una confianza mutua que nos permita desarrollar pilotos e iniciativas de manera conjunta".

No es muy habitual observar en el mercado actual una relación en la que un mayorista hace reposar la mayor parte de su negocio en un único fabricante (en el caso de V-Valley Vinzeo el porcentaje supera el 90 %). La particular apuesta, a juicio de Pestaña, no entraña ningún riesgo. "Nos permite estar muy cerca del fabricante y enfocar al 100 % nuestros esfuerzos hacia el canal con HPE", explica. "No se duda a la hora de recomendar la oferta".

El equipo consagrado a HPE, del que forman parte 25 personas, está compuesto por *business developer managers*, técnicos de preventa y de postventa (capaces de desarrollar proyectos fuera de España de la mano del *partner* que lo lidere), profesionales de marketing y personas centradas en operaciones. Es el único mayorista que dispone de un centro de soluciones con toda la tecnología de HPE para su uso por parte del canal, además ofrece servicios en laboratorio, como es el caso de integración, masterización o serigrafiado, entre otros.

La financiación al canal es clave. Para ayudarle a poner en marcha sus proyectos, el distribuidor puede solicitar apoyo a través de HP Financial Services o bien acudir a los servicios financieros de V-Valley Vinzeo.

Junto a HPE, el mayorista trabaja con fabricantes complementarios, como es el caso de Microsoft, con el que está desarrollando proyectos vinculados con Azure. Además, dentro de la estructura de V-Valley, existe una potente división de seguridad, integrada por más de 20 personas, así como un área de servicios *cloud* enfocados al canal.

De Partner Ready a HPE Next

La estrategia de canal de la marca reposa en su programa Partner Ready. Se trata, como explica Pestaña, de un programa flexible que permite a los *partners* registrarse, certificarse y especializarse en el segmento que más se ajuste a su perfil de negocio: soluciones, tecnologías o servicios.

Cuenta con el Partner Ready Portal, desde el que es posible acceder a las herramientas que componen todo el ciclo de ventas: formación, marketing, *pricing*, configuradores, precios especiales, *deals*, servicios, *orders*, compensación, programas de demo, etc.

En el terreno de la formación, además del portal SEISMIC, donde se recoge información de producto, especialmente útil es el programa *Continuing Learning* que permite, de manera sencilla, orientar e incentivar a los distribuidores para actualizar su conocimiento de las soluciones y servicios de la marca. V-Valley Vinzeo, además, pone a disposición de sus clientes un centro Pearson para completar su formación en todo aquello que requieran.

A finales de 2019, HPE introdujo algunas novedades en el programa que han permitido agilizar el proceso de acceso y registro al programa *("On boarding")* de los distribuidores que además es posible llevar a cabo a través de los mayoristas oficiales de HPE.

También se ha mejorado el programa de *"Deal registration"*, lo que aporta una mayor protección para los *partners* y sus negocios; y el acceso a equipamientos para llevar a cabo pruebas de concepto (POC) y demostraciones. En este último apartado, HPE ha facilitado a V-Valley Vinzeo la única cabina de almacenamiento híbrida (Primera) que hay disponible en el mercado español.

Esta actualización es una antesala para el nuevo programa de canal que la marca está definiendo, HPE Next. HPE está realizando test con los mayoristas, para implementar nuevos procesos comerciales, políticas y capacidades de TI que transformarán la experiencia que nos brinda HPE al canal.

V-Valley Vinzeo
Tel.: 91 490 46 55

¿Quieres conocer qué te ofrece este tándem?

Entra y conoce sus últimas promociones

La impresión 3D, al servicio de la sanidad

¿Cómo reinventarse para luchar contra el Covid-19?

La crisis sanitaria a la que se enfrenta el planeta ha obligado a muchas compañías de impresoras 3D a reorientar su estrategia. Han dejado a un lado las ventas de dispositivos y se han centrado en la producción de suministros sanitarios, tan necesarios para ayudar a la lucha contra el Covid-19. Así se desprende de los últimos datos publicados por Context.

Olga Romero

Según el análisis de la consultora los envíos de impresoras durante el primer trimestre han decrecido un 11 % en lo que refiere a los dispositivos personales. También experimentaron retrocesos los dispositivos de diseño (un 22 %) y las máquinas industriales (un 23 %). La única categoría que ha cerrado en positivo este período es la profesional, que creció un 26 %.

A medida que la pandemia se controle y las economías vuelvan a la normalidad, existe un gran potencial para el mercado de impresoras 3D. Potencial que está siendo demostrado durante esta crisis sanitaria, en la que gracias a las impresoras 3D se ha podido responder de manera inmediata a las necesidades del sector sanitario. Numerosas empresas y colectivos han puesto en marcha diferentes iniciativas para intentar contribuir en la lucha contra la pandemia.

Empresas tecnológicas

HP, con la colaboración de su comunidad de fabricantes digitales, ha puesto en marcha toda su maquinaria de impresión 3D para luchar contra el Covid-19. El objetivo de esta iniciativa es conseguir dotar a todos los hospitales del mundo de unas piezas médicas impresas en 3D que cumplan con los estándares de calidad y seguridad. Las primeras aplicaciones que han empezado a validar y producir son: abridores de puerta con manos libres, ajustadores de mascarillas y protecciones faciales. Asimismo, la compañía ha colaborado con el Hospital Príncipe de Asturias, ubicado en Alcalá de Henares (Madrid), en la fabricación de un circuito respiratorio con el cual

se mejora la oxigenación de los pacientes con coronavirus. Se trata de una pieza clave que permite la unión de una alargadera de oxígeno, una mascarilla de aerosol, una bolsa de reservorio y un filtro antibacteriano con una válvula PEEP.

Otra de las compañías que ha querido poner su granito de arena ha sido Ticnova. Varias tiendas gestionadas por el distribuidor están fabricando viseras sanitarias homologadas gracias a sus impresoras 3D. Para apoyar la iniciativa la compañía esta ofreciendo a las tiendas involucradas bobinas de filamento PLA gratuitamente. Tal es el compromiso que algunos responsables se han llevado las impresoras a casa para conseguir mayor nivel de producción.

Sector de la automoción

En la lucha contra el Covid-19 el sector del automóvil no se ha querido quedar atrás y han estado al píe del cañón colaborando. Algunas empresas han llegado a reinventar su cadena de fabricación, como es el caso de la española SEAT. En la fábrica de la compañía durante unas semanas no se han producido coches, sino respiradores de emergencia a partir de la adaptación del motor de los limpiaparabrisas.

El dispositivo, denominado OxyGEN, ha sido autorizado por la Agencia Española de Medicamentos y Productos Sanitarios. La producción de este respirador de emergencia se ha realizado en la línea de montaje del SEAT León y cuenta con más de 80 componentes electrónicos y mecánicos. Además, pasa un exhaustivo control de calidad con esterilización de luz ultravioleta.

En el proceso de industrialización, liderado por SEAT, han colaborado otras entidades como Protofy, OxyGEN, HP, las fuerzas y cuerpos de seguridad del Estado, la Universidad de Barcelona o varios centros hospitalarios, entre muchos otros.

En estos momentos SEAT también está trabajando y analizando la viabilidad de otros proyectos que la compañía espera comunicar una vez que hayan pasado todas las pruebas sanitarias y se obtenga la autorización por parte de las autoridades correspondientes. De esta manera el fabricante muestra su firme compromiso para ayudar tanto al sistema sanitario como a sus profesionales.

Renault también ha querido contribuir a la lucha contra el Covid-19 y ha fabricado pantallas de protección. Esta acción ha sido posible gracias a más de 160 empleados de la compañía que han puesto a trabajar sus impresoras 3D particulares, pero también las que Renault tiene en sus laboratorios de Palencia, Valladolid y Sevilla. Los trabajadores han estado fabricando estas máscaras las 24 horas del día y en un mes han conseguido entregar 50.000 en hospitales, residencias de mayores, supermercados, farmacias, protección civil y policía de una veintena de localidades.

Coronavirus Makers

Coronavirus Makers es una iniciativa ciudadana, organizada por las Comunidades Autónomas, que está formada por voluntarios y particulares que fabrican material de protección en sus casas mediante impresoras 3D. Esta acción solidaria arrancó como un pequeño grupo de voluntarios comunicados a través de Telegram. Actualmente reúne a más de 16.000 usuarios registrados con perfiles muy variados, como sanitarios, ingenieros, profesionales de la logística, comunicadores, universidades y muchas otras iniciativas públicas y privadas, siempre sin ánimo de lucro.

A principios de abril la estructura de Coronavirus Makers había conseguido fabricar más de 350.000 pantallas de protección, las cuales han sido repartidas por hospitales y centros sanitarios de toda España. Actualmente, los voluntarios de esta iniciativa siguen trabajando para desarrollar nuevos dispositivos de protección y mejorar los modelos ya existentes. Pero también están elaborando un modelo de respiradores electromecánicos y mantienen contacto continuo con los profesionales médicos para estudiar la fabricación de otros dispositivos útiles en estos momentos y que se puedan llevar a cabo con impresoras 3D.

El mayorista establece un protocolo para asegurar la salud de sus empleados

#EsprinetNoPara: el mayorista mantiene su actividad, blindando a su plantilla frente al Covid-19

Preservar, por encima de todo, la salud de su plantilla, asegurar la recepción de las entregas y mantener la actividad con los clientes. Esos fueron los tres pilares en los que Esprinet ha hecho reposar su protocolo de actuación tras las medidas que el Gobierno adoptó para detener la expansión de la pandemia del Covid-19. Luis Bartolo, responsable de logística del mayorista, recuerda que el Grupo, cuya sede central está en la italiana región de Lombardía, se anticipó, incluso, al Decreto Ley del Gobierno para hacer frente al Covid-19. "El 8 de marzo ya se estableció un protocolo de prevención interno para toda la compañía".

Marilés de Pedro

La seguridad de los empleados ha sido el pilar fundamental. La compañía también se anticipó con la compra de material de protección individual, "necesario para poder garantizar el trabajo y la seguridad de los empleados". Una medida vital, más cuando unos días después del Decreto Ley del 14 de marzo, el sector TIC fue declarado esencial para mantener la actividad económica. "Gracias al departamento de servicios generales de Esprinet, se adquirieron EPI, mascarillas y guantes; y se distribuyó gel hidroalcohólico, instalándose dispensadores en toda la empresa", explica. La compañía estableció un protocolo de seguridad interno e insistió en el cumplimiento de todos los protocolos marcados por las autoridades sanitarias en relación a la distancia de seguridad, la higiene, las medidas sanitarias o la desinfección continua de las instalaciones.

Un completo protocolo, como explica Bartolo, que se ha completado con un abanico de medidas complementarias que incluye información constante, ayudas en los desplazamientos, flexibilización de horarios, turnos o vacaciones, etc. "Nos hemos puesto por completo a disposición de nuestros trabajadores".

El mayorista, además, ha decidido conceder una gratificación económica al personal de almacén, por el esfuerzo que ha llevado a cabo en estas complicadas semanas. "Entendieron que éramos, y somos, una empresa esencial", remarca Bartolo.

Mantenimiento de la actividad

La actividad, preservada la salud de los empleados, se ha mantenido y Esprinet ha garantizado tanto la recepción de las soluciones de sus fabricantes como la entrega a sus clientes. "No se ha parado la venta de ningún tipo de material", asegura. Evidentemente, la mayor demanda de todas las soluciones relacionadas con el teletrabajo (portátiles, monitores, las impresoras, teclados, ratones, consumibles, etc.) ha crecido de manera desorbitada, lo que ha provocado alguna rotura de *stock*, posteriormente subsanada.

Futuro

De cara a las próximas semanas, la compañía va a mantener la misma escrupulosa seguridad, incluyendo la instalación de termógrafos a la entrada de todas las entradas de la empresa. "Estamos perfilando un protocolo de seguridad muy exhaustivo", adelanta. "Está claro que estamos viviendo un cambio a nivel mundial y que tenemos que adaptarnos a una nueva sociedad y a los nuevos lugares de trabajo".

