



linkedin



twitter



newsbook.es

>> La revista del distribuidor informático

# Newsbook

Tai  
editorial

Año XXXI N° 326 Mayo 2025

0,01 Euros

## Rendimiento superior a tu alcance con Windows 11 Pro

HP ZBook Firefly



HP recomienda Windows 11 Pro para empresa



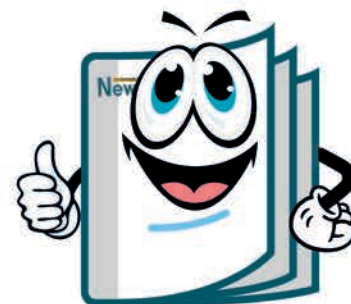
Consulta con tu mayorista habitual.



esprinet



TD SYNnex



¿Nos sigues en  
Linked **in**?



En 2024, España ocupó la octava posición a nivel mundial en el ranking de los países con más ataques de *ransomware*

## Ciberseguridad y amenazas: el "binomio" que crece en paralelo

**L**as empresas españolas siguen invirtiendo en sistemas y en soluciones de ciberseguridad. Según datos de la consultora Context, el área de la ciberseguridad fue uno de los apartados que mejor se comportó el pasado año, con el área del software creciendo casi un 7 %. Áreas como la seguridad en la nube, la protección de las identidades, el



desarrollo del Zero Trust y las tecnologías vinculadas con el MDR y el XDR fueron algunos de los segmentos de inversión prioritarios.

Frente a la protección, las amenazas. Entre ellas, el *ransomware* se mantiene como el ataque con más devastación. España se sitúa como el octavo país en el mundo más atacado por este *malware*.

Sigue en pág. 23



El Grupo Esprinet apuesta por el valor añadido para consolidar su liderazgo

### "El rol del mayorista está evolucionando hacia un habilitador de la tecnología"

El segmento del mayoreo atraviesa una transformación significativa, impulsada por la digitalización y la creciente competencia. Alessandro Cattani, CEO del Grupo Esprinet, explica que "la clave está en evolucionar hacia un modelo de mayor valor añadido", manteniendo al mismo tiempo una posición sólida en el negocio de volumen. En este sentido, destaca el papel del grupo como habilitador estratégico dentro del ecosistema tecnológico, ofreciendo soluciones que responden a las nuevas demandas del mercado. Cattani reafirma el compromiso con su política de adquisiciones, especialmente en nichos de alto valor, como parte del proceso de diversificación y crecimiento.



Sigue en pág. 6



### La sostenibilidad: el reto por colocarse en el centro del negocio



Poco a poco, las empresas y los organismos públicos, impulsados por el sentir de la sociedad, están colocando la sostenibilidad en el centro de su estrategia de negocio y de desarrollo. Más allá del cumplimiento normativo, la sostenibilidad se percibe como una herramienta para mejorar la competitividad, fortalecer la reputación y hacer crecer el negocio.

Sigue en pág. 39



# Sostenibilidad y seguridad: doble ese de oportunidad

Siempre a la búsqueda de oportunidades. Ese es el espíritu que pinta la personalidad de negocio de un gran parte del canal. Inmersos los distribuidores en uno de los apartados de mercado más atractivos, el carácter de las TIC, siempre cambiantes y con un ritmo endiablado en lo que se refiere a la innovación, exige estar siempre alerta.

Muchas son las áreas en las que el ecosistema de distribuidores puede poner su atención. Un panorama cuya amplitud dificulta la especialización, término que la mayoría vincula con la rentabilidad; y que genera oportunidades continuas; así convive el entorno de la nube, por ejemplo, que ya exhibe una cierta "madurez", con la "irrupción" de la IA, que lo ha revolucionado todo.

Aunque lo impregna todo, no vamos a referirnos "directamente" a esta última, sino a dos segmentos que llevan unos cuantos años sonando con fuerza. Uno, sin duda, de una manera mucho más contundente y poderosa que el otro; pero ambos con atractivas dosis de rentabilidad.

La contundencia corresponde a la seguridad, que es uno de los apartados más bendecidos por la oportunidad. Lleva años exhibiendo crecimientos de doble dígito y, según las previsiones que maneja la consultora IDC, el gasto global en este apartado experimentará un crecimiento del 12,2 % en este ejercicio. Un aumento, predice, que estará impulsado por la creciente complejidad y frecuencia de las ciberamenazas, aceleradas por la inteligencia artificial generativa (GenAI) y la inteligencia artificial en general.

La inversión en ciberseguridad alcanza un casi infinito número de entornos: desde el resucitado puesto de trabajo hasta la nube, pasando por los olvidados dispositivos móviles, las aplicaciones, la red o el *edge*, a los distribuidores se les abren tantos campos de actuación como de amenazas por detectar y detener. Un segmento en el que la oferta de servicios gestionados se torna en uno de los apartados de más clara rentabilidad; ahora bien, modelar un perfil de MSSP exige formación y especialización; y ya sabemos lo huérfanos que nos encontramos de talento. Una situación que, oh paradoja, alienta y explica el despliegue de este modelo gestionado.

La otra gran oportunidad, esta mucho más incipiente y etérea, es la sostenibilidad. Un término que algunas empresas exhibían hace tiempo como condimento de marketing, y que ahora parece haberse convertido, al menos para muchas, en un elemento conformador de su estrategia de negocio. Según la "Consulta de desarrollo sostenible 2024 realizada por el Pacto Mundial de la ONU España" 7 de cada 10 empresas españolas ya dispone de una estrategia o un plan de sostenibilidad y el 84 % de las compañías ve la sostenibilidad como una ventaja competitiva. Un panorama que debe aprovechar el canal, para convertirse en un consultor de las empresas, colocando la tecnología como una herramienta al servicio de la sostenibilidad.

De ambas oportunidades damos buena cuenta en los dos especiales que se incluyen en este número de mayo; oportunidades que presentan, cada una de ellas, una madurez y una idiosincrasia propia pero que, sin duda, señalan un camino largo y rentable. 

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 Servimedia S.L., empresas colaboradoras del responsable que tratarán los datos con las mismas finalidades. Siendo conservados mientras no manifieste su oposición a seguir recibiendo el servicio solicitado. Puede usted ejercer los derechos de acceso, rectificación o supresión de sus datos, dirigiéndose a arco@taieditorial.es para más información al respecto, puede consultar nuestra Política de Privacidad en <https://taieditorial.es/politica/>

## En primera persona Grupo Esprinet



Alessandro Cattani, CEO

6

## Especial Seguridad en el canal



Check Point, Exclusive Networks, Kaspersky, Sophos y V-Valley defienden esta oportunidad

23

## En Portada

## La mujer en el sector TIC



La inteligencia artificial, nuevo desafío

16

## Especial Sostenibilidad

Acer, Canon, Esprinet, HP y

Vertiv: la sostenibilidad como

clave para el futuro **Pág. 39**

## En profundidad

Samsung **Pág. 9**

Aumenta su oferta de tabletas con

la nueva Galaxy Tab S10F

V-Valley **Pág. 10**

Celebración de su Cybersecurity

Summit

HP **Pág. 50**

El PC, clave en el desarrollo de la IA

HPE **Pág. 52**

Alejandro Martín explica las

novedades para su canal

Vertiv **Pág. 54**

Presenta las tendencias de los

centros de datos

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  
Bárbara Madariaga • barbara@taieditorial.es

### PUBLICIDAD

David Rico • david@taieditorial.es

### PRODUCCIÓN

Marta Arias • marta@taieditorial.es

### OTRAS PUBLICACIONES

directorTIC

tpvnews

PYMES

Negocios en informática

ciberseguridadTIC.es

EDITA



T.A.I. Editorial, S.A.

(Técnicos Asesores Informáticos Editorial, S.A.)

[www.taieditorial.es](http://www.taieditorial.es)

Avda. Fuencarral, 68

28108 ALCOBENDAS (Madrid)

Tel.: +34 91 661 61 02

E-mail: [correo@taieditorial.es](mailto:correo@taieditorial.es)

### MIEMBRO DE



FEDERACION INTERNACIONAL DE LA PRENSA PERIODICA

### DISTRIBUCIÓN

Publistat Publicidad Directa, S.A.

C/ Fundidores, 53 (Pol. Ind. Los Angeles)

28906 Getafe - Madrid

Tel.: 91 683 76 92

### DEPÓSITO LEGAL

M-20480-2002

### ISSN

1696-6147

Impreso en

papel ecológico



# ¡VIVE LA EXPERIENCIA MSP!

Una mañana con...

## N-N-ABLE

## &edorteam

**10 DE JUNIO | 11:00 H.**  
**ESPACIO JORGE JUAN | MADRID**

**REGÍSTRATE**



**ADM**  
Cloud & Services

**TE RECORDAMOS NUESTRA**  
**III EDICIÓN**  
**ROAD SHOW 2025**

**SEVILLA · VALENCIA · VALLADOLID**



**¡INSCRÍBETE!**

El área ibérica ya supone más del 50 % de la rentabilidad

# "El rol del mayorista está evolucionando hacia un habilitador de la tecnología"

El segmento del mayoreo atraviesa un momento de transformación, donde los actores más importantes están adaptando sus estrategias a un entorno cada vez más competitivo y digitalizado. En este contexto, Alessandro Cattani, CEO del Grupo Esprinet, aborda el crecimiento de la compañía, destacando su evolución hacia el valor añadido y explica cómo, además de mantener su fuerte posicionamiento en el sector de volumen, el grupo ha sabido adaptarse a las nuevas demandas del mercado, convirtiéndose en un habilitador clave en el ecosistema tecnológico.

 Bárbara Madariaga

**2** 023 y 2024 han sido años complicados para el segmento del mayoreo. Según datos de la consultora Context, en las regiones en las que opera el Grupo Esprinet, 2023 estuvo marcado por el decrecimiento del mercado (1,6 % en España, un 4 % en Italia y un 5 % en Portugal). En 2024 el panorama ha mejorado, con crecimientos, pequeños, en España e Italia (0,3 y 0,5 %, respectivamente); y un 7 % en Portugal. ¿Qué lectura se hace de estos dos complicados años y, lo más importante, prevé una consolidación de ese crecimiento en el mercado del mayoreo en los países donde opera?

Somos positivos, lo son los analistas y lo somos nosotros también. Después de la pandemia experimentamos años de altibajos, sin embargo, la situación parece haberse estabilizado. Observamos que la utilización del canal mayorista por parte de los fabricantes ha aumentado en comparación con años anteriores. Esto se debe a varios factores. El primero, la recuperación de la demanda de consumo. Las familias habían reducido sus compras debido a la inflación, pero tras el aumento del salario mínimo y la disminución de los tipos de interés, que ha aliviado las hipotecas, hemos observado un repunte en la compra de tecnología. Asimismo, estamos viendo una recuperación significativa en las ventas de PC. Después de cinco años ha llegado el momento de renovar la tecnología, especialmente con el fin del soporte para Windows 10. De hecho, ya lo hemos observado en este primer trimestre, donde se ha dado una re-



Alessandro Cattani,  
CEO del Grupo Esprinet

cuperación notable en este mercado. Además, y no menos importante, vemos una excelente dinámica en las empresas impulsada por la transformación digital. Esto requiere una inversión continua, ya sea en inteligencia artificial o en actividades más básicas que no se habían abordado previamente, lo que ha generado mucha innovación. Sin embargo, esta evolución, que trae consigo grandes oportunidades, también presenta riesgos significativos, ya que las nuevas tecnologías se traducen en amenazas cibernéticas cada vez más potentes, lo que genera una alta demanda en el sector. En este contexto, los analistas, los fabricantes y nosotros prevemos un crecimiento de un dígito en el canal mayorista para el sur de Europa

durante este año. De cara a los próximos años, todos los indicadores apuntan a un mercado con un futuro prometedor.

**En este panorama, el Grupo Esprinet acaba de presentar sus resultados, con excelentes números: como grupo se creció un 4 %, con un ascenso del 6 % en Italia y del 8 % en España; por encima en ambos casos del comportamiento del negocio global del mayoreo. ¿Cuáles son las claves que explican estos números positivos en ambos países?**

2023 fue un año muy complicado. Después de un 2021 y 2022 con récords de rentabilidad, al final de 2022 nos encontramos con niveles de stock excesivos. Durante 2023 nos enfocamos en limpiar ese stock, lo hicimos sin incurrir en pérdidas y de manera eficiente, pero, evidentemente, perdimos algunas oportunidades de mercado. En 2024 hemos vuelto a operar de forma más estable y en línea con las condiciones normales del mercado. En el sector de volumen en el que trabajamos, especialmente en el ámbito de impresoras y electrodomésticos de consumo con nuestra marca Esprinet, hemos hecho un trabajo excelente.

Hace años que estamos invirtiendo de manera significativa en la distribución de valor añadido a través de nuestra marca V-Valley y todas esas inversiones se han traducido en una aceleración notable de nuestra presencia en el mercado de valor. V-Valley es el resultado de inversiones en personas, empresas, procedimientos, la incorporación de nuevos fabricantes y la oferta de un nivel de servicio excepcional al mercado.

## ¿Cuál es el peso estratégico que ha alcanzado España? ¿Qué destacaría de su desempeño en los últimos años?

El grupo ibérico, que abarca España y Portugal, representa algo menos del 40 % de nuestra facturación, pero ya supera el 50 % de nuestra rentabilidad. Esto se debe a que en España hemos acelerado significativamente en el sector del valor añadido. Creo que este es un punto clave. Esprinet en España ha tenido una respuesta muy positiva y lo que esperamos de nuestro equipo es que siga creciendo a un ritmo alineado con el mercado, o incluso ligeramente por encima, siempre con un control estricto de los costes. No vemos un mercado en el que se puedan aumentar los precios considerablemente, por lo que es crucial mantener un control eficiente del nivel de stock y del capital circulante. Esta es la forma de generar valor para nuestros accionistas. Al vincular estos objetivos, estamos empujando al equipo a encontrar maneras de ofrecer a nuestros clientes un servicio de calidad superior. Este es el enfoque que siempre seguimos en nuestra estrategia de satisfacción del cliente. Es importante entender las necesidades de nuestros clientes, distribuidores y minoristas y trabajar para ofrecerles un servicio mejor que el de la competencia. A veces lo conseguimos, a veces no, pero si miramos nuestra historia, creo que hemos logrado hacerlo un poco mejor que otros, lo que nos ha permitido seguir creciendo.

**Echando un vistazo a los resultados, destaca el comportamiento de V-Valley, la división de soluciones avanzadas, con un crecimiento del 10 %. Desde hace años, el grupo ha llevado a cabo una transformación de su estrategia de negocio, con un foco decidido en el desarrollo de este complejo mercado del valor. ¿Qué ha sido clave para conseguir estos resultados?**

Hay dos razones principales. La primera: el mercado demanda soluciones para la transformación digital. Nosotros somos vendedores y vendemos lo que el mercado necesita. Es cierto que hay grandes volúmenes de PC, de impresoras o de teléfonos, pero en los últimos años las empresas han comenzado a renovar sus modelos de negocio y para hacerlo han necesitado software y soluciones complejas, lo que abre oportunidades de venta para quienes ofrecen valor añadido, como V-Valley. Esta es, en parte, una respuesta natural a las demandas del mercado.



## “V-Valley es el resultado de inversiones en personas, empresas y procedimientos”

La segunda razón es que vender valor añadido es un desafío y, como ocurre con las soluciones más complejas, lo que se ofrece como valor añadido suele llevar consigo márgenes más altos. Nuestros accionistas siguen exigiendo más valor y mayores beneficios. Por eso, la estrategia del grupo es continuar invirtiendo en nuestra línea histórica de negocio, que es el volumen, alentando a nuestro equipo a defender, si es posible, su cuota de mercado, controlando costes y evitando excesos de stock. Al equipo dedicado al valor les decimos que hay grandes oportunidades en áreas como la inteligencia artificial, la ciberseguridad y la nube. Todos los temas claves de los últimos años están en el mundo del valor.

Nuestro objetivo es ganar cuota de mercado y generar beneficios. Y generamos beneficios porque estamos ofreciendo soluciones complejas. Vender un PC o impartir formación requiere un alto nivel de automatización en los procesos. En cambio, vender una solución de ciberseguridad demanda profesionales con certificaciones y conocimientos técnicos especializados. Los clientes y fabricantes deben pagar por este *know-how* y por nuestra capacidad para gestionar un entorno tan complejo. En España somos el mayorista más grande en volumen, aunque no somos el líder en el sector del valor añadido. Nuestro objetivo es acercarnos cada vez más a esa primera posición, pero no tanto por ser el número uno o dos. Lo que realmente necesitamos es garantizar a nuestros accionistas una rentabilidad que les sea atractiva y la rentabilidad se encuentra princi-

palmente en el sector del valor. ¿Qué se necesita para destacar en este campo? Personas con talento. Aunque la automatización juega un papel, éste es un sector donde el valor añadido de las personas es crucial. Por eso nos estamos enfocando en contratar, formar y retener a los mejores profesionales. Cuanto más crecemos, mejor. Ser el número uno es solo una meta para motivar a nuestro equipo, no un objetivo en sí mismo.

**El Grupo Esprinet compete con los principales mayoristas: algunos de ellos con un perfil generalista, similar al del grupo; y otros con un perfil más especializado. ¿Qué hace diferente al Grupo Esprinet?**

Nuestra principal diferencia es la hispanidad. El concepto es simple: todo lo que invertimos en esta área lo hacemos porque el mercado lo demanda, no porque tengamos estrategias revolucionarias. Sencillamente, el mercado lo pide y nuestro trabajo es ofrecerle lo que necesita. La diferencia clave, como mencionaba antes, es que estos son proyectos donde el valor de los recursos humanos es fundamental. Creemos que tener un equipo muy hispano, que hable el idioma no solo en términos lingüísticos sino también culturalmente, es crucial. Necesitamos personas que realmente entiendan y vivan en España, algo que nos diferencia de la competencia. En el Grupo Esprinet dejamos un nivel de autonomía significativo. Yo puedo marcar la estrategia, que es sencilla: seguir al mercado, ofrecer un entorno agradable y rentable para nuestros inversores y colabora-

# EN PRIMERA PERSONA

dores, y permitir que nuestro equipo local se adapte a las necesidades del mercado.

**Es esencial, para mantener la fortaleza financiera, el desarrollo de los negocios de volumen, donde la competencia es enorme y los márgenes mucho más ajustados. ¿Qué marca la estrategia en este apartado?**

En Italia y España ya contamos con una posición muy sólida. Ahora, el objetivo es identificar nichos de mercado que aún no hemos explotado completamente. Por ejemplo, en España estamos explorando sectores como la papelería, el mercado audiovisual profesional y el *gaming*. Son áreas que ya hemos desarrollado bastante bien en Italia, pero que en España todavía no hemos aprovechado lo suficiente.

Además, otro de nuestros enfoques es mejorar el nivel de servicio que ofrecemos a nuestros clientes. Con el tiempo, los clientes han evolucionado y actualmente tienen un mayor conocimiento tecnológico. Aun así, todavía necesitan apoyo en procesos que antes no eran tan relevantes, pero que ahora lo son cada vez más. El dinero es más escaso y muchos están buscando opciones como el *leasing* o el alquiler. También hay un creciente enfoque en la sostenibilidad, por lo que el reciclaje y el reacondicionamiento de equipos se han convertido en temas claves. Los clientes necesitan ayuda para hacer frente a estos nuevos desafíos, que antes no existían, pero ahora son problemas reales que debemos convertir en oportunidades.

**La división Zeliotech fue creada en Italia el pasado año. ¿Qué objetivos se persiguen con ella en este 2025? ¿Para cuándo su implantación en España?**

Aún no la tenemos en España, pero la idea es abrir cuanto antes. Es una cuestión de encontrar los contratos adecuados para los productos y fichar al equipo necesario. Nos gustaría poder hacerlo este año, pero no depende solo de nosotros.

En cuanto a los objetivos, es un mercado potente, pero también depende mucho de los incentivos de los distintos gobiernos. Para nosotros es obligatorio estar presentes en varios países, porque siempre habrá países donde el gobierno reduzca los incentivos y la demanda caiga, mientras que en otros aumenten y la demanda suba. Por eso lo necesitamos. Ha-

blando de objetivos específicos, puedo decir lo siguiente: en 2011 lanzamos V-Valley en Italia, con una facturación de 114 millones de euros. El año pasado V-Valley estaba presente en Italia, España, Portugal y Marruecos y en términos de ventas brutas alcanzamos alrededor de 1.200 millones de euros. Ahora lanzamos Zeliotech, en su primer año ha logrado unos ingresos de alrededor de 160 millones de euros. Esperamos tener un negocio que alcance los mil millones en 10 años.

La oportunidad de mercado existe. Aún no hemos definido objetivos a largo plazo, pero claramente hay potencial. No es un mercado de nicho en el que se pueda pensar en facturar 200 millones de euros. Es un mercado donde existen jugadores europeos que facturan 3.000 millones de euros, entre otras cifras. Es un mercado enorme. Por lo tanto, hay una gran expectativa de poder añadir una cantidad significativa de facturación y beneficios al grupo.

**En los últimos años hemos asistido en el mercado del mayoreo a un proceso, creciente, de consolidación; siendo el Grupo Esprinet exponente de ello. ¿Cree que este proceso va a continuar?**

Sí, creo que sí. Es un mercado donde la cantidad y la potencia de la tecnología es tan grande que requiere de personas, inversiones y herramientas adecuadas y los pequeños mayoristas tendrán cada vez más dificultades. Además, los fabricantes siguen consolidando el número de mayoristas, por lo que creo que en Europa seguirá una tendencia similar. Si miramos Estados Unidos, seis mayoristas controlan el 90 % de la facturación del mercado mayorista. En Europa somos 200 y el mercado es un poco más pequeño. Y eso es algo a tener en cuenta.

Al final es una cuestión económica. Los márgenes son muy bajos y se necesita volumen para ser rentable. Si no se tiene volumen, no es sostenible. Por lo tanto, creo que la consolidación va a ocurrir sí o sí, principalmente por razones económicas más que por otros factores.

**¿Seguirá el grupo con esta política de adquisiciones?**

Sí, nos gustaría continuar con nuestra estrategia, centrada en los nichos, especialmente en aquellos de alto valor añadido donde podamos incorporar nuevos fabricantes, clientes o per-

sonas con experiencia, siempre que el precio sea adecuado. Queremos seguir haciendo adquisiciones.

Nuestros nichos están principalmente en el ámbito del valor añadido y en los de servicios que podemos encontrar en Italia, España y Portugal. Fuera de estos países, llevamos años buscando mayoristas de tamaño medio a grande para dar un paso adelante y crear nuevas oportunidades, replicando lo que hemos logrado previamente en Italia, luego en España, y ahora estamos mirando en Portugal. Las zonas de interés son siempre las mismas: Alemania, Austria, Francia, Benelux, Reino Unido e Irlanda.

Llevamos tres años buscando fuera de España y aún no hemos encontrado nada. Es posible que durante los próximos tres años tampoco encontremos nada, pero esa es la realidad.

**Observando lo que ha pasado en el mercado TIC en los últimos años, ¿desempeñan ahora los mayoristas un papel con mayor valor? ¿Incrementarán su peso estratégico en los próximos años?**

Todos los análisis indican un crecimiento, aunque aún pequeño, pero sigue siendo significativo. Actualmente, estamos en alrededor del 47 % del total del *go-to-market* de los fabricantes de tecnología, excluyendo claramente los servicios, mientras que hace 10 años estábamos cerca del 40 %. Por lo tanto, ha habido un incremento. Ha crecido y sigue creciendo. La tecnología se está volviendo cada vez más compleja, con un número creciente de fabricantes, lo que acelera la llegada de nuevas tecnologías. Creemos que el mayorista del futuro no solo será el lugar donde se busca la tecnología, sino también el lugar donde se obtiene toda la información necesaria para elegir, instalar, poner en marcha y mantener esa tecnología. Será un rol más como habilitador de la tecnología que simplemente un "supermercado" donde compras productos. Nosotros pasamos mucho más tiempo ahora en la gestión de la preventa que en la entrega o simplemente en la distribución del producto. El rol del mayorista está evolucionando hacia un habilitador y eso es un reto, pero también una oportunidad. Si lo haces bien, puedes generar más valor añadido, fidelizar a los clientes y tener un rol más sólido dentro del ecosistema en su conjunto. 

La nueva serie está preparada para integrarse con otros dispositivos del ecosistema de Samsung

# Samsung potencia su presencia en el mercado de las tabletas con la nueva Galaxy Tab S10 FE

**S**egún explicó David Alonso, vicepresidente y director del negocio de movilidad de Samsung para España y Portugal, el mercado de las tabletas está creciendo entre el 4 % y 5 %, aunque la evolución del primer trimestre ha sido muy positiva y se ha registrado un crecimiento de dos dígitos.

Al mismo tiempo en el mercado se observa una polarización entre la gama alta y la baja. En la primera no se está produciendo un incremento acelerado en la parte más premium, pero sí que está creciendo la parte cuyo precio supera los 600 euros.

A pesar de que las ventas se concentran en la gama más baja, el lanzamiento el año pasado del modelo S9 FE que estaba en un nivel intermedio, en un rango de precio entre 400 y 700 euros, fue un hito para Samsung, convirtiéndose en un modelo superventas, según destacó Alonso. "En B2B, en el segmento de la educación y en el segmento personal ha tenido una aceptación muy grande", confirmó el directivo. "El cliente estaba buscando más funcionalidad y más prestaciones que en las tablets más básicas del mercado"

## Características

Este éxito ha motivado el lanzamiento de la serie Galaxy S10 FE que aspira a repetir el incremento de las ventas. Esta nueva tableta se caracteriza por su pantalla más grande y sus biseles más finos.

La pantalla Galaxy Tab S10 FE+ de 13,1 es casi un 12 % más grande que la FE+ anterior. Ofrece una frecuencia de actualización de 90 Hz y un nivel de visibilidad de hasta 800 nits HBM. Además, gracias a los ajustes automáticos de Vision Booster se mejora el brillo y la calidad de la imagen incluso en el exterior.

La serie FE, que también cuenta con la certificación IP68, ofrece funciones para mejorar la productividad como la capacidad de cambiar sin esfuerzo entre aplicaciones para lograr una multitarea mejorada y capacidades de IA. Entre estas capacidades figura la opción de "Circle to Search" con Google para la búsqueda de información. Además, facilita la traducción de texto y proporciona ayuda para realizar otras tareas como la resolución de pro-



Samsung ha lanzado una nueva tableta para los usuarios que demandan más prestaciones a sus dispositivos con un modelo que está a caballo entre la gama básica y la alta. Se trata del Galaxy Tab S10 F y de su versión S10 FE+ que se han diseñado para ofrecer una experiencia de usuario óptima y enriquecida con la inteligencia artificial tanto para las tareas de entretenimiento como para las de trabajo.

 Rosa Martín

blemas matemáticos, la corrección ortográfica, etc.

Los asistentes de inteligencia artificial se pueden activar al pulsar la tecla Galaxy AI Key en la funda teclado y ajustarse según las preferencias de los usuarios.

Esta novedad integra una cámara trasera de 13 MP y permite incrementar la creatividad con otra serie de herramientas instaladas. Además, una de sus grandes ventajas es que está preparada para integrarse con otros dispositivos del ecosistema de Samsung. Y todo con la garantía de seguridad de la plataforma Samsung Knox. 

Nueva edición del V-Valley Cybersecurity Summit



# Cuatro años creando conexiones, conocimiento y negocio

A

lberto López, responsable del área de ciberseguridad de V-Valley para España y Portugal, recordó que este foro, más allá del *networking*, es un espacio donde surgen sinergias concretas, y celebró el crecimiento del área de ciberseguridad: "Éramos doce personas y ahora somos 77. Hemos multiplicado por 20 nuestra facturación en siete años". Su intervención dejó clara la filosofía que impregna todo el proyecto: "Sentido común, cercanía y compromiso. Eso es lo que nos define". A partir de ahí, la jornada se articuló en cinco bloques temáticos que abordaron desde la gobernanza hasta las operaciones, pasando por arquitectura, desarrollo e inteligencia de amenazas.

La conducción del encuentro corrió a cargo del periodista y presentador de televisión José Yélamo, quien actualmente dirige el programa *laSexta Xplica*.

## Gobernanza y seguridad

Lo que nació como un debate sobre la creciente complejidad regulatoria en ciberseguridad —con normativas como NIS2, DORA o GDPR como puntos de partida— acabó convirtiéndose en una conversación mucho más amplia sobre el papel de la facilidad tecnológica, el valor del integrador y la necesidad de una mayor colaboración y transparencia entre fabricantes y *partners*.

Consolidado ya como uno de los encuentros más valiosos del canal de ciberseguridad en España, el evento anual de V-Valley, celebrado los días 3 y 4 de abril, en la localidad de La Granja, en Segovia, alcanzó su cuarta edición con la participación de más de 170 profesionales. Un evento que apuesta por un formato que combina debates, reuniones estratégicas y muchas oportunidades reales de negocio. A10 Networks, Acronis, Allied Telesis, Arexdata, Check Point Software, Cloudflare, CyberArk, Elastic, Entrust, Iberlayer, Kaspersky, OpenText, ReeVo, Sectigo, SonicWall, Trellix, Trend Micro, TU, WatchGuard y Zebra fueron los fabricantes presentes en el evento; junto a Lidera Cloud y Esprifinance.

 Rosalía Arroyo

David Gasca, *head of marketing & operations cybersecurity* en V-Valley, fue el encargado de abrir el bloque con una reflexión sobre el momento actual: la proliferación de regulaciones de ciberseguridad y el desafío que representa para las empresas proteger la cadena de suministro desde distintos ángulos: identidad, continuidad de negocio y resiliencia.

Rocío Martínez, responsable de Entrust Digital Identity para España, recordó cómo Europa innova a través de la regulación: "NIS2 y DORA son una oportunidad. Estamos en el centro de ambas, con un enfoque de identidad digital y criptografía". Subrayó, no obstante, la ambigüedad de estas normativas y la necesidad de contar con expertos para su interpretación y cumplimiento.

Aitor González, *senior solutions engineer* de Acronis, puso el foco en los proveedores de servicios como pieza clave para acompañar a las empre-

sas en este viaje regulatorio asegurando que “nuestros clientes —los *partners*— necesitan herramientas usables, pero también formación y respaldo ante la escasez de talento técnico”.

Uno de los giros claves del debate llegó cuando se planteó si ofrecer plataformas “fáciles de usar” podría devaluar el papel de los integradores. La conversación se polarizó entre quienes defendían la simplicidad como vía para mejorar la eficiencia y quienes advertían del peligro de trivializar la complejidad de la ciberseguridad.

Karina Rojas, *channel sales manager* de CyberArk, reconoció con humor la envidia que le produce la sencillez de otras plataformas, mientras Alan Vázquez, *partner account manager* de ReeVo, defendió la necesidad de soluciones que permitan aglutinar tecnologías heterogéneas de forma coherente. Por su parte, Eusebio Nieva, director técnico de Check Point Software, recordó que “todas las plataformas son fáciles... hasta que pasa algo”. Para él, el verdadero valor del integrador está en ser ese “pegamento” entre soluciones heterogéneas, ofreciendo personalización y cobertura real a los clientes.

Profesionales del sector destacaron durante el encuentro la necesidad de una perspectiva crítica sobre ciertos mensajes de los fabricantes. Uno de ellos señaló la falta de claridad en las referencias al cumplimiento de DORA, mencionando cómo la promesa de soluciones “con un par de clics” dificulta el trabajo de los integradores.

Otro profesional, tras una intensa preparación para obtener una certificación técnica, enfatizó la importancia de que el cliente valore esa dedicación, advirtiéndole que el mensaje de plataformas “fáciles de usar” podría perjudicar a los *partners*.

Desde una perspectiva práctica, se añadió que la aparente sencillez de algunas soluciones lleva a los clientes a buscar ayuda profesional ante incidentes como el *ransomware*, subrayando que la seguridad requiere acompañamiento experto en todas las etapas del proyecto.

Elena García-Mascaraque, directora *world-wide partner ecosystem growth* de WatchGuard Technologies, amplió el foco recordando que la mediana empresa también necesita ciberseguridad, pero con presupuestos ajustados y pocos recursos técnicos. Por eso, las plataformas deben ser eficientes, sí, pero también adaptables a la realidad de cada cliente: “Vamos con Ferraris, repletos de prestaciones, a clientes que no saben cómo manejarlos. Necesitamos soluciones ajustadas al perfil de cada empresa”. Javier Barandiarán, *cybersecurity alliance and partner manager* de Opentext Cybersecurity, añadió un apunte clave sobre la cadena de suministro y el uso de librerías *open source*, especialmente en aplicaciones

de IA, “como un nuevo vector de riesgo que los *partners* también deben ayudar a mitigar”.

Aunque la agenda inicial ponía el foco en regulación, identidad y gobernanza, el debate evolucionó hacia una reflexión más profunda sobre cómo fabricantes e integradores deben colaborar de forma más honesta, estratégica y realista. La tensión entre “facilidad de uso” y “valor del integrador” quedó claramente expresada, así como la necesidad de construir un discurso conjunto frente al cliente, que combine tecnología, servicios y experiencia operativa.

## OT, IoT y un nuevo paradigma de protección

En el segundo bloque, el foco se desplazó hacia los entornos IT/OT y la necesidad de repensar las arquitecturas de seguridad ante la explosión del IoT y la creciente digitalización de infraestructuras críticas. La digitalización de las infraestructuras críticas, el crecimiento del IoT y la convergencia de entornos IT y OT han transformado radicalmente la superficie de exposición

de las organizaciones. Esta evolución exige una revisión profunda de los modelos de protección, una mayor especialización y una colaboración constante entre fabricantes e integradores.

Fabricantes y expertos coincidieron en que la visibilidad, la segmentación, el control de identidades

máquina y la aplicación del modelo Zero Trust son más relevantes que nunca.

Andrés Peñarubia, *alliance manager* de Elastic, insistió en la importancia de la visibilidad. A través de una analogía sencilla pero eficaz, explicó que tener visores apuntando a puntos críticos no garantiza un control total si se ignora lo que ocurre entre ellos. “No hay forma de proteger lo que no se ve”, concluyó.

Juan Asensio, country manager de AIO Networks, centró su intervención en el papel cada vez más crítico del IoT, que se ha convertido en una puerta de entrada para ataques distribuidos: “El aumento de bots conectados está impulsando ataques DDoS masivos”. Denunció que muchas organizaciones están externalizando responsabilidades al migrar a la nube, lo que transforma también el rol del integrador, y aseguró que “del destornillador a la consola en la nube, el integrador también se reinventa”.

José Miguel Domínguez, director de la unidad de negocio de Auto-ID de V-Valley, en representación de Zebra, puso el foco en el hardware como eslabón crítico de la cadena de seguridad, asegurando que “hay una oportunidad de negocio inmensa en entornos como almacenes, mataderos u hospitales, donde abunda el IoT basado en Android”, insistiendo en la importancia de

“NIS2 y DORA son una oportunidad”





contar con dispositivos que cumplan normativas y sean interoperables con las plataformas del *partner*.

Fernando Ruiz, *presales manager* para Iberia de Allied Telesis, propuso una mirada histórica sobre la evolución de las redes, del aislamiento al multi-servicio, y advirtió que las redes OT siguen siendo un "reducto" difícil de integrar. Afirmando que los responsables OT viven de espaldas a IT por miedo a los riesgos, "y con razón", propuso tender puentes, pero desde el respeto a los protocolos y particularidades de cada entorno. "Antes de hablar de seguridad, hay que entender cómo funciona una red OT".

Asegurando que "el 5G abre un espectro nuevo de amenazas" y que tenemos que anticiparnos con herramientas que permitan evaluaciones constantes, Jorge Villaescusa, *sales engineer* de Trend Micro, abordó el impacto del 5G privado y la necesidad de mantener visibilidad continua ante una diversidad creciente de dispositivos conectados.

Karina Rojas, responsable de canal de CyberArk, aportó una estadística reveladora: "Por cada identidad humana hay 45 no humanas", lo que implica que, más allá de los usuarios, existen infinidad de dispositivos y sensores con credenciales que deben ser protegidas. "Muchos clientes no saben ni cuántas identidades de máquina tienen. Ahí es donde el *partner* tiene que liderar".

Pedro David Marco, fundador y CEO de Iberlayer, ejemplificó el problema con un caso real: un casino estadounidense fue *hackeado* a través del termómetro *wifi* de un acuario. Preguntando si realmente era necesario que ese termómetro tuviera *wifi*, planteó que, a veces, "el problema no es lo que no se protege, sino lo que nunca debió estar conectado".

Juan Molina, *partner solutions engineer* de Cloudflare, ahondó en las posibilidades de aplicar Zero Trust incluso en entornos sin agentes al tiempo que alertaba sobre el auge de ataques impulsados por IA: "Ya no hace falta una red zombi de millones de dispositivos. Con pocos servidores inteligentes se puede hacer mucho daño".

Defendiendo la especialización como vía para acceder a un mercado que sigue siendo reactivo, José Antonio Morcillo, director de canal de Kaspersky en España y Portugal, aportó una visión desde el canal: "Los clientes saben que necesitan seguridad OT, pero no están viendo integradores especializados", lo que, aseguraba, "genera desconfianza".

Fernando Ruiz volvió a intervenir para diferenciar entre OT e IoT, recordando que muchas veces se tratan como sinónimos. "Son mundos distintos, con riesgos distintos. En IoT el problema es que casi nada está diseñado con la seguridad en mente". Puso como ejemplo el riesgo en universidades donde miles de estudiantes conectan sus dispositivos a la red institucional: "¿Quién protege eso?".

En su intervención de cierre, David Gasca reivindicó la necesidad de repensar las arquitecturas desde la base, considerando todos los vectores de ataque, desde el *cloud* hasta el dispositivo más inesperado. Juan Asensio y Juan Molina coincidieron en la importancia de actuar cerca del origen del problema, controlando el tráfico y aplicando políticas de Zero Trust. El mensaje final fue claro: la seguridad no puede seguir siendo una reacción. Debe ser una estrategia compartida entre fabricantes, integradores y clientes. Y eso exige tecnología, visión y mucha más colaboración.

## Aplicaciones, desarrollo y seguridad en la era del multicloud

El tercer bloque abordó uno de los puntos más críticos y menos visibles de la ciberseguridad moderna: el desarrollo seguro del software. Con una creciente dependencia de entornos *multicloud*, una explosión de API, una adopción masiva de librerías *open*

*source* y un número creciente de desarrolladores con acceso a entornos híbridos, la conversación abordó los riesgos estructurales del ecosistema digital moderno. Desde la gestión del código hasta la protección de identidades privilegiadas, pasando por la trazabilidad del software y el impacto de la inteligencia artificial, el debate dejó claro que el software —más que nunca— es la primera línea de defensa (y de exposición).

David Gasca abrió el bloque con una reflexión que sintetiza el desafío: "Las empresas se están exponiendo más. Nos protegemos, sí, pero luego trabajamos en entornos híbridos, *multicloud*, con coordenadas de seguridad norte-sur, este-oeste, y eso cambia las reglas del juego".

Eusebio Nieva fue claro en su diagnóstico: "No se puede proteger la nube como se protege un entorno *on-premise*. Hay que cambiar el paradigma". Apostó por tecnologías de seguridad comunes que permitan simplificar la protección en distintos entornos, evitando soluciones fragmentadas. Al ser

## La convergencia de entornos IT y OT ha transformado la superficie de exposición

preguntado por la diferencia entre empresas nativas *cloud* y tradicionales, fue rotundo: "Los nativos *cloud* suelen equivocarse menos. Tienen mejor interiorizado el modelo y son más conscientes de los riesgos". Aun así, recordó que en todos los casos el éxito depende de tres pilares: "Tecnología, procesos y personas".

Durante su intervención Javier Barandiarán puso sobre la mesa datos concretos: "El 80 % de las brechas de seguridad tienen origen en el software de aplicación". Explicó cómo su compañía ha apostado por crear alianzas tecnológicas para cubrir todas las etapas del desarrollo seguro: desde el análisis estático y dinámico, hasta la detección de vulnerabilidades en librerías *open source* (como con Sonatype) o el entrenamiento de desarrolladores mediante *gamificación* (Secure CodeWarrior). "Muchos clientes nos piden cubrir más. Y eso requiere plataformas que integren todo. No pueden seguir gastando el 4 % del presupuesto de ciberseguridad solo en integrar herramientas dispares".

Andrés Peñarubia defendió el valor del software libre asegurando que no se le puede estigmatizar al tiempo que recordaba que hoy "todo está montado en Linux, incluidos los sistemas críticos. No lo habrán hecho tan mal". Insistió en que el problema no es la tecnología en sí, sino cómo se integra, cómo se gestiona y si se mantiene la trazabilidad en toda la cadena. Su defensa del enfoque DevSecOps apuntó a la necesidad de continuidad entre desarrollo, operaciones y seguridad porque "no pueden ser mundos separados". Barandiarán matizó que el riesgo no está sólo en la seguridad; también en la sostenibilidad de las librerías utilizadas: "El 80 % de las librerías *open source* están mantenidas por una o dos personas. Eso es un riesgo empresarial enorme".

Juan Molina abordó el problema desde la capa de aplicación explicando que muchas brechas se producen por falta de control sobre las API y componentes de terceros como el JavaScript: "Necesitas saber si un JS *open source* ha cambiado sin tu permiso" porque si algo falla, "el responsable eres tú". Reivindicó herramientas *cloud* que permitan monitorizar y gestionar todos estos elementos al tiempo que defendía el uso de plataformas de Zero Trust con capacidades CASB para integrar entornos multinube bajo políticas comunes.

Karina Rojas aprovechó la coincidencia con el Día Mundial de la Protección en Cloud para resaltar el problema de los accesos privilegiados en entornos de desarrollo recordando que hay muchos desarrolladores con muchos accesos a muchas nubes. "El cliente no sabe cuántos ni qué privilegios tienen". Subrayó la oportunidad de negocio que representa esta problemática poniendo como ejemplo que en CyberArk hay más de 1.000 desarrolladores que "no son administradores, pero tienen privilegios críticos.

Ahí hay negocio para los *partners*".

También alertó sobre la necesidad de no incomodar al desarrollador, porque "si le complicas un paso, buscará cómo saltárselo".

El bloque dejó claro que la seguridad del desarrollo no puede seguir tratándose como una capa adicional. Debe estar integrada desde el

inicio, con herramientas unificadas, políticas coherentes y especialización. En un entorno donde el software se compone de miles de piezas conectadas, con múltiples orígenes y responsables, la visibilidad y la colaboración son fundamentales. Un entorno en el que el papel del *partner* vuelve a ser esencial: como asesor, como integrador y como catalizador de una cultura de desarrollo seguro.

## Threat Intelligence: entre la anticipación y la IA ofensiva

El cuarto bloque del encuentro se adentró en un terreno donde la tecnología y el análisis se cruzan con la estrategia y la intuición: el universo de la Threat Intelligence. Dámaso Ramos, responsable de servicios en V-Valley, abrió la conversación con una pregunta provocadora: "¿Queremos ser inteligentes o simplemente listos?". Una reflexión que sirvió para enmarcar el debate: anticiparse es tan importante como saber reaccionar y, para ello, tanto la inteligencia humana como la artificial tienen un papel esencial.

Alan Vázquez explicó cómo el SOC de ReeVo utiliza inteligencia, tanto preventiva como reactiva, integrando datos de múltiples fuentes para protegerse de amenazas de día cero. Destacó el uso de SOAR y SIEM para bloquear IP maliciosas detectadas en la *deep* y *dark web* explicando que son capaces de "ver IP atacando vulnerabilidades conocidas y las cortamos antes de que lleguen. Eso no lo pueden hacer ni medio millón de humanos". Por su parte, José Antonio Morcillo recalcó la importancia de estar presen-

## La seguridad debe ser una estrategia compartida entre fabricantes, integradores y clientes





tes en los foros donde realmente se gesta el cibercrimen. "El 85 % de las amenazas proviene de zonas como Rusia, China o Corea. Si no estás allí, no sabes lo que viene", al tiempo que subrayaba que la verdadera Threat Intelligence requiere "infiltración, experiencia y capacidad de anticipación". La conversación pronto derivó hacia el uso de la inteligencia artificial. David Baldomero, *senior systems engineer* de Trellox, destacó su valor en tareas de detección, investigación en lenguaje natural y reducción del ruido: "Tener una IA como copiloto nos permite centrar el esfuerzo donde realmente hay un problema", comentaba, al tiempo que planteaba la cuestión emergente de la IA contra IA, anticipando un nuevo tipo de enfrentamiento técnico.

Jorge Villaescusa apeló a la necesidad de una inteligencia proactiva, capaz de identificar patrones antes de que se materialicen en un ataque: "Parece ciencia ficción, pero es real: podemos actuar antes de que el ataque ocurra".

Sergio Martínez, director general de SonicWall, alertó de que los atacantes también están aprovechando la IA para detectar vulnerabilidades con mayor precisión, encadenar ataques de manera más eficiente y ofuscar y borrar rastros. "El cibercrimen tiene todo el tiempo del mundo. Y ahora, también, todas las herramientas".

Rocío Martínez abrió un nuevo frente: la IA generativa como fuerza laboral. "Vamos a tener cientos de agentes que contarán como empleados. ¿Cómo protegemos una empresa con 400.000 agentes virtuales?". Propuso adoptar una mentalidad de brecha asumida (*assume breach*) y repensar los métodos de defensa.

"Usamos IA para ayudar a los administradores a ser más ágiles y seguros", decía Karina Rojas, al tiempo que recordaba que la IA también puede facilitar la configuración de productos complejos como los sistemas de gestión de privilegios.

Asegurando que la IA no existe, sino que lo que hay son sistemas de aprendizaje sin supervisión, Pedro David Marco recordó que pueden ser enve-

nenados "para que acepten como legítimo lo que debería ser bloqueado".

Subrayando el papel de los integradores para acompañar a los clientes en una adopción segura, Javier Barandiarán alertó sobre la inseguridad inherente a los modelos generativos: "El 48 % de las empresas está usando IA con datos públicos o preentrenados. Sólo el 20 % entrena con datos propios".

Morcillo volvió a intervenir para recordar que, sin visibilidad global, no hay defensa efectiva: "Si los ataques son globales y tú solo ves lo que pasa en España, vas con los ojos vendados". También señaló que el verdadero valor del MDR reside en la inteligencia, más que en la tecnología de detección.

Elena García-Mascaraque apostaba por combinar inteligencia colectiva, automatización sensata y experiencia: "Primero hay que entender los procesos, luego automatizar y, sobre todo, aplicar experiencia. Ser listos también es parte de la inteligencia".

El bloque concluyó con una sensación de ambivalencia. La IA ofrece herramientas sin precedentes, pero también plantea riesgos y retos éticos. La Threat Intelligence requiere acceso, experiencia y contexto, pero también un ecosistema de colaboración. Como apuntó Juan Molina, la combinación de Zero Trust con MFA sigue siendo un escudo robusto, incluso ante amenazas simuladas por IA. Cerró Alan Vázquez: "Acabaremos tratando a la IA como a un empleado más: con permisos, privilegios y controles. Solo así evitaremos que se convierta en el eslabón más débil".

## Seguridad de las operaciones

En el último bloque del encuentro, la conversación se centró en la seguridad de las operaciones. El debate giró en torno a modelos de SOC, la gestión del talento, la automatización y los desafíos operativos que enfrentan los equipos de ciberseguridad. Dámaso Ramos, responsable de servicios de V-Valley, abrió el bloque apuntando directamente a tres ejes

claves: la compartición de inteligencia, la automatización que algunos empiezan a cuestionar y la dificultad para retener profesionales cualificados.

Javier Fernández, *enterprise regional sales manager* de Sectigo, reflexionó sobre el valor de la inteligencia compartida entre entidades públicas y privadas, y el papel que

puede desempeñar una red nacional de SOC. "Lo importante es tener una entidad que permita colaborar entre todos para estar preparados ante cualquier ataque, venga de donde venga", aseguró, añadiendo un matiz interesante sobre el SOAR: "No basta con orquestar, hay que tener capacidad de ejecutar con inteligencia detrás". Reafirmó que la seguridad 100 % no existe, porque el eslabón más débil sigue siendo el humano. Por ello,

La seguridad de las operaciones es  
un equilibrio entre herramientas,  
procesos y personas

aunque la inteligencia artificial puede filtrar grandes volúmenes de eventos, "siempre tiene que haber un humano que diga: hasta aquí ejecutamos", explicó Fernández.

David Baldomero reforzó esa idea asegurando que la IA "no puede reemplazar el juicio humano, pero sí ayudarnos a digerir la telemetría imposible y señalar dónde actuar".

Uno de los temas recurrentes fue la fuga de talento. Elena García-Mascaque reivindicó la experiencia como factor diferencial y propuso una redefinición del modelo SOC: "Cada vez vemos modelos más híbridos, distribuidos geográficamente, incluso con colaboración entre MSP y fabricante". Apuntó que uno de los principales factores de fuga es la repetitividad del trabajo del analista, lo que se traduce en fatiga profesional. "Cuanto más tedioso es el trabajo, más probable es que se vayan". Su solución: herramientas diseñadas para liberar al analista de tareas repetitivas y aumentar el valor de su trabajo.

Javier Barandiarán compartió una experiencia similar: "Los SOC pierden talento porque les damos tareas que antes hacía una máquina. Hay que invertir en automatización para evitar quemar a los analistas". Explicó cómo tecnologías de auto-triage permiten reducir la carga operativa, especialmente en la gestión de vulnerabilidades de aplicaciones.

David Gasca cerró el bloque con una propuesta tan sencilla como potente: "Si eliminamos las tareas repetitivas con herramientas, necesitaremos menos personas. Y a esos pocos, podremos pagarles más y ofrecerles un trabajo más estimulante".

Una conclusión pragmática que pone el foco en la necesidad de rediseñar los equipos SOC no solo desde la tecnología, sino desde la gestión del talento y el bienestar profesional.

Este último bloque consolidó una idea presente en todo el encuentro: la tecnología es necesaria, pero insuficiente. Automatizar, compartir información, usar inteligencia artificial... todo suma. Pero si no se cuida al profesional que está al otro lado de la consola, cualquier arquitectura de seguridad será siempre vulnerable por su eslabón más humano. La seguridad de las operaciones, en definitiva, es un equilibrio entre herramientas, procesos y personas.

A lo largo de los cinco bloques, quedó patente que la ciberseguridad ya no es sólo una cuestión técnica. Es un desafío de gestión, de estrategia y de confianza. Las plataformas pueden ser más fáciles de usar, pero el papel del integrador sigue siendo imprescindible. La inteligencia artificial ofrece herramientas sin precedentes, pero también plantea nuevos riesgos. El talento técnico es escaso y valioso, pero también difícil de retener si no se crea un entorno profesional más atractivo.

Desde el *compliance* hasta las operaciones, pasando por el desarrollo seguro o el Threat Intelligence, los temas tratados evidencian una necesidad común: cooperar más, compartir más, escuchar más. Fabricantes, distribuidores y *partners* tienen en sus manos la posibilidad de crear un ecosistema más eficiente, más transparente y más humano. Como quedó claro en La Granja, la ciberseguridad no se vende: se construye. Y para eso, nada mejor que sentarse a hablar. Juntos. 



## Tenemos toda la información que necesitas

Para profesionales del canal de distribución TIC



**Newsbook**  
**Negocios**  
en informática  
**Newsbook.es**

Para los CISO de las compañías



**ciberseguridadTIC.es**

Para el C-Level de mediana y gran empresa



**directorTIC**  
**directorTIC.es**

Para gerentes de pymes



**PYMES**  
**revistapymes.es**

POS, captura de datos y retail



**tpvnews**  
**tpvnews.es**

La necesidad de fomentar las vocaciones STEM sigue siendo prioritaria

# La mujer sigue luchando para consolidar su papel en el sector TIC

Luces y sombras se observan en el camino de la mujer hacia la plena igualdad en el sector tecnológico. Algunas barreras van cayendo, pero queda todavía mucho por hacer para lograr la equiparación salarial y conseguir las mismas oportunidades de desarrollo profesional que los varones. Una representación de mujeres ejecutivas del sector TIC comparte su experiencia, analiza el papel que la mujer está desempeñando en el ámbito tecnológico y explica cómo se está enfrentando a los nuevos desafíos que plantea la irrupción de nuevas tecnologías como la inteligencia artificial.

🔗 Bárbara Madariaga

🔗 Marilés de Pedro

🔗 Rosa Martín

**E**n los últimos años, la brecha salarial se ha ido reduciendo, tal y como refleja Funcas en un informe que indica que desde el año 2012 al 2022 la brecha salarial de las mujeres españolas se ha reducido en 10 puntos, pasado del 18,7 % al 8,7 % en este periodo, aunque la edad marca todavía diferencias siendo las generaciones más mayores las que sufren una brecha salarial mayor. Lo más positivo es que entre los menores de 25 años las mujeres ganan, de promedio, más por hora que los hombres. Estos datos del mercado laboral general

no son totalmente extrapolables al sector tecnológico porque la presencia de la mujer es escasa todavía, una carencia más acusada en puestos de responsabilidad. Las directivas coinciden en señalar que es indudable el avance, pero que el sector TIC no avanza al mismo ritmo que el mercado general. Inés Bermejo, directora general de HP en España y Portugal, destaca que "en el sector TIC la evolución de esta brecha ha sido más compleja y no siempre ha seguido el mismo ritmo de mejora". Las diferencias salariales que sufren las profesionales más veteranas se gestaron en el ini-

cio de su carrera en el que la brecha salarial era más acusada, lo que ha supuesto una equiparación más lenta, aunque también se observan otros obstáculos como la discriminación por edad, las interrupciones en la carrera profesional por motivos familiares y la falta de oportunidades.

Por el contrario, las profesionales más jóvenes se enfrentan a una brecha menor por varios motivos entre los que se encuentran "la creciente preparación académica y específica de las mujeres, las políticas de conciliación implantadas por algunas empresas y la mayor



**Maite Ramos**  
directora general de NetApp Iberia

"No basta con abrir más oportunidades de acceso al sector tecnológico, sino que es necesario transformar la cultura empresarial para garantizar que las mujeres puedan desarrollarse plenamente en él"

predisposición a la formación interna", según explica Carmen Muñoz, directora general de Exclusive Networks en Iberia.

Las razones para que esta brecha persista obedecen a varios factores y no solo a las diferencias en la remuneración directa. Elena García-Mascaraque, directora *worldwide partner ecosystem growth* de WatchGuard Technologies, identifica algunos de los factores estructurales del sector como "la menor presencia de mujeres en posiciones de liderazgo y en áreas de mayor especialización técnica, que son las que suelen estar mejor remuneradas".

"La falta de transparencia en las políticas salariales y la poca visibilidad de las mujeres en altos cargos contribuyen a perpetuar estas desigualdades", añade Luisa Paolucci, consejera delegada de V-Valley. Ángeles Delgado, presidenta de Fujitsu en España, resalta que aún persisten desafíos para el

avance de la mujer en el sector, especialmente en posiciones de mayor responsabilidad y entre las profesionales de mayor edad. Y recalca que "la equidad salarial no solo es una cuestión de justicia, sino también de competitividad y retención del talento".

### Talento y formación

La menor presencia de las féminas en el sector tecnológico agrava el problema que tiene el sector de escasez de profesionales. Los datos estadísticos confirman esta situación. Según

"La falta de graduadas en STEM es una realidad"

recoge el INE, en 2023 el 16 % de las empresas españolas disponía de especialistas en TIC y, aunque el 38 % de estas compañías empleaba a mujeres, solo el 8 % contaba con al menos el 50 % de sus profesionales de género femenino. A juicio de Maite Ramos, directora general de NetApp Iberia, esta situación "no solo afecta a las profesionales del sector, sino que

tiene implicaciones mucho más amplias, ya que la tecnología no es solo una industria más, sino un motor clave para el desarrollo futuro en todos los ámbitos".

En la base de esta falta de mujeres profesionales en el terreno tecnológico, que repercute en la carencia de talento cualificado, se



**Marta González**  
Alliance & Channel Partner Sales director para Iberia de Salesforce

encuentra la formación en disciplinas STEM. En este sentido, Marta González, *Alliance & Channel Partner Sales director* para Iberia de Salesforce, recalca que la "falta de graduadas en STEM es una realidad y hemos de abordarlo desde la infancia para lograr que las niñas se sientan atraídas por nuestra industria".

Ramos cree que para dar la vuelta a la realidad que apunta a que en España solo 8 de cada 100 estudiantes de carreras científicas son mujeres es necesario derribar ciertos prejuicios y obstáculos como "la falta de referentes femeninos y la percepción errónea de que



**Pilar Martín**  
vicepresidenta de Ventas de TD Synnex en España

"Hay que pelear por políticas flexibles que ayuden a la conciliación familiar y, sobre todo, ponerse límites a una misma, priorizando tu bienestar"

## EN PORTADA

tienen menor capacidad en estas áreas". Pilar Martín, vicepresidenta de Ventas de TD Synnex en España, coincide con esta opinión y señala que "en los sector TECH y STEM hay todavía mucho camino por recorrer. La desigualdad sigue siendo un desafío considerable en el sector TIC".

María Herranz, directora de la Organización de Partners en Cisco España, ahonda en esta idea y

"Las empresas tecnológicas deben reconocer que se requieren mayores inversiones en cultura, diversidad, políticas y formación"

afirma que "las empresas tecnológicas deben reconocer que se ha llegado a un punto de no retorno y que se requieren mayores inversiones en cultura, diversidad, políticas y formación para tener éxito en el futuro".



**María Herranz**

directora de Organización de Partners en Cisco



**Inés Bermejo**

directora general de HP en España y Portugal

### La inteligencia artificial, nuevo reto

La irrupción de la inteligencia artificial plantea un nuevo reto a las profesio-

nales porque aquí se vuelve a repetir el parámetro de una participación limitada. Según datos del Foro Mundial de la Unesco solo un 22 % de las mujeres están participando en su desarrollo. Patricia Núñez, directora de la divi-

"El liderazgo femenino en TIC seguirá creciendo si seguimos abriendo camino y demostrando que el talento no tiene género"

## Mujeres en el canal mayorista

En el sector tecnológico la presencia de la mujer es limitada, un problema que se acentúa en el canal mayorista, aunque desde este segmento se está trabajando intensamente para corregir este des-

equilibrio. Pilar Martín, Luisa Paolucci y Carmen Muñoz coinciden en la importancia de la formación continua para consolidar su posición en el sector y ascender a nuevos puestos. En este sentido, Muñoz



destaca las iniciativas que desde Exclusive Networks se están poniendo en marcha para identificar y retener el talento. "Para nosotros es muy importante crear cantera", recalca. Para lograrlo tienen programas de prácticas para estudiantes de grados o másteres de áreas relacionadas con las tecnologías, ofrece programas de *mentoring* internos y desde hace un par de años está en funcionamiento la "Exclusive Academy", un programa de formación interno diseñado para potenciar las capacidades tanto de los empleados como de los socios comerciales.



**Elena García-Mascaraque**  
directora worldwide partner ecosystem growth de WatchGuard Technologies

"En el sector de la ciberseguridad las habilidades femeninas son muy valoradas por nuestra capacidad de resiliencia, empatía y cuidado"

Para Adela de Toledo, *country manager* de Pure Storage Iberia, a pesar de que los datos globales no son positivos, en nuestro país hay signos esperanzadores. Aporta un dato alentador, recogido en un estudio de Randstad, presentado el pasado mes de diciembre: el 45,2 % de los

sión de PCSD de Lenovo en Iberia, considera que es cierto que no hay mucha participación femenina en el desarrollo de la IA, por lo que esta baja presencia hay que considerarla como "una llamada a la acción y una oportunidad de mejora porque no hay duda que necesitamos diversidad en los equipos que trabajan en su desarrollo para evitar sesgos". La directiva señala que para su desarrollo, que basa en los datos que se introducen, "es clave que haya mujeres entrenándola". Anna Coll, *B2B channel sales manager* de Samsung España, comparte esta visión y señala que se debe abordar con urgencia este nuevo reto. "Es fundamental impulsar la participación femenina en IA desde la educación hasta el ámbito profesional".

"Es fundamental rodearse de mentores y colegas que confíen en nuestras capacidades"

profesionales cualificados en inteligencia artificial son mujeres, pero matiza porque considera "que sigue siendo necesario fomentar esa tendencia positiva para que la formación se convierta en dedicación y lograr reducir la brecha de género".

Esta directiva indica que para avanzar en el terreno de la IA se necesita un compromiso por parte de las instituciones públicas y privadas para fomentar la educación científica y tecnológica desde edades tempranas, visibilizar referentes femeninos que inspiren a las nuevas generaciones y ofrecer programas de mentoría.



**Carmen Muñoz**  
directora general de Exclusive Networks

"Las mujeres en puestos directivos tenemos una misión primordial en promover el cambio y servir de ejemplo para el resto de las mujeres de nuestras organizaciones"

## Medidas

Las ejecutivas coinciden en señalar que es necesario seguir impulsando los programas que promueven la igualdad y seguir tomando medidas para que las mujeres puedan cerrar las brechas que impiden su desarrollo profesional en el ámbito de la IA y en el

sector tecnológico en general. Ramos cree que el sector tiene que dar un gran paso porque "no basta con abrir más oportunidades de acceso, sino que es necesario transformar la cultura empresarial para garantizar que las mujeres no solo entren en el sector, sino que puedan desarrollarse plenamente en él".



**Luisa Paolucci**  
consejera delegada de V-Valley

Dentro del terreno del desarrollo de la IA, Paolucci aboga por "asegurar una IA ética y responsable integrando la perspectiva de género en todas las etapas del desarrollo, desde el diseño hasta la implementación".

Pilar Martín pone el acento en el apoyo al carácter emprendedor de la mujer en este apartado y señala que "es necesario incentivar la financiación de startups de IA lideradas por mujeres".

## Consejos a las nuevas generaciones

Las ejecutivas que han superado diversos obstáculos en sus carreras y cuentan con una rica experiencia profesional son las voces más autorizadas para aconsejar a las nuevas generaciones de mujeres que quieran trabajar en el sector. La mayoría coincide en señalar a la confianza en una misma como el principal consejo para poder desarrollarse profesionalmente, superando los prejuicios previos sobre la capacidad de las mujeres en un ámbito mayoritariamente masculino. La formación continua, rodearse de una red de

mentores que les acompañe y aceptar nuevos desafíos son otros de los consejos que ofrecen a las jóvenes que están dando los primeros pasos en el sector.

Patricia Núñez les recomienda que confíen en sus habilidades al postularse para nuevos roles. "No es necesario cumplir con el 100 % de los requisitos; una buena actitud y un 70 % de encaje pueden ser suficientes", destaca. Y añade que "experimentar diferentes roles dentro de la empresa, especialmente en áreas como

la de producto y operaciones, les pueden proporcionar una visión integral del negocio".

Luisa Paolucci les anima a "ser resilientes y persistentes. Los desafíos forman parte del camino, pero con determinación y esfuerzo es posible alcanzar grandes logros".

"El sector tecnológico ofrece un sinfín de oportunidades. La clave está en atreverse a aprovecharlas y en tener la ambición de ser protagonistas de esta revolución", añade Ángeles Delgado.



Para García-Mascaraque un aspecto fundamental para que la mujer pueda trabajar con igualdad tanto en el sector TIC como en otros,

ahora que la IA transformará muchos sectores, es la necesidad de integrar la formación tecnológica en todos los ámbitos profesionales.

Apela al concepto de "bilingüismo tecnológico" que supone que "el sistema educativo debe poner más foco en este concepto donde cada una de las materias que se imparten en los currículos de las diferentes profe-

desarrollarse profesionalmente".

A juicio de las directivas, las medidas que se tendrían que poner en marcha para dar un empujón a la presencia de la mujer en la industria TIC abarcan desde la formación y capacitación en competencias digitales hasta las políticas empresariales inclusivas, la difusión de historias de éxito de mujeres profesionales en el sector y la creación de redes de apoyo. En

este último aspecto, María Herranz comenta que es necesario establecer "programas de mentoría donde profesionales experimentadas guíen y apoyen a mujeres que inician su carrera en el sector tecnológico o bien para candidatas con especial potencial para puestos directivos".



**Adela de Toledo**  
country manager de Pure Storage Iberia

"Son necesarias políticas de conciliación efectivas que faciliten el equilibrio entre la vida laboral y la personal"

Adela de Toledo insiste en otro aspecto clave para que las jóvenes opten por el sector tecnológico para trabajar. "Son necesarias políticas de conciliación efectivas que faciliten el equilibrio entre la vida laboral y la personal permitiendo a las mujeres desarrollarse plenamente en sus carreras".

A pesar de que queda mucho por hacer y se necesita continuar impulsando la participación de la mujer en el sector con una combinación de medidas, en algunos ámbitos las profesionales están muy bien valoradas. Este es el caso de la ciberseguridad. García-Mascaraque comenta que en este sector "las habilidades femeninas son muy valoradas por nuestra capacidad de resiliencia, empatía y cuidado".

### Experiencia personal

En los últimos años el avance de la mujer en los puestos de liderazgo en el sector ha sido significativo, pasando la presencia de mujeres del 5 % en el año 2000 al 19 % en la actualidad. Este salto no ha estado exento de escollos y dificultades que superar. La experiencia personal de las ejecutivas lo demuestra. Ángeles Delgado señala que todos los desafíos que ha ido encontrando en su carrera los ha visto como oportunidades, como "momentos clave para aprender, evolucionar y reforzar mi capacidad de adaptación". Cada obstáculo ha sido un estímulo para crecer, lo que le ha ayudado a entender que el liderazgo "no se trata solo de alcanzar un puesto, sino influir, transformar y aportar valor".



**Ángeles Delgado**  
presidenta de Fujitsu en España

"Es fundamental impulsar la participación femenina en IA desde la educación hasta el ámbito profesional"

La fórmula de Anna Coll para superar las dificultades que se han ido presentando en su carrera profesional ha sido contar con una red de apoyo profesional tanto dentro como fuera de la empresa y apostar por "la formación continua y, sobre todo, no temer al cambio".

Para Adela de Toledo uno de los grandes retos que ha tenido que afrontar durante su carrera ha sido la superación de los prejuicios de género porque "el sector TIC sigue siendo mayoritariamente masculino", lo que supone que las mujeres tienen que demostrar constantemente su valía profesional. Su propuesta para superar esta barrera es mantener una red de apoyo y especializarse en áreas estratégicas para fortalecer las habilidades profesionales. Las dudas sobre la valía profesional por ser las TIC un campo masculino también han estado presentes en la trayectoria de Pilar Martín, quien señala que para superarlo es fundamental "confiar en una misma y demostrar tu experiencia con resultados tangibles", aunque también reconoce que la conciliación familiar es una tarea complicada que puede llevar a una sobrecarga de responsabilidades y estrés.

Para paliar esto subraya que "hay que pelear por políticas flexibles que ayuden a esta conciliación y, sobre todo, ponerse límites a una misma, priorizando tu bienestar".

Ramos cree que todavía hay barreras

"La equidad salarial no solo es una cuestión de justicia, sino también de competitividad y retención del talento"



**Anna Coll**  
B2B channel sales manager de Samsung España

invisibles, a pesar del avance de la mujer en puestos directivos, y cree que la falta de referentes es un desafío. "Cuando no ves mujeres en puestos de liderazgo, cuesta imaginarse ahí", recalca.

En este aspecto insiste Luisa Paolucci, quien considera que esta falta de representación femenina en roles de liderazgo puede "resultar desmotivador". Y al mismo tiempo, piensa que el síndrome del impostor sigue siendo un reto a superar con ayuda de colegas y confianza en uno mismo. "Es fundamental reconocer y desafiar estos pensamientos negativos, así como rodearse de mentores y colegas que confíen en nuestras capacidades".

María Herranz también apunta a los sesgos inconscientes junto a la falta de representación y la escasez de modelos a seguir como los principales retos que ha afrontado en su trayectoria. Una situación similar a la que menciona Marta González quien destaca que ha superado estos sesgos con "seguridad y confianza".

Carmen Muñoz también indica que la conciliación ha sido un reto durante su carrera por la dinámica del mercado y la sociedad y considera

que ante las nuevas generaciones las directivas tienen un papel decisivo para romper barreras. "Las mujeres en puestos directivos tenemos una misión primordial en promover este cambio; impulsando las medidas de conciliación, desarrollando políticas de RRHH focalizadas en la búsqueda de talento, en los



**Patricia Nuñez**

directora de la división de PCSD de **Lenovo** en Iberia

### "Es clave que haya mujeres entrenando la IA"

La juventud ha sido uno de los hándicaps que ha afrontado Patricia Nuñez en algunas ocasiones porque tenían una percepción preconcebida sobre ella, aunque ha logrado cambiar esa impresión con "la confianza en mi trabajo y los resultados obtenidos".

La directora general de HP en España y Portugal considera que a lo largo de su

trayectoria ha tenido que afrontar diversos retos similares a los de otras profesionales, pero contar con un equipo ha sido una de las claves para superarlos. "He confiado en mis mentores y he

planes de desarrollo de carrera, *mentoring* y *coaching* de líderes y, por supuesto, sirviendo de ejemplo para el resto de las mujeres de nuestras organizaciones", argumenta.

creído siempre en sacar lo mejor de cada uno de los desafíos que se han presentado", explica. En su opinión, "el liderazgo femenino en TIC seguirá creciendo si seguimos abriendo camino y demostrando que el talento no tiene género".

Una visión parecida tiene Elena García-Mascaque, quien indica que la adaptación al entorno absolutamente cambiante ha sido un reto durante su carrera, aunque cree que uno de los mayores está "en nosotras mismas: en creer en nuestras capacidades y romper con los sesgos que nos han condicionado". Para solventar este problema señala que hay que confiar en "nuestro talento, que dejemos a un lado la autoexigencia excesiva, que nos apoyemos en comunidades de mujeres para construir redes de apoyo y que no pongamos límites a nuestras aspiraciones". 📺

## Iniciativas



La mayoría de las grandes empresas tecnológicas tiene programas para fomentar la incorporación de las mujeres al sector e impulsar la carrera de sus profesionales. Las directivas consideran que estas iniciativas son necesarias para lograr la igualdad. Por ejemplo, Cisco ha puesto en marcha diferentes acciones y programas como una "universidad" interna para mejorar la capacitación de sus emplea-

dos y a través de la Cisco Networking Academy, una organización sin ánimo de lucro ya ha formado en competencias digitales a 350.000 alumnos, siendo 40.000 mujeres. También ha lanzado otros programas para desarrollar el talento femenino como el JUMP o Women Action Network, entre otros.

Samsung organiza un Innovation Campus para formar a los jóvenes, mientras que Salesforce tiene en marcha el proyecto "Women in Leadership" para el avance de la mujer hacia el liderazgo y la red de apoyo "Salesforce Women Network". HP también desarrolla varias iniciativas para favorecer a la mujer. Una de ellas es "STEM for Girls" en la que participan 40 voluntarias, la mayoría ingenieras, que acuden como referentes a diferentes eventos relacionados con la tecnología. Y WatchGuard a través de la comunidad Women of WatchGuard (WOW) potencia el desarrollo profesional y el *networking* entre las mujeres del sector.



# **Ciberseguridad: negocio sin límite**

## España avanza en ciberseguridad empresarial

Según el informe "El estado de la ciberseguridad en España" de Deloitte, aunque muchas organizaciones han actualizado sus modelos de gobernanza, persisten brechas en la preparación ante incidentes y en la integración de la seguridad con los objetivos del negocio. Frente a amenazas más sofisticadas y nuevas regulaciones, las empresas deben adaptarse rápidamente para fortalecer su resiliencia y protegerse de riesgos emergentes.

 Bárbara Madariaga

**L**a ciberseguridad ha dejado de ser un simple tema técnico para convertirse en un eje estratégico de las empresas. Esta es una de las conclusiones más destacadas de la sexta edición del informe "El estado de la ciberseguridad en España" de Deloitte, que refleja un avance en la implicación de la alta dirección en este ámbito. Sin embargo, el estudio también subraya importantes brechas en la comprensión, ejecución y preparación ante incidentes, lo que pone de manifiesto que aún queda un largo camino por recorrer para integrar la ciberseguridad de manera efectiva en las decisiones empresariales.

Una de las conclusiones más relevantes del informe es la situación de la gobernanza en las organizaciones españolas. Aunque el 59 % de las empresas ha actualizado sus modelos, un 28 % aún trabaja con estructuras poco definidas y un preocupante 13 % no tiene ninguna estructura de gobernanza en ciberseguridad. Además, tan solo el 42 % de las empresas ha establecido comités específicos para alinear la ciberseguridad con los objetivos del negocio, lo que muestra que la integración sigue siendo insuficiente. Deloitte señala que la ciberseguridad es una prioridad estratégica, pero que aún no se comprende completamente su impacto real en el negocio. Las nuevas normativas europeas, como NIS2 y DORA, están ejerciendo una presión creciente sobre los directivos, exigiendo una mayor rendición de cuentas. Sin embargo, un 26 % de los responsables de seguridad considera que sus directivos no son plenamente conscientes de su responsabilidad legal en caso de incidentes.

### La ciberseguridad en terceros y la IA

Otro de los puntos críticos que aborda el informe es la gestión de la ciberseguridad en terceros. Aunque el 71 % de los CISO considera a los proveedores como una de las mayores amenazas, solo el 29 % de las empresas se siente segura con respecto a sus proveedores críticos. Más de la mitad de las empresas tampoco utiliza herramientas específicas para gestionar estos riesgos, lo que pone de manifiesto una vulnerabilidad significativa en la cadena de suministro. Además, la inteligencia artificial, a pesar de su potencial para mejorar la protección, se está convirtiendo en un arma de doble filo. Según el informe, el 49 % de las empresas ya la aplica en sus procesos de ciberseguridad, pero más del 50 % no contempla medidas específicas para proteger estos

abordar los riesgos derivados de la IA.

La resiliencia operativa también sigