



facebook



twitter



newsbook.es

>> La revista del distribuidor informático

Newsbook

Tai
editorial

Año XXVIII N° 293 Mayo 2022

0,01 Euros



HP WOLF SECURITY

Procesador Intel® Core™ i7



HP WOLF SECURITY
ESTABLECE TU PRIMERA LINEA DE DEFENSA



¿Nos sigues
en
LinkedIn?



**No te pierdas
todo lo que
sucede en
el canal de
distribución**

Newsbook

El pasado mes de abril se concedieron las primeras ayudas del Kit Digital

Digitalizar la pyme: ahora o, ¿nunca?

Las pymes, que dan forma al 99 % del tejido empresarial español, son el motor de la economía española. Unas empresas que, junto a la Administración Pública y a las grandes empresas, son receptoras de los fondos NextGenerationUE. El programa específico para ellas es el Kit Digital, que cuenta con un presupuesto inicial de 3.000 millones de euros. Su primera fase, con 500 millones, se puso en marcha el pasado mes de marzo; y de su buena ejecución depende una buena parte de la recuperación de España. Todos los actores del sector tecnológico tienen su parcela de responsabilidad para hacer que las pymes aprovechen esta oportunidad. Esprinet, Ingram Micro, Sage, Sophos y Wolters Kluwer ya han asumido la suya. 

Sigue en pág. 34



La unidad de valor de Esprinet Ibérica quiere crecer en todas sus áreas de negocio

“Es más importante que nuestros clientes nos digan que somos los mejores, que ser el número uno”



La unidad de valor de Esprinet Ibérica, V-Valley, ya suma una década de recorrido en el mercado. Una trayectoria jalonada de compras estratégicas que la han llevado a situarse en segunda posición en el mercado del valor del sur de Europa. Para Javier Bilbao-Goyoaga, presidente de V-Valley Iberia, Vinzeo y miembro del consejo de Esprinet, el ranking, aunque guarda su parcela de importancia, reduce drásticamente su protagonismo ante la opinión de los clientes. “La clave es ser va-

lorado como el número uno por los clientes”, señala.

En el último año fiscal de Esprinet, récord en la historia del mayorista, la unidad creció un 46 %, con el entorno de la nube y el segmento de la seguridad como principales artífices del ascenso. 

Sigue en pág. 6

Seguridad en el canal

La seguridad sigue siendo una de las áreas con más grandes y mejores perspectivas de crecimiento. Según pronostica IDC el ascenso este año se cifra en un 7,7 %, un baremo que hasta el año 2024 se situará en un 8 %. Un apartado en el que el canal es pieza fundamental. Mayoristas y distribuidores han conformado desde hace años potentes estructuras técnicas y comerciales para aprovechar las oportunidades de este mercado. 

Sigue en pág. 17

Los ciberataques, la otra contienda bélica entre Rusia y Ucrania

La invasión de Rusia a Ucrania ha desencadenado otro conflicto en el terreno digital. El ciberespacio se ha convertido en campo de batalla en el que se han producido numerosos ciberataques para influir en la opinión pública y destruir activos importantes en los países enfrentados. Los especialistas en ciberseguridad señalan que los ciberataques han crecido en todo el mundo y recomiendan no bajar la guardia y aplicar todas las medidas posibles de protección porque en el ciberespacio no hay fronteras y tanto las empresas como los ciudadanos pueden convertirse en objetivos. 

Sigue en pág. 30

Digitalizar la pyme: ahora es el momento

Son los héroes de la economía española. Las pymes, que suman el 99 % del tejido empresarial español, son las responsables del 62 % de nuestro PIB y las creadoras del 74% del empleo. Sin duda, han sido las más golpeadas por la crisis económica que ha desatado la pandemia y deberían ser receptoras prioritarias de los fondos NextGenerationUE procedentes de la Unión Europea. Según los datos publicados por el Ministerio de Seguridad Social a finales de 2021 nuestro país contaba con 1.411.902 empresas, frente a las 1.489.733 que tenía en febrero de 2020, antes de que irrumpiera la pandemia. Esto supone 77.831 empresas menos que entonces, a pesar de que 2021 ha terminado con una ganancia neta de 23.427 compañías. La llegada de la covid-19, a principios de 2020, provocó una fuerte destrucción durante los meses de marzo y abril: 133.757 empresas tuvieron que cerrar, todas ellas pymes y autónomos. Es cierto que ha existido una recuperación, pero no se ha logrado alcanzar los números de 2019.

Fortalecer y recuperar a este segmento es esencial para impulsar la economía española. Y la buena ejecución de los fondos Next GenerationUE es clave. El programa específico para ellas, como es de sobra conocido, es el Kit Digital, que cuenta con un presupuesto inicial de 3.000 millones de euros. Su primera fase, con 500 millones, se puso en marcha el pasado mes de marzo; y a mediados de abril se anunció que las primeras ayudas ya habían llegado a más de 2.000 empresas. A pesar de ciertas dificultades en el diseño de este primer kit (que está centrado en empresas de 10 a 49 empleados), el éxito de la convocatoria está fuera de toda duda: Red.es recibió 50.000 solicitudes en el primer mes, 10.000 más de las previstas.

En estos primeros compases, la Administración Pública, consciente de los limitados recursos que tiene Red.es, ha sabido involucrar a las empresas. La creación de la figura del agente digitalizador ha obtenido también una enorme acogida: a finales del mes de abril ya se habían registrado más de 6.000 entidades con este perfil.

En el caso del sector tecnológico la actividad ha sido incesante: fabricantes y mayoristas, que ya llevaban muchos meses informando y tratando de facilitar los trámites, no siempre sencillos, han subido su nivel de implicación. En esta labor de comunicación, hay mensajes esenciales. Uno de ellos es dejar claro que esos 12.000 euros, que esta primera fase tiene como dotación máxima para cada empresa, no son una subvención ni, por supuesto, señalan la cuantía máxima de su transformación. Se trata de un "mero" impulso a su proceso de digitalización. Una cuantía, cuya ejecución, además, está sujeta a revisión posterior por parte de la Administración.

No es baladí tampoco el papel de los agentes digitalizadores, muchos de ellos integrantes del canal de distribución. Su mayor reto, además de la labor de evangelización y consultoría, es adelantar a las empresas adjudicatarias el importe del kit para que puedan ejecutar el proyecto.

El reto, por tanto, es enorme. España se juega mucho en el envite. Se calcula que el efecto positivo de la ejecución de los fondos contribuirá en casi dos puntos (un 1,8) al PIB. El Fondo Monetario Internacional (FMI) ha rebajado en un punto nuestras previsiones de crecimiento para este año, pasando del 5,8 al 4,8 %, lo que señala una criticidad mayor en la ejecución. Mayor reto, pues. Y, sobre todo, para las pymes. 

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 Cia, 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 tae@taieditorial.es para más información al respecto, puede consultar nuestra Política de Privacidad en <https://taieditorial.es/politica/>

En primera persona V-Valley/Esprinet



6
Javier Bilbao-Goyoaga, presidente de V-Valley Iberia, Vinzeo y miembro del consejo de Esprinet

Especial Seguridad en el canal



17
Fortinet, Samsung, VMware y WatchGuard desgranán sus políticas de distribución en el campo de la seguridad

Debate Pymes, canal y fondos NextGenerationUE



34
Esprinet, Ingram Micro, Sage, Sophos y Wolters Kluwer

En portada

Mujeres TIC Pág. 10
Las disciplinas STEM, materia a conquistar 

La guerra en el ciberespacio Pág. 30
El conflicto bélico entre Rusia y Ucrania también es digital 

En profundidad

Context Pág. 9
Ligero retroceso del negocio mayorista en el primer trimestre 

Ibermática Pág. 16
Consigue los mejores resultados de su historia en 2021 

Dynabook Pág. 36
El canal sigue marcando la estrategia 

Red Hat Pág. 38
Reorienta su estrategia de canal 

F5 Pág. 40
El software marca la proa de negocio 

Netskope Pág. 42
Su nuevo programa de canal tiene la capacitación de los socios como piedra angular 

Décimo eje del plan España Digital 2025 Pág. 44
Los derechos digitales 

Dell Technologies Pág. 46
Reafirma su apuesta por el canal en España 

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

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   FEDERACION INTERNACIONAL DE LA PRENSA PERIODICA

DISTRIBUCIÓN **Publístic Publicidad Directa, S.A.**
C/ Fundidores, 53 (Pol. Ind. Los Angeles)
29306 Getafe - Madrid
Telf. 91 683 76 92

DEPÓSITO LEGAL M-20480-2002 Impreso en papel ecológico 

ISSN 1696-6147

Esprinet estrena nuevo portal para el comercio electrónico B2B

Ya está disponible el nuevo portal web para la venta B2B de Esprinet. El mayorista quiere ofrecer una experiencia de compra personalizada a sus clientes y proveedores, por eso ha incluido una función de búsqueda personalizada.

El nuevo portal web de Esprinet ha renovado sus contenidos y diseño. Un proceso de renovación en el que han estado involucrados diferentes departamentos y que ha estado dividido por fases. Una primera fase de estudio que dejó paso al análisis y diseño para finalizar con la ejecución y pruebas. La versión anterior del sitio web del mayorista alcanzó los 900 usuarios conectados, 31.000 clientes y 94 millones de páginas visualizadas en el último año.

Esprinet ha desarrollado este nuevo portal B2B basándose en datos y respetando la normativa RGPD. Los usuarios recibirán comunicaciones publicitarias personalizadas, las cuales estarán basadas en el interés de negocio de los clientes. Además, la fuerza comercial podrá hacer uso de un nivel de servicio adicional, ya que podrá proponer una oferta de productos a sus clientes teniendo en cuenta sus compras específicas.

"Este nuevo sitio web ha sido realizado totalmente a nivel interno tras una atenta escucha de las nece-

sidades de nuestros clientes", ha comentado Alessandro Cattani, administrador delegado del Grupo Esprinet. El directivo ha explicado que el nuevo portal supone "un importante cambio de perspectiva que sitúa al cliente y sus necesidades en el centro de nuestro enfoque de negocio con el fin de obtener la satisfacción del cliente y garantiza a los vendedores estrategias comerciales más directas y selectivas". 

Esprinet
esprinet.com

Ingram Micro amplía su oferta de ciberseguridad con las soluciones de AuthUSB

Ingram Micro ha firmado un acuerdo de distribución con AuthUSB, empresa española especialista en soluciones de ciberseguridad, para llevar al canal las soluciones para la protección de los entornos OT e infraestructuras críticas. Las soluciones de AuthUSB se fundamentan en la premisa de la "seguridad desde el diseño", forman parte del catálogo CPSTIC del CCN y cuentan con una clasificación de nivel ALTO del ENS.

Através de esta nueva alianza, el mayorista amplía su oferta de ciberseguridad y aporta a su red de socios soluciones innovadoras.

Antonio Anchustegui, responsable del área de Ciberseguridad en Ingram Mi-

cro España, comenta que "el acuerdo con AuthUSB aportará ventajas a las dos compañías ya que permitirá involucrar a nuestros *partners* de canal en nuevas soluciones de ciberseguridad y colaborar con un fabricante que ha sido reconocido con el premio Cybersecurity Ventures, otorgado por el INCIBE,

como una de las tres mejores empresas de ciberseguridad de España".

"La digitalización de todos los entornos y la convergencia de redes aisladas y las redes conectadas expone a los entornos OT a una mayor superficie de ataque y a amenazas. Junto con Ingram Micro, equiparemos a nuestros *partners*

y clientes de las capacidades de hacer frente a estas nuevas amenazas con un equipo sólido y que nos permita de forma conjunta abordar nuevos mercados y proyectos", añadió María Cobas, CMO y socia de AuthUSB. 

Ingram Micro
ingrammicro.com



PUBLICACIONES

Para profesionales del canal de distribución TIC



Para los gerentes de la pyme



Para C-Level de mediana y gran empresa



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



La unidad de valor del grupo Esprinet, V-Valley, consolida su posición como número dos en el sur de Europa

"Mucho más importante que el *ranking* es la capacidad de ejecución. La clave es ser valorado como el número uno por los clientes"

Se cumplen 10 años de los primeros pasos de la unidad de valor de Esprinet. Una década en la que se ha consolidado una potente apuesta, bajo el nombre de V-Valley, que ha crecido hasta convertirse en punta de lanza de la actual estrategia. En el último año fiscal, récord en la historia del mayorista, la unidad creció un 46 %, con el entorno de la nube y el segmento de la seguridad como principales artífices del ascenso. Javier Bilbao-Goyoaga, presidente de V-Valley Iberia, Vinzeo y miembro del consejo de Esprinet, repasa el pasado y el presente de una unidad destinada, en un próximo futuro, a liderar el crecimiento del grupo

 Marilés de Pedro

Todo en la vida lleva un recorrido. También para V-Valley. Para alcanzar la sólida posición que hoy ocupa, se ha andado un camino que tuvo dos momentos claves: en 2016, Esprinet adquirió Itway; y en junio de 2020 la compra de GTI señala un punto de inflexión importante. Una trayectoria que transcurre, a su vez, en el grupo Esprinet, que también vivió una importante integración con Vinzeo. ¿Cómo valoraría todo este proceso?

Desde un punto de vista de trayectoria, ha sido un proceso bastante lógico y natural. Incluso antes de las dos compras se observaba, tanto en Esprinet como en Vinzeo, ciclos de expansión desde una perspectiva local. En el caso de Vinzeo, por ejemplo, hace muchos años ya se pusieron en marcha propuestas convergentes, en aquel momento disruptivas, entre el mundo de la telefonía y los entornos TI. La integración con Es-

prinet fue muy cómoda: tras estos cinco años, hemos asumido un modelo de gestión, con dos compañías que se mueven en un modelo de "semi" competencia, pero manteniendo una gran dosis de autonomía.

Sigue siendo un modelo muy peculiar...

No, creo que es un modelo muy común. Hay modelos similares en muchas industrias, sobre todo en las unidades de servicio. Quizás sea peculiar en modelos muy verticales; sin embargo, en nuestro caso es absolutamente natural. Y una de las grandes ventajas es que permite a las personas desarrollar mejor el negocio, resolviendo de manera eficiente las necesidades de los clientes y de los fabricantes. En nuestro caso, la suma de uno más uno, ha sido más de dos. Y lo vemos



Javier Bilbao-Goyoaga, presidente de V-Valley Iberia, Vinzeo y miembro del consejo de Esprinet

en los números: hemos crecido, tanto por parte de Vinzeo como de Esprinet, con muy buena orientación y desarrollando, de manera conjunta, el proyecto de valor de V-Valley. En este periodo, en algunos momentos hemos tenido que acelerar algunos procesos para construir un *portfolio* consistente de tecnologías y eso se ha hecho gracias a las adquisiciones. Desde Vinzeo y Esprinet se abordaron, con eficacia, el desarrollo del área del centro de datos o las redes, pero nos faltaba más foco en segmentos como la nube, el software o la ciberseguridad; que se ha conseguido con estas compras.

En este mercado del valor conviven mayoristas especializados en este apartado, tanto grandes como de nicho, junto a compañías generalistas, que han conformado unidades de valor. ¿Ya compiten en igualdad de condiciones? ¿Los generalistas han logrado visibilizar su desarrollo del valor?

Sí. Nosotros competimos con los dos modelos de mayoristas: los grandes, generalistas, que cuentan con sus divisiones de valor; y las compañías especializadas, tanto grandes como con un tamaño menor. Con los primeros, las diferencias son pocas, pero los pequeños aportan una rapidez de actuación, que es su gran ventaja. Desde V-Valley hay que ser capaz de ofrecer la calidad de servicio que dan los pequeños, basada en la rapidez, la flexibilidad y la adaptación, a muy corto plazo, a las necesidades de clientes y fabricantes. Y sin someternos a grandes procesos internos o a tomas de decisiones alejadas del mercado. Queremos ser tan buenos, rápidos y efectivos como las compañías "pequeñas" y locales con la capacidad financiera y el *compliance* que aportamos las multinacionales. Nos hace diferentes la vocación de dar un servicio como si fuésemos los más pequeños del mercado. No estamos preocupados por el ranking. Aunque sea importante, porque en el negocio de volumen genera economías de escala, presencia y capacidad de llegada al mercado; lo más importante es la capacidad de ejecución.

En 2017, tras la compra de Itway, la facturación en V-Valley Iberia se movía entre los 85 y los 90 millones de euros en España. La compra de GTI elevó ese baremo por encima de los 300 millones de euros en 2020. Hace un par de años, aseguraba que se podía duplicar el negocio en cinco años... ¿Se va por buen camino?

Sí. Es un objetivo que requiere crecer por encima del 16 %. Mantenemos una enorme vocación de ascenso orgánico y asumimos un crecimiento externo como algo muy natural. Tenemos una buena capacidad de integración de equipos y de organizaciones; y hay que ponerlo en valor; por lo que es alcanzable a largo plazo ese crecimiento.

2021 fue el mejor de la historia del Grupo Esprinet, con récord en los ingresos (más de 4.600 millones de euros) y en el beneficio neto

(creció un 39 %). Clave fue el comportamiento del área de valor, con un crecimiento del 46 %, con 874 millones de euros de facturación. ¿Cómo valoraría el peso que tiene el área de valor en estos resultados? ¿Qué ha sido clave?

Estamos muy contentos con este enorme crecimiento que ha sido bastante equilibrado. Hemos conseguido un negocio con mucha consistencia y coherencia. De ese crecimiento, casi un 55 % procede de estos procesos de adquisición y un 45 % ha sido orgánico; lo que concede una estructura muy equilibrada y la sensación de que estamos haciendo las cosas bien.

El año pasado fue cualitativamente espectacular. Se creció en todas las líneas de negocio; y no solo por las adquisiciones, sino por nuestra ca-

“Queremos crecer en todas las áreas por encima del mercado y mejorar nuestra participación”

pacidad de ampliar enormemente la base de clientes en nuestro gran *driver* de crecimiento que ha sido el *cloud*. Los *partners* que vendían las soluciones tradicionales del centro de datos están promoviendo una venta híbrida y esto ha impulsado enormemente nuestro negocio. Hemos conformado una oferta *cloud* muy competente y muy integrada con el centro de datos.

El segundo *driver* de crecimiento ha sido la ciberseguridad. Creamos hace años un equipo de primerísimo nivel que ha aportado una visión sobre cómo aproximarnos a los diferentes clientes y fabricantes. Es el ejemplo de cómo actúa una empresa pequeña en un entorno de gran multinacional. Se ha dotado a una "pequeña" organización, como en este caso la seguridad, de muchísima autonomía. Este es nuestro secreto. En todos nuestros negocios intentamos contar con equipos muy autónomos de gestión, con grandes capacidades técnicas; y trasladarlas de una forma muy sencilla a sus clientes.

¿Y el área del centro de datos?

También estuvimos muy potentes. En 2020, con la pandemia, muchos de los proyectos se retrasaron y se han ejecutado en 2021. Hemos abierto nuevas líneas de servicios, como Patrimonio, que ha sido muy exitoso. Nuestro balance, muy sane-

ado, lo ponemos al servicio de nuestros clientes para facilitarles la ejecución de operaciones en este entorno.

En el entorno *cloud* el crecimiento al que se refiere alcanzó, a nivel global en el Grupo, un 183 %. ¿Sigue siendo Microsoft la marca de referencia?

Sí. Es un fabricante estratégico. Tiene una oferta muy bien adaptada a la estructura empresarial española. Son capaces de adaptar esa filosofía de multinacional a una necesidad local. Nuestra alianza nos permite ir abordando diferentes segmentos y sobre ellos estamos construyendo ofertas consistentes. Estamos ayudando a que un *reseller* tradicional del centro de datos sea capaz de hacer ofertas híbridas de una forma simple y natural. Ese es el secreto. Se trata de democratizar la tecnología. Las soluciones *cloud* eran para las grandes multinacionales y hoy son accesibles para todo tipo de empresas.

En este ámbito, Esprinet cuenta con una plataforma *cloud*, presentada a finales de 2020. Un proyecto que llega con cierto "retraso" en relación con las plataformas de otros competidores. ¿Qué la diferencia?

Su desarrollo es una de las prioridades para este año. Hemos hecho un enorme esfuerzo organizativo, migrando y fusionando la plataforma de la que disponía GTI. Además de su oferta, hemos sabido aprovechar el enorme conocimiento de sus equipos técnicos, inyectando una enorme inversión. El esfuerzo ha fructificado en nuestra plataforma de *marketplace*, que está siendo un éxito y que aún ganará mucho más este año, con funcionalidades adicionales y ofertas complementarias.

El hecho de ser los últimos en desplegar una plataforma como ésta nos ha permitido corregir algunos errores que hemos observado en otras. Hemos conseguido que la compra, la navegación y la consola de gestión a la que damos acceso a nuestros *partners* sea sencilla y eficiente. Nuestro crecimiento en el área *cloud* está directamente relacionado con el uso de esta plataforma.

El área más tradicional es el segmento del centro de datos. Un apartado en el que HPE tiene un enorme peso. Una compañía que ha sabido virar su foco de negocio en los últimos cuatro años para potenciar el área "como servicio".

EN PRIMERA PERSONA

¿También está virando su proa V-Valley con ella al mismo ritmo? ¿Cómo valoraría el trabajo?

Estamos, incluso, intentando girar más rápido. Cuando compramos GTI, el racional estratégico que estaba detrás era darnos entrada al mundo *cloud* para generar ofertas consistentes. Soy un firme creyente de la transformación del modelo de negocio que está haciendo HPE. GreenLake está más implantado, posiblemente, en los Estados Unidos que en Europa, ya que el modelo todavía está más orientado a las grandes corporaciones. Nuestra misión es ayudar a un fabricante como HPE, y a cualquier otro que se mueve en este entorno del centro de datos, a adaptar estas fórmulas a la realidad de la pyme española. Y también de la gran corporación. Nuestro papel básico es democratizar el uso de la tecnología *cloud* para la pyme. Tenemos que ser capaces de hacer esa transformación con el fabricante.

También cuenta con su parcela de protagonismo el área de la videovigilancia, el IoT o la identificación automática (heredad de Diode). ¿Qué peso estratégico tiene este negocio en V-Valley?

Tanto la compra de Diode en España como de Dacom en Italia en el área de la identificación automática y la captura de datos nos ha permitido tener una posición razonablemente relevante en este negocio donde el canal y las necesidades de servicio son bastante diferentes. Somos capaces de abordarlo de una forma distinta. Este negocio se ha visto afectado por la falta de suministro. Sin embargo, tenemos una enorme vocación de crecer mucho. Y hacerlo, además, fuera de los tres países que conforman nuestro grupo.

El área vinculada con el puesto de trabajo, las comunicaciones unificadas y la productividad es segmento de oportunidad. Tras la explosión de algunas áreas vinculadas con este apartado en los dos últimos años, ahora, con una demanda más estable, ¿qué objetivos se marcan?

Este área lo vemos con mucho interés, sigue creciendo y todavía no tenemos una posición relevante. Existe una multiplicidad de fabricantes y una cierta atomización de los canales. En nuestro caso, vamos a hacer una apuesta mucho

más consistente en algunos fabricantes, que tenemos identificados, para abordar sus canales de manera más específica. Tenemos que conseguir que los *partners* que se dedican a este negocio puedan acceder a los productos en las condiciones que lo necesitan.



Y, este año, ¿qué peso se quiere lograr en el negocio de Esprinet Ibérica? ¿Qué negocios cree que serán las grandes estrellas?

Nuestro objetivo es alcanzar los dos dígitos de crecimiento. Además de la seguridad y el *cloud*, también queremos crecer mucho en áreas como las redes y la identificación automática. Sin descuidar, por supuesto, el centro de datos. No podemos dejar que ningún área se quede atrás. En todas queremos crecer por encima del mercado y mejorar nuestra participación. Tenemos muchísima ambición. Va a ser clave también nuestra oferta de dispositivo como servicio (DaaS), basada en nuestra experiencia en el mercado en la nube y en el segmento del *renting*.

Si en 2021 se facturaron casi 1.700 millones de euros y el objetivo es que en 2024 se alcancen 2.200 millones de euros. ¿La mayor parte de la responsabilidad corresponderá a V-Valley?

Sí. Tenemos una orientación muy clara hacia el desarrollo de este apartado; aunque no se puede olvidar la apuesta hacia algunas áreas de la electrónica de consumo. Tiene que quedar claro que no estamos abandonando el volumen. Ahora bien, el área de valor es el que tiene que aportar un mayor crecimiento, que no es tanto la facturación incremental, sino cómo esa facturación

cualitativamente tiene que dirigirse hacia áreas que aporten un valor añadido adicional. Por tanto, V-Valley asume unos retos más agresivos y más elevados; con más recursos.

¿Ya se tienen "visualizadas" algunas compañías para seguir incrementando el crecimiento inorgánico?

Sí. Tenemos algunas que nos gustaría materializar este año. Es muy complejo ya que tenemos procesos en marcha, pero siempre es difícil decir cuándo fructificarán. Lo que sí está clara es, más que nuestra vocación de compra, la de ayudar a consolidar el mercado del sur de Europa.

Y, asentado como el número dos en el segmento del valor en el sur de Europa, ¿será posible acercarse al número uno?

No es muy importante ser el número uno, ni el dos o el tres. Para mí la clave es ser valorado como el número uno. Es más importante que nuestros clientes

nos digan que somos los mejores, que ser el número uno en tamaño. Per se, el número uno no tiene valor. De cualquier manera, en el segmento del valor el tamaño es menos importante. En el segmento del volumen, por las economías de escala que se generan en las infraestructuras logísticas, de administración, etc.; es más importante. En el área del valor es clave la inversión. Por ejemplo, el peso de ingenieros en la plantilla de V-Valley, que suma 570 en el grupo, es del 45 %. Se necesita conocer la tecnología y cómo el *partner* tiene que implantarla en el cliente final.

V-Valley, al igual que el resto de los mayoristas, está haciendo un enorme esfuerzo en informar sobre los fondos europeos NextGenerationUE. ¿Cuál es su percepción? ¿Qué se torna clave para conseguir un buen aprovechamiento en este apartado?

El efecto que van a tener estos fondos va a ser muy potente. Cuesta que aterricen ya que en la actualidad no más del 27 % de los fondos se está ejecutando, pero, al final, va a generar un motor, no solo para la pyme, destinataria del Kit Digital, sino para el resto. Van a generar un impulso para nuestra industria tecnológica. Y estoy convencido de que llegarán. 

V-Valley
v-valley.es

El área de los distribuidores que se dirigen a la pyme crece un 4 %

El negocio de los mayoristas retrocede un escueto 2 % en España en el primer trimestre

La consultora desgrana el comportamiento en cada uno de los meses: en enero el negocio decreció un 5 %. Idéntico baremo arrojó febrero, esta vez de crecimiento; para concluir el trimestre con otro 5 % de retroceso en marzo. Por canales, es el grupo de distribuidores que se dirigen a la pyme quienes exhiben un mejor comportamiento. Su negocio crece un 4 %, según los datos de Context. Junto con el corpúsculo de *etailers* que venden en la empresa, cuya facturación creció un escueto 1 %, son los únicos que crecen. El negocio de los distribuidores corporativos decrece un 3 % mientras que el área del *retail* retrocede un 6 %. El mayor decrecimiento corresponde al área de los *etailers* que se vuelcan en el negocio de consumo, que se cifra en un 13 %.



En un 2 % cifra la consultora Context el retroceso del negocio de los mayoristas en el primer trimestre de este año. Un decrecimiento que ha provocado el negocio vinculado con el volumen, que ha retrocedido un 7 %; y que ha sido casi compensado por el ascenso de las áreas vinculadas con el valor, que en este periodo se ha situado en el 7 %. Hay que tener en cuenta que el negocio realizado en este 2022 se compara con los resultados del mismo trimestre del pasado año, en el que se creció un 20 %; el mejor del pasado 2021.

Marilés de Pedro

Sectores industriales

La consultora analiza la situación de cada uno de los sectores industriales. Las dificultades que aún persisten en el suministro afectan especialmente a áreas como la movilidad en el PC, que desciende un 13 %; y las telecomunicaciones (donde está incluido el negocio de los teléfonos inteligentes), que retrocede otro 13 %. El área de la impresión decrece un 9 % y los consumibles asociados lo hacen un 7 %. En el lado del crecimiento, destaca el software (11 %), los *displays* (27 %), las soluciones vinculadas con las redes (32 %), los discos duros (23 %) o el área del hogar digital y el *smart office* (20 %). Los servidores exhiben un escueto crecimiento del 4 %.

Por canales, es el grupo de distribuidores que se dirigen a la pyme quienes exhiben un mejor comportamiento. Su negocio crece un 4 %

Categorías

Por categorías, al igual que sucede con los sectores industriales, lógicamente portátiles y teléfonos inteligentes retroceden con idéntico baremo: un 14 %. Las tabletas decrecen un 12 % y los equipos de sobremesa un 8 %.

Crece el software de seguridad (15 %), las tarjetas gráficas (33 %), los discos duros sólidos internos (46 %), los televisores (168 %), los monitores (5 %), los procesadores (12 %), el software de gestión de almacenamiento (26 %) o los switches de red (5 %). 

Context
contextworld.com

Solo el 12 % de los estudiantes que profesa carreras STEM en España son mujeres

STEM o no STEM: esa es la cuestión vocacional



Las mujeres siguen sin caer rendidas a las disciplinas STEM (*Science, Technology, Engineering and Mathematics* o, lo que es lo mismo, Ciencia, Tecnología, Ingeniería y Matemáticas). ¿Las razones? Tan múltiples como las vocaciones: educación, sesgos históricos, insuficientes medidas igualitarias, falta de diversidad, poca visibilidad de referentes femeninos... Junto a la libertad, innegociable, en la toma de su rumbo profesional, es necesario analizar por qué las mujeres siguen siendo minoría en estos campos. El futuro profesional se pinta del color de estas materias, lo que exige que las féminas sumen su talento a las mismas. De ello depende también una gran parte del progreso de la sociedad.

➤ Marilés de Pedro

➤ Rosa Martín

➤ Olga Romero

Brecha STEM
En España, solo el 12 % de los estudiantes que opta por carreras STEM son chicas, según se desprende del informe "Empleo IT y mujer: 10 profesiones con futuro", elaborado por Infoempleo y la Universidad Internacional de la Rioja (UNIR). Un informe que señala que las mujeres que trabajan en puestos relacionados con la ciencia y la tecnología apenas representan el 2 % del empleo femenino. "A las niñas no les atrae este tipo de estudios porque no tienen ejemplos claros y les faltan referentes en ámbitos como el científico, el matemático o el tecnológico", señala Helena Herrero, presidenta de la región sur de Europa de HP. La fa-

milia —los padres— son un elemento clave en el impulso y la motivación de las niñas a la hora de inculcarles el interés y la determinación de cursar ese tipo de estudios, eliminando los sesgos y estimulando su interés por este tipo de disciplinas. "Resulta imprescindible que el sistema educativo se adapte mejor a este cambio social", completa.

Una carencia que empieza a notarse mucho antes de alcanzar la etapa universitaria. Según el estudio de la Universidad de Comillas "Estudios STEM en España y participación de la mujer", del total de estudiantes de Formación Profesional matriculados en el curso 2019-20, únicamente un 3,3 % eran mujeres que habían optado por una rama STEM. En el caso de los

estudios universitarios, el informe de la universidad señala que en ese curso solo el 7,9 % eran mujeres. La educación que recibimos en casa y en el colegio, la falta de diversidad en el sector y el compromiso por parte de las instituciones son, para Ana Carolina Cardoso, directora de canal de APC by Schneider Electric, las áreas desde las que se debe abordar esta carencia. La directiva, sin embargo, observa que hay una evolución positiva. "Es un proceso que requiere tiempo para, por un lado, tener más referentes de mujeres y madres que sean directivas y, por otro lado, las empresas puedan consolidar sus políticas de diversidad", explica. Los colegios profesionales calculan que en España hay una ingeniera por cada ocho ingenie-



Helena Herrero
presidenta de la región sur de Europa de HP

“A las niñas no les atrae este tipo de estudios porque no tienen ejemplos claros y les faltan referentes en ámbitos como el científico, el matemático o el tecnológico”

Según un estudio de la revista Science, las niñas a partir de los seis años ya empiezan a considerar que son menos inteligentes que los niños debido a cómo perciben los estereotipos de género que les marcan qué actividades son propias de cada género. “Por eso, resulta tan importante dejar que las niñas se ensucien, experimenten, se equivoquen, compitan por ser más rápidas, subir más alto y no solo fomentar su faceta de cuidadoras o de trabajo en equipo. Los juguetes que se eligen o las actividades lú-

presidenta de software y servicios para el canal en EMEA de Xerox, reitera que hay que trabajar en una única dirección. “Hay que transmitir a las niñas que, si quieren, pueden. Querer es poder”. No hay unas carreras de chicos y otras de chicas. “Las niñas no eligen carreras STEM porque piensan que no van a ser capaces de sacar adelante estos estudios y porque carecen de referentes femeninos en profesiones científicas y técnicas”. Un informe de la patronal tecnológica DigitalES señalaba que el 25 % de los estudiantes de Se-

ros y el informe PISA señala que el 12 % de los chicos quiere trabajar en sectores relacionados con la ciencia o la ingeniería, mientras que ese porcentaje en las chicas se reduce al 5,2 %. Eulalia Flo, directora general de Commvault en España y Portugal, recuerda que las profesiones STEM son las más demandadas hoy en día. “Y lo serán aún más en el futuro”. Una demanda que hace imprescindible que las mujeres se formen en ellas para que “tengan las mismas oportunidades de diseñar el futuro”. Para Flo hay que cambiar la forma en la que se está promocionando estas disciplinas con el objetivo de incluir la mirada femenina y la perspectiva de género. “Es importante dar voz a esas mujeres, sobre todo si aportan esa diferencia de perspectiva, esa visión más holística de cómo sus contribuciones aportan resultados tangibles”.

“Hay que ser capaces de motivar a las niñas y de terminar con la idea de que las carreras STEM son cosa de hombres”

dicas que se potencian son tanto o más importantes en esta etapa que cualquier programa de promoción de las STEM”, determina la directiva de Commvault. Educación y visibilidad de los referentes femeninos son las dos recetas fundamentales que Montserrat Peidró, directora general de ALSO Cloud Spain, recomienda para incrementar el número de niñas que se decanten por las disciplinas STEM. Junto a ellas, la pasión y las ganas. “El mundo que conocemos hoy es tecnológico; y entrar en el mundo de la tecnología es simplemente formar parte del mundo en el que vivimos”, señala. Ingeniera de formación, está convencida de que “hay que ser capaces de motivar a las niñas y de terminar con la idea de que las carreras STEM son cosa de hombres”. Mariola Martínez, presidenta de España y vice-



Montserrat Peidró
directora general de ALSO Cloud Spain

cundaria, Bachillerato y FP no escogerían formarse en ramas STEM debido a que desconocen las oportunidades laborales que ofrecen estos itinerarios. “Hay que visualizar qué oportunidades ofrece cada grado universitario”, insiste la directiva de Xerox.

Oportunidad de negocio

La Agenda España Digital 2025 tiene como objetivo incrementar en 20.000 profesionales el número de especialistas TIC en los próximos años, lo que demuestra que el sector TIC está batiendo récords en creación de empleo. LinkedIn prevé que en los próximos cinco años se podrían crear más de dos millones de empleos relacionados con la



Carmen Muñoz
directora general de Exclusive Networks
en España y Portugal

“Las mujeres tenemos que creer en nuestras capacidades, romper las barreras y promover el cambio”

Segmento de la distribución

El área de la distribución es un segmento poblado, y liderado, por hombres. Sin embargo en España hay dos valiosas excepciones: Carmen Muñoz y Montserrat Peidró, que lideran, respectivamente, la estrategia de Exclusive Networks y de ALSO Cloud. No son solo ellas los únicos referentes femeninos en sus organizaciones: el 61 % de los empleados de ALSO en España y el 80 % de su equipo de dirección es femenino y, a nivel mundial, la proporción de mujeres dentro del grupo está cercana al 45 %, muy por encima del nivel medio del sector de las TIC que se situó justo por debajo del 25 % en 2020 según Eurostat. "Hay muchísimo talento femenino y lo más interesante es cómo se complementa de manera recíproca con el talento masculino", explica Peidró. En el seno de Exclusive Networks son cinco las mujeres que ejercen

de *country managers*. "Los ratios entre mujeres y hombres irán mejorando gracias a nuestra política de diversidad, que incluye la búsqueda activa de nuevo talento, apoyada por acuerdos y alianzas con centros educativos para despertar el interés de las nuevas generaciones en ciberseguridad", señala Carmen Muñoz. "Las mujeres tenemos que creer en nuestras capacidades, romper las barreras y promover el cambio. Y las mujeres en puestos directivos tenemos un papel clave para propiciar esta evolución impulsando las medidas de conciliación, desarrollando políticas de recursos humanos focalizadas en la búsqueda de talento, en los planes de desarrollo de carrera, *mentoring* y *coaching* de líderes y, por supuesto, sirviendo de ejemplo para el resto de mujeres de nuestras organizaciones".

tecnología, pero no solo en el sector tecnológico. "Necesitamos más mujeres que trabajen en *cloud computing*, ciberseguridad e inteligencia artificial", recuerda Carolina Castillo, directora de Operaciones y Marketing de Microsoft, que puntualiza que también se requieren más profesionales certificadas y conocedoras de la tecnología de negocio. "En el mundo actual, en el que son claves el *big data* y el *business intelligence*, muchos roles exigen aptitudes técnicas. Es el caso, por ejemplo, de los científicos de datos, los comerciales, los jefes de ventas, los profesionales que proporcionan el servicio al cliente, el trabajo de campo y los consultores de finanzas y operaciones".

De la incorporación de la mujer a estas disciplinas depende el progreso de España. Durante la Semana de la Educación Emprendedora, Samsung organizó una mesa de debate en la que participaron expertos sobre emprendimiento digital



Ana Carolina Cardoso
directora de canal de APC by Schneider Electric

"La educación cumple un rol muy importante"

femenino. Anna Coll, B2B Channel Sales manager de la multinacional, recuerda que una de las grandes conclusiones fue que la incorporación de las mujeres a las profesiones STEM es crucial para España. "La tendencia para los últimos años no es positiva", valora. Las previsiones son que la brecha de féminas respecto a los hombres se agudizará en la ingeniería informática: en los años 80, cuando era una licenciatura, había un 40 % de mujeres y en la actualidad, en algunos centros, su presencia no alcanza el 10 %. "La causa principal de esta preocupante tendencia señala un problema estructural, en el que la educación cumple un rol muy importante para revertir esta tendencia desde los primeros años escolares".

Papel público

Carmen Muñoz, directora general de Exclusive Networks en España y Portugal, señala que el pa-



Anna Coll
B2B Channel Sales manager de Samsung

pel de las instituciones públicas es clave a través de la puesta en marcha de programas dirigidos a divulgar y concienciar de las disciplinas STEM entre las féminas. Una labor que une a la difusión y sensibilización a través de los medios de comunicación. "La inclusión de campañas publicitarias y especiales informativos en los medios ejercerá un papel fundamental". La directiva insiste en la educación en edades tempranas, en la eliminación de estereotipos y en la identificación

"La falta de niñas que quieren estudiar carreras STEM es un proceso que empieza en la infancia y que debemos abordar desde múltiples áreas"

de referentes femeninos. "El uso de las redes sociales y la familiarización de los entornos digitales de los jóvenes son un facilitador para captar la atención y el interés de las chicas y su participación en este tipo de carreras".



Carolina Castillo
directora de Operaciones y Marketing de Microsoft

“El sector TIC sigue siendo un sector muy masculinizado y hay que trabajar para que sea más diverso”

Carolina Moreno, vicepresidenta de ventas en EMEA y directora general para el sur de Europa de Liferay, corrobora que las instituciones públicas, junto a las privadas y desde todos los ámbitos sociales, deberían ser ejemplo en lo que a conciliación y teletrabajo se refiere y sentar las bases para unas buenas prácticas. A su juicio, las instituciones públicas deben ayudar a eliminar los estereotipos creados alrededor de la tecnología y apoyar una educación igualitaria donde la innovación y la ciencia estén presentes y sean protagonistas del desarrollo económico y social en igualdad de condiciones, con independencia de géneros. “Esta educación debe mostrar aspectos tan relevantes como la creatividad, el impacto en la mejora de la sociedad o el dinamismo en el sector, que dan una visión más real de estas disciplinas TIC, de su situación actual y del potencial que tienen”.

Adela de Toledo, *country manager* de Pure Storage Iberia, corrobora que las instituciones públicas tienen un papel esencial. “Marcan las directrices que empresas y ciudadanos deben seguir”. Según el Instituto Europeo de la Igualdad, España es el sexto país europeo con mayor Índice de igualdad de género. Sin embargo, reconoce que aún queda lejos del objetivo real: la auténtica igualdad. “El trabajo que hacen instituciones públicas y organizaciones privadas es fundamental para avanzar en este sentido”, insiste.

Liderazgo femenino

Según el informe “Brecha salarial y presencia directiva de mujeres 2021”, elaborado por Eada Business School e Icsa Grupo, las mujeres ocupaban el 18,8 % de los puestos directivos en España, dos puntos por encima de los datos de 2020. Asegura Ángeles Delgado, presidenta de Fujitsu España, que la pandemia ha ralentizado la evolución de las mujeres en

“Estamos lejos de poder presumir de ser un país igualitario”



Adela de Toledo
country manager de Pure Storage Iberia

puestos directivos, lo que “requiere ahora darle un nuevo y decidido impulso”. Una situación que ha conducido a una reflexión en muchas organizaciones con una positiva conclusión: “El factor de igualdad de género adquiere una importancia cada vez mayor como elemento transformador de las organizaciones, los negocios y la sociedad”, señala. No en vano, la Organización Internacional del Trabajo (OIT) señala que las mujeres en puestos directivos aumentan el rendimiento empresarial de la organización. “Hay que analizar y transmitir a las mujeres qué supone la transformación digital en clave femenina”, analiza. Un proceso en el que se gana flexibilidad y conciliación, y acceso a nuevos sectores donde ahora prima el conocimiento. Y la oportunidad “de contribuir al diseño de una nueva

España, quinto país de la Unión Europea con la mayor tasa de desempleo femenino en el sector tecnológico

Según Eurostat, España es uno de los países europeos que presenta mayor tasa de desempleo femenino en el sector científico y tecnológico. En el caso de mujeres con formación superior el baremo de paro se sitúa en el 10,8 %; una cifra que solo superan Turquía, Grecia, Montenegro y Macedonia del Norte, con 15,6 %, 13,5 %, 12,5 % y un 10,8 %, respectivamente. En el caso de mujeres sin formación superior, el porcentaje asciende a más de un 24 %, solo por debajo de Grecia (25,2 %) y Montenegro (24,8 %). Después de Grecia, España es el segundo país con más diferencias en el paro entre hombres y mujeres: de 3 % y 6 % entre hombres y mujeres con estudios y sin estudios superiores. República Checa, Alemania y Países Bajos son los países con menor tasa de desempleo en mujeres con formación superior: 1,1 %, 1,4 % y 2 %, respectivamente; y una tasa de desempleo en mujeres sin formación superior del 4,4 %, 5,4 % y 6,5 %, respectivamente. Los países vecinos de España, Portugal y Francia, cosechan una tasa de desempleo en mujeres con formación superior del 4,6 % y 4,30 %, respectivamente; y del 9,1 % y 12,6 % en cuanto a desempleo en mujeres sin formación superior. Italia presenta tasas similares con un 4,4 % de desempleo en mujeres con formación superior y un 14,4 % de desempleo en mujeres sin formación superior.



Ángeles Delgado
presidenta de Fujitsu España

“Hay que analizar y transmitir a las mujeres qué supone la transformación digital en clave femenina”

sociedad en la que la opinión del 50 % de la población no puede ser excluida”.

Un panorama que en el caso de la Administración Pública presenta un panorama más halagüeño. Según los últimos datos del INE, el porcentaje de mujeres que ostentan altos cargos en la Administración General del Estado alcanza ya el 43,5 %. Sin embargo, en las organizaciones del IBEX 35 sólo se situó en el 27,7 %; aunque algo mejor, aún hay camino por recorrer. Otro dato positivo es la presencia de mujeres en los Consejos de Administración, que se ha duplicado en los últimos 7 años y seguirá aumentando. “Hay que trabajar intensamente en hacer llegar estos mensajes y dar mayor visibilidad a las muchas mujeres que son referentes en campos científicos y tecnológicos, buscando nuevas y creativas maneras de llegar a todas las mujeres”, explica Delgado; quien destaca, como un magnífico ejemplo de cómo hacer esto de forma innovadora, el recientemente convocado Premio Hortensia Roig de literatura infantil para inculcar a las niñas el gusto por la tecnología.

En España el porcentaje de mujeres en el sector TIC que ocupa cargos directivos (un 34 %) es similar al general, cifrado en un 35 %. Un panorama que, para Carolina Moreno, exige un camino de mejora. “Las compañías debemos seguir trabajando en el ámbito de las políticas y los planes de igualdad con más y mejores iniciativas”, señala. “A pesar de los esfuerzos que realizamos, a nivel país no estamos en el punto

que queremos y hay que incidir sobre dos aspectos fundamentales. Primero, las compañías debemos seguir trabajando en el ámbito de las políticas y los planes de igualdad con más y mejores iniciativas”. En segundo lugar, señala, habría que destacar la confianza. “Las niñas y jóvenes de hoy en día, que son las profesionales del futuro, tienen que creer en sí mismas y convencerse de que son perfectamente válidas”.

Mujeres en el sector TIC

Para Helena Herrero, en el sector tecnológico, a pesar de ser uno de los que más han progresado, todavía se perciben bastantes diferencias. Según un estudio de la Comisión Europea sobre la mujer en el sector digital sólo 24 mujeres de cada 1.000 se gradúan en estudios TIC, y de ellas, sólo 6 trabaja en el sector tecnológico. “Una de las mayores dificultades radica en la falta de referentes en estos sectores. Esto hace que las niñas no se vean atraídas por este tipo de carreras porque no tienen ejemplos de mujeres en estos ámbitos. Por eso, es muy importante visibilizar a las mujeres que están desarrollándose profesionalmente en el ámbito científico, matemático o tecnológico y hacer que estos perfiles femeninos sean modelos a seguir para las jóvenes estudiantes”.

Carolina Castillo reconoce que el sector TIC sigue siendo un sector muy masculinizado. “Hay que trabajar para que sea más diverso”. La directiva señala que la falta de talento digital es un problema y la escasez de perfiles adecuados para cubrir las necesidades de las empresas se acentúa en el caso de las mujeres. “Tenemos un

problema de falta de talento digital. El mundo va más rápido que los perfiles disponibles para adoptar y acelerar la disrupción. Y este gap es aún mayor si hablamos de mujeres”.

Según IDC, el 46 % de las empresas españolas tiene problemas para encontrar los perfiles digitales que necesita y un porcentaje cercano al 80 % prevé retrasos y cancelaciones en sus proyectos por no contar con personas con las habilidades requeridas. “Por lo tanto, existe una demanda urgente de formar talento cualificado con capacidades digitales, la formación en STEM es una prioridad en la que no tienen cabida las distinciones de género”, señala la directiva de Microsoft.

Según un informe del Instituto Europeo de Igualdad de Género, al paso que vamos, alerta Adela de Toledo, se necesitarán tres generaciones para alcanzar el objetivo de igualdad plena. La pandemia ha influido negativamente en este progreso. “Podemos ver una mejora, pero estamos lejos de poder presumir de ser un país igualitario”. La directiva de Pure Storage señala, por ejemplo, que sólo uno de cada cinco profesionales de inteligencia artificial son mujeres, según IndesIA, la asociación para la aplicación de la inteligencia artificial en la industria. “Todos —hombres y mujeres— tenemos un papel que desempeñar para animar a más mujeres a trabajar y a estudiar estas materias”.

Una carrera en la que sigue siendo pieza fundamental la conciliación. “En España sigue existiendo un reto en el camino hacia la igualdad: el de la conciliación”, reivindica Carmen Muñoz.

“Las niñas y jóvenes de hoy en día, que son las profesionales del futuro, tienen que creer en sí mismas y convencerse de que son perfectamente válidas”



Carolina Moreno
vicepresidenta de ventas en EMEA
y directora general para el sur de Europa de Liferay

"A pesar de que la pandemia ha supuesto un antes y un después en los modelos de trabajo de las compañías y una mayor flexibilización, ésta sigue siendo un freno muy importante para conseguir una mayor presencia femenina en puestos directivos".

Iniciativas sobre el terreno

Todas las empresas tecnológicas muestran su compromiso con la igualdad con iniciativas concretas. En el caso de APC by Schneider Electric, los objetivos se centran en aumentar la diversidad de género un 50 % en la contratación, un 40 % en la gestión de primera línea y un 30 % en los equipos de liderazgo. La compañía tiene en marcha la iniciativa We Mean Teach, "una iniciativa que tiene como objetivo visibilizar los perfiles femeninos STEM dentro y fuera de la compañía y crear un ecosistema que permita a las mujeres compartir con la comunidad los retos que conlleva para nosotras trabajar en posiciones STEM", comenta Cardoso.

En Fujitsu España, las mujeres suponen el 33 % del órgano de dirección de la empresa. Entre las iniciativas más destacadas que tienen en marcha destaca "Empowering Woman's Talent", que aborda "un amplio abanico de medidas, no sólo de conciliación, sino también de confianza", puntualiza Ángeles Delgado.

Fomentar el emprendimiento femenino a través de los programas Samsung Innovation Campus y Samsung DesArrolladoras dentro de su estrategia "Tecnología con propósito" es objetivo de Samsung. Dos iniciativas con las que han formado a más de 3.000 mujeres españolas, impulsando el talento en las profesiones



Mariola Martínez

presidenta de España y vicepresidenta de software y servicios para el canal en EMEA de Xerox

"Las profesiones STEM son las más demandadas hoy en día. Y lo serán aún más en el futuro"

STEM y preparándolas para las profesiones más demandadas.

Samsung DesArrolladoras es un programa que surge para disminuir la escasez y la brecha de género existente en España en el campo de la ingeniería y la tecnología, además de para impulsar el talento femenino en este ámbito. "Las participantes pueden aprender los lenguajes de programación más demandados", puntualiza Coll.

Commvault cuenta con un programa de mentorazgo para impulsar la trayectoria de mujeres con un alto potencial. Desde hace siete años, además, despliega la iniciativa "Women in Technology" (CV WiT), una comunidad global cuyo objetivo es fomentar el avance de las mujeres en la tecnología mediante la creación de redes, formación y tutorías. En la actualidad cada región de Commvault dispone de un grupo WiT activo, que crece año tras año, centrado en capacitar a las mujeres y ayudarles a desarrollar sus carreras profesionales dentro de la empresa. Además, el grupo apoya distintas causas sociales para fomentar el interés de las mujeres en materias STEM.

HP trabaja con asociaciones como Junior Achievement, la Fundación Universidad Empresa y otras instituciones locales para realizar actividades que fomenten las vocaciones STEM. Junto a ello, está presente en eventos y ferias tecnológicas para las nuevas generaciones como es el caso de YoMo (*Youth Mobile Congress*). Desde hace años, organiza HP CodeWars, un evento local diseñado como una competición educativa centrada en la estimulación de la vocación de los jóvenes, con especial foco en las niñas. "Necesitamos más que nunca que este talento STEM sea diverso y que continuemos incrementando el número de mujeres



Eulalia Flo

directora general de Commvault en España y Portugal

en estas disciplinas", insiste Helena Herrero. Liferay ha anunciado su primer Plan de Igualdad en España. "Queremos ratificar nuestro compromiso con la diversidad, la igualdad y la inclusión", explica Carolina Moreno. Actualmente la plantilla en España de Liferay, donde el perfil mayoritario es el de ingenieros y desarrolladores de producto, se distribuye entre un 37 % de mujeres y un 63 % de hombres. "Este plan contiene un amplio conjunto de medidas y protocolos para garantizar una mayor equiparación de los sexos en todos los departamentos", señala. En los puestos directivos, Liferay España cuenta con una paridad completa entre hombres y mujeres.

Microsoft lleva años colaborando con otras organizaciones y entidades para derribar los estereotipos y cerrar esta brecha. Además, cuenta con la iniciativa MakeWhatsNext "en la que englobamos todas nuestras acciones de fomento de habilidades digitales en las niñas", recuerda Carolina Castillo.

Los Premios WONNOW, que impulsa junto a Caixabank, son un buen ejemplo. "Impulsamos estos galardones para fomentar el talento femenino y promover la diversidad y la presencia de mujeres en el ámbito de la tecnología y las ciencias desde el inicio de su carrera profesional", explica Castillo. También participa y colabora en otras iniciativas, como los Premios Ada Byron junto a la Universidad de Deusto, para ayudar a dar visibilidad al trabajo de mujeres en

el ámbito STEM. Por último, su iniciativa MakeWhatsNext engloba todas sus acciones de fomento de habilidades digitales en las niñas. 

"Hay que transmitir a las niñas que, si quieren, pueden. Querer es poder"

Su cartera de pedidos para los próximos dos años asciende a 370 millones de euros

El negocio digital, motor del crecimiento de Ibermática en 2021

"Hemos cerrado el mejor año de nuestra historia", declaró Juan Ignacio Sanz, CEO de Ibermática, al valorar los resultados obtenidos en 2021. La compañía ha alcanzado los 276 millones de euros, lo que supone un incremento del 8,8 % y un beneficio de 11,3 millones de euros. Estos resultados superan los 260 millones que consiguió en 2008, su facturación más elevada hasta 2021, y rebasan las previsiones marcadas por la propia compañía.

 Rosa Martín

Las razones de este crecimiento se encuentran en el buen comportamiento de su negocio tradicional de externalización de servicios u *outsourcing*, que ha ascendido a 156 millones de euros, y por el impulso del negocio digital que engloba bajo el nombre de Advanced Solutions, que ha rondado los 120 millones de euros (119,5 millones).

Este último terreno, que aglutina todo el nuevo negocio que se ha puesto en marcha en sus últimos planes estratégicos, está siendo el motor del crecimiento al lograr un incremento del 53 % desde 2018 hasta 2021. En este periodo los ingresos han crecido desde los 78,1 millones de 2018 hasta los 119,5 de 2021.

Este rápido crecimiento en los últimos tres años augura que esta área sea la de mayor proyección para los próximos años. En este apartado los proyectos de transformación digital han alcanzado 27,6 millones de euros, los servicios en la nube, 24,5 millones; el negocio en torno a SAP, 24,4 millones; Smart Factories, 24,1 millones; el negocio sobre las soluciones de Microsoft, 8,6 millones; Ciberseguridad, 7,1 millones; y Analítica e Inteligencia Artificial, 3,2 millones.

En el ámbito del *outsourcing*, sus resultados también son positivos, aunque como reconoce el directivo su ritmo de crecimiento ha sido más lento. Un dato significativo es que ha incrementado su cifra de contratación un 84 % hasta los 416 millones de euros.

Sanz subrayó que los resultados han sido muy buenos porque "hemos aprovechado el momento del mercado, pero los profesionales han funcionado muy bien". En este sentido, la compañía presume de contar con una tasa de rotación de personal del 10 % cuando la media del sector se sitúa en el 25 %.

Ibermática ha seguido creando empleo en 2021. Ha incorporado a 287 profesionales, ascendiendo su plantilla a 4.075 trabajadores. Y planea seguir incrementando su equipo, a pesar de la escasez del talento y de la elevada demanda de perfiles TIC en nuestro país.

Una de las ventajas que ofrece a los profesionales es la opción de trabajar "a la carta", es decir, la opción de poder elegir entre el formato presencial, en remoto o híbrido.

Próximos objetivos

El CEO de Ibermática avanzó que la intención de la compañía es seguir en esta línea ascendente incrementando sus ingresos tanto por la vía orgánica como por las adquisiciones. En 2021 ha comprado la compañía denominada El Arte de Medir, especialista en análisis de datos, y su intención es incorporar otra empresa especializada este año en sus áreas de interés que son la analítica, la inteligencia artificial y la tecnología de SAP y de Salesforce.

En el plano económico, la compañía quiere alcanzar un crecimiento del 5 % hasta situar su cifra de negocio en 290 millones de euros y lograr un incremento de 1,6 millones de euros hasta conseguir 12,9 millones.

En el ámbito de Advanced Solutions el objetivo es alcanzar 146 millones de euros, 26 millones más que en 2021. Y en el campo de los servicios a empresas su intención es que Manufacturing alcance 68 millones de euros, Consumer 57 millones, Administración Pública 50 millones, Seguros Financieros y Seguros 35

millones, Utilities 32 millones, Telecomunicaciones y Medios de Comunicación 31 millones y Salud 17 millones de euros.

Para lograr estos objetivos se apoyará en la gestión de los fondos Next-GenerationEU con el fin de conseguir 10 millones en proyectos, el impulso a la innovación para su propia cartera de soluciones y el trabajo de su equipo.

Sanz también destacó que en 2023 cumplen 50 años en el mercado, un hito que marcará el comienzo de un nuevo plan hasta 2025 para alcanzar los 500 millones de facturación y 5.000 empleados. 



Juan Ignacio Sanz,
CEO de Ibermática



**No hay seguridad
sin canal**

Ciberseguridad everywhere:

presente y futuro de los servicios gestionados de ciberseguridad



El incremento de las ciberamenazas, el déficit de talento y la fragmentación de los entornos de ciberseguridad son los principales catalizadores del incremento del consumo de la seguridad como servicio en España.

Este año está resultando especialmente interesante desde el punto de vista de la ciberseguridad. Por una parte, motivado por el incremento del número y sofisticación de las amenazas de seguridad y la falta de habilidades de seguridad que obligan a las organizaciones a repensar su estrategia de ciberseguridad, y por otra, la reciente guerra de Rusia y Ucrania, que está multiplicando los ciberataques (especialmente a entidades financieras e infraestructuras críticas), con crecimientos de hasta un 56 % en el número de ciberataques en los últimos dos meses.

Este crecimiento del número y variedad de ciberataques (cada día se producen más de 200.000 ataques de *ransomware*) hace que se requiera una mayor diversidad de defensas. Por ello, las organizaciones buscan mejorar la seguridad de su infraestructura de red y recibir

servicios avanzados de asesoramiento para proteger adecuadamente sus organizaciones. Por otra parte, la escasez de habilidades de seguridad y la dificultad y los gastos de reclutamiento y retención de profesionales de seguridad cualificados de un grupo de mano de obra finito (así como la importancia de evitar el agotamiento de los analistas de seguridad), están llevando a las organizaciones españolas a adoptar nuevos enfoques de seguridad que mejoren la seguridad de su infraestructura de red, así como servicios avanzados de asesoramiento que ayuden a proteger adecuadamente sus organizaciones. El mercado de la seguridad en España refleja esta transformación de las organizaciones, donde se produce un desplazamiento de la seguridad perimetral hacia la seguridad del dato. En concreto, las prioridades para este año en la empresa española (en materia de ciberseguridad) están estructuradas alrededor de la con-

fianza digital (aspecto clave de las empresas que debe medirse, y parte de ello está relacionado con la seguridad y privacidad de los datos), la resiliencia empresarial (entendida como "empresa mínima viable" o lo que es lo mismo: la infraestructura, el acceso y los datos necesarios para que los procesos críticos de la empresa sigan funcionando en cualquier situación), así como la soberanía de los datos, especialmente importante en Europa con las regulaciones locales y de la UE.

Estas tres prioridades afectan de manera directa a la cartera de seguridad de los proveedores y sus enfoques tienen un impacto material en la evolución comercial y estructural de las plataformas, los productos y los servicios; por ejemplo, la seguridad como servicio.

De esta manera, en un entorno híbrido *multi-cloud* que es donde confluirá el tráfico de datos, el consumo de los servicios de seguridad se dará a través de servicios gestionados de seguridad y de integración. De manera concreta, con un crecimiento respecto del año pasado del 7,7 %, IDC prevé que el mercado de seguridad en España alcanzará los 1.749,3 millones de euros en 2022 y para el año 2025 podría superar la barrera de los 2.200 millones de euros, manteniendo ritmos de crecimiento similares que se acercan al doble dígito. Los segmentos de mayor crecimiento son los relativos a servicios gestionados de seguridad (11,8 %), servicios de integración (11,8 %) y servicios de red (10,6 %).

El auge del consumo de la seguridad como servicio se dará de manera decidida en las organizaciones como alternativa para abordar la fragmentación de los entornos de seguridad actuales, así como para paliar el aumento de la complejidad de las infraestructuras y el ritmo al que surgen las nuevas tecnologías y amenazas. 

José Antonio Cano
Director de análisis de IDC

Los socios apuestan por la certificación en Samsung Knox

La seguridad es una parte esencial en la nueva era móvil y el canal apuesta por una mayor formación en este ámbito. En lo que llevamos de 2022, nuestros socios han realizado un 173 % más de cursos con respecto al año pasado.

Tras dos años de transformación en nuestro tejido empresarial por la pandemia, las empresas han comprobado los beneficios que les aportan las tecnologías móviles. Desde la agilización y control en tiempo real de las operativas hasta la respuesta inmediata al usuario; la movilidad ha dado como resultado una mejora en la toma de decisiones y, por lo tanto, una mayor productividad, eficiencia y competitividad. La seguridad se ha convertido en un eje fundamental dentro de la digitalización. Todos los procesos de negocio deben desarrollarse con fiabilidad y la información corporativa debe estar protegida ante cualquier tipo de ataque o intromisión por parte de terceros. En Samsung, la seguridad forma parte intrínseca de nuestro porfolio. Samsung Knox se incluye de fábrica en nuestros dispositivos, que están protegidos desde el chip hasta el software. Por otro lado, sabemos que las amenazas crecen y se transforman muy rápidamente. Nuestro equipo de I+D, formado por un 25 % de la plantilla, analiza las vulnerabilidades más sofisticadas y continúa desarrollando las capacidades de Knox. El mejor ejemplo es Samsung Knox Vault, incluido en la gama S22, que incluye un procesador y una memoria seguros que aíslan por completo los datos sensibles del sistema ope-



rativo, como contraseñas, datos biométricos o claves de Blockchain. Nuestros socios de canal también son muy conscientes de la importancia de la seguridad. Empresas de todo tipo acuden a ellos como los principales referentes en digitalización; y conocen muy de cerca sus necesidades y preocupaciones. El año pasado adquirieron un grado muy elevado de especialización por la demanda de sus clientes y este año la tendencia sigue en crecimiento. En lo que llevamos de este año, España es el segundo país de Europa con más cursos realizados en nuestra plataforma de formación (*Samsung Business Academy*), un 173 % más con respecto a 2021. Además, somos el tercer país de Europa en conseguir un mayor número de certificaciones.

En definitiva, el canal de distribución sigue formándose en productos y soluciones, no sólo para cumplir con la demanda de la industria, sino también para formar parte de nuestro programa de canal SMVP (*Samsung Mobile Valued Partner Programme*). El canal sabe que el verdadero valor de una propuesta comercial va más allá de las especificaciones de un dispositivo y se asienta en la seguridad y soluciones que aporta un ecosistema móvil.

Samsung es un socio de confianza para la transformación digital de las empresas, ya que somos uno de los principales fabricantes móviles que ofrece una seguridad de vanguardia, a través de Samsung Knox. Colaboramos con INCIBE en España y nuestros dispositivos están certificados por el CCN.

Para nosotros es una satisfacción que nuestros socios puedan apoyarse en nuestras soluciones para cumplir con las necesidades y expectativas de sus clientes. El aumento de las formaciones en seguridad demuestra que quieren ofrecer un servicio de calidad y ser los mentores de todas las empresas que están abordando su transformación digital. Gracias a Samsung Knox pueden ofrecer soluciones de vanguardia a sus clientes y convertirse en una parte esencial de la digitalización de las empresas españolas. 

Para nosotros es una satisfacción que nuestros socios puedan apoyarse en nuestras soluciones para cumplir con las necesidades y expectativas de sus clientes. El aumento de las formaciones en seguridad demuestra que quieren ofrecer un servicio de calidad y ser los mentores de todas las empresas que están abordando su transformación digital. Gracias a Samsung Knox pueden ofrecer soluciones de vanguardia a sus clientes y convertirse en una parte esencial de la digitalización de las empresas españolas. 

Anna Coll
Responsable de canal en Samsung Electronics

SD-WAN, la nube, el desarrollo de la seguridad gestionada y la protección de los entornos industriales, oportunidades para el canal

"Es el **mejor momento** para ser parte del ecosistema de *partners* de Fortinet"



Ha sido un año espectacular", insiste. Sato señala la enorme expansión que ha experimentado el área de SD-WAN, donde Fortinet ha conseguido situarse como líder en el apartado que Gartner define como WAN Edge Infrastructure. Un negocio cuyos proyectos se vinculan en muchas ocasiones con el área SD-Branch. "Gracias a la integración nativa de las soluciones de acceso (switches y puntos de acceso), es posible ofrecer una conectividad segura de la oficina remota, trasladando las políticas de seguridad a los puntos de acceso", explica. Una convergencia que permite que un proyecto de SD-WAN se multiplique por dos o por tres. "La red, por tanto, ejerce de palanca", explica. "Nuestro canal tradicional, vinculado con la ciberseguridad, ha observado un complemento y una oportunidad de negocio en el área de las redes". De hecho, el acercamiento de Fortinet a estas soluciones lleva el nombre de Network Security, lo que apela, directamente, a la seguridad de red. En España, Fortinet ya cuenta con 16 *partners* que exhiben la especialización en SD-WAN. "Se trata de un negocio que nació unido al ahorro de costes y que está evolucionando hacia el control de los datos y de las aplicaciones", explica. A su juicio, SD-WAN está en la agenda de inversión de los responsables TI de las compañías. Una aseveración refrendada por el hecho de que en la facturación de la multinacional más del 16 % estuvo vinculada con una SD-WAN segura en 2021.

La consolidación de la plataforma Security Fabric, que aúna soluciones perfectamente integradas que llevan la protección hasta el último rincón, también ha sido clave. Una estrategia que, como recuerda Sato, casa a la perfección con el concepto de ciberseguridad Mesh que entona Gartner. "Es una arquitectura que, aplicando la máxima automatiza-



Guillermo Sato,
director de canal de Fortinet

Reconoce Guillermo Sato, director de canal de Fortinet, el excelente año fiscal que cerró la compañía el pasado 31 de diciembre. A nivel mundial la compañía facturó 4.180 millones de dólares, lo que supuso un potente ascenso del 35 %. Sin desvelar, como es norma en la casa, cifras locales, el responsable de canal explicó que la estrategia de Fortinet está perfectamente alineada con las tendencias del mercado: el desarrollo de SD-WAN, la protección de los entornos del teletrabajo, la expansión de la seguridad en la nube y la consolidación de los modelos de seguridad gestionada. Áreas que señalan las máximas oportunidades en este 2022.

Marilés de Pedro

ción, simplifica las tareas de adquisición, operación y soporte".

Los buenos resultados han permitido ampliar el equipo local, con incorporación de profesionales para el negocio en áreas como la seguridad de los entornos industriales o para el desarrollo de la nube. También ha crecido la plantilla destinada a dar soporte al canal.

Repaso al programa de canal

Hace un par de años la marca lanzó su programa de canal, Fortinet Engage, que un año después se actualizó a Engage 2.0. Un programa que reparte a los *partners* en cuatro categorías: Advocate, Select, Advanced y Expert. "Contamos con un amplio canal; con *partners* especializados y perfiles muy diferentes".

En el último año el canal ha incrementado el número de compañías que lo conforman, tanto en el segmento de la pyme como en el área *enterprise*. "Ha crecido la facturación media de los *partners*", asegura. "Todos los *partners* han crecido con Fortinet".

El programa permite a los *partners* adoptar diferentes modelos de negocio: el desarrollo de la seguridad en la nube, la reventa de hardware y la oferta de servicios gestionados. Fortinet les ofrece herramientas y la capacidad para que se diferencien, con el objetivo último de que mejoren su beneficio. "No se trata de que seleccionen entre un modelo u otro, sino de que escojan lo que mejor les encaje", explica. El negocio MSSP ha tenido un enorme desarrollo. "Está creciendo muchísimo", desvela. El panorama de mercado, valora, es muy propicio. "Más del 40 % de las pymes no tiene ningún tipo de concienciación o especialización en temas de seguridad. Viven ajenas al mundo de la ciberseguridad". Un dato, contundente, que se une al hecho de que más del 65 % de las medianas y las pequeñas cuentas reconocen que han sido atacadas. "Muchas de estas compañías no tiene un responsable de TI. Mucho menos alguien con conocimiento en el área de la seguridad; lo que propicia que sea un segmento en el que encaja a la perfección el modelo de seguridad gestionada".

Prácticamente la totalidad de las soluciones de Fortinet está accesible en un formato de pago

Los mayoristas, claves

Con un negocio que transcurre en su totalidad a través del canal, Arrow y Exclusive Networks conforman el dueto mayorista. En este 2022 van a jugar un papel especial en el desarrollo del negocio de la pyme. También en la expansión de los modelos de seguridad gestionada y en la protección de los entornos de la nube.

"Su papel es esencial", reitera. "Su compromiso para extender el número de certificaciones en el canal es muy importante".

por uso. "No se requiere ningún desembolso inicial. Las empresas conocen cuál es el coste y qué beneficio pueden esperar".

Fortinet llevó a cabo una encuesta a principios de año entre sus *partners* de EMEA en la que cerca del 80 % aseguraba que ya tenía en mente o estaba desplegando servicios gestionados de ciberseguridad. En España, aunque el grupo de *partners* que se declaran formalmente MSSP está conformado por una treintena de compañías, Sato asegura que están trabajando, bajo este modelo, con cientos de *partners*. "España está siendo punta de lanza en Europa ya que de esos 30, alrededor de 8 están impulsando soluciones más allá del negocio más tradicional de Fortinet, identificado con el *next generation firewall*, como es el caso del *email*, WAF, DDR o SIEM", desvela.

"Ha crecido la facturación media de los *partners*"

Explosión del negocio de la nube

El desarrollo del área de la nube es uno de los focos de negocio prioritarios. El año pasado Fortinet simplificó el acceso a este modelo y ha seguido facilitando a los *partners* tradicionales su evolución hacia este mercado. "El canal tradicional volcado en el desarrollo de la seguridad y las redes no tiene absolutamente nada que ver con los *partners* nacidos en la nube. Está focalizado en el despliegue de la seguridad pero no conoce las particularidades de cada uno de los hiperescalares. Y, al contrario,

los *partners* especializados en los entornos de la nube nos aportan un enorme valor pero la seguridad no forma parte de su negocio", analiza. El programa de canal de Fortinet ofrece un *go to market* generalizado para todos, con formaciones específicas para cubrir esas carencias. "Ya contamos con una decena de *partners* tradicionales que están evolucionando hacia la seguridad en la nube".

La marca ha simplificado los requisitos para que los *partners* especializados en los hiperescalares consigan las certificaciones que les den acceso a la seguridad. Sato asegura que ya están empezando a trabajar con alguno de los *partners* más relevantes de cada uno de los hiperescalares (Azure, AWS y Google).

Batería de especializaciones

A las tradicionales especializaciones del programa de canal (Adaptive Cloud Security, LAN Edge&SD-Branch, Secure SD-WAN y Data Center), Fortinet unió el año pasado tres más: seguridad en los entornos industriales, Security Operations, para la gestión óptima del SOC; y Zero Trust Access.

Sato reconoce una buena cobertura en SD-WAN y en el área de acceso. "Está en auge la certificación de Zero Trust Access. Ante el auge del teletrabajo y la digitalización del negocio el perímetro ha desaparecido por lo que resulta fundamental controlar a qué datos y aplicativos se accede. El canal está viendo la oportunidad".

También está en plena expansión la especialización de protección de los entornos industriales, un área en la que han reforzado el equipo con profesionales con un alto conocimiento en este apartado. "Ya somos un referente", asegura. "Aunque nuestra madurez en este apartado es menor, contamos con importantes referencias en el despliegue de esta protección; por lo que es clave contar con *partners* especializados para que sean realmente la punta de lanza con la que ir de la mano a proyectos específicos y complejos". Por último, la protección del *cloud* también está creciendo de manera importante. 

WatchGuard quiere incrementar su cobertura de canal

"Cada vez más, nuestro canal está desarrollando una venta cruzada"



WatchGuard quiere crecer a doble dígito este año. Tras dos excelentes ejercicios para el mercado de la seguridad, en este 2022 todo apunta a que siga creciendo y la marca quiere seguir incrementando su negocio y su participación en el mercado. Su canal es pieza fundamental para lograrlo. Tras un 2021 en el que la integración entre los canales de WatchGuard y la "antigua" Panda Security ha continuado, en este 2022 el foco principal va a estar puesto en potenciar la venta cruzada entre las diferentes soluciones del fabricante.

Marilés de Pedro

La estrategia de canal de WatchGuard reposa en su programa WatchGuard ONE. Una iniciativa que ha acogido a los distribuidores de Panda Security y que persigue la completa integración de socios y negocios. Tres son las áreas prioritarias. La primera y principal es la potenciación de la venta cruzada. "Permite al *partner* mantener a su cliente lo más protegido posible", recuerda Carlos Vieira, *country manager* de WatchGuard en España y Portugal. "Hay una tendencia clara hacia los servicios XDR, que permiten contar con una solución de seguridad sincronizada que incluye el perímetro, el puesto de trabajo y el área de la nube".

Durante el pasado 2021 prosiguió la integración de los canales. "Los distribuidores están percibiendo la enorme oportunidad que se les abre con nuestra oferta, ahora mucho más extensa con la incorporación de las soluciones del puesto de trabajo", recuerda.

Muchos *partners* de Panda Security han abierto su negocio a las áreas de autenticación multifactor (MFA), de seguridad de red y de protección inalámbrica de WatchGuard. Y, al contrario. "Hemos obtenido resultados muy interesantes en esta venta cruzada durante 2021", desvela. "Sin embargo, apenas estamos en la primera fase de esta estrategia".

Junto a esta venta, Vieira señala la importancia de aumentar la cobertura del canal. "Tenemos que conseguir que los *partners* incrementen sus operaciones con WatchGuard, comprando más de manera regular. Hay que ganar participación de mercado, bien a la competencia o tratando de ganar nuevos clientes que contaban con una protección insuficiente". Por último, es esencial retener a los *partners*.

Tirón de la autenticación multifactor (MFA)

Junto al desarrollo de las soluciones del puesto de trabajo, que fue una de las áreas que más creció el pasado año, el área de la autenticación multifactor (MFA) señala un apartado con un enorme crecimiento. "Ha crecido de manera exponencial el número de empresas que han percibido el valor de contar con este tipo de soluciones", desvela. Muchas pymes, continúa, ya cuentan con una solución MFA, muy económica de implementar, y que mitiga un gran nú-

mero de problemas en el acceso a los dispositivos, a las aplicaciones corporativas (ya sea en la nube u *onpremise*) o al puesto de trabajo remoto.

WatchGuard ha conseguido casi duplicar la facturación en esta línea de negocio en el primer trimestre de 2022. "Ha sido clave el conjunto de *partners* que vienen del mundo Panda y que, adoptando un modelo de venta cruzada, han comercializado estas soluciones". Vieira prevé que esta tendencia de crecimiento va a continuar. "La facturación todavía es pequeña pero el ascenso es enorme. Cada vez tendrá un mayor peso en nuestras líneas de negocio".

Desarrollo de la seguridad gestionada

El despliegue de la seguridad gestionada es otro área de foco prioritario. "Los *partners* tienen que dar el salto hacia estas fórmulas de negocio", explica. La seguridad es cada vez más compleja, recuerda, y faltan recursos especializados en el mercado. "Las empresas pequeñas, sobre todo, no tienen capacidad para contar con profesionales en sus plantillas dedicados a la protección de sus sistemas".

A su juicio, los modelos de venta tradicionales, en los que el canal hacía la instalación y "desaparecía" del entorno del cliente, van a disminuir. "La creciente complejidad que va ganando la seguridad requiere que los *partners* cuenten con SOC, más o menos grandes, que les permitan ofrecer a sus clientes estos modelos".

Ahora bien, no todos los clientes van a optar por fórmulas gestionadas. "Habrá espacio para todos", prevé. En WatchGuard, sin embargo, continúan evangelizando para que los *partners* abracen estas fórmulas. "Quien no las dé, va a tener más complicado el negocio en los próximos años".

Dentro de la amplia oferta de la marca para estos servicios,

"Los distribuidores están percibiendo la enorme oportunidad que se les abre con nuestra oferta, ahora mucho más extensa con la incorporación de las soluciones del puesto de trabajo"

Vieira señala que son las áreas del puesto de trabajo y de la seguridad perimetral las que presentan más facilidades para que un *partner* se inicie en estos modelos. "No tiene sentido ofrecer un servicio gestionado en el puesto de trabajo que no se despliegue también en el perímetro, en los entornos del *cloud* o de SD-WAN", razona. WatchGuard ha realizado una gran inversión para permitir la integración con herramientas de SIEM, de monitorización o provisión de servicios, por ejemplo. 

WatchGuard
watchguard.es

Acceda al vídeo desde el siguiente código QR



"Cada vez más, nuestro canal está desarrollando una venta cruzada"



Panorama de amenazas

WatchGuard evaluó el panorama de amenazas que marcó el último trimestre de 2021 con un informe en el que el equipo de investigación de la marca encontró un número récord de detecciones de *malware* evasivo. Las amenazas avanzadas aumentaron en un 33 %, lo que indica un nivel de amenazas *zero-day* más alto que nunca.

Las detecciones de red también continuaron con una trayectoria ascendente, lo que pone de manifiesto la complejidad de la seguridad en este entorno. Los especialistas de WatchGuard señalan que se siguen atacando viejas vulnerabilidades. Además, al crecer las redes de las organizaciones, a medida que se conectan nuevos dispositi-

vos, las viejas vulnerabilidades quedan sin parchear, por lo que la seguridad de la red se vuelve más compleja.

WatchGuard señala que las amenazas de *malware* se detectaron en EMEA a un ritmo mucho mayor que en otras regiones del mundo. De hecho, en esta zona se detectó *malware* por los Firebox (49 %) a un ritmo casi o superior al doble de otras regiones del mundo (América 23 % y APAC 29 %).

Otra de las conclusiones es que el 78 % del *malware* enviado a través de conexiones cifradas es evasivo. En general, el 67 % de las detecciones de *malware* llegó a través de una conexión cifrada, y dentro de esas detecciones de *malware*, el 78 % era amenazas

zero-day evasivas que eluden las detecciones básicas. Esto continúa la tendencia observada en trimestres anteriores. Estas amenazas a menudo pueden detenerse en el perímetro configurando los *firewalls* para descifrar y analizar el tráfico entrante, un paso que, por desgracia, muchas organizaciones no dan. "Durante dos años hemos abandonado la seguridad en la red ya que nos hemos enfocado en el puesto de trabajo", analiza Carlos Vieira. "Seguimos viendo clientes que no tienen una solución de UTM, ni una solución de *firewall*, ni de servicios en el perímetro de *antimalware* avanzado o de servicios para mitigar el *phishing*. De ahí este aumento de amenazas en la red".

España es el segundo país de Europa con más cursos de seguridad dirigidos al canal

"La ciberseguridad es el eje fundamental de la transformación digital"

El canal percibe la enorme oportunidad que hay en torno al mercado de la seguridad. Como bien recuerda la responsable de canal, los procesos de transformación digital que se han acelerado en los dos últimos años, no solo implican la adquisición de terminales, sino otros aspectos básicos como la formación en herramientas digitales o la protección. "La ciberseguridad es el eje fundamental de esta transformación digital".

España es el
tercer país de
Europa con más
partners
certificados

Seguridad y canal

Samsung Knox es el pilar de la estrategia de seguridad de Samsung. Una plataforma disponible en todos los dispositivos de la marca, desde la gama de entrada hasta los equipos *premium*; protegiendo desde el chip, a nivel de hardware, hasta el software del dispositivo. Samsung cuenta con Business Academy, un portal donde los *partners* tienen acceso a sesiones de formación de las soluciones y a la certificación en la plataforma Knox, para acceder a su comercialización y gestión.

La marca cuenta con tres certificaciones en seguridad. Associated, una certificación que dura unos 45 minutos, y que explica qué es Knox y qué usos ofrece en el ámbito empresarial. "Cuando un *partner* está comercializando



Anna Coll,
B2B Channel Sales manager de Samsung

En Samsung la seguridad, que lleva el nombre de su plataforma Samsung Knox, va unida inexorablemente a la movilidad. Desde hace años ha sido obsesión de la multinacional incorporar a su canal "móvil" a este negocio, lo que le ha llevado a desplegar una exhaustiva formación a través de su Business Academy. Una labor que se ha visto recompensada por el nutrido grupo de *partners* que contaban, a final de 2021, con alguna de las certificaciones en Knox. Un número que situó a España en cabeza de Europa. Anna Coll, B2B Channel Sales manager de la multinacional, asegura que la seguridad ya está integrada en el discurso de negocio del canal.

 Marilés de Pedro

Especial Seguridad en el canal

nuestros dispositivos, no solo debe referirse a las especificaciones de los mismos, sino ser capaz de apelar al concepto de solución. La certificación les pueda ayudar en esta labor". Knox Professional, con una duración de unas dos horas, está más enfocada a profesionales comerciales con perfiles con un cierto grado técnico. La más completa es Knox Expert, que se alarga durante dos días, y que se imparte en inglés desde el centro de Samsung de I+D en Polonia. Está absolutamente destinada a los equipos técnicos, que deben aprobar un examen posterior, y es obligatoria para todos aquellos *partners* que quieran comercializar licencias Knox. "Deben tener suficientes conocimientos para gestionar la consola de Knox y ser capaces de ofrecer un servicio de posventa".

Anna Coll valora de manera muy positiva la involucración del canal con la seguridad. El pasado año España se situó como el país de Europa con más socios certificados. "Los *partners* están viendo que sus clientes, en sus procesos de digitalización, exigen una segura gestión de su parque de dispositivos y que la información que éstos guardan esté protegida".

En el primer tramo de este 2022, España se ha situado como el segundo país de Europa con más cursos realizados (más de 500), lo que supone un 170 % de crecimiento respecto al mismo periodo del año pasado. En cuanto al número de certificaciones, es el tercer país con más *partners* certificados. "Hay que seguir impulsando que los *partners* se certifiquen en este tipo de herramientas", insiste. Coll puntualiza, consciente del alto compromiso y conocimiento, que no es obsesión del equipo de canal que los *partners* obtengan su

certificación en Expert. "Pero sí les empujamos a que consigan la Associated o la Profes-

sional", puntualiza. "Y les incentivamos a ello desde nuestro programa de canal". Para establecerse en alguna de las categorías del mismo (Platinum, Gold, Silver y Registered), es indis-

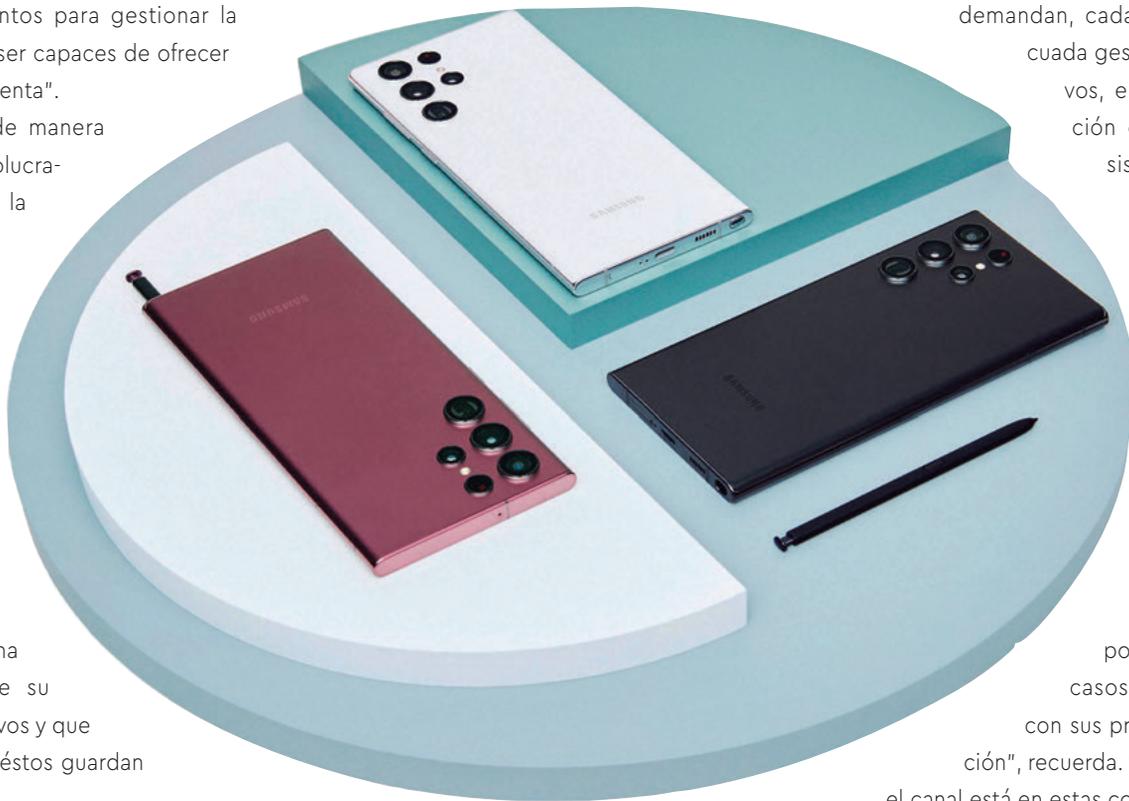
como mínimo, el mismo número de certificaciones que conseguimos el pasado año", desvela. "Es muy importante conseguir que los *partners* que estén certificados las renueven, lo que demostraría su grado de satisfacción con Samsung". Junto a ello, el objetivo de incrementar, en la mayor medida posible, el número de *partners* nuevos que se sumen a este negocio. "Espero que acabemos el año como el primer país de Europa en número de *partners* certificados", sonríe.

Grandes oportunidades

Coll no ve barreras a la expansión de la seguridad en el canal. "Está viendo que sus clientes demandan, cada vez más, una adecuada gestión de sus dispositivos, el control y actualización de las versiones de sistemas operativos, etc.". Unos *partners* que despliegan su cobertura desde el autónomo hasta la gran cuenta, con "parada" en la pyme, el segmento, a juicio de la responsable de canal, que más recorrido tiene por cubrir. "En muchos casos están arrancando con sus procesos de digitalización", recuerda. "La oportunidad para el canal está en estas compañías".

Samsung
samsung.com

"Es muy importante conseguir que los *partners* que cuenten con alguna certificación en Samsung Knox la renueven cada año"



pensable contar con alguna certificación y haber cursado formación en la academia. Coll recuerda que la seguridad exige una formación continua. Hay que mantenerse al día, más en materia de protección, con un panorama cada vez más complejo y en el que las amenazas siguen creciendo. Aunque las certificaciones tienen una validez de dos años, Samsung pide a su canal que las renueve cada año. "Tenemos que mantener,

Acceda al vídeo desde el siguiente código QR



"La ciberseguridad es el eje fundamental de la transformación digital"



El desarrollo del canal es básico en el despliegue de la seguridad



"La seguridad ya es parte del ADN de VMware"

Ya nadie duda del decidido foco de VMware en el segmento de la seguridad. Con la enorme ventaja que le permite su privilegiada, y cada vez más extensa posición en los sistemas tecnológicos de las empresas, la marca ha reivindicado su particular filosofía en el entorno de la seguridad que lleva el apellido de intrínseca. Su canal, como ha sucedido en cada uno de los "nuevos" mercados hacia los que ha extendido su primigenia oferta, es pieza básica en este seguro despliegue.

 Marilés de Pedro

La seguridad que defiende VMware se engarza en el diseño. En un mercado en el que la tecnología ha extendido sus dominios hasta los últimos rincones, la seguridad debe alcanzarlos también. Roto definitivamente el perímetro, los sistemas de protección se han acoplado a un entorno híbrido y *multicloud* para abarcar dispositivos, aplicaciones y redes. Francisco Verdugo, *senior partner solution engineer* de VMware, explica que la seguridad intrínseca responde a un enfoque apoyado en varios pilares. "El objetivo es incluir la seguridad en todas y cada una de las soluciones que tenemos en nuestro portfolio, que es enorme". No se trata, específica, de incluirla como una capa superpuesta. "La seguridad forma parte del ADN de VMware". Una seguridad basada en el contexto y que busca la máxima simplicidad. "No tanto en las firmas, la seguridad debe estar basada en el contexto, en el análisis del dispositivo que se

utiliza, los procesos del sistema, los usuarios, la red que se utiliza, etc.". Un contexto que permite una toma de decisiones mucho más inteligente y eficiente, interceptando, incluso, ataques y amenazas no conocidas. "Incluso en la capa del hipervisor es mucho más fácil disfrutar de visibilidad en un entorno virtualizado o *cloud* que tenga nuestro *stack*", determina. Pilar fundamental es permitir la interconexión entre distintos silos. "Hay que hacer cómplices a los profesionales que desarrollan su labor en el entorno de la infraestructura y de las redes",

"No tanto en las firmas, la seguridad debe estar basada en el contexto"

explica. El análisis del contexto permite detectar las vulnerabilidades sin consumir recursos, ni llevar a cabo un análisis de red. "Los procesos se simplifican y se rompe con los silos". Engarzada también en el objetivo de VMware

de hacer de los modelos de suscripción una de sus vías principales de negocio, la oferta de seguridad ya puede ser ofrecida bajo estas fórmulas. Incluso ya se ha integrado en la oferta de los proveedores de servicio con los que colabora VMware, lo que les permitirá comercializar la seguridad embebida en sus proyectos.

Foco en el canal

Compañía 100 % canal, VMware también requiere del ecosistema de *partners* para desplegar su oferta de seguridad. Una propuesta que exige a los distribuidores aplicar idéntica filosofía estratégica que la que tiene la marca. Al concebirse la seguridad como una pieza embebida en todas las áreas tecnológicas, los *partners* deben apostar por su integración en todos sus proyectos. "Necesitamos que los *partners* se habiliten tanto a nivel comercial como técnico", reconoce Verdugo. La marca quiere ampliar su capilaridad, alcanzando a todo tipo de *partners*. Una labor que

Especial Seguridad en el canal

tiene en el canal mayorista un aliado fundamental. "Son nuestro brazo extendido para detectar y formar a nuevos *partners*".

Dentro del programa de canal de VMware, Partner Connect, hay dos competencias específicas para el mercado de la seguridad (EndPoint Protection y Network Security), a las que próximamente se unirá SASE. Para conseguir las, primero, el *partner* deberá estar registrado en PartnerConnect, el portal mundial para el canal. Cada *partner* necesita contar en su plantilla con dos profesionales, con un perfil comercial, que hayan completado los VSP (VMware Sales Professional); y otras dos personas con un perfil preventa que hayan superado los cursos VTSP (VMware Technical Sales Professional). En ambos casos se trata de cursos gratuitos online. Por último, tienen que contar con un profesional, con perfil técnico, que debe superar un curso de especialización (*postsale*). En este último caso, supone un coste.

Especialmente importante para VMware es la promoción de sus competencias máster en servicios, que permiten al canal desplegar su oferta propia en los clientes. Las competencias específicas en el área de la seguridad incluyen una parte técnica apta para servicios. Dependiendo de la competencia existen varios cursos a elegir con su examen correspondiente. VMware incentiva al *partner* en todo el ciclo de venta. En el área de la preventa, la marca está subvencionando pruebas de concepto y consultorías de preventa. En el proceso de venta, se blinda la oportunidad al *partner* que la ha abierto y que la ha registrado, con descuentos desde un 5 % hasta un 30 %, dependiendo de la tecnología. También cuenta con incentivos una vez cerrado el proyecto. Especialmente in-



Francisco Verdugo,
senior partner solution engineer de VMware

“Necesitamos que los *partners* se habiliten tanto a nivel comercial como técnico”

centivado es el modo de suscripción con *rebates* que pueden alcanzar hasta un 22 %.

Oportunidad en seguridad

Aunque la proa principal del crecimiento de VMware señala al desarrollo del área de las aplicaciones emergentes y, por supuesto, la implantación de los modelos *multi-cloud*, la seguridad es una enorme área de oportunidad. “Año a año seguimos creciendo tanto en facturación como en el número de *partners* que conocen nuestras soluciones de seguridad”, señala. “Siempre hay muchas oportunidades para crecer ya que la

seguridad está vinculada a todas las áreas de negocio: acompaña a todos los casos de uso y a todas y cada una de las soluciones que ayudan a nuestros clientes en su día a día”. 

VMware
vmware.es

Acceda al vídeo desde
el siguiente código QR 



“La seguridad es parte
del ADN de VMware”

Enorme oportunidad

El negocio de la ciberseguridad es uno de los más boyantes del universo tecnológico en los últimos años. A finales del pasado año, IDC hacía sus previsiones para este 2022 y preveía que el negocio en torno a la seguridad en España se incrementaría un 7,7 %, con un 8 % de ascenso hasta 2024. “La ciberseguridad, no solamente en nuestro país sino a nivel mundial, es cada vez más importante. En el caso de España, además, es más relevante ya que se parte de un modelo en el cual se ve a la seguridad como un gasto, no como una inversión”. Sin embargo, Francisco Verdugo reconoce que las empresas españolas, sobre todo las pymes, se

han dado cuenta de que cada vez es más importante tener una estrategia de seguridad.

Verdugo pronostica un enorme crecimiento para este apartado ya que se ha extendido a todos los ámbitos. “Incluso los desarrolladores empiezan a tener en cuenta la seguridad desde la fase de diseño de sus programas y sus aplicaciones”, Ya hay tecnologías en las cuales el modelo de seguridad está incluido como diseño. “Se está abriendo cada vez más espectro, la seguridad se incluye dentro de la propia *cloud* o cómo se protegen los servicios o las aplicaciones”.

¿Por qué incluir el *threat hunting* en su *portfolio*?

Crece el interés por el *threat hunting*. Según Pulse, el 32 % de los responsables de TI afirma que sus organizaciones planea reforzar su postura de seguridad de los *endpoints* añadiendo un programa de *threat hunting* a su estrategia global de seguridad.

Y

no es de extrañar ya que es una potente herramienta para defender a sus clientes aportando a sus servicios valor añadido, pues permite descubrir e interrumpir a tiempo las amenazas internas y externas que han eludido los controles basados en la tecnología antes de una infracción; aumenta las tecnologías de seguridad con la experiencia humana para reducir el tiempo de permanencia; dota a los equipos de seguridad de los conocimientos necesarios para desbaratar a los adversarios a gran escala; o alimenta el esfuerzo continuo por reducir la superficie de ataque y mejorar las capacidades de detección automatizada.

¿Está preparado para llevar sus servicios de seguridad al siguiente nivel?

Los MSPs que estén considerando aprovechar la oportunidad y poner en marcha un servicio de *hunting* deberían evaluar lo siguiente:

- 1 - Toda organización es un objetivo, independientemente de su tamaño, sector o ubicación.**
- 2 - Las amenazas se mueven más rápido que nunca.** Recuerde la velocidad a la que operan y evolucionan las amenazas.
- 3 - Por tanto, el *threat hunting* es ahora una necesidad para todas las organizaciones. Ya no es un "nice-to-have".** La oportunidad de proporcionar el servicio de valor añadido del *threat hunting* es relevante.



4 - La velocidad, la escala y la coherencia son fundamentales. El *hunting* debe poder realizarse con rapidez y a gran escala. Esto requiere procesos estructurados y repetibles, tecnologías maduras, visibilidad a largo plazo y *hunters* de amenazas respaldados por una amplia gama de productos, con una profunda experiencia, conocimiento e inteligencia sobre amenazas.

5 - Estructure sus acciones de *hunting* utilizando el marco MITRE ATT&CK. Las soluciones de WatchGuard vienen reforzadas con muchas técnicas ATT&CK identificadas, permitiendo así al equipo de seguridad centrar sus esfuerzos en hacer frente a las amenazas de seguridad aprovechando la información bien definida que proporciona el marco y que nuestro equipo de ciberseguridad ha ampliado.

6 - Aproveche la oportunidad. Siempre es más fácil vender a los clientes existentes, y los servicios de seguridad para *endpoints* no son una excepción. Los *partners* que ya ofrecen servicios de seguridad encontrarán en WatchGuard EDR, WatchGuard EPDR y el servicio de *threat hunting* una extensión natural de su actual oferta de servicios.

7 - Si no puede hacerlo internamente, considere nuestro servicio de *threat hunting*. Por último, si no puede hacerlo internamente, asegúrese de asociarse con un proveedor que pueda hacerlo. Elegir el adecuado puede simplificar la prestación de servicios básicos y nuevos servicios de seguridad gestionados a lo largo del tiempo.

Nuestro servicio de *threat hunting*, incluido en WatchGuard EDR y WatchGuard EPDR, es una potente herramienta que permite a los MSP añadir un servicio de *hunting* como parte de su oferta. Permite detectar las amenazas antes de que se produzca el daño y mejora las defensas contra futuros ataques a sus clientes.

Aprenda cómo puede ampliar sus soluciones añadiendo este servicio leyendo nuestro último eBook *Your threat hunting service program simplified with WatchGuard* e inicie el camino del servicio de *threat hunting* con WatchGuard Advanced Endpoint security. 

Iratxe Vázquez
Senior product marketing manager de
WatchGuard Technologies

¿Cómo pueden ayudar los *partners* a abordar los pilares de la seguridad de los clientes?

Si hay dos grandes aspectos por los que las empresas deberían preocuparse son, en primer lugar, la capacidad de ofrecer experiencias excepcionales a los usuarios. La segunda es asegurar lo que se ha convertido en algo cada vez más fragmentado: las aplicaciones, los dispositivos y la infraestructura que forman la base sobre la que se construyen estas experiencias.

Pero las empresas luchan por cubrir ambos frentes y necesitan la ayuda de sus *partners* para superar la percepción actual de que la seguridad sigue siendo un obstáculo, lo cual es especialmente cierto cuando se trata de realizar cambios: el 61 % de los equipos de TI y el 52 % de los desarrolladores afirman que las políticas de seguridad asfixian su propia innovación. No es difícil entender por qué: llevamos años ajustando nuevas soluciones y productos para protegernos de las nuevas amenazas y defender una superficie cada vez mayor, una tendencia que se ha acelerado con el incremento del trabajo híbrido.

El resultado es que el parque informático de muchas organizaciones se ha convertido en una maraña compleja de plataformas, sistemas y soluciones que los enfoques de seguridad tradicionales no pueden proteger.

Ahora hemos llegado a un punto en el que, para poner orden en el caos, las empresas necesitan la ayuda de socios capacitados que puedan convertir un gran abanico de soluciones (y perspectivas) de seguridad en una defensa intrínseca que no sólo proteja contra amenazas sofisticadas, sino que permita a las empresas impulsar experiencias de usuario innovadoras.

La capacidad de los socios de analizar el entorno informático de una empresa de forma integral, junto con las necesidades del negocio, es lo que les sitúa en la mejor de las posiciones para ayudarles a desarrollar un plan

que logre este equilibrio tan importante.

Los socios deben saber que la "seguridad" se divide en tres categorías: usuarios, cargas de trabajo y operaciones. Los usuarios tienen que poder trabajar, utilizar las aplicaciones, los datos y los servicios que deseen, de la manera que quieran, en el lugar que elijan. Las cargas de trabajo, las aplicaciones y los datos deben



ser totalmente seguros, pero igual de dinámicos; es decir, deben poder moverse y compartirse cuando sea necesario. En cuanto a las operaciones, la implementación real de la seguridad tiene que ofrecer una protección total sin restricciones que sea capaz de proporcionar una detección, protección y respuesta adecuada. Además de estas diferentes perspectivas está la confianza cero. Con el fin de ofrecer una seguridad dinámica en la empresa actual, cada vez son más las empresas que buscan adoptar este enfoque de la seguridad.

La oportunidad de los *partners*: ser polivalente

Todo esto supone una complejidad y un reto importantes. Sin embargo, también es una oportunidad para los socios, que consiste en ser esa luz en la oscuridad, ese orden en el

caos. Ayudar a hacer operativa la verdadera confianza cero, a consolidar proveedores y soluciones para que todos los productos de seguridad se comporten como tienen que hacerlo y garantizar que no haya solapamientos ni lagunas.

En todo este proceso resulta imprescindible la labor de conectar todas las partes de la empresa que luchan por conectarse entre sí. Los equipos de TI y los desarrolladores, a los que se les confía la innovación, se sienten asfixiados por la seguridad. Para ser innovadores y ofrecer experiencias de usuario excepcionales es necesario que los diferentes equipos trabajen en colaboración. Parte del problema es que los

desarrolladores, los informáticos y los equipos de seguridad hablan idiomas diferentes. Sin embargo, los *partners* pueden interactuar con ellos haciéndose entender y transmitiéndoles las prioridades y necesidades de otros departamentos. En eso consiste ser polivalentes, utilizar su visión informada pero distante y su función de soporte para ayudar a resolver los problemas de la empresa.

Con la ayuda de los socios, las empresas pueden convertir el caos en orden y la complejidad en innovación sin comprometer la seguridad. Aunque ésta se ha considerado siempre un obstáculo para el cambio, ahora debería verse como todo lo contrario, una de las herramientas vitales para realinear el negocio y ofrecer la primera gran línea roja de la empresa moderna: experiencias de usuario excelentes. 

El número de ciberataques ha crecido en todo el mundo durante el conflicto



El ciberespacio, otro campo de batalla

La invasión de Rusia a Ucrania ha tenido en paralelo a la contienda física otra en el espacio digital, que persigue inutilizar los sistemas y causar daños tanto en la operativa de las instituciones como de las empresas con el fin de paralizar Ucrania, influir en la opinión pública y destruir activos importantes. Los principales especialistas en seguridad han analizado este combate digital, las implicaciones que puede tener en nuestro país y cómo se pueden proteger tanto las entidades públicas como las empresas y ciudadanos.

 Rosa Martín

El pasado 24 de febrero comenzó la invasión de Rusia a Ucrania y en paralelo se incrementó el número de ataques contra sitios del Gobierno ucraniano y otros organismos. La División de Inteligencia de Amenazas de Check Point Software Technologies, Check Point Research, detectó en los primeros tres días de la contienda un incremento

de los ciberataques contra el Gobierno y el sector militar de Ucrania de un 196 %, frente al 4 % en los ataques a organizaciones rusas. Estos datos indican que la denominada "ciber guerra" es un factor que puede desestabilizar e inclinar la balanza para ganar la contienda. Los ciberataques que se han detectado se pueden dividir en función del atacante. Uno de ellos son los ataques del tipo APT (amenazas persis-

tentes avanzadas), que tratan de conseguir ventajas a través del espionaje o sabotaje. Los actores de este tipo de amenazas tienen muchos recursos, conocimientos y actuarían como complemento al mundo real. "Los actores de amenazas Gamareddon, Cyclops Blink o PandoraBlade serían un claro ejemplo en este contexto, ya que se detectó un incremento significativo de su actividad coincidiendo con el

España, ¿objetivo?

Los especialistas opinan que nuestro país no es un objetivo prioritario en este conflicto digital, pero al formar parte de la Unión Europea, que está apoyando a Ucrania, podría ser atacada. Sergio Bravo, de Bitdefender, indica que el riesgo de sufrir un ataque no es el mismo en todas las organizaciones y depende de la relación con Ucrania. Actualmente no existe un registro oficial de campañas dirigidas de grupos pro-rusos contra España, pero sí que se han tomado algunas medidas, según les consta a los expertos. “En el ciberespacio no hay límites o fronteras por lo que una herramienta que fue diseñada para realizar un ataque a Ucrania podría ser utilizada contra España”, argumenta el *Threat Intelligence engineer* de ThreatQuotient. Albers, de ESET, recalca que nuestro país cuenta con un Centro Nacional de Protección de Infraestructuras Críticas, un Centro Criptológico Nacional, INCIBE y distintos CERT profesionales que

velan por la seguridad de las empresas tanto públicas como privadas. “Esto no significa que no seamos vulnerables, pero las puntuaciones obtenidas en las pruebas que realiza el índice de ciberseguridad global nos deja en los primeros puestos. El principal problema se encuentra en que no se destinan los suficientes recursos para detectar y bloquear ataques comunes que pueden ser evitados aplicando medidas de seguridad básicas”.



Una opinión similar mantiene Ramiro Céspedes, Threat Intelligence Engineer de ThreatQuotient, quien señala que el gobierno ruso lleva años financiando y patrocinando de manera directa e indirecta a múltiples agrupaciones que llevan adelante operaciones en el ciberespacio. El gobierno ucraniano también reaccionó durante los primeros días solicitando la participación de voluntarios para formar un ciberejército. “Los principales ataques llevados a cabo por este grupo han sido ataques de denegación de servicio (DDoS) contra sitios web del gobierno de Rusia y contra desarrolladores rusos en plataformas como GitHub. Las acciones de este grupo han estado más enfocadas en el volumen que en la precisión, pero aun así han logrado comprometer diferentes activos del gobierno ruso”, añade.

Para Josep Albers, director de investigación y concienciación de ESET España, también han sido relevantes los ataques dirigidos a infraestructuras críticas como los ISP y las conexiones satelitales. Miguel Ángel Fañanás, director de Europa Occidental en VU, cree que la contienda está desarrollando nuevas tácticas de ingeniería social, por lo que el panorama de los ataques está cambiando constantemente, aunque señala que en gran parte “apuntan a impactar el marco de la desinformación, teniendo el foco en los medios de noticias oficialistas de cada país”.

Ataques más peligrosos

A la hora de determinar qué tipo de ataques son más peligrosos, los especialistas señalan que son los que consiguen sus objetivos. Para Sergio Bravo, *Iberia sales director* de Bitdefender, el Wiper es uno de los más dañinos porque “el cifrado de datos resulta irreversible”. A su juicio, estos ataques están diseñados para causar el mayor daño posible, suelen ser oportunistas y no están dirigidos con precisión.

“Todos los ataques dirigidos con estrategia son dañinos”

David Sancho, investigador senior de Amenazas y responsable del Equipo de Investigación de Trend Micro, opina que los ataques de DDoS y los de alteración de contenidos o “*defacement*” son los que crean más daño a corto plazo y se pueden hacer sin grandes conocimientos técnicos. “Son fáciles de realizar y difíciles de prevenir”, resalta.

Mario García, director general de Check Point Software para España y Portugal, indica que “hablar de peligrosidad en ataques es muy re-

lativo. Todos lo son. Dependiendo de la importancia del objetivo, en un momento puede ser devastador y ocasionar muchos problemas directos e indirectos. Todos los ataques dirigidos con estrategia son dañinos”.

Los expertos consideran también que los ataques a las infraestructuras críticas son especialmente dañinos; aunque hay que tener en cuenta que todos los ataques pueden tener distintas consecuencias. “La cuestión es que muchos ataques pueden llevar factores externos y efectos derivados más allá de la víctima original. Cada ataque exitoso

puede suponer un riesgo secundario que no es obvio al principio. Afortunadamente, no todos los ataques tendrán consecuencias peligrosas, pero eso no significa que debamos ser benévulos con ellos”, recalca Shier, de Sophos. Céspedes, de TreatQuotient, apunta que otro tipo de ataques con importante repercusión son los de la desinformación porque “pueden infligir un serio daño en la moral de las tropas y ciudadanos de ambos bandos y podrían tener un impacto político muy alto”.



“La seguridad es una inversión y no un gasto”

Sector público y empresas

En este panorama de ciberataques los organismos del sector público y las empresas están en el punto de mira de los atacantes, pero el nivel de preparación para combatir estas amenazas no es siempre el adecuado y va unido al presupuesto de seguridad, según señalan los especialistas en ciberseguridad. El Security Report 2022 de Check Point Software señala que los ciberataques a servicios públicos se incrementaron un 46 % en 2021, en comparación con 2020, registrándose 736 amenazas semanales por organización dentro de los servicios públicos a nivel mundial. Estos datos

revelan que es necesario articular estrategias de seguridad y ser proactivos para combatir estas amenazas.

Los especialistas coinciden en señalar que mantenerse a salvo de un ataque es prácticamente imposible, pero que siempre hay que tomar medidas para dificultar estos ataques. “Detrás de cada amenaza siempre existe un humano y el conocimiento de sus

intenciones, motivaciones, capacidades e infraestructura que aporta la inteligencia de amenazas es la única forma para tratar de ir un paso por delante de los atacantes”, insiste Miguel de Castro, de CrowdStrike.

Biasini, de Cisco Talos, añade que, con independencia de la situación actual, “los sistemas heredados, la mala higiene de la ciberseguridad y el software obsoleto pueden tener impactos catastróficos en cualquier organización”.

El analista de Seguridad en el GREAT de Kaspersky indica también que hay que considerar que la seguridad debe “considerarse como un proceso y

no como un estado”. Y, al mismo tiempo, destaca que “la seguridad es una inversión y no un gasto”. Los especialistas creen que ahora es el mejor momento para que las empresas revisen sus planes de ciberseguridad, intensifiquen la búsqueda de vulnerabilidades, analicen sus accesos y registros, y elaboren un plan de crisis.

La recomendación de Cisco Talos es que las empresas y organizaciones con vínculos con Ucrania habiliten y examinen con cuidado sus registros, apliquen parches y, además de diseñar un plan de crisis, habiliten la autenticación multifactor.

Sophos también indica que es aconsejable monitorizar cualquier movimiento inusual en las redes a medida que avanza el conflicto, mientras que Check Point Software considera que, además de contar con un buen software de protección y de hacer *backup* de forma periódica, es imprescindible dar una formación en ciberseguridad a los empleados para que sean la primera barrera ante cualquier incidente.

Para ThreatQuotient las empresas deberían contar con un responsable de la estrategia de ciberseguridad y mejorar los sueldos de los especialistas para captar y retener talento en este apartado.

ESET recalca que es imprescindible, además de aplicar las medidas de seguridad consideradas básicas desde hace tiempo, realizar auditorías constantes para detectar posibles agujeros y solucionarlos a tiempo.

Bitdefender añade un consejo más: la revisión de la guía Shields UP, elaborada por la CISA (Agencia de Seguridad de Infraestructura y Ciberseguridad en Estados Unidos). 



Consejos de seguridad para el ciudadano

Los ciudadanos pueden ser víctimas de ciberdelincuentes que pueden aprovecharse de su solidaridad con los refugiados y los afectados por el conflicto mediante campañas de *phishing* y otras extorsiones. Los especialistas en ciberseguridad aconsejan estar alerta y mantener unas buenas prácticas para evitar caer en estafas. No se deben abrir correos de usuarios desconocidos, ni hacer clic en enlaces adjuntos y, por supuesto, no se tienen que facilitar datos a través de estos canales. Es recomendable contar con contraseñas robustas que combinen los números con las mayúsculas y los símbolos; y además cambiarlas cada cierto tiempo. Y, por supuesto, señalan que no es conveniente tomar parte en el conflicto participando en grupos de *hackers* porque posiblemente se estén cometiendo delitos graves.



Debates en Newsbook

Pymes, canal y fondos NextGeneration UE

- Ya se ha puesto en marcha la **primera fase del Kit Digital**, abierta para empresas de entre 10 y 49 empleados. ¿Cómo valoran esta primera fase? ¿Están notando que el mercado pyme se está moviendo?
- ¿Qué se echa de menos por parte de la **Administración Pública**? ¿O se ha iniciado de forma correcta todo este proceso?
- En la **función divulgadora** que están desarrollando, tanto los fabricantes como los mayoristas, y en algunos casos como agentes digitalizadores (en el catálogo ya hay 6.000 entidades, con un ritmo de 500 agentes a la semana), **¿qué dificultades están encontrando?** ¿Qué están trasladándoles las empresas o, en el caso de los mayoristas, el canal?
- Parece que las empresas se decantan por **invertir las ayudas del Kit Digital** en la creación de una **página web**. Así es la principal conclusión que establece el informe

"Radiografía de intereses de la pyme frente a las soluciones del programa Kit Digital", desarrollado por Cosmomedia, compañía española de marketing digital especializada en la digitalización de pymes y autónomos. **¿Qué soluciones son claves para, de verdad, potenciar la digitalización de las pymes?**

- El **hardware se ha quedado "fuera"** de esta primera fase ¿Es lógico?
- Tras esta primera fase, cuyo bono es de **12.000 euros**, se abrirá un segundo segmento para pequeñas empresas o microempresas entre 3 y menos de 10 empleados, con una cuantía de 6.000 euros y, por último, un tercer grupo en el que se sitúan las pequeñas empresas y microempresas de entre 1 y menos de 3 empleados y personas en situación de autoempleo, con una ayuda de 2.000 euros. ¿Se observan **más oportunidades** en estos apartados?



Acceda al debate, los vídeos y al *whitepaper* desde el siguiente enlace:

<https://newsbook.es/pymesfondosnextgenerationue>



Esprinet

“Estamos cerrando paquetes, muy cómodos de vender, que se implementan de manera sencilla en las empresas”

“Nuestro canal es fuerte y muy amplio. El reto es hacer llegar al cliente un mensaje claro, trasladando el beneficio de las soluciones”



Ingram Micro



“Estamos fomentando que nuestro canal ayude a que las empresas, aprovechando el incentivo del bono, puedan hacer una inversión mayor”

“Donde más podemos apoyar a la red de agentes digitalizadores que forman parte de nuestro canal es en la financiación de los proyectos”

Sage

“La economía española está informatizada, pero no está digitalizada”

“El reto, apasionante, es que hay dinero para poder hacer una transformación digital en un entorno que solo estaba informatizado”



Sophos



“Hemos buscado un paquete de medidas lo suficientemente potente para cubrir de la mejor manera la seguridad de las empresas”

“No estamos hablando solo de soluciones. La Administración Pública pretende que, posteriormente a su aplicación en la empresa, haya un seguimiento del kit digital”

Wolters Kluwer

“12.000 euros no salvan a una empresa de 10 a 49 empleados. Lo que la salva es el proyecto empresarial de transformación”

“Necesitamos que todos los actores que intervienen en ese proceso de transformación del negocio estén perfectamente formados, preparados y alineados”



La compañía ha vendido más de 100.000 equipos en España en su último año fiscal

"Ni Dynabook ni nuestros dispositivos van a fallar al canal"



Maite Ramos,
directora general de la filial ibérica de Dynabook

Maite Ramos ha cumplido dos años al frente de la filial ibérica de Dynabook. Dos ejercicios, no exentos de dificultad, en los que la directiva ha asentado su estrategia en los valores que marcaron la estela de la "antigua" Toshiba: enorme capacidad fabril, seguridad y fiabilidad. Una herencia que quiere mantener a toda costa y que le ha llevado a acometer cambios en la estrategia, tanto a nivel de canal como de producto, para reforzar su propuesta de valor.

Cuatro años después de que Sharp anunciara la compra del negocio del PC en Toshiba, el nombre de Dynabook quiere seguir reforzando su entidad en el mercado. Sin perder su esencia originaria. "Junto a la poderosa fortaleza de Foxconn, es crucial mantener los valores que identificaron a Toshiba", insiste. "Para muchos clientes son esenciales la seguridad y la fiabilidad de la que siempre ha hecho gala". La BIOS propietaria de la marca es estandarte en este crítico apartado.

Ramos destaca también la capacidad de las fábricas, lo que ha llevado a renovar completamente la línea de producto. "Cada trimestre lanzamos máquinas nuevas", recuerda.

Potente estrategia

Tras analizar en profundidad cuál era la propuesta de valor diferencial de la compañía, Ramos estableció algunos cambios, lo que condujo a una reordenación de la estrategia de canal y de la hoja de ruta de los productos en el mercado. El tercer pilar fue la entrada en el Catálogo de Patrimonio, que ha sido clave para acceder a proyectos importantes en el área de la Administración Pública.

Recién concluido su año fiscal el pasado 31 de marzo, la marca ha comercializado más de 100.000 unidades, lo que sitúa a la filial como número dos en volumen en Europa, por encima de países como Alemania, Francia o Italia. "En términos de rentabilidad, probablemente estemos muy cerca de ser el número uno", completa.

Clave ha sido el mercado de la educación. Dynabook ha participado en dos grandes proyectos, uno con más de 50.000 unidades en el marco de "Educa en Digital". Ramos recuerda que es esencial contar con el producto adecuado y aunque es un segmento en el que el dispositivo más demandado de manera tradicional ha sido el portátil de 11", ahora están lanzándose iniciativas con pantallas más grandes. "Se trata de proyectos, a través de Patrimonio, para nutrir tanto

a profesores como a alumnos, en los que estamos muy presentes".

Tres gamas, tres

Dynabook ha mantenido la denominación de las tres gamas profesionales de ordenadores portátiles que comercializaba Toshiba en el mercado español: Satellite Pro para el segmento de entrada, Tecra, para la gama media; y Portégé para la gama más alta. La compañía ha organizado la distribución de los productos para que la hoja de ruta al mercado estuviera completamente optimizada. "Era muy importante que los productos de las gamas Portégé y Tecra contaran con un canal específico para su distribución", explica. "Son marcas muy reconocidas, que llevan muchos años en

 Marilés de Pedro

el mercado y que necesitan ser comercializadas por los *partners* adecuados", explica. La venta de un Portégé, insiste, permite a los *partners* ofrecer a sus clientes un producto con un enorme valor. "Si falla, Dynabook lo arregla y, además, le devuelve el dinero; un argumento absolutamente diferencial para el canal. Había que darle la oportunidad de que pudiera contárselo a sus clientes". Aunque la gama Portégé señala el escalón más alto, con precios medios en torno a los 1.000 euros, Ramos desvela su apuesta por los Tecra. "Son imbatibles en la relación calidad y precio. No hay otros iguales en el mercado". Una distribución, más cuidada y selectiva, que no alcanza a la gama Satellite, que exhibe otras prestaciones diferentes. Las 14" han sido siempre el sello de identidad de la compañía y próximamente van a lanzar un equipo, en este tamaño, "fantástico; con un diseño que va a sorprender", adelanta.



100 % canal

Reordenar al canal fue otra de las vías estratégicas. La estructura de Platinum y Gold, las dos categorías más importantes, ha mantenido el mismo número de compañías (en torno a las 100 entre ambas) pero se han cambiado algunos nombres. "Es esencial observar las compañías que forman parte del canal y analizar su evolución y su crecimiento. Debe ser un ecosistema dinámico". Ramos explica que fue prioritario establecer alianzas con grandes *partners*. "Se trata de compañías con un enorme valor, que deben mantener una evolución y un negocio constante". Una exigencia que asegura que todos los *partners* disfruten de condiciones similares e idéntico respeto y cuidado por parte de Dynabook. "Hay que cuidar y respetar el canal al 100 %". En un mercado tan dinámico, "se revisa trimestralmente la estructura y se analiza a cada *partner*". No se olvida el desarrollo de la categoría Silver. Dynabook cuenta con un profesional, que cuenta con apoyo externo, para promoverla. "Esta categoría no estaba optimizada", valora. "Estamos tratando de darles más soporte y la importancia que se merecen. Hay que reavivar ese canal ya que desarrollan un modelo de *run rate* que no se puede perder". Dynabook les

ofrece una mayor cercanía y contacto directo con la marca. Asegura Ramos que, tras este proceso de reordenación, ya cuenta con los *partners* con los que quieren trabajar. "Por supuesto, seguiremos trabajando para completar el canal, siempre de manera dinámica, pero ya disfrutamos de una buena estructura".

Mirando al nuevo año fiscal

De cara a los próximos meses y al nuevo año fiscal, que arrancó el pasado 1 de abril, el objetivo de la directora general es consolidar los cambios. "Hay que estabilizar todo lo que hemos hecho hasta ahora y generar confianza. Volver a poner en valor la marca", insiste. Una estabilidad que tiene su pilar en el canal. "Cuidar a los *partners* es esencial". El peso, crítico, que

tienen los acuerdos con los socios Platinum se torna en un vital pilar de negocio. "Tienen que vernos como un jugador importante en su negocio". Sin desvelar los objetivos concretos para este ejercicio, Ramos asegura que

"Era muy importante que los productos de las gamas Portégé y Tecra contaran con un canal específico para su distribución"

Dynabook no va a fallar. Ni a clientes, ni a *partners*. "Quiero que el canal tenga confianza absoluta. Ni nuestros dispositivos, ni el equipo de Dynabook va a fallar al canal".

Tras consolidar el negocio en el área pública y el peso, creciente, que tiene el sector de la educación, Ramos señala el reto de impulsar el área de las cuentas privadas, en el que también tiene que recuperar algunas cuentas, con el soporte imprescindible del canal. 

Su objetivo es aportar innovación a través de la tecnología de código abierto

"Estamos haciendo cambios para adoptar una filosofía de, primero, el cliente; pero el *partner* siempre"

Red Hat está reorientado su estrategia de canal para generar nuevos ingresos a sus *partners*. Su intención es que su red de socios pueda colaborar estrechamente con la compañía para ofrecer más servicios, acompañar a los clientes en sus procesos de transformación digital y aprovechar las nuevas oportunidades de negocio que ofrecen la nube híbrida abierta, el edge y la adaptación de su sistema operativo Red Hat Enterprise Linux a nuevos entornos.

 Rosa Martín

E

l mercado de las soluciones de código abierto en España sigue presentando nuevas oportunidades de negocio, a pesar de que ya tiene cierta madurez. Javier García Fiaño, director del ecosistema de *partners* de Red Hat en España y Portugal, señala que, tomando como referencia a las empresas del IBEX 35, hace un poco más de una década la presencia de los productos de Red Hat era casi simbólica, pero en la actualidad está presente en el 80 % de estas empresas. "Desde que Red Hat llegó a España han sido años de crecimiento constante a doble dígito", recalca. Este ritmo de crecimiento da idea de la evolución al alza del mercado del software de código abierto. Un crecimiento que ha ido unido al desarrollo del canal de este tipo de soluciones. García Fiaño reconoce que hay muchos *partners* que han nacido para dedicarse exclusivamente a este tipo de software, pero todavía queda mucho camino por recorrer y en algunos aspectos sigue siendo un mercado incipiente. "Es maduro, por un lado, pero a la vez incipiente. Hay mucha demanda todavía".



Javier García Fiaño, director del ecosistema de *partners* de Red Hat en España y Portugal

Estrategia

Para responder a esta demanda Red Hat está poniendo en marcha este año una estrategia basada en la colaboración y el ecosistema de *partners*. La colaboración, como señala el directivo, forma parte de su razón de ser, pero ahora quiere ir más lejos y trabajar estrechamente con su red de socios para resolver los problemas cada vez más complejos de las empresas en el ámbito de las TI. "Somos conscientes de que la solución a los problemas complejos no puede venir de un único actor, tiene que venir de un conjunto de actores que construyan una solución". Por este motivo, está dando un giro importante en su relación con el canal para que el ecosistema de *partners* sea más relevante. La intención es que su modelo, basado en la suscripción y en el desarrollo de software colaborativo, llegue a más clientes y *partners*. "Estamos rediseñando nuestra estrate-

"Los *partners* están contribuyendo por encima del 75 % al negocio global de Red Hat"

gia con los *partners*, ampliando las áreas que les dejamos a ellos para generar negocio alrededor de nuestras tecnologías", explica García Fiaño.

Uno de los primeros pasos de esta reorientación ha sido una nueva segmentación del mercado ibérico para incrementar el número de clientes que atiende a través de sus *partners*. Su objetivo es que sus socios puedan ofrecer nuevos servicios a estos clientes. Este nuevo enfoque va unido a su foco actual que, desde el punto de vista tecnológico, se encuentra en la nube híbrida abierta y en aportar soluciones innovadoras al mercado. "Este modelo de desarrollo de software colaborativo basado en un código abierto produce ratios de innovación mucho más altos. Recibir innovación en el menor tiempo posible es una ventaja competitiva", señala el responsable de Red Hat. Al mismo tiempo, la compañía cree que sus *partners* pueden aprovechar las oportunidades alrededor del *edge*, que supone llevar la capacidad de cómputo a los dispositivos que utiliza el usuario final. Y, por supuesto, todas las nuevas posibilidades que presenta la adaptación de su sistema operativo. "Estamos trabajando con muchas comunidades para personalizar Red Hat Enterprise Linux y aligerarlo lo suficiente para buscar casos de uso adicionales como pueden ser en la automoción o en la industria 4.0".

Formación y recursos

Los cambios que ha hecho en su estrategia de canal, que también han llegado a la dirección con la elección de Stefanie Chiras para dirigir el canal a nivel global y de Santiago Madruga para liderarlo en EMEA, están dirigidos a prestar más apoyo a sus *partners*, que se organizan en tres categorías —Ready, Advanced y Premier— dentro de su programa de canal. Este programa no ha sufrido cambios significativos porque la intención de Red Hat es que acaparen más negocio. "Estamos haciendo cambios en la estrategia y tratando de generar sinergias internas que nos den compromisos claros y fuertes en nuestra fuerza comercial para adoptar una filosofía de cliente primero, pero *partner* siempre", explica el directivo. La intención es que la contribución de sus socios al negocio crezca. "Los *partners* están contribuyendo por encima del 75 % del negocio global de Red Hat. Lo que queremos es incrementarlo y colaborar con ellos en el 100 % de las oportunidades", recalca.

Para que los *partners* puedan acaparar más negocio es imprescindible la formación y la capacitación. Por este motivo, está impulsando la especialización y dotando a sus *partners*



de nuevos recursos para formarse. El pasado mes de julio lanzó en EMEA el programa "Red Hat Container Platform Specialist" para que sus *partners* se especializaran en contenedores. Está especialización, que formaba parte de la iniciativa "Leading with Container", ha sido muy bien acogida por los *partners* en nuestro país y ha tenido su reflejo en el

incremento del registro de oportunidades, otra ventaja que ofrece a sus socios para respetar su negocio.

Además, ha lanzado 17 cursos gratuitos dentro del portal "Red Hat Training and Certification". Esta novedad supone un nuevo paso para ayudar al

canal y, como avanza el responsable, su intención es que en los próximos meses se pueda acceder a todo el catálogo sin coste alguno.

Esta nueva ventaja se suma a las que ya ofrecía como la atención a través de los *partners account managers*, las herramientas y los fondos de marketing para la generación de nuevo negocio, el registro de oportunidades, los recursos técnicos, etc.

Estos beneficios van encaminados a reforzar el trabajo conjunto con su red de *partners* ya que su intención es potenciar esa colaboración para seguir creciendo. "El objetivo es seguir creciendo a doble dígito desde un punto de vista de negocio y que a través de esta tecnología de código abierto podamos seguir llevando la innovación a los departamentos de informática de nuestros clientes", concluye Javier García Fiaño. 

Red Hat
redhat.es

“Este modelo de desarrollo de software colaborativo basado en un código abierto produce ratios de innovación mucho más altos”

El peso del software en su negocio alcanzó el 45 % en el cuarto trimestre de su último año fiscal

El software se consolida como motor del crecimiento de F5

Buena culpa de este giro de 180 grados la tiene su actual CEO, François Locoh-Donou, que hace casi un lustro observó que había que dirigir la mayor parte de la inversión hacia el componente inteligente que marcaba el diseño de las aplicaciones, el elemento central sobre el que pivotaba F5. "Debíamos seguir garantizando su disponibilidad, su rendimiento y su seguridad; pero su desarrollo había cambiado", recuerda Luis Miguel Cañete, director del canal de F5 en España y Portugal.

Aposentada en los entornos más tradicionales, donde reinaban las aplicaciones de misión crítica, que había que mantener, la compañía decidió arrancar una nueva etapa para adaptarse a un panorama en el que mandaba la nube: mientras que la demanda de las aplicaciones tradicionales crecía en torno a un 4 %, los nuevos entornos, donde reinaban las aplicaciones *cloud*, empezaban a explotar.

Un proceso de transformación, en el que todavía se encuentran, y que ha tenido un punto de inflexión en su último año fiscal, ejercicio récord, en el que el software se erigió en el motor de crecimiento. Tras unos años con ascensos de un dígito, F5 facturó 2.600 millones de dólares, lo que supuso un 11 % de crecimiento, con el software exhibiendo un ascenso del 37 %. Un protagonismo que se ha repetido en su primer trimestre fiscal, concluido el pasado 31 de diciembre, en el que el software galopó al 47 %. "Es notoria nuestra entrada en el desarrollo de las aplicaciones modernas", explica Cañete. "Estamos viviendo una enorme explosión: si en 2019 se contabilizaban 1 billón de aplicaciones a nivel mundial, en 2025 se prevé alcanzar 5 billones", recuerda.

El objetivo, señalado hace un par de años, es lograr que el peso del software se sitúe en un 80 % en 2024. Cañete, que no asegura el reto, sí está



Luis Miguel Cañete,
director del canal de F5 en España y Portugal

Hace apenas cuatro años el software apenas generaba el 20 % del negocio de F5. Hoy, según rezan los resultados del último tramo del año fiscal que acabó en septiembre, ya representa el 45 % de sus ingresos, convirtiéndose en el motor de su crecimiento. Un giro estratégico que tiene su penúltimo capítulo en el reciente lanzamiento de su plataforma F5 Distributed Cloud Services, que supone su primer paso en el exigente mercado del software como servicio. Una andadura que el canal también tiene que recorrer.

Marilés de Pedro

convencido de que la evolución es tremendamente positiva. "Estamos aprovechando la enorme expansión de las aplicaciones, basada en un nuevo diseño"; pero puntualiza: "Nuestra actual estrategia no trata de cambiar los productos de hardware por los de software". El hardware, por tanto, seguirá siendo una parte muy importante de la cifra de la compañía. "Queremos seguir creciendo en este apartado; tal y como lo hemos hecho hasta el momento".

El paso hacia el SaaS

El pasado mes de febrero la marca anunciaba la disponibilidad de F5 Distributed Cloud Services, su plataforma para servir su propuesta de seguridad, *networking multicloud* y soluciones de computación, basadas en el *edge*, en un formato de software como servicio. La primera solución que se ofreció fue F5 Distributed Cloud WAAP, para la protección de API y de aplicaciones web, a la que se han añadido otras. "Hemos reaccionado ante lo que el mercado está demandando", asegura Cañete. Una plataforma que ya está disponible en Microsoft Azure y que se extenderá al resto de los grandes hiperescalares.

Cañete insiste en que F5 sigue invirtiendo en el hardware. "Debemos seguir soportando a nuestros grandes clientes (bancos, operadoras, etc.) cuyas aplicaciones de misión crítica siguen residiendo en sus centros de datos". La marca ha renovado sus plataformas, transformándolas gracias al diseño de una arquitectura más modular y más preparada para las exigencias futuras.

Reto en el canal

El ecosistema de *partners* debe ser compañero obligado en esta estrategia. Junto a los *partners* con un perfil más tradicional, conviven compañías, nativas digitales, con una vocación más clara hacia el software y los servicios. Unos y otros, explica Cañete, deben acompañar a F5 en este camino. "Todavía hay muchos clientes y mucho *partners* resistentes al cambio; pero estamos caminando junto a ellos en esta transformación". Aunque, reconoce, que esta vocación por el software no se torna obligatoria, "los *partners* que lo hagan, crecerán al mismo ritmo que lo estamos haciendo nosotros".

El programa de canal de la marca, Unity+, que ya cumple dos años y medio de existencia, también tiene que reflejar esta nueva realidad. F5 está trabajando en su adaptación. "Tiene que dar cabida a los nuevos perfiles de *partners*, no solo los nativos digitales sino todos aquellos con un modelo MSSP", desvela. También demanda una evolución en las métricas. "Por encima del volumen, que sin duda sigue siendo importante, hay que valorar la especialización y el conocimiento de los *partners*". Los proyectos de software

"Todavía hay muchos clientes y muchos *partners* resistentes al cambio; pero estamos caminando junto a ellos en esta transformación hacia el software"

exigen nuevas valoraciones. "El volumen de negocio generado en torno al hardware no tiene nada que ver con el despliegue de los proyectos de software", alerta. "Y esto debe ser contemplado en el nuevo programa".

En el actual programa existen 3 categorías (Platinum, Gold y Silver). En España la marca cuenta con 3 *partners* Platinum (Telefónica, NTT y IBM), 7 *partners* Gold (la cifra global suma 11, pero incluye algunos *partners* con cobertura internacional que apenas tienen presencia en España) y 2 *partners* Silver. El resto son *partners* acreditados.

Dueto mayorista

El dueto mayorista está conformado por Arrow y Westcon. Una pareja que también debe acompañar a la marca en este enfoque. Cañete valora su continua actualización. "El canal, en muchas ocasiones, se muestra abrumado por el tsunami de soluciones que generan los procesos de transformación digital. A los *partners* les resulta realmente difícil seguirlo". Una tarea que los mayoristas sí son capaces de absorber. "Conocen nuestra oferta, se mantienen completamente actualizados y ofrecen ese conocimiento al canal".

Cada uno de ellos mantiene un equipo dedicado al 100 % a F5. "Son una extensión de nuestras capacidades". Junto al soporte que brindan a los *partners* tradicionales, también despliegan una importante labor de identificación y reclutamiento de nuevas empresas. 



Netskope impulsa su ecosistema de *partners* con su nuevo programa de canal



Francisco Machuca,
channel manager de Netskope

El nuevo programa de Netskope descansa, como apunta Francisco Machuca, *channel manager* de la compañía para Iberia, en tres pilares fundamentales: la capacitación del canal, la seguridad y la flexibilidad, y una tecnología 360. Sobre este último aspecto el directivo explica que el objetivo de la compañía ha sido crear un programa en el que todos los *partners*, sea cual sea su tipología, encuentren su sitio.

Machuca profundiza en otra de las patas clave de Evolve Partner Program subrayando que "para Netskope la capacitación del canal es fundamental" por varias razones. En primer lugar, la compañía quiere impulsar su crecimiento de una manera rápida y ágil. En segundo lugar, "buscamos un canal con una especialización muy alta porque las empresas no tienen más remedio que abrirse al *cloud* ya que la seguridad en la nube se ha incrementado", comenta. Y, en tercer lugar, por la manera de entender Netskope la relación con sus *partners*. "Para nosotros un *partner* es un socio real con el que trabajamos codo con codo, que entiende nuestra tecnología y saca el mayor rendimiento de ella", explica el directivo. Además, destaca el apoyo que Netskope brinda a su ecosistema de *partners*. "Somos una empresa 100 % canal, todo lo que trabajamos en Iberia lo hacemos a través de nuestro mayorista Exclusive Networks".

"Un *partner* es un socio real con el que trabajamos codo con codo, que entiende nuestra tecnología y saca el mayor rendimiento de ella"

 Olga Romero

El pasado mes de marzo Netskope, líder para *security service edge* (SSE) en el Cuadrante Mágico 2022 de Gartner, presentó Evolve Partner Program. Un nuevo programa de canal con el que la compañía ofrece a sus socios nuevos beneficios, incentivos y oportunidades orientados a incrementar la rentabilidad y acelerar el crecimiento de su red de *partners*.

Niveles de asociados

Evolve Partner Program cuenta con tres niveles de socios: autorizado, *gold* y platino. "La diferencia entre los niveles de *partners* son los descuentos e incentivos que tienen cuando llegan a los objetivos que se marcan en cada nivel", explica. El nivel autorizado es el más bajo y está dirigido a todas las compañías que quieran convertirse en *partners* de Netskope. Para ello únicamente deben alcanzar el nivel de capacitación que la compañía exige que, como asegura Machuca, "es el mínimo, solo necesitamos que sepan explicar bien nuestro producto porque ofrecemos una suscripción y tenemos que asegurarnos que nuestro canal conoce la solución para evitar que llegue un mensaje distorsionado al cliente".

Sobre los otros dos niveles el responsable de canal para Iberia comenta que "las diferencias entre los *partners gold* y platino están en el nivel de técnicos certificados, capacitación que tienen y nivel de facturación". En España Netskope tiene actualmente ocho *partners gold* y un *partner platino*. "Lo que buscamos con este nuevo programa es incentivar al canal para que gane más dinero vendiendo nuestras soluciones y poder así acelerar la venta a través de nuestra red de socios", afirma. Otros de los puntos destacados de Evolve Partner Program, aparte de los descuentos e incentivos, son las nuevas especializaciones y la ampliación de las vías de certificación técnica. A través de ambos aspectos Netskope materializa su apuesta por lograr un canal de distribución sólido y especializado. "La piedra angular, en torno a la que giran todos nuestros servicios, es la capacitación del ecosistema de *partners*", señala Machuca. Para lograr una alta especialización de sus socios la compañía dispone, tal y como explica el directivo, de "un programa de formación muy amplio orientado a la tipología de cada *partner* y a lo que quiera hacer".

2022: objetivos y fondos europeos

En febrero comenzó el nuevo año fiscal para Netskope. Un año para el que la compañía se ha propuesto "multiplicar



“La capacitación de nuestro ecosistema de *partners* es fundamental porque somos una empresa 100 % canal”

por dos, como mínimo, lo alcanzado en nuestro año fiscal 22". Un objetivo para el que Machuca se muestra optimista ya que en España el equipo de ventas ha pasado de siete personas a 18 entre los meses de noviembre, fecha en la que Machuca entró a formar parte de Netskope, a marzo. Los fondos NextGenerationEU serán los grandes protagonistas de este 2022 y supondrán una oportunidad de negocio para el canal de distribución. Por eso Netskope tiene puestas en marcha dos iniciativas relacionadas con las ayudas europeas. "Hemos desarrollado dos aproximaciones: una para el apartado de ciberseguridad, en el que entra toda nuestra oferta de navegación segura y control de aplicaciones, y otra para la parte de conexiones seguras, donde se encuentra nuestra oferta ZTNA", detalla. Una completa oferta que los *partners* de Netskope, algunos de ellos acreditados ya como agentes digitalizadores del programa Kit Digital, podrán ofrecer a sus clientes con el objetivo de acelerar la transformación digital de las pymes y garantizar la seguridad de los entornos de trabajo a través de la implementación de las soluciones de ciberseguridad necesarias. 

Netskope
netskope.es

La ley que regula el teletrabajo es otra de las medidas de este eje



Los derechos digitales, objetivo del 10º eje del Plan España Digital 2025

El 10º eje del plan España Digital 2025 está centrado en los derechos digitales. La intención del Gobierno es garantizar los derechos de las personas en un mundo digital. La elaboración de una Carta de Derechos Digitales era el principal objetivo de este eje y se ha conseguido. En julio de 2021 se aprobó la carta que contiene en seis categorías todos los derechos para garantizar las libertades y la igualdad en el medio digital y en los nuevos entornos laborales, empresariales y en otros específicos.

Rosa Martín

cesos de reflexión que se están dando en Europa sobre los derechos digitales para garantizar una digitalización humanista.

La carta recoge en seis categorías los derechos digitales. La primera está dedicada a los derechos de la libertad entre los que se encuentran el derecho a la identidad en el entorno digital, a la protección de datos, al

pseudonimato, a no ser localizados y perfilados, a la ciberseguridad y a la herencia digital.

La segunda categoría recoge cinco derechos de igualdad. Entre estos derechos figuran el de la igualdad y a la no discriminación, al acceso a Internet y a la protección a las personas menores de edad.

La tercera categoría es la dedicada a los derechos de participación y de conformación del espacio público. Incluye el derecho a la neutralidad de Internet, la libertad de expresión y la libertad de información, a recibir libremente información veraz y a la educación digital y a la participación ciudadana por medios digitales. En este bloque también se recogen los derechos digitales de la ciudadanía en su relación con las Administraciones Públicas.

La cuarta categoría recoge los derechos del entorno laboral y empresarial, mientras que la quinta está dedicada a los derechos en entornos específicos. En esta última se incluyen seis derechos entre los que figuran el derecho de acceso a los datos con fines de investigación científica o histórica, estadísticos o de innovación y desarrollo, el derecho a un desarrollo tecnológico y un entorno digital sostenible y los derechos ante la inteligencia artificial o el empleo de las neurotecnologías.

El último eje del Plan España Digital 2025 tiene tres objetivos principales: reforzar los derechos de la ciudadanía en el mundo digital, ofrecer certidumbre tanto a las empresas como a los particulares y a las Administraciones Públicas en el uso de las tecnologías y aumentar la confianza de los ciudadanos en el uso de las tecnologías digitales.

Dentro de este eje se encuentran cuatro medidas principales. La primera y más destacada es la elaboración de una Carta de Derechos Digitales, la segunda es el fomento del humanismo tecnológico, la tercera es la relacionada con la participación en iniciativas europeas y debates internacionales en materia de derechos digitales y la última se refiere a la modernización del marco laboral aplicable al trabajo a distancia.

Carta de Derechos Digitales

La Carta de Derechos Digitales se ha planteado como un marco de referencia para garantizar los derechos de los ciudadanos y las empresas en la nueva era digital. Su finalidad es sentar las bases para garantizar la protección de los derechos individuales y colectivos; y contribuir a los pro-



La sexta categoría es la de las garantías y la eficacia en la que se indica que todas las personas tienen derecho a la tutela administrativa y judicial de sus derechos en los entornos digitales de acuerdo a la legislación vigente y que el Gobierno adoptará las disposiciones oportunas, en el ámbito de sus competencias, para garantizar la efectividad de la carta.

Otras medidas

Junto con la publicación de la Carta de Derechos Digitales, el eje contempla otras medidas como el fomento del humanismo digital a través de la creación de iniciativas y espacios de debate para analizar el impacto de la tecnología en la sociedad y generar ideas para construir un futuro más justo. La intención del Gobierno es trabajar para que estas iniciativas impacten en cuatro áreas claves: la innovación pública, la confianza y la seguridad digital, el crecimiento justo y equitativo y el empoderamiento ciudadano. Otra de las medidas es la participación en iniciativas europeas y debates internacionales en materia de derechos digitales. En este sentido, el Ejecutivo quiere que España refuerce su presencia en foros de gobernanza digital a ni-

vel internacional. En este terreno se encuentran espacios como los comités o foros para la protección de los derechos de los menores en Internet, la privacidad y la protección contra el contenido dañino en línea con la Comisión Europea, el Consejo de Europa y la OCDE; y la hoja de ruta para la cooperación digital de las Naciones Unidas, entre otros.

La última medida es la relacionada con la modernización del marco laboral aplicable al trabajo a distancia. El Gobierno aprobó en julio de 2021 la Ley 10/2021, de 9 de julio, de trabajo a distancia, que regula esta modalidad laboral para asegurar la productividad y los derechos de los trabajadores.

La aprobación de esta ley y la publicación de la Carta de Derechos Digitales suponen que el objetivo de este eje esté prácticamente cumplido, aunque todavía falta profundizar en el desarrollo del humanismo digital, cuyo nivel de avance está en el 50 % —según calcula el Gobierno—, y en la participación en los foros internacionales en materia de derechos digitales. En este último aspecto, se ha avanzado un 80 % de lo previsto hasta el año 2025.

El Ejecutivo quiere que España refuerce su presencia en foros de gobernanza digital a nivel internacional

El Ejecutivo quiere que España refuerce su presencia en foros de gobernanza digital a nivel internacional. En este último aspecto, se ha avanzado un 80 % de lo previsto hasta el año 2025.

Plan España Digital 2025
agendadigital.gob.es

DERECHOS DIGITALES



1. Derechos y libertades en el entorno digital
2. Derecho a la identidad en el entorno digital
3. Derecho a la protección de datos
4. Derecho al pseudonimato
5. Derecho de la persona a no ser localizada y perfilada
6. Derecho a la ciberseguridad
7. Derecho a la herencia digital



8. Derecho a la igualdad y a la no discriminación en el entorno digital
9. Derecho de acceso a Internet
10. Protección de las personas menores de edad en el entorno digital
11. Accesibilidad universal en el entorno digital
12. Brechas de acceso al entorno digital



13. Derecho a la neutralidad de Internet
14. Libertad de expresión y libertad de información
15. Derecho a recibir libremente información veraz
16. Derecho a la participación ciudadana por medios digitales
17. Derecho a la educación digital
18. Derechos digitales de la ciudadanía en sus relaciones con las Administraciones Públicas

DERECHOS DIGITALES



19. Derechos en el ámbito laboral
20. La empresa en el entorno digital



21. Derecho de acceso a datos con fines de archivo en interés público, fines de investigación científica o histórica, fines estadísticos, y fines de innovación y desarrollo
22. Derecho a un desarrollo tecnológico y un entorno digital sostenible
23. Derecho a la protección de la salud en el entorno digital
24. Libertad de creación y derecho de acceso a la cultura en el entorno digital
25. Derechos ante la inteligencia artificial
26. Derechos digitales en el empleo de las neurotecnologías



27. Garantía de los derechos en los entornos digitales
28. Eficacia

Fuente: Carta de Derechos Digitales

Uno de sus focos actuales es la implantación del proyecto APEX

"En España el canal es extremadamente importante"

El directivo explicó que teniendo en cuenta las tendencias actuales del mercado como la explosión de los datos, el auge del *multicloud*, la aparición de nuevas arquitecturas TI y la inteligencia artificial, la compañía está adaptándose a las nuevas necesidades y desarrollando una estrategia en dos sentidos. Uno se dirige a consolidar y modernizar su *portfolio*, en el que destacan los PC y las soluciones de infraestructura y almacenamiento. En este terreno se encuentra inmerso en el desarrollo del proyecto APEX para ofrecer la tecnología como servicio. La otra dirección de su estrategia está encaminada a la búsqueda de nuevas oportunidades en áreas como el *edge*, los servicios *multicloud* y la gestión de los datos, entre otras.

Canal

Majdalani resaltó que la intención es "invertir donde se puede mejorar y seguir trabajando en nuestro negocio core". Dentro de esta estrategia, el ecosistema de *partners* seguirá jugando un papel clave para atender a las nuevas necesidades de los clientes y extender en el mercado los nuevos modelos de consumo.

La compañía tiene previsto unificar criterios para que todos los *partners* de su programa de canal, con independencia de su perfil, disfruten de todos los beneficios y recursos. Dell se caracteriza por ser una empresa que escucha tanto a los clientes como a los *partners*, según resaltó el directivo. Por este motivo, el respeto al canal es máximo a pesar de mantener la venta directa, reservada para los clientes históricos y fundamentalmente para la venta de soluciones para el puesto de trabajo. Su propósito es construir relaciones ajustadas a las características de los *partners* y a las de los mercados en los que operan.

El peso que está adquiriendo el canal en su estrategia se cuantifica en el volumen de negocio que acapara, ya que más del 55 % de sus ingresos proceden de las ventas del canal. El crecimiento del canal fue un 10 % mayor que el de la compañía y el de los mayoristas fue el doble que el de la propia Dell. Estos datos se unen al buen comportamiento del negocio durante el último año que creció un 17 % y alcanzó los 100.000 millones de dólares. En nuestro país, los resultados también han sido muy positivos y como indicaron tanto Majdalani como el director de canal en España y Portugal, Nacho Martín, hay un buen clima de negocio, a pesar de la incertidumbre por el contexto mundial.



Diego Majdalani,
presidente de Canal Internacional de Dell Technologies

Dell sigue impulsando su estrategia de canal y apostando por mantener un sistema mixto entre la venta directa e indirecta, aunque cada vez tiene más peso el canal. Diego Majdalani, presidente de Canal Internacional de Dell Technologies, ha analizado la situación del canal español durante su visita a nuestro país y ha afirmado que el "canal es extremadamente importante" tanto por su capacidad como por los resultados obtenidos durante el último año.

 Rosa Martín

El canal en nuestro país está desplegando el proyecto APEX, aunque cuenta con el buen resultado de Flex on Demand. En este sentido, Martín resaltó que "permite que el cliente, junto con el *partner*, defina el tipo de arquitectura que necesita". La gran ventaja es que paga un fijo mensual por la infraestructura que utiliza, pero dispone de una parte adicional instalada por la que paga solo si tiene que usarla.

La novedad es que este modelo se está extendiendo hacia la reventa para que el *partner* pueda ofrecer servicios. Y en esta modalidad el papel de los mayoristas es fundamental como un "agregador de servicios para otros *partners* más pequeños" como recalcó Majdalani.

El presidente del Canal Internacional de Dell reiteró que se encuentra satisfecho con los resultados del canal en nuestro país y subrayó que su intención es seguir invirtiendo de cara al futuro. 

Dell Technologies
dell.es

Experiencia, calidad e innovación

TU MAYORISTA DE CONFIANZA



MÁS DE
30 AÑOS
CONTIGO



AMPLIO
PORTFOLIO



DMI PRO



LOGÍSTICA



DROPSHIPPING



EQUIPOS
A MEDIDA



4
DELEGACIONES



CALIDAD Y
MEDIO
AMBIENTE



CALCULADORA
PVP



ÁREA WEB
PRIVADA

DMI

Computer

TU MAYORISTA
DE CONFIANZA

www.dmi.es



El portal de la digitalización para Pymes

Ponemos a tu disposición un **amplio catálogo de soluciones** para tu empresa. Además, contamos con los partners perfectos para acompañarte en el proceso. Haz crecer tu negocio con la asesoría de nuestros expertos.

Descubre cómo beneficiarte de los fondos Next Generation. Toda la información para **conseguir subvenciones públicas** para tu negocio.



CONSULTORÍA
TECNOLÓGICA

IMPLANTACIÓN
DE SOLUCIONES



FORMACIÓN
Y CURSOS

AYUDA EN FONDOS
Y SUBVENCIONES