Esprinet
Tel.: 902 201 146

Acceda al vídeo desde aquí

Los *partners* tienen la oportunidad de disfrutar de ingresos recurrentes con este producto

Nvoice para Microsoft Teams de NFON mejora la comunicación de las empresas

Nvoice para Microsoft Teams es una solución del catálogo de soluciones prémium de NFON, que surge de la integración de Cloudya, el sistema de telefonía en la nube de la compañía, con la herramienta de colaboración de Microsoft. Esta combinación permite mejorar la comunicación de la empresa, tanto interna como externa, con *partners* y clientes. Entre sus ventajas figura el ahorro de costes, la mejora de la productividad, el poder disfrutar de las ventajas de la centralita en la nube en cualquier lugar, y la flexibilidad al comercializarse por pago por uso. Claudio Morán, director de operaciones de NFON, subraya que es un producto atractivo para el canal por la base instalada de Microsoft Teams, la facilidad de implantación y su rentabilidad.

Rosa Martín

Claudio Morán, director de operaciones de **NFON**

En la transformación del puesto de trabajo y la digitalización de la empresa juegan un papel fundamental las comunicaciones unificadas por la mejora de la productividad que proporcionan. Este peso queda reflejado en los últimos datos de IDC que señalan que, este año, el 50 % de las herramientas para las comunicaciones unificadas y la colaboración estarán basadas en la nube y prevé que crezcan alrededor del 3 % hasta 2021.

NFON aporta a este proceso de transformación digital su sistema de telefonía en la nube para empresas, denominado Cloudya, que permite que los usuarios puedan hacer negocios en cualquier lugar ya que puede estar instalado tanto en dispositivos fijos como en móviles y ofrece "calidad, robustez y fiabilidad *"made in Germany"* para que las comunicaciones estén siempre disponibles", según resalta Morán.

Integración con Microsoft Teams

Este sistema se ha integrado con Microsoft Teams dando como fruto de esta unión a Nvoice para Microsoft Teams, un producto que incrementa la capacidad de colaboración de la solución de Microsoft al facilitar la emisión y recepción de llamadas entre los empleados de la organización y los colaboradores externos, tanto usuarios de Microsoft Teams como con los que no tienen esta herramienta.

Los usuarios pueden disfrutar de todos los beneficios que ofrece Cloudya como llamadas salientes, colas, IVR, controles de tiempo, etc., desde el dispositivo que tiene instalado Microsoft Teams. Además, la solución garantiza la seguridad de las comunicaciones con la robustez de la arquitectura de NFON, que cumple todos los estándares de calidad. A la vez, según recalca Morán, la conexión entre la centralita y la solución de Microsoft se hace de forma encriptada usando TLS.

Acceda al vídeo desde aquí

Nvoice para Microsoft Teams, la solución de NFON para enriquecer la colaboración en la empresa

Ventajas para el canal

Para los *partners* del canal de NFON este producto les ofrece diversas ventajas como el acceso a un mercado muy extenso por el nivel de penetración de Microsoft Teams. Al mismo tiempo, al ser una solución cuya arquitectura está en la nube y comercializarse bajo un modelo de suscripción, puede optar a ingresos recurrentes.

Y desde el punto de vista de la implantación no es necesario contar con la certificación de Microsoft, lo que permite que esté disponible para cualquier *partner* de la red de NFON.

Esta solución es rentable para el canal y pone en sus manos un producto que ahorra costes a las empresas, que puede convivir con otros sistemas y les asegura su productividad.

Morán también resalta que sus socios del canal tienen la garantía de que es una solución que utilizan más de 4.000 usuarios, lo que hace que esté "perfectamente probada".

NFON
Tel.: 91 061 66 00

Crece la concienciación de las empresas en torno a la protección de sus datos

El *backup*: blindarse frente al *ransomware* en la era del Covid-19

Aunque no han cambiado sustancialmente sus técnicas, los *hackers* han aprovechado la expansión de la pandemia del Covid-19 para intensificar sus ataques de *ransomware*. El despliegue masivo del teletrabajo y el aumento del consumo de aplicaciones y servicios en la nube, en muchos casos sin una adecuada política de protección, expandió, como el fuego, la superficie de ataque, lo que ha dejado al descubierto las carencias de las empresas españolas en el ámbito del *backup*. Sin embargo, las principales empresas que ofrecen este servicio reconocen que ha aumentado la concienciación.

Marilés de Pedro

Antes del dramático mes de marzo, los ataques de *ransomware* ya habían aumentado un 12 % en el mes de febrero. Según el estudio Cyber Protect, que Acronis realiza de forma periódica, en el mes de marzo el 37% de las empresas españolas se mostraba muy preocupada por el riesgo del *ransomware* y el 43 % temía una violación de datos. Marzo y abril han detectado un enorme incremento de los ciberataques relacionados con el *phishing*, el *ransomware* y los *criptolocker*. Los ciberdelincuentes han utilizado como gancho el Covid 19 para conseguir el éxito de sus ataques.

"Los ficheros de *backup*, estén donde estén, son objetivo primordial de los atacantes"

El auge del teletrabajo, provocado por las medidas de confinamiento adoptadas para detener la

pandemia, exigió un despliegue de ordenadores portátiles y equipos de sobremesa corporativos en los hogares. Unos dispositivos, a los que había que dotar de una seguridad adecuada, en la que el *backup* debía ser una pieza esencial. "Un *backup* fácil, sencillo, sin intervención del empleado y que le permitiera trabajar con la garantía de recuperar toda la información si fuese necesario", explica José Manuel Petisco, director general de Veritas en España y Portugal.

Este despliegue masivo del teletrabajo ha estado acompañado de un uso intensivo de las herramientas de comunicación por parte de los trabajadores. Muchos de ellos, además, era la primera vez que hacían uso de ellas en un contexto profesional. "Algunas de estas herramientas de colaboración se han convertido en objetivos principales para los *hackers*, que intentan desplegar sus ataques de *ransomware*, tanto en las infraestructuras tecnológicas de las empresas como en los dispositivos de los usuarios", alerta Petisco.

Más usuarios conectados a la red, con un mayor tiempo de exposición y un uso intensivo de herramientas y equipos que no siempre exhibían adecuadas medidas de protección. Un panorama que se erigía en la tormenta perfecta para el despliegue de *ransomware*. "Este tipo de ataques es capaz de encriptar los discos remotos, los discos en la nube, los discos extraíbles y los *pendrives*. Los ficheros de *backup*, estén donde estén, son objetivo primordial de los atacantes", alerta José Manuel Arnaiz, CEO de Loozend. "Es imperativo disponer de una herramienta que impida totalmente el borrado de los ficheros históricos y, sin embargo, la mayoría sí lo permite", recomienda.

Unos ataques de *ransomware* que no conocen límites, ni sectores de actividad. "Incluso los hospitales están siendo víctimas de este tipo de ataques", recuerda Eulalia Flo, directora general de Commvault en España y Portugal. "No sólo se usa el *ransomware* para cifrar archivos, sino que se están pidiendo rescates para no desvelar datos confidenciales que han sido robados". Flo también alerta de otros problemas que se están observando, no ya de vulnerabilidades, sino de mala configuración por parte de los usuarios. "Las plataformas de videoconferencia, por ejemplo, están siendo configuradas de forma incorrecta, lo que está permitiendo que personas ajenas a las organizaciones puedan entrar en reuniones privadas y lanzar ataques de *phishing* o de *ransomware*". El mayor problema en todos estos casos "es que una gran parte de las organizaciones no tiene un plan de recuperación ante desastres. Por tanto, si son víctimas de un robo de datos o de un ataque de *ransomware*, no tienen forma de recuperarse cuando lo necesitan".

> "No sólo se usa el *ransomware* para cifrar archivos, sino que se están pidiendo rescates para no desvelar datos confidenciales que han sido robados"

¿Se hace bien el *backup*?

Uno de los principales problemas es que las empresas carecen, en muchos casos, de una verdadera estrategia de gestión y protección a lo largo del ciclo de vida del dato. "Algunas compañías siguen haciendo *backup* de los distintos silos de almacenamiento", alerta Eulalia Flo. La explosión del teletrabajo ha dejado en evidencia las carencias que existen en la protección de los puestos de trabajo. Aunque, como recuerda la máxima responsable de Commvault, los datos críticos deberían de estar en un repositorio corporativo y usarse escritorios virtuales, "la realidad es que muchos empleados trabajan en local y guardan datos críticos para la organización en sus propios dispositivos, lo que resulta muy peligroso ante un ataque de *ransomware*".

Algunas empresas cuentan con políticas de *backup* incompletas, que no incluyen una copia externalizada, como explica Javier Miquel, director general de Mast Storage. "No pueden acceder físicamente a su copia en local", insiste. Unas carencias que se hacen mucho más visibles en la actualidad, por el riesgo que supone el aumento del teletrabajo con conexiones poco o nada seguras, y porque los ataques de *ransomware* siguen creciendo cada día. "Aún hay empresas que no externalizan, o lo hacen con servicios que no están pensados para ello, con los riesgos que eso supone. Además, pocas empresas verifican periódicamente si se están haciendo bien las copias, y si los datos copiados son válidos y restaurables", completa.

Los ciberdelincuentes siguen haciendo uso del "tradicional" *phishing* como el método preferido para lanzar sus ataques de *ransomware*. Si lo hacen a través del correo electrónico, resulta más "sencillo" para el usuario comprobar la dirección antes de abrir un enlace, sin embargo, en los servicios de mensajería instantánea no se espera una intervención maliciosa y, como consecuencia, es más fácil que un *hacker* se haga pasar por alguien que no es. "En estos tiempos de confinamiento y teletrabajo un clic equivocado puede costarle a una compañía miles e, incluso, millones de euros", alerta José Manuel Petisco.

A su juicio, las soluciones de *backup* y de *appliances* específicos con capacidades de bastionado "deben ser prioridad".

Restringir la protección a únicamente la información de los servidores es otro problema recurrente. "Las tecnologías tradicionales de *backup* son muy poco prácticas y costosas para proteger los PC individuales", cree José Manuel Arnaiz. "Sin embargo, es evidente que muchos de los usuarios siguen teniendo información relevante en sus discos locales", reconoce. "Es injusto culparles por ello; por lo que es mucho mejor seleccionar tecnologías más modernas que den cobertura a esta información. Es el caso, por ejemplo, de certificados digitales, ficheros grandes, temporales de Office, la papelera de reciclaje, configuraciones, favoritos..., por no mencionar el software y las licencias. Por tanto, es necesario proteger esa información que está ubicada en los equipos de los usuarios".

> "Aún hay empresas que no externalizan, o lo hacen con servicios que no están pensados para ello, con los riesgos que eso supone"

¿La mejor ley para aplicar un *backup*? La que siempre ha regido el mercado (3-2-1): las empresas deben contar con tres copias de sus datos, dos de las cuales están en diferentes medios de almacenamiento y la tercera debe estar ubicada en un repositorio externo.

Javier Miquel insiste, de cualquier modo, que no se trata solo de comprar un determinado software. "Es básico entender la problemática del *backup* y planificar una estrategia que defina la manera de llevar a cabo esta tarea", insiste. "La pregunta clave que debe hacerse la empresa es qué plan de contingencia tiene para proteger su *backup*. Tan importante es la metodología del *backup* como la tecnología". Una filosofía que debe incluir un análisis del *backup* y de las necesidades del cliente. "Hay que planificar una estrategia en la que se definan los plazos para hacer la copia, los dispositivos y las máquinas virtuales objeto de la misma, etc.".

La subida a la nube

Lógicamente, la nube no es ajena a este panorama. Se calcula que el negocio *cloud* se habrá triplicado en 2023 y en 2019 alcanzó un crecimiento de más de un 25 %. "Se está evolucionando desde las licencias tradicionales a una tecnología basada en nube", recuerda Alessandro Perotti, *channel manager* para Italia e Iberia de Acronis. "La copia de seguridad de datos es una pieza importante en la estrategia general para proteger todos los aspectos de los datos, aplicaciones y sistemas en cuanto a seguridad, accesibilidad, privacidad, autenticidad y seguridad (SAPAS)".

La nube es uno de los principales impulsores de la aceleración de los negocios digitales modernos y a medida que aumenta la dependencia hacia los entornos *cloud* se requiere que las organizaciones empleen estrategias de gestión y protección de datos que sean sólidas, que estén de acuerdo a las diferentes regulaciones y que a su vez sean lo suficientemente flexibles para agilizar la continua transformación, al tiempo que mitigan los riesgos por la posible pérdida de esa información o incumplimiento regulatorio. "Sin embargo, son muchas las empresas a las que el Covid-19 les ha pillado de improviso en este aspecto", alerta Petisco. "En las últimas semanas se ha realizado un gran despliegue para ayudar a las empresas a poder adaptarse a los entornos *cloud* y, por tanto, a la necesidad de realización de *backups* de las cargas de trabajo que realizan en las diferentes nubes y sus

servicios, con el fin de proteger toda la información que tienen en estos entornos".

Se trata, como apunta José Manuel Arnaiz, de protegerse, entre otras variantes de ataques, de los *ransomcloud*. "Un concepto nuevo, pero desgraciadamente muy real, que atacan directamente la información en la nube, encriptándola, y pidiendo un rescate", explica. La nube, expone, no es tan segura como mucha gente piensa. "Lo ideal en un caso de uso exhaustivo de la nube es sincronizar en local, y proteger en otro sitio también la información local, de manera que haya siempre las tres copias", insiste.

¿Más concienciación?

Los fabricantes, a pesar de esta complicada situación, reconocen que ha aumentado la concienciación en las empresas. "Esta crisis ha sacado a la luz la necesidad de una tecnología fiable", apunta Perotti. "La copia de seguridad ya no solo es un valor añadido, sino una clara necesidad de seguir siendo relevante en el negocio. Más que sólo respaldo, la protección cibernética es como la quinta necesidad humana esencial después del aire, la comida, el sueño y el refugio".

Perotti explica que en este periodo muchas empresas han migrado temporalmente sus servidores a servicios *cloud* para poder seguir dando servicio a sus clientes o para permitir que sus trabajadores pudieran seguir trabajando, lo que va a permitir que "las empresas que todavía estaban reticentes, prueben esta tecnología, y vean que sus datos están seguros en esos almacenamientos *cloud*. Tras esto, es obligatorio el *backup*, por lo que se incrementarán las ventas en este tipo de producto".

Se trata, como apunta Javier Miquel, no solo de *backup* y de protección de datos, sino de continuidad de negocio. "Tras un ataque de *ransomware*, el coste que supone recuperar los datos es, como mínimo, de 1 o 2 bitcoins, lo que significa entre 6.000 y 12.000 euros", alerta.

"Sin embargo, puede ser muy superior. Conocemos empresas a las que se les ha pedido 200.000 euros de rescate", desvela. Su esperanza es que aumente la concienciación de la necesidad de realizar un *backup* con garantías de restauración.

La incorrecta sensación de seguridad de las empresas es otro problema que debe mejorar. "Muchas organizaciones piensan que están preparadas para hacer frente a una crisis, pero la verdad es que no lo están. Y no lo saben porque no han hecho las pruebas necesarias", alerta Eulalia Flo.

Incrementar la resiliencia y la agilidad tomarán mayor protagonismo a la hora de reevaluar las iniciativas y revisar prioridades. "La definición de escenarios de recuperación en función de la criticidad de los entornos llevará a una revisión de las estrategias de gestión y protección de los datos", explica. "Hay que crear políticas de recuperación frente a distintos escenarios y además probar su efectividad". La directiva de

> "En estos tiempos de confinamiento y teletrabajo un clic equivocado puede costarle a una compañía miles e, incluso, millones de euros"

Commvault desvela que las empresas están contratando seguros frente al *ransomware*. "Sin embargo, en caso de que sea necesario recuperar el entorno, no será posible si no existen copias de seguridad de la información que se ha perdido o si éstas copias son dispersas y resulta imposible saber en qué orden hay que recuperar los archivos para volver a operar con normalidad".

José Manuel Arnaiz cree que se ha incrementado muchísimo el valor de los activos digitales y también la necesidad de protegerlos. "En la era de inteligencia artificial, el Internet de las Cosas y el *big data*, tener toda nuestra información bien resguardada es un derecho, pero también una obligación ineludible. No hacerlo es una grave irresponsabilidad individual y de las empresas".

¿En qué se ha crecido?

Las empresas han notado un incremento de sus ventas. En el caso concreto de Mast Storage, se ha incrementado un 15 % el número de peticiones de empresas que necesitan un servicio de *backup online* durante el confinamiento por no poder acceder físicamente a cambiar discos o cintas de sus sistemas de *backup* local.

Durante el mes de abril, observando la situación tan complicada que estaban atravesando muchas empresas, la marca decidió no cobrar el servicio Mast Backup Online. "Es una medida extraordinaria que alcanzar tanto a los clientes actuales como a nuevos clientes que puedan necesitar esta solución durante el confinamiento", explica Javier Miquel.

Las pymes

Tras un ataque, los riesgos que se abren para las empresas son enormes. Según calcula Acronis, el 50 % de las empresas que recibe un ciberataque acaba cerrando. "Muchas pymes no tienen una percepción muy clara de dónde tienen almacenados sus datos y cómo están protegidos", opina Perotti. "Todas las organizaciones deben tener un plan claro de recuperación ante desastres", aconseja. "Las pymes deberían realizar un ejercicio de emergencia y probar si pueden restaurar con éxito todos los datos requeridos y cuánto tiempo les lleva hacerlo. Un ejercicio que, sin duda, les puede aportar información valiosa sobre su nivel de resiliencia".

La experiencia de Mast Storage en este campo de la pyme se extiende más de dos décadas y en la actualidad gestionan el *backup* diario de más de 6.000 empresas en España, siempre a través de su canal. Miquel explica que durante los últimos años han comprobado que muchas pymes cuentan con un departamento de informática pero no con un responsable encargado de gestionar exclusivamente la política de *backup*. Para "remediarlo", el fabricante cuenta con un equipo técnico propio que supervisa las copias diarias de los clientes, notifica cualquier incidencia y asesora sobre cómo resolverla. "Formamos el tándem perfecto con el distribuidor o la casa de software y el responsable TI de la empresa".

José Manuel Arnaiz asegura que el tejido empresarial español muestra idéntica vulnerabilidad que la de cualquier otro país. "Cada ordenador del mundo recibe de media más de 6 ataques de *ransomware* al año y en España recibimos nuestra ración", contabiliza. El CEO de Loozend reconoce que es fundamental que las empresas mantengan actualizados los sistemas operativos y las aplicaciones, así como el uso de un antivirus para detectar la presencia de un ataque. "Ahora bien, es vital disponer de un *backup* de toda la información y que éste esté bien protegido. Es la única garantía para no perder información".

> "Tras un ataque de *ransomware*, el coste que supone recuperar los datos es, como mínimo, de 1 o 2 bitcoins, lo que significa entre 6.000 y 12.000 euros"

Eulalia Flo explica que han notado que algunos proyectos se han acelerado. "Muchas organizaciones han tenido que adaptar sus sistemas de forma rápida para dar servicio al incremento de demanda *online* e incluso han tenido que dotar de más infraestructura y adaptar las propias aplicaciones para satisfacer nuevas exigencias". La directiva recuerda que hay que ir más allá del *backup* y pensar en los escenarios de recuperación. "Estamos ampliando el concepto a la gestión inteligente de los datos que incluye entender qué datos tenemos, dónde están y quién tiene acceso a ellos para gestionar su ciclo de vida". La marca está organizando una serie de seminarios *online* en los que dan información para acelerar los proyectos en la nube, cómo proteger el puesto de trabajo o el entorno ante un ataque de *ransomware*, cómo migrar el *backup* tradicional a la nube de forma segura y efectiva, o cómo hacer frente a una recuperación ante desastres.

En el caso de Loozend, cuya andadura en el mercado es joven, el crecimiento es relevante. "El crecimiento del teletrabajo, basado en muchos casos en infraestructura doméstica, nos hace mucho más vulnerables a los ataques y, por tanto, a las pérdidas accidentales", recuerda Arnaiz. "En muchos casos se trata de ordenadores que no están diseñados para estar encendidos todo el día, con una antigüedad que conlleva un riesgo de averías en los discos duros, los sistemas operativos y las aplicaciones, que en muchos casos están desactualizadas; también el uso de *routers* no profesionales y aunque las comunicaciones sean encriptadas en VPN, nos hacen más vulnerables; por lo que es más necesario protegerse".

En el caso de Veritas, una de sus principales apuestas es la última versión de su producto estrella, NetBackup 8.2., que ha puesto especial atención al entorno de la nube, con más de 60 conectores. La marca asegura que la copia de seguridad, el almacenamiento y la deduplicación sean sencillos, todo en un solo dispositivo.

Intel Core i9-10980HK ha alcanzado los 5,3 GHz

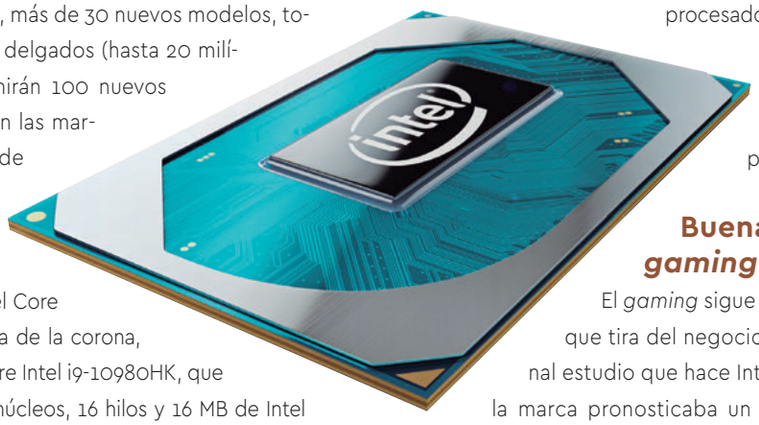
Intel Core serie H de 10ª generación

concede una nueva dimensión al juego portátil

"Es el procesador para portátiles más rápido que Intel ha lanzado nunca". Patricia Pozuelo, directora de tecnología de Intel Iberia, señala el rasgo más destacado de los nuevos miembros de la serie H (la que está centrada en los portátiles de más alto rendimiento) de la 10ª generación de Intel Core. "Con el Intel Core i9-10980HK, que se constituye en la joya de la corona de esta familia, hemos alcanzado los 5,3 GHz". Una capacidad que iguala a los equipos portátiles con las opciones de sobremesa, lo que asegura a los jugones (y a los creadores de contenido) la misma experiencia de usuario, con independencia de la plataforma por la que opten.

Marilés de Pedro

Pozuelo explicó que más del 60 % de los modelos incluidos en esta serie H exhiben un rendimiento por encima de los 5 GHz, "esencial para disfrutar de todo lo que puede ofrecer un videojuego". Intel presentará, en colaboración con sus principales *partners*, más de 30 nuevos modelos, todos ellos con formatos muy ligeros y delgados (hasta 20 milímetros de grosor). "A los que se unirán 100 nuevos diseños, siempre en colaboración con las marcas principales, en los segmentos de consumo, profesional y en el entorno de las estaciones de trabajo".



La nueva serie H se reparte, como es tradicional, en torno a 6 opciones (Intel Core i9, Intel Core i7 e Intel Core i5). La joya de la corona, como apunta Patricia Pozuelo, es el Core Intel i9-10980HK, que además de los 5,3 GHz, integra ocho núcleos, 16 hilos y 16 MB de Intel Smart Cache. "Es un procesador que, comparado con una solución de hace tres años, proporciona hasta un 54 % más de fotogramas por segundo en *gaming*, hasta un 44% de mejora en el rendimiento general y hasta 2 veces más rápido en renderización de vídeo 4K y exportación", explica. La opción intermedia, el Intel Core i7-10750H, llega a los 5 GHz y está pensado tanto para los creadores de contenido como para los jugones menos avanzados que los que optarían por la joya. Ofrece hasta un 44% más de fotogramas por segundo en el disfrute de los juegos o hasta un 33% de mejora en el rendimiento general. Junto a él, también está el Intel Core i7-10875H, con hasta 5,1 GHz Turbo, ocho núcleos y 16 hilos. Por último, las opciones de i5, alcanzan los 4,5 GHz.

Todos estos procesadores integran tecnología Turbo Boost Max Technology 3.0, Wifi 6, lo que permite hasta un 40 % más de velocidad y que las descargas se realicen 3 veces más de rápido; e integran Intel Optane.

Pozuelo no olvidó referirse a las oportunidades que abren estos procesadores a los creadores de contenido. "Hay más de 60 millones de creadores de contenido a nivel mundial y más del 50 % de los compradores de portátiles de *gaming* crean contenido".

Buenas ventas de equipos *gaming*

El *gaming* sigue siendo uno de los factores principales que tira del negocio del PC en España. Según el tradicional estudio que hace Intel a mitad de año, el pasado ejercicio la marca pronosticaba un buen comportamiento de este segmento y, según la encuesta, el 39 % de los jugones aseguraba que iba a comprar un equipo en los próximos 12 meses. Ignacio Jiménez, responsable del negocio *gaming* en España, reconoció que el segmento del *gaming* acabó con doble dígito de crecimiento en nuestro país, a nivel general. "Es un apartado que, durante el confinamiento que estamos soportando en España, ha crecido", reconoció. "Los equipos *gaming* han experimentado una subida. Lo que no podemos prever es si este crecimiento se mantendrá o no las próximas semanas".

> Los equipos de *gaming* han crecido en España durante el periodo de confinamiento provocado por el Covid-19

Intel
Tel.: 91 432 90 90

La ciberseguridad en tiempos de coronavirus

La seguridad: objetivo "común" de empresas y *hackers* durante el Covid-19

La seguridad se ha convertido en el objetivo principal de empresas y *hackers* durante el Covid-19. Las primeras, para brindarla y hacerla infranqueable a los ataques de los segundos. Los ciberdelincuentes son conscientes de los beneficios que pueden obtener de un contexto como el actual. "Es habitual que durante determinadas situaciones planeen campañas con el único objetivo de engañar a sus potenciales víctimas para obtener crédito económico sin importarles los daños que pueden provocar", ha explicado Marco A. Lozano, responsable de ciberseguridad para empresas del Instituto Nacional de Ciberseguridad (INCIBE).

Olga Romero

Actualmente los *hackers* se están sirviendo de la crisis sanitaria para crear ataques. Unas amenazas que se van adaptando a la evolución de la situación, "de tal modo que los mensajes progresan al mismo ritmo que la realidad del momento", ha afirmado Lozano. Porque, como ha matizado el responsable de INCIBE, "el propósito es engañar al mayor número de usuarios y empresas posible".

Está claro que la pandemia del Covid-19 está suponiendo un reto para las empresas y una gran oportunidad para los ciberdelincuentes. Por eso las principales compañías de seguridad han analizado cómo ven el panorama actual.

Principales carencias en la seguridad de las empresas

El teletrabajo ha sido la principal preocupación de organizaciones y empleados. Para Eusebio Nieva, director técnico de Check Point para España y Portugal, "el último mes ha supuesto un gran reto en términos de ciberseguridad, debido a que las empresas no contaban con la in-

fraestructura necesaria para teletrabajar de forma segura". La protección de los diferentes dispositivos conectados a la nube corporativa es, a su juicio, una de las principales carencias a las que se han enfrentado las compañías.

Esta opinión la comparte José de la Cruz, director técnico de Trend Micro Iberia. "El confinamiento ha supuesto un reto tecnológico para todas las empresas, ya que nunca nos habíamos visto en la situación de que toda la plantilla se encontrase trabajando remotamente".

Sobre esta cuestión, Jorge López, *systems engineer* en Fortinet para España y Portugal, ha valorado la importancia de realizar un análisis de riesgos. Mientras que las empresas que han llevado a cabo este estudio previo han estado preparadas para abordar esta situación, "el resto no ha tenido más remedio que actuar de la mejor manera posible, adaptándose a la nueva realidad". Son estos análisis de riesgos los que brindan a las organizaciones la información necesaria para reaccionar de la mejor forma posible.

A la gestión de riesgo también se ha referido María Campos, vp de Cytomic, quien aboga por la necesidad de contar con un plan de seguridad y de respuesta a incidencias que minimice los peligros más frecuentes a los que se enfrentan las organizaciones. "En las últimas semanas numerosas compañías han tenido que improvisar sobre la marcha. Mientras esto ocurre, los ciberdelincuentes aprovechan la situación para incrementar sus ataques", explica.

En este contexto Sergio Martínez, Iberia *regional manager* de SonicWall, ha puntualizado que este incremento inesperado del trabajo en remoto "se ha producido en un entorno en el que muchas empresas no tienen suficientes licencias de red privada (VPN) o capacidad en sus dispositivos de acceso remoto para atender este incremento de usuarios". Debido a esta situación los empleados se ven obligados a buscar otras maneras de conectarse a las aplicaciones y datos corporativos, "muchas veces de forma no segura".

Borja Pérez, *country manager* de Stormshield Iberia, identifica, como grandes carencias en cuanto a la seguridad en el teletrabajo, el hecho de que "en España culturalmente no estamos preparados para el trabajo en remoto, porque prima el trabajo presencial". Por ello, "las empresas no han visto la necesidad de invertir en seguridad, lo que se traduce en falta de preparación, aunque siempre hay excepciones".

La visión de INCIBE

Los expertos de INCIBE han detectado diferentes tipos de ataques que emplean principalmente técnicas de ingeniería social. Estas amenazas emplean principalmente el correo electrónico, pero también han observado casos que usan otro tipo de medios como el teléfono, la mensajería instantánea, los SMS o la creación de páginas web fraudulentas. Entre los principales argumentos empleados destacan la suplantación de servicios de logística, un falso servicio técnico, la recopilación ilegítima de datos, remedios y curas del Covid-19, servicios de difusión de vídeos, música o juegos y suplantación de entidades financieras o administraciones públicas, entre otras.

En cuanto al teletrabajo Lozano ha puntualizado que "no se trata de un riesgo, sino más bien de una nueva situación que nos expone a posibles peligros en el uso de las tecnologías en un entorno de trabajo fuera de lo común; o, al menos, no usado de manera convencional". Por eso desde INCIBE aconsejan:

- Acceder a los servicios de una empresa a través de VPN.
- Primar el uso de dispositivos corporativos frente a los personales.
- Uso de contraseñas robustas y del doble factor de autenticación.
- Cifrar el equipo y realizar copias de seguridad con frecuencia.
- Uso preferente del cable para la conexión a Internet.
- Vigilar el tipo de correos recibidos.

Para cualquier consulta, de particulares o empresas, INCIBE tiene disponible el teléfono 017, gratuito y confidencial.

Para Anastasia Sotelsek, *principal sales engineer* de CyberArk, "la principal carencia es que muchas organizaciones no protegen sus cuentas privilegiadas y solo una correcta gestión de las mismas ayuda a mitigar el riesgo que corren los datos y activos más valiosos de una organización", ha indicado.

Los ciberdelincuentes y sus "nuevas" fórmulas de ataque

El Covid-19 ha provocado una sensación de vulnerabilidad para todas las empresas. "El teletrabajo, las videoconferencias familiares, los videojuegos, las plataformas de televisión o el uso de las redes sociales han sido el "caldo de cultivo" idóneo para el *phishing*, que se ha constituido como una nueva forma de pandemia virtual", ha explicado Juanjo Galán, *business strategy* de All4Sec. Pero las VPN o la conexión remota de escritorios también han sido objetivo de los ataques. Sin olvidar la expansión de las *fake-news*, "una lacra que nos afecta a todos por igual y que nos conduce a menudo a comportamientos irracionales".

Borja Pérez, de Stormshield Iberia, coincide con Galán en la gran presencia de campañas de *phishing* que utilizan la pandemia como gancho. "También hay un incremento importante del

phishing por SMS suplantando la identidad de varias empresas; así como ataques a organizaciones de la salud a través de Netwalker", explica. "Aunque no tenemos la certeza de que sean ataques dirigidos, sino más bien una campaña masiva que ha impactado también en la sanidad".

Por su parte, Samuel Bonete, *regional sales manager* de Netskope Iberia, ha hablado sobre los ataques híbridos. Un tipo de amenaza "en la que los delincuentes utilizan la nube para la distribución de *malware*". Los *hackers* dejan un *malware* en una instancia de Office 365 comprometida y de esta manera el usuario cree estar accediendo a su aplicación pero, en realidad, lo que está haciendo es infectando.

Desde Cisco Talos, la división de ciberinteligencia de Cisco, han alertado de campañas de *malware* y *phishing* con temática sobre Covid-19, ataques contra organizaciones que realizan investigaciones, desinformación y sitios web fraudulentos que pretenden vender mascarillas médicas. Eutimio Fernández, director de ciberseguridad de Cisco España, ha confirmado que "España tiene el porcentaje más alto de incidentes de seguridad en Europa como resultado de abrir un email no deseado: un 54 % frente a la media europea del 41 %".

Bitdefender monitoriza constantemente la forma en la que las amenazas se adaptan a las nuevas realidades. Juan Grau, *regional sales manager* de la compañía, ha comentado que "los usuarios de dispositivos móviles se han convertido en un objetivo prioritario". Los expertos de Bitdefender han observado que los *hackers* se han "centrado en las aplicaciones que más se utilizan en esta situación como, por ejemplo, el rastreador de la OMS, las aplicaciones de interacción social, de productividad o las enfocadas al ocio", ha explicado Grau.

> "Los mensajes cambian al mismo ritmo que la realidad del momento", Marco A. Lozano, (INCIBE)

Alfonso Ramírez, director general de Kaspersky en Iberia, ha hablado de Ginp, "un troyano bancario que hemos identificado". Este *malware* tiene una elevada incidencia en España ya que el 83 % de las víctimas de este ataque procede del territorio nacional. "Usa la pandemia Covid-19 como cebo y solicita dinero a cambio de información sobre personas próximas e infectadas por coronavirus", ha matizado.

"Las situaciones de caos son perfectas para los atacantes ya que crean situaciones de incertidumbre nuevas que facilitan su tarea", ha comentado Daniel Varela, ingeniero especialista de seguridad para el sur de Europa en F5 Networks. Desde la compañía están observando el aumento de ataques de *phishing* para extraer información personal y que además sirven para ataques más complejos. Por eso Varela ha destacado que "es básico que recibamos educación en esta materia. Es la manera más efectiva de prevenir los ataques".

Cambio de tendencia para la ciberseguridad

La pandemia del Covid-19 ya forma parte de la historia española y mundial. Esta situación excepcional cambiará la vida de la población, pero aportará muchos conocimientos. Una idea que comparte José de la Cruz, de Trend Micro Iberia. "Marcará un cambio de tendencia en las empresas al permitir y/o fomentar el teletrabajo. Esto tendrá un impacto claro y directo en cómo las organizaciones protegen sus activos: infraestructuras, datos y usuarios".

Para Daniel Varela, de F5 Networks, "el teletrabajo ha venido para quedarse". Esta situación ayudará a perder los miedos a que la productividad pueda verse afectada y las empresas están invirtiendo mucho esfuerzo para implantar o mejorar las soluciones que lo permiten. "Garantizar la seguridad de estos entornos de teletrabajo va a sufrir una importante demanda".

La situación actual ha dejado clara la "gran dependencia que tenemos de estar conectados y, si no estamos preparados, reconocer los peligros a los que nos debemos enfrentar", ha comentado Josep Albors, responsable de concienciación e investigación de Eset España. Ante esta situación las empresas deben entender la importancia de proteger los equipos y trabajar de una forma segura. "Sin seguridad y conectividad, su negocio pende de un hilo".

En esta misma línea se manifiesta Iván Mateos, *sales engineer* de Sophos Iberia, que insiste en la importancia de la ciberseguridad en cualquier entorno y momento. "Si antes era de vital importancia para las organizaciones contar con sistemas de seguridad avanzados, ahora se ha hecho visible que la ciberseguridad no es un asunto de segundo nivel". Mateos recuerda que los ciberdelincuentes siempre están preparados para aprovechar cualquier situación con la que puedan crear campañas de *malware*.

"La sociedad tiene que aprovechar lo aprendido en relación a las nuevas formas de hacer las cosas, lo que trae consigo un notable incremento de la exposición y la necesidad evidente de contemplar la ciberseguridad como un factor de diseño de todos estos servicios", ha comentado Rafael Rosell, director comercial de S2 Grupo. Durante este tiempo de confinamiento no solo se ha aprendido a teletrabajar: también a realizar diferentes trámites en remoto o prestar servicios no presenciales.

Desde Check Point tienen claro que la pandemia del Covid-19 va a traer cambios, tanto en el ámbito del teletrabajo como en una mayor concienciación sobre la importancia de estar protegidos en el mundo virtual. "La prevención es la mejor estrategia de protección", ha afirmado Eusebio Nieva. Por eso recomienda a todas las empresas contar con herramientas para garantizar la seguridad de los datos y los dispositivos.

Sergio Martínez, de SonicWall, explica que "el cambio que estaba previsto para los próximos cinco años se ha realizado en tan solo 15 días". La transformación ha sido tan rápida que ha provocado numerosas disrupciones y problemas que han aprovechado los ciberdelincuentes para crear una lista de ataques como *malware*, troyanos o *phishing*, entre otros. Se trata de un cambio que "nos ha pillado desprevenidos", insiste.

El teletrabajo: ¿qué riesgos abre y de qué manera hay que protegerse?

Eutimio Fernández, de Cisco España, recomienda que "hay que pensar en los usuarios y en sus puestos de trabajo como si nunca trabajaran dentro de un perímetro". Es fundamental disponer de la misma protección en cualquier entorno. La conexión VPN, los mecanismos de verificación multifactor, la seguridad *cloud* y DNS y la protección de cualquier dispositivo o terminal son las cuatro soluciones claves para garantizar un teletrabajo seguro.

Con el teletrabajo el robo de credenciales de VPN o la seguridad de los dispositivos son nuevos vectores de ataques que los *hackers* pueden explorar. "Para mitigar estos riesgos, se recomienda proteger el acceso con privilegios a sistemas críticos como soluciones de Zero Trust, autenticación biométrica y aprovisionamiento *just-in-time*", ha explicado Anastasia Sotelsek, de CyberArk.

Pero las prácticas de teletrabajo también han generado "estrés tecnológico", recuerda María Campos, de Cytomic, lo que se traduce en un aumento de los fallos y de los riesgos asociados que no se pueden eliminar pero que "las empresas deben tener presente para determinar medidas razonables y prácticas para mitigarlos". Para conseguir este objetivo hay que disponer de soluciones avanzadas y actualizadas, así como el empleo de programas de detección y respuesta en los *endpoints*.

Guillermo Fernández, *sales engineer* del sur de Europa en WatchGuard Technologies, ha afirmado que "nunca ha sido más importante para los empleados tomar un papel activo en la lucha contra los ciberataques, ya que el teletrabajo ha ampliado la superficie de ataque". Para ayudar a las empresas a protegerse, desde la compañía comparten una serie de consejos como hacer que la red doméstica sea privada, emplear contraseñas seguras, vigilar los correos electrónicos y emplear una conexión VPN.

Sobre los riesgos que trae el teletrabajo Samuel Bonete, de Netskope Iberia, explica que "lo primero en lo que piensan los usuarios es en los riesgos derivados de la protección de un perímetro ya inexistente". Según datos de la compañía el 85 % del acceso a Internet va dirigido a aplicaciones SaaS en la nube. "Los dispositivos son personales y si rápidamente no se logra un control en tiempo real de lo que está pasando, realmente la exposición a fugas de información y amenazas es muy grande".

Para Jorge López, de Fortinet, "la protección del *endpoint* debe ser similar a la que se tiene cuando se está conectado a la red de la oficina". Desde la compañía aconsejan protegerlo con software de protección avanzado del *endpoint*,

que debería disponer de tecnología EDR capaz de detectar *malware* basado en firmas. López también opina que para el acceso remoto "se debería disponer de terminadores de túneles que cifren las comunicaciones y dimensionados para soportar la carga de todos los usuarios trabajando al mismo tiempo".

La sanidad: un sector crítico

Durante el estado de alarma el sector sanitario está recibiendo el reconocimiento por parte de toda la sociedad. Algo totalmente merecido por el gran esfuerzo que están realizando, junto a otros sectores de primera necesidad, para salir de esta situación lo antes posible. Pero los *hackers* también han puesto el ojo en el sistema sanitario, así como en otros servicios esenciales como la alimentación, la logística, la seguridad, los transportes o las telecomunicaciones. Ante esta situación el Centro Nacional de Protección de Infraestructuras y Ciberseguridad (CNPIC) ha mantenido el nivel cuatro de alerta, para ser capaz de responder a situaciones de alto riesgo.

En Bitdefender son conscientes de que el sector sanitario siempre ha sido uno de los más expuestos a las ciberamenazas y esta crisis ha incrementado este peligro. "El número de ciberataques contra hospitales ha aumentado significativamente en los últimos meses", ha comentado Juan Grau. Uno de los ataques más utilizado es el *ransomware* que "consigue bloquear el acceso a los ordenadores, logrando detener la actividad normal".

Jospe Albors, de Eset, coincide con Grau en que el sector sanitario está pasando por el momento más crítico. "No podemos permitir que un ciberataque deje fuera de juego infraestructuras tan críticas como los hospitales", ha recordado. Asimismo, ha hablado sobre los ataques dirigidos y otros que han sido lanzados de manera indiscriminada y que han llegado a afectar a algún centro sanitario.

Según datos de un informe de Kaspersky, las vulnerabilidades en las organizaciones sanitarias proceden de dos situaciones. Por un lado, la falta de atención a los riesgos de la digitalización. Y, por otro, la falta de conciencia del personal sobre la importancia de la ciberseguridad. Con estas debilidades "el peligro que supone que los ciberataques en instituciones sanitarias tengan éxito es enorme", ha indicado Alfonso Ramírez. La información que manejan estas organizaciones es crítica y, si el ataque triunfa, se pone en riesgo la resolución del diagnóstico del enfermo, su cuidado y la evolución.

La crisis del Covid-19 aumenta la concienciación sobre la importancia de la seguridad para las empresas y organizaciones

Continuando el hilo de la información confidencial y sensible de la que disponen los hospitales, Iván Mateos, de Sophos, ha corroborado la opinión de Ramírez sobre el altísimo coste que puede suponer el robo, la pérdida o la simple alteración de dichos datos. Mateos ha puesto como ejemplo "un ataque de denegación de servicio que deje caído un sistema de citas o consultas o un médico que no pueda acceder al historial de un paciente hace que sistemas de seguridad perimetral con capacidades de IPS o WAF sean esenciales".

Guillermo Fernández, de WatchGuard, recuerda que el *phishing* y el *ransomware* siguen liderando el ranking de ataques. "Se está realizando un importante esfuerzo de concienciación para ayudar a los centros hospitalarios a ver los riesgos a los que están expuestos". El Gobierno, explica, a través del CCN, del CNI y de otros organismos, está trabajando para la protección de estos entornos tan críticos.

Por su parte, Rafael Rosell, de S2 Grupo, también ha destacado el elevado riesgo de los centros sanitarios y los delicados datos que guardan. Sin embargo, el directivo cree que la protección ha sido correcta. "Al menos no se han tenido noticias de compromisos relevantes o problemas graves en los entornos sanitarios".

Por último, Juanjo Galán, de All4Sec, ha hablado sobre los riesgos a los que se enfrentan las infraestructuras esenciales que vienen "catalogados en función del nivel de amenaza que suponen para la prestación de servicios básicos". En la lista de ataques, aparecen en cabeza los que afectan a la disponibilidad de los sistemas o al robo de información. "También se están viendo un gran número de intentos de suplantación de la identidad o manipulación de la información que reciben los ciudadanos".

Están llevando a cabo acciones conjuntas para dar a conocer las soluciones

Esprinet y Midway Technologies unen fuerzas para impulsar la transformación digital

Pedro Miguel Santos Luna, CEO de **Midway Technologies**, junto a **Francisco José Ponce**, COO, y **Juan Luis Susillo**, CTO

Esprinet mantiene una alianza estratégica con Midway Technologies, una joven compañía centrada en el valor y especialista en la tecnología en la nube, que persigue extender las soluciones *cloud* de Microsoft entre sus clientes y marcar la diferencia en el mercado. Ambas compañías comparten la misma filosofía de servicio al cliente y su intención es afianzar esta colaboración, que se basa en la flexibilidad y la agilidad, para acompañar a las empresas en su proceso de digitalización.

Rosa Martín

El Grupo Esprinet lleva tiempo invirtiendo tiempo y recursos para detectar y fidelizar a *partners* estratégicos que le aporten valor añadido a su oferta y que le permitan diferenciarse de la competencia. Dentro de esta estrategia se enmarca el acuerdo que mantiene con Midway Technologies. Luisa Paolucci, *cloud project head* de V-Valley, subraya que desde el área *cloud* y EaaS del mayorista se está trabajando de manera estrecha con Midway Technologies y el acuerdo se ha ido afianzando por su "gran interés en el camino hacia la transformación digital de la mano de Microsoft". "Esprinet nos ha demostrado una cercanía, agilidad y flexibilidad similar a la que nosotros prestamos a nuestros clientes. Esto para nosotros es diferenciador", añade Pedro Miguel Santos Luna, CEO de Midway Technologies.

Midway

Midway Technologies trabaja siguiendo un modelo de apoyo a sus clientes en alguna de las fases de ejecución de un proyecto o en la totalidad. Su propuesta se concreta en cuatro líneas de servicios principales:

- **Análisis** de ciberseguridad.
- Proyectos de **transformación IT** para adecuar las infraestructuras hacia el *cloud* o mejorarlos para ser más ágiles.
- **Operación** y **evolución** de los sistemas, aplicaciones de negocio y la seguridad.
- **Gestión** y **optimización** del licenciamiento de Microsoft.

Objetivos

El objetivo principal de su alianza es potenciar todas las soluciones *cloud* de Microsoft, cubriendo todas las necesidades que van desde la infraestructura pura en modo *cloud* hasta los entornos híbridos, la seguridad, el *backup* y los planes de contingencia.

"Gran parte de nuestro negocio se centra en soluciones de transformación digital en Azure y Office 365 siguiendo las mejores prácticas de seguridad en estos entornos. Esprinet nos ha ayudado mucho en el acercamiento y posterior crecimiento dentro de Microsoft", confirma Santos Luna.

Están trabajando en proyectos de migración total o parcial, en el ámbito del *disaster recovery*, *backup* y en la gestión remota de dispositivos con total seguridad. Al mismo tiempo, están poniendo en marcha diferentes acciones con el fin de potenciar todas las habilidades de Midway desde el punto de vista de marketing y de negocio. "Todas estas iniciativas tienen como objetivo visibilizar soluciones específicas de Midway dentro del marco de Microsoft Azure", señala Paolucci.

Grupo Esprinet
Tel.: 976 766 110

Midway Technologies
Tel: 954 869 759

Se han desarrollado numerosas iniciativas para ayudar a la sociedad en esta crisis

El sector TIC será el aliado de la empresa para la recuperación económica

La pandemia del Covid-19 ha provocado una crisis sanitaria y económica y el sector tecnológico se ha puesto a disposición de empresas e instituciones para aportar su conocimiento y recursos para combatir esta situación. Las principales asociaciones del sector, que agrupan al grueso del tejido empresarial tecnológico y de la economía digital, consideran que su papel está siendo clave para combatir los problemas que acarrea esta situación y auguran que será un motor para salir de la crisis económica.

Rosa Martín

Carina Szpilka, presidenta de **Adigital**

En el análisis de la situación y en el papel que está desempeñando la tecnología, Francisco Hortigüela, director general de AMETIC, subraya que "nadie podría imaginar cómo abordar esta situación en la que nos encontramos, sin ayuda de la tecnología". Carina Szpilka, presidenta de Adigital, añade que "esta crisis ha dado visibilidad a la importancia de la digitalización. Es ya innegable que los dispositivos, las herramientas y las plataformas digitales son ya parte fundamental de la sociedad y de la economía del país".

> "Hemos avanzado en pocas semanas un proceso de digitalización que nos hubiera llevado años"

Las empresas del sector TIC han hecho un esfuerzo para que tanto las empresas como los ciudadanos en sus hogares puedan disponer de todas las herramientas para seguir con su actividad profesional y disfrutar del ocio. En este sentido, Alicia Richart, directora general de DigitalES, recalca que "el ecosistema de empresas digitales está colaborando para que la actividad de las empresas, así como el trabajo y el ocio desde los hogares, siga funcionando en la medida de lo posible. Desde los operadores de telecomunicaciones hasta fabricantes de equipamiento, consultoras, *marketplaces* o medios de pago".

"El teletrabajo es un gran catalizador de la digitalización de las compañías"

Francisco Hortigüela, director general de **AMETIC**

Facilitadores del teletrabajo

Este trabajo intenso ha servido para que las empresas pudieran activar el teletrabajo, aunque muchas no estaban preparadas para dar este paso. Hortigüela reconoce que la mayoría de las empresas no estaban preparadas para el teletrabajo porque incluso las que tenían esta fórmula implantada no la tenían para toda la plantilla a la vez. Por este motivo, destaca que muchos de sus asociados han puesto a disposición de las empresas de manera gratuita soluciones para resolver las necesidades más inmediatas.

La directiva de DigitalES cree que la tecnología ha facilitado que, con soluciones sencillas, se haya podido poner en marcha el teletrabajo y no ha sido un gran problema para las empresas.

Szpilka apunta que muchas empresas no estaban preparadas y las inversiones precipitadas del principio para implantar el teletrabajo son un parche. "El teletrabajo es más que las herramientas, tiene mucho de cultura de la organización y de cómo gestionamos las relaciones con nuestros equipos. Esa parte tendremos que revisarla si queremos aprovechar todo lo bueno del trabajo en remoto"

Digitalización

Los portavoces de las asociaciones consideran que esta acelerada implantación del teletrabajo ha permitido avanzar en el proceso de digitalización. "Hemos avanzado en pocos días o semanas un proceso que nos hubiera llevado años", explica Hortigüela. Nuestro país estaba poco acostumbrado al teletrabajo, por lo que para muchas compañías ha sido su primera experiencia para probar el trabajo en remoto y han podido descubrir sus beneficios para la conciliación familiar, el medio ambiente y la productividad. A juicio de Szpilka el teletrabajo es "sin duda un gran catalizador de la digitalización de las compañías".

Esta situación ha hecho que la digitalización se vea como un instrumento para combatir la pandemia, pero también revela que la tecnología será imprescindible para lograr la recuperación. "Sabemos que será fundamental aprovechar al máximo nuestras capacidades tecnológicas para iniciar el camino de la recuperación. La conectividad no será el único vector, la inteligencia artificial y el tratamiento del *big data*, así como la capacidad predictiva que consigamos, van a ser muy importantes", resalta Richart.

Acciones para combatir el Covid-19

El sector tecnológico se ha volcado en ayudar a las autoridades a luchar contra el Covid-19 poniendo su *expertise* y tecnología al servicio de la sociedad. Hay múltiples ejemplos, pero algunos de los más significativos han sido el despliegue de las redes y de la infraestructura de las comunicaciones móviles y fijas como las que han hecho en los hospitales de campaña y los hoteles medicalizados Telefónica y Vodafone; y las *apps* específicas para el autodiagnóstico como la que se hizo en la Comunidad de Madrid en las que colaboraron empresas de la talla de Telefónica, Goggo Network, Google y Ferrovial.

IBM también ha ofrecido gratuitamente su tecnología de inteligencia artificial para informar sobre el Covid-19; y Accenture ha ofrecido técnicas de IA para reducir la presión sobre los servicios de emergencia. "Todas las grandes empresas españolas están mostrando una gran generosidad y solidaridad con los efectos de la pandemia, realizando múltiples donaciones y poniendo en ocasiones su capacidad productiva y logística al servicio de la lucha contra la misma", destaca Richart.

Iniciativas

Ante esta situación de crisis por la pandemia, todas las asociaciones han puesto en marcha diferentes iniciativas para ayudar tanto a sus empresas asociadas como a la sociedad a afrontar

esta situación. AMETIC ha colaborado con el Ministerio de Industria, Comercio y Turismo para incrementar el volumen de fabricación de respiradores artificiales homologados para las UCIs de los hospitales.

DigitalES puso en marcha un gabinete de crisis diario desde el principio del confinamiento para analizar las novedades de la evolución, las medidas adoptadas y establecer mecanismos de colaboración. También está coordinando con el Ministerio de Educación la donación de material tecnológico para que los niños y jóvenes puedan continuar estudiando a distancia.

Adigital ha lanzado la página web, #TECHforCOVIDSpain, con el fin de aglutinar todas las iniciativas tecnológicas desarrolladas por las empresas y la ciudadanía para reducir el impacto de la crisis y dar visibilidad a los proyectos que se están llevando a cabo. A la vez, ha ampliado el programa de formación con talleres específicos sobre el trabajo en remoto desde el área de AdigitalLabs. Y, desde su área legal, está apoyando a los negocios de *ecommerce* sobre todo para informarles de las novedades legales que están marcando las Administraciones Públicas.

Crisis económica y recuperación

La crisis sanitaria lleva aparejada una crisis económica por el parón de la actividad. El sector TIC y de la economía digital no es ajeno a esta recesión, a pesar de partir de una cierta ventaja ya que la mayoría de las empresas ha podido continuar con su actividad. Los representantes de las asociaciones no pueden precisar en cuánto se verá afectado el sector, pero coinciden en que sí que se verá afectado. Hortigüela indica que "es probable que a nuestro sector la crisis le afecte menos que a otros, ya que la digitalización va a jugar un papel fundamental para superar esta crisis sanitaria, económica y social".

La directiva de DigitalES apunta que, aunque las empresas tecnológicas están teniendo un papel muy activo en esta crisis, esto no significa que tengan una mejor actividad de negocio. "En la medida en que la demanda se va a ver gravemente afectada por el parón económico nuestras empresas sufrirán igual que el resto del tejido productivo".

Para superar esta situación las empresas del sector parten con la ventaja de que la tecnología es la base para impulsar la digitalización que es un motor para el crecimiento.

Szpilka señala que lo más importante es aprender de esta situación y adaptarse con una visión a largo plazo a las nuevas tecnologías; aunque también "el Gobierno debe mejorar las regulaciones e invertir en I+D+i, mientras que las empresas privadas, pequeñas y grandes, deben invertir en mejorar el contexto y la educación tecnológica".

En AMETIC consideran que la digitalización debe incrementarse tanto en la Administración como en las empresas y, al mismo tiempo, se tienen que tomar medidas para reactivar la industria. Para lograr esto último propondrá al Gobierno la creación de un consejo asesor para la reindustrialización y la transformación industrial. Este consejo debería estar formado por expertos y se encargaría de impulsar proyectos para la digitalización de sectores estratégicos como la salud, el turismo, la movilidad y la cadena alimentaria.

Alicia Richart, directora general de **DigitalES**

Richart destaca que hay que apoyar con más fuerza la transformación digital porque se traducirá en un mayor crecimiento económico. Un estudio de Deloitte sobre el impacto de la digitalización en España señala que un incremento del 10 % en el Índice de digitalización DESI contribuye con un punto porcentual al crecimiento del PIB. "Hay que apoyar a las empresas del sector y contar con un marco regulatorio y fiscal estable que fomente la innovación, el conocimiento y la inversión para generar así empleo y crecimiento".

> "Será fundamental aprovechar al máximo nuestras capacidades tecnológicas para iniciar el camino de la recuperación"

Las soluciones en torno al puesto de trabajo, claves en estos meses

Dell bombea soporte financiero y formación a su canal

Aunque la incertidumbre aprieta y la situación provocada por las medidas adoptadas en España para parar la expansión de la pandemia del Covid-19 no es sencilla, los distribuidores de Dell están manteniendo su actividad. Ignacio Martín, director del canal, asegura que están llevando a cabo un buen número de actividades, muchas de ellas vinculadas con la formación. "Aunque hay una enorme preocupación por lo que deparará el futuro, se mantienen muy activos", asegura. Para apoyarles en estos momentos, ha anunciado medidas de apoyo financiero, algunos cambios importantes en los programas de *rebates* y en la provisión de fondos de marketing; así como un refuerzo importante en sus iniciativas de formación.

Marilés de Pedro

Ignacio Martín, director del canal de **Dell**

Medidas para ayudar al canal

Las medidas que ha puesto en marcha Dell para aliviar al canal tocan dos áreas: potenciar la formación y ayudar a aliviar su situación financiera.

Dell ha anunciado que va a pagar de manera anticipada hasta el 50 % de los fondos de marketing que el canal genera por sus ventas. Unos fondos que se pagan a posteriori pero que, ahora, va a anticipar. Para ello solo se pide al distribuidor un plan de actividades (que podrán ejecutar, como mínimo, hasta octubre). "Reciben una inyección monetaria que les permite mejorar su flujo de caja". La marca también ha alargado el plazo, hasta el mes de junio, para aquellos socios que ya habían recibido estos fondos de marketing.

La formación es pilar clave. Dell ofrecerá capacitación gratuita para los *partners* Metal, categoría que identifica a las compañías capaces de desarrollar servicios de implantación de las soluciones de almacenamiento. Se incluyen las tecnologías de Unity, Unity XT, Blu-ray y Data Protection 4400 (el modelo más comercializado por el canal). "Cuánta más capacidad atesoren para implantar este tipo de servicios, más líneas de rentabilidad podrán abrir".

También han cambiado la política de *rebates*. En el caso del *"Growth target"*, que se cobraba si el *partner* alcanzaba el objetivo de crecimiento pactado con Dell, ahora el *partner* lo recibe desde el primer euro que venda. También los mayoristas han visto flexibilizadas las condiciones de sus *rebates* trimestrales. Viendo los picos de demanda de algunas soluciones (como son las vinculadas con la movilidad), la marca ha decidido generar un único *rebate* semestral, en lugar de los dos trimestrales, que compute el negocio de los seis meses, lo que facilita al mayorista su consecución, aunque descienda la demanda en el segundo trimestre.

Por último, la marca ha potenciado las soluciones de Dell Bank, tanto para clientes finales como para los *partners* a través de Dell Financial Services (DFS). "Aquellos clientes finales que ahora prefieren convertir su inversión en una fórmula de *opex* pueden hacerlo a través de este programa de financiación. Al mismo tiempo, y para que el *partner* no vea penalizado sus ingresos, recibe el montante completo de la operación en 2 ó 3 días".

Dell también ha concedido un mayor plazo a los *partners* adscritos al programa de *factoring* (Working Capital Solutions), en el que están incluidos Wells Fargo e IBM, alargándolo hasta los 90 días, en lugar de los 45 o 60 habituales.

Análisis de la situación

En estas semanas de confinamiento, Martín reconoce el aumento de las soluciones vinculadas con el puesto de trabajo (portátiles y accesorios). "Nuestros mayoristas, que contaban con un *stock* suficiente, satisficieron la demanda". Tras la ralentización, lógica, que se produjo en la producción, la marca ha recobrado la actividad, moviendo parte de la capacidad productiva a Polonia.

Tras este *boom* del teletrabajo, prevé un aumento de las soluciones de hiperconvergencia, que permiten desplegar entornos virtuales, así como la seguridad de los entornos del puesto de trabajo. "El canal puede convertirse en un asesor de esta protección ante sus clientes indicándoles si el entorno está adecuadamente protegido y que las aplicaciones están bien definidas".

En el área de los segmentos, prevé que los entornos financieros, los seguros o la sanidad harán crecer su inversión. "La Administración Pública va a dar definitivamente un salto para acelerar la implantación de la administración digital".

Dell
Tel.: 91 722 92 00

La marca celebró de manera virtual su tradicional reunión de canal

IBM arma al canal frente al Covid-19

A pesar de que la situación no invita al optimismo, los socios pueden mantenerse cerca de los clientes y ayudarles, a su vez, a hacer frente a sus enormes retos de negocio. Mercedes Lucena, directora de IBM *partner ecosystem* en España, reconoció que posiblemente se vaya a un mercado de menos oportunidades, "pero éstas serán más relevantes y de mucho más valor para los clientes". Si algo bueno tiene la crisis es que no ha parado los procesos de transformación digital. Al contrario, "los ha acelerado y se han enfocado a unos mejores resultados financieros". Aunque el gasto en TI se vea afectado en este 2020 en España, Lucena destacó que hay áreas como "la colaboración, la seguridad o la nube que probablemente crecerán". IBM está haciendo un foco especial en relajar las condiciones que le exige para que el canal ponga el foco en los más importante: servir a los clientes. Para ello, por ejemplo, han extendido las fechas para la presentación de los planes de marketing, han retrasado la renovación de las certificaciones hasta final de año o han aumentado la frecuencia en el cobro de rebates para mejorar la liquidez, entre otras acciones.

Mercedes Lucena, directora de ***IBM partner ecosystem*** en España

Ayudar a la comunidad de *partners* a superar, con éxito, la complicada situación que ha pintado la expansión de la pandemia del Covid-19 es objetivo prioritario para IBM. Para ello, ha puesto a trabajar a su potente maquinaría para producir una artillería completa que arme al canal con agresivas promociones, un mayor soporte financiero, campañas de marketing y mejores condiciones de venta.

Marilés de Pedro

Clave el área Systems

El área Systems sigue siendo clave para IBM y su oferta se reparte entre su potente y longeva gama de *mainframe*, Power y las soluciones de almacenamiento y *backup*. Santiago García, *IBM Systems partner ecosystem leader*, señaló los tres apartados en lo que la marca cree que el canal puede desarrollar mayores oportunidades en los próximos meses.

Uno es el área Flash, con las cabinas Flash Systems 5000 como puntal de referencia. "Debe ser la puerta que nos abra numerosas oportunidades en la mayor parte de los clientes", explicó. Para potenciar este apartado Flash, la marca ha lanzado una oferta en la que es posible adquirir ahora los equipos, pero el pago se haría en octubre.

La segunda solución clave es el software Spectrum Protect Plus. En los últimos años la innovación que se ha aplicado a este producto ha sido enorme. "Es una solución muy focalizada en los contenedores y soporta un gran número de entornos", explicó. Es un software que "detecta de manera automática si hay cambios en los datos, si hay fraude o si hay una brecha de seguridad ya que integra soluciones cognitivas", relató. La seguridad es crítica y contar con un *backup* bien hecho es esencial. A su juicio, es una enorme oportunidad para el canal. "Muchos clientes no hacen *backup* o no los actualizan", aseguró.

Spectrum Protect Plus ha aumentado los entornos que soporta, incluyendo Office 365. Con un panorama en el que más del 80 % de los clientes de IBM que están trabajando en remoto hacen uso de esta plataforma, García insistió en lo importante que es recordar a las empresas que tienen que hacer *backup* de esta *suite*. IBM ofrece 90 días de demo del producto.

El tercer apartado es HealthCheck. "El teletrabajo y la potenciación del *ecommerce* han incrementado los problemas relacionados con la configuración de sus sistemas. El canal tiene que ayudar a las empresas a revisar sus arquitecturas", recomendó. Las demandas de los clientes vienen, por un lado, por aumentar el rendimiento de la instalación, debido al incremento del teletrabajo; y, por otro, debido a una disminución de la actividad, han solicitado una reducción de costes. "Con estos HealthCheck podemos proponer reducciones de TCO en determinadas cargas, no solo en el área Power sino también en las soluciones de almacenamiento y *mainframe*".

Área de servicios y soporte financiero

También el área de servicios ha determinado 3 ofertas para que el canal pueda incrementar su valor en torno a las áreas de continuidad de negocio, soluciones para el trabajo en remoto y el acceso seguro a las aplicaciones. Si la continuidad de negocio es esencial, en época de crisis se torna obligatoria. Marcos Sabaté, IBM Services, alertó acerca de dos servicios claves: Resiliency Review (consultoría) y Cyber Recovery as a Service (solución de recuperación: IBM Resiliency Orchestrator). "Podemos realizar un test gratuito al cliente para analizar su situación y ver cómo podemos ayudarle".

Promoción de IBM Cloud y cognitive software

IBM ha definido 20 ofertas, tanto en formato *onpremise* como SaaS, en las últimas semanas para ayudar a su canal a comercializar, en estos momentos, su oferta de *cloud* y de software. "Tienen todo el sentido del mundo en el momento actual", definió Germán Sánchez, *IBM cloud & cognitive partner ecosystem leade*r. La marca, a través de ofertas concretas gratuitas a 90 días, quiere que el canal permanezca cercano a sus clientes, para cubrir sus necesidades actuales, con ofertas concretas.

Una oferta dirigida, entre otros apartados, a la continuidad de negocio en las áreas de infraestructura como servicio, que incluye servicios de consultoría (COS) y de servidores virtuales; o en torno a VMware. También en el atractivo área de los datos y la inteligencia artificial, con el uso de la tecnología de IBM de manera gratuita durante 3 meses; o en el apartado de la colaboración (a través, por ejemplo, de Aspera), "muy importante ante el aumento enorme del teletrabajo".

IBM también va a potenciar el área de Sterling. "Muchas empresas han sufrido una disrupción de la cadena de suministro, sobre todo en el área del *retail*, por lo que han necesitado una mejora de sus procesos online", explicó Sánchez. No olvidó el área de la seguridad. "Se ha incrementado la necesidad de proteger a los empleados que están trabajando de manera remota e IBM está ofreciendo herramientas gratuitas durante el periodo de trial", expuso. La oferta también alcanza el área de IBM Garage. "El equipo técnico de IBM está disponible, para cualquier consulta y área", remarcó. "Hay cientos de demos que el canal puede utilizar para familiarizarse con los productos".

En el ámbito del teletrabajo IBM está trabajando para habilitar accesos remotos a los PC físicos de los empleados e implantar soluciones de escritorio o aplicaciones virtuales en IBM Cloud o de forma tradicional. Por último, en el ámbito del acceso seguro a las aplicaciones, IBM está ofreciendo una prueba gratuita de 60 días para el acceso remoto (hasta de 5 aplicaciones).

IBM ha diseñado campañas específicas para este periodo complicado. Germán Ruiz, *channel IBM Global Financing* (IGF), recordó los dos elementos básicos que deben permanecer siempre en este orden financiero: la liquidez y la gestión del riesgo. "Quiero mandar al canal un mensaje de tranquilidad ya que IGF va a seguir ayudándole, con el mismo nivel de servicio, aunque con un riesgo distinto". La financiación es clave en los proyectos: según IDC, su uso incrementa las posibilidades de ganar una operación en un 28 %. En 2019 más de 120 *partners* de IBM solicitaron este tipo de servicios, con más de 300 clientes soportados gracias a ello. Más del 45 % del canal recibió soporte financiero y más del 75 % del área Systems (*Power*, *mainframe* y almacenamiento) fue financiado. La financiación en el área del software creció un 53 %.

La marca mantiene sus campañas de financiación a tipo 0 en el área Systems a 24 meses (Power y almacenamiento) y en el área de software (licencias y SaaS). Gracias a la colaboración con los mayoristas, han lanzado una campaña, tipo 0, para todas las renovaciones y mantenimientos; y otra iniciativa, muy atractiva, en la que ofrecen al canal tres meses de carencia y 9 pagos mensuales.

El área de los servidores (*scale out* y *midrange*) y el almacenamiento Flash (con las gamas 5000, 7000 y 9000) también cuentan con una campaña de 3 meses de carencia y 36 pagos mensuales, no a tipo 0 pero sí con un buen interés.

Promoción del marketing digital

"La crisis está cambiando la manera de hacer el marketing que ahora va a ser 100 % digital", recordó Íñigo Osoro, *IBM vicepresident & CMO* de España, Portugal, Grecia e Israel. Para afrontar este reto, la marca ha llevado a cabo una iniciativa, IBM 4 Virtual Enterprise, para diseñar campañas digitales adaptadas a la nueva realidad que se puedan lanzar de manera rápida, con contenidos predefinidos, para ayudar a la fuerza comercial a que esté cerca del cliente. Unas campañas que cuentan con contenidos digitales específicos, dependiendo del objetivo que se persiga, que incluyen la definición de correos electrónicos tipos, *webinar*, contenidos y vídeos para utilizar en redes sociales y *call to action*.

Todo el contenido generado está a disposición de los *partners*.

Clave en esta estrategia es IBM My Digital Marketing, una plataforma digital automatizada, que la marca ya lanzó hace unos meses, y que puede ayudar al canal a acelerar su transformación digital en el área del marketing. "Permite hacer campañas *end to end* de marketing en todas las áreas claves de la oferta de IBM", explicó Michiel Hasker, *IBM partner ecosystem marketing leader.*

Una plataforma que cuenta con un enorme número de contenidos, miles de *assets*, *microsites*, páginas de referencia, casos de éxito, etc. que permiten ajustarse a todo tipo de necesidades de marketing con agilidad y flexibilidad. Especialmente importantes son los datos que permiten medir el impacto de cada una de las campañas.

Está disponible para todos los *business partners* de IBM, sin ningún coste. "Permite ejecutar con agilidad y rapidez las campañas de co-marketing para llegar al mercado de manera eficiente", explicó Hasker. La plataforma incluye campañas predefinidas que permiten la personalización por parte del *partner* (logo, contenidos propios, eventos propios, etc.). IBM ha lanzado un incentivo de 2.000 dólares para todos aquellos *partners* que decidan utilizar, por primera vez, la plataforma.

IBM
Tel.: 91 397 66 11

El *phishing* sigue siendo el arma esgrimida en el 95 % de los ataques

Los *hackers* aprovechan la expansión del Covid-19 para multiplicar sus ataques

Mario García,
director general de **Check Point** en España y Portugal

No son ataques diferentes, ni utilizan técnicas distintas, pero son más masivos, usan nuevos ganchos vinculados con el Covid-19 y se aprovechan de la vulnerabilidad de seguridad que ha desencadenado la adopción masiva del teletrabajo, las conexiones permanentes a Internet o el consumo desorbitado de las plataformas de uso digitales. Eusebio Nieva, SE de Check Point, describe, con precisión, la actividad que han desplegado los *hackers* aprovechando el nuevo panorama que ha desencadenado la expansión de la pandemia. "No han variado su forma de trabajar", puntualiza, pero "el Covid-19 les ha permitido, desgraciadamente, incrementar el éxito de sus ataques". Una situación que describe como la "tormenta perfecta" para el cibercrimen. "Hay más usuarios en la red, más vulnerables, con más miedo y que tienen una enorme necesidad de buscar información sobre la pandemia".

Marilés de Pedro

Ejemplo claro de este complicado panorama es el número de dominios registrados entre enero y marzo con el término Covid-19: 51.000. "El 9 % de los mismos son maliciosos o sospechosos de serlo", calculó Nieva. "Lo que es un número elevadísimo".

Lo que no ha variado un ápice ha sido la fórmula utilizada para realizar los ataques: el *phishing* sigue siendo el arma esgrimida en el 95 % de los mismos y la superficie alcanza, además de los usuarios del teletrabajo y la videoconferencia, a los hospitales, las infraestructuras críticas, organismos oficiales, servicios en la nube y los móviles.

Para lanzar estas campañas de *phishing*, Check Point apunta a Apple (10% del total de ataques) como la marca más empleada. Netflix le sigue los pasos (9 %), además de Yahoo o Whasapp (6 %). Otras marcas famosas en este ranking son Microsoft (3 %) o Amazon (1 %).

Nieva alertó de la peligrosidad del ataque conocido como "*business email* compromiso", en el que se busca engañar a los altos cargos de las empresas para que lleven a cabo pagos indebidos. "Supone el 40 % de las pérdidas por cibercrimen en el último año, lo que ha sumado 1.700 millones de dólares a nivel mundial".

> "El teletrabajo ha llegado y lo ha hecho para quedarse definitivamente"

No faltaron tampoco las alertas acerca de las numerosas *"fake news"* que ha provocado la pandemia. Nieva recordó la necesidad de acudir, siempre, a los canales oficiales. "Tenemos que ser completamente higiénicos en las búsquedas de las fuentes de información y meter en cuarentena todos aquellos datos que lleguen de los canales no oficiales".

Falta de preparación para el teletrabajo

La precipitada incorporación al teletrabajo de las empresas en España ha permitido a los *hackers* contar con una enorme extensión de ataque. Mario García, director general de Check Point en España y Portugal, ha percibido una falta de preparación de las empresas para el desarrollo del trabajo en remoto. "Algunas empresas no contaban con la infraestructura necesaria y otras han tenido que comprar equipos para suplir esta carencia". La seguridad, a su juicio, tampoco estaba planificada. "No estaban implantadas, de forma adecuada, estrategias de Zero Trust y los dispositivos no estaban suficientemente protegidos". Tampoco el entorno *cloud*, al que muchas empresas han "acudido" ante la falta de infraestructura física, ha contado con suficiente excelencia.

"Para hacer un uso adecuado del *cloud*, se necesita conocimiento y, además, se requiere seguridad", alertó. "A la gente le ha pillado con el paso cambiado y se ha convertido en un cuello de botella".

El uso de herramientas de videoconferencia ha crecido de manera desorbitada, lo que también ha servido a los hackers para ampliar su campo de actuación; así como el *Shadow IT*. "Los usuarios utilizan herramientas no autorizadas por sus empresas que no cumplen con las adecuadas políticas de seguridad", explicó Nieva.

Cambio de paradigma

Las empresas son conscientes de esta situación. Según un estudio llevado a cabo por Check Point, el 95 % de empresas reconoce que tienen retos de seguridad adicionales relacionados con el teletrabajo. Un 61 % se muestra preocupada por los riesgos de seguridad y los cambios que se necesitan para facilitar el teletrabajo, mientras que mejorar la seguridad del acceso remoto (55 %) y los puntos finales (49 %) son preocupaciones que señalan como destacadas.

Mario García recomendó que hay que provocar un cambio de paradigma. "La primera preocupación ha sido asegurar el funcionamiento de la empresa", recordó. "Ahora hay que garantizar la seguridad, tanto desde un punto de vista físico como lógico de los trabajadores remotos y de la información", aseguró. "Es importante habilitar nuevas formas de continuidad del negocio y nuevas maneras de llevarlo a cabo". Porque, como reitera, "el teletrabajo ha llegado y lo ha hecho para quedarse definitivamente".

> "Hay más usuarios en la red, más vulnerables, con más miedo y que tienen una enorme necesidad de buscar información sobre la pandemia"

"Tenemos tecnología suficiente para luchar contra los *hackers*"

La buena noticia es que la tecnología con la que se cuenta es suficiente para paliar los ataques de los *hackers*. Además de la imprescindible formación del usuario, Nieva recomendó el uso del *anti-phising* (Zero Day y multifactor) y el Sandboxing y la limpieza de documentos continua. "Hay ataques a Excel en el que éstos aparecen embebidosExcel en el que en un macro", alertó. No olvidó insistir sobre las actualizaciones "compulsivas" y sobre el uso correcto de las herramientas de videoconferencia. "El uso del doble factor de autenticación es vital", completó.

En los dos últimos meses Mario García reconoció que se ha elevado la inversión en torno al puesto de trabajo, con soluciones de VPN y filtrado de usuarios; así como en torno a los dispositivos móviles. También el apartado *cloud*, con un aumento de las soluciones de software como servicio (SaaS), de infraestructura como servicio (IaaS) y de control en la nube.

Check Point
Tel.: 91 799 27 14

Samsung presenta los nuevos *smartphones* 5G de la familia Galaxy A

Samsung ha presentado dos nuevos *smartphones* Galaxy A con conectividad 5G: los modelos Galaxy A71 5G y el Galaxy A51 5G. Estos dos nuevos teléfonos inteligentes cuentan con la pantalla Infinity-O, cámara cuádruple y batería de larga duración.

Luis de la Peña, director de marketing de la división de movilidad de Samsung en España, comentó que el objetivo de la compañía con estos nuevos dispositivos "es ofrecer a las personas innovaciones imprescindibles y experiencias potentes, con un rango variado de precios, pero sin comprometer las características esenciales de nuestros dispositivos".

Los nuevos modelos encierran en un cuerpo, disponible en colores pastel, una pantalla Super AMOLED Infinity-O de 6,5" en el dispositivo A51 5G y de 6,7" en el caso del modelo A71 5G. Gracias a la conectividad 5G permiten compartir fotos o vídeos al instante y jugar sin experimentar retardo en la acción. Disponen también de la plataforma Samsung Knox integrada para asegurar toda la información que contienen.

Estos dispositivos completan sus características con una batería de 4.500mAh de larga duración y carga rápida, 128 GB de almacenamiento interno y Micro SD de hasta 1TB. Por supuesto, no olvidan el elemento, imprescindible de las cámaras. En el caso del A71 5G, la principal ofrece 64 megapíxeles y en el A51 5G ésta alcanza los 48 megapíxeles. Al mismo tiempo, disponen de una cámara ultra angular de 12 megapíxeles, una cámara macro de 5 megapíxeles y otra de profundidad de 5 megapíxeles.

Los dos modelos se benefician del ecosistema completo de aplicaciones y servicios inteligentes de Samsung, que incluyen Bixby (Vision, Lens Mode, Routines), Samsung Pay y Samsung Health.

Samsung
Tel.: 91 714 36 00

HP lanza la impresora Neverstop Laser para el trabajo en casa

HP ha lanzado una nueva impresora con depósito de tóner recargable. Se trata de la nueva HP Neverstop Laser, que está diseñada para usuarios que teletrabajan. Esta novedad, que forma parte de la familia Neverstop Laser, no necesita la recarga del tóner hasta alcanzar las 5.000 páginas impresas, lo que supone un coste de menos de un céntimo por página, según ha calculado la marca.

María César, directora general de impresión de HP en España y Portugal, explicó que "cada vez hay más trabajadores que realizan sus tareas desde casa y necesitan una tecnología fiable, fácil de usar y que ofrezca una experiencia de impresión sin interrupciones".

La nueva impresora láser destaca porque permite ahorrar con cada recarga. Según resalta la compañía, los *kits* de recarga de tóner cuestan menos y producen hasta 2,5 veces más páginas en comparación con los cartuchos similares de HP.

La impresora HP Neverstop es un modelo siempre conectado, que permite el envío de impresiones y escaneos de forma muy sencilla y desde cualquier lugar. Permite también el envío de faxes y el pedido del *kit*.

Este dispositivo permite la organización de documentos mediante Smart Tasks, a través de la HP Smart App, lo que simplifica el trabajo y el ahorro de hasta un 50 % de tiempo.

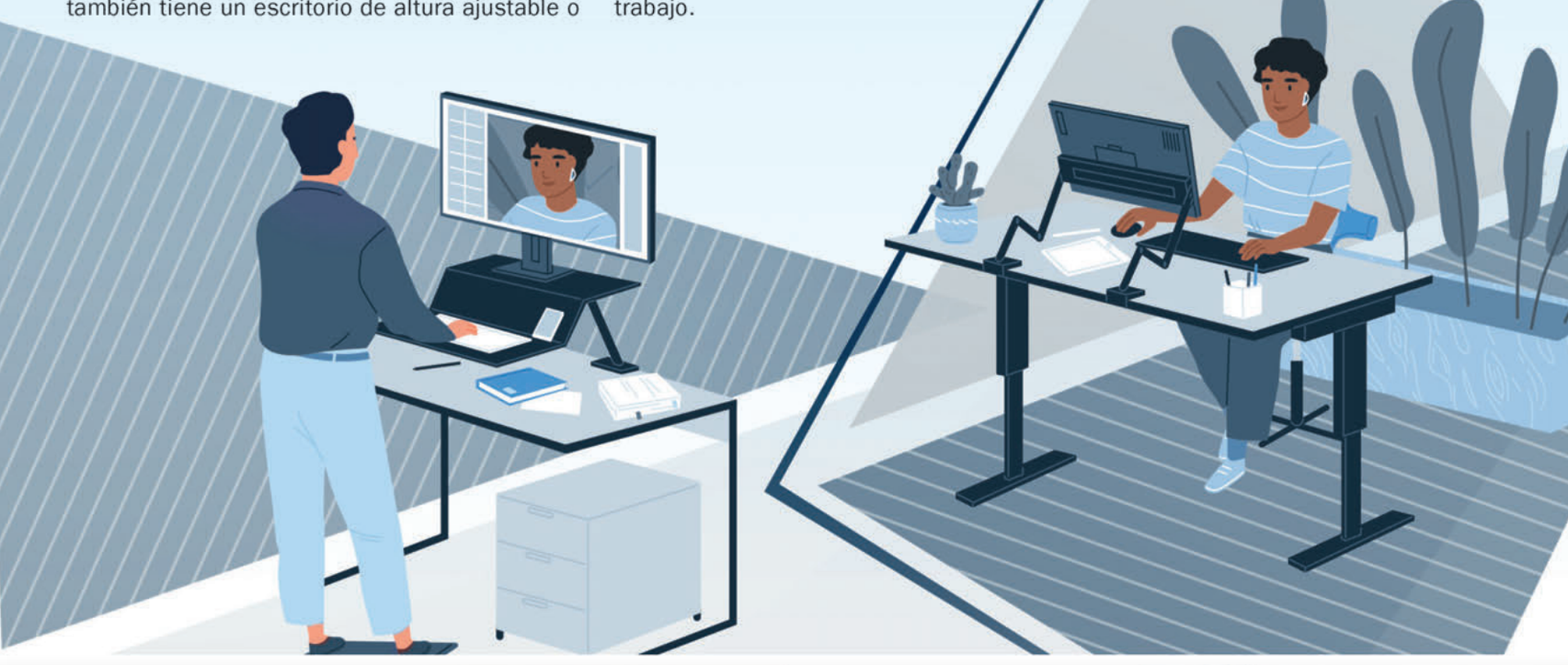
Otra de las ventajas de esta familia, que cuenta con dos modelos de red, es su diseño y certificación para el ahorro de energía. Además, está fabricada con más de un 25 % de plástico reciclado y el *kit* de recarga del tóner está compuesto por un 75 % de plástico reciclado.

HP
Tel.: 902 027 020

HOME OFFICE

ERGONOMÍA EN TU HOME OFFICE CON LOS PRODUCTOS DIGITUS

La oficina en casa es básicamente una estación de trabajo de computadora que es instalada por la compañía en la privacidad del empleado. Los medios de comunicación más comunes en la oficina en casa son, por ejemplo, el PC, el portátil o el smartphone. Sin embargo, es aún mejor si también tiene un escritorio de altura ajustable o alternativamente se levanta y se pone de pie. Esto ayuda a protegerte de permanecer en una posición sentada durante demasiado tiempo - que pasa demasiado rápido, cuando estamos centrados en las tareas, en el nuevo ambiente de trabajo.



DA-70614

REGLETAS ELÉCTRICAS

DA-90389

MARCOS DE MESA

DA-70881

ESTACIONES DE ACOPLAMIENTO

DA-90504

GESTIÓN DE CABLES

SOPORTES DE MONITOR

DA-90346

DESTRUCTORAS

DA-81605

ELEVADOR DE MONITORES

DA-90358

ADAPTADOR MULTIPUERTO

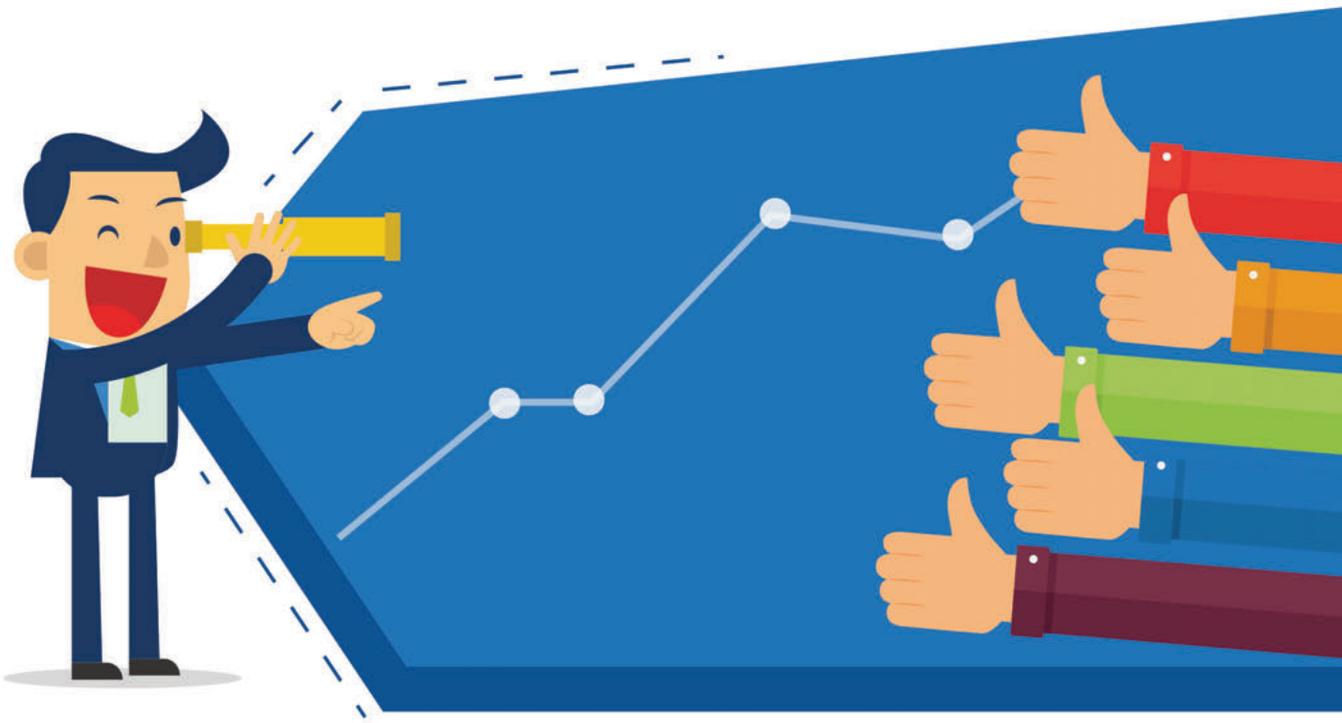
DA-70855

Estos componentes le ayudan a conseguir el 100 por ciento de su rendimiento en casa. Escanea el código QR para llegar a los productos en DMI.

www.dmi.es

Together is Better

Tu éxito, nuestro objetivo



esprinet®

Esprinet Ibérica
Campus 3·84
Nave 1, Calle Osca, 2
Pol. PLAZA
50197, Zaragoza,
info_es@esprinet.com
Teléfono: **976766110**

SATISFACTION GUARANTEED

b2b.esprinet.com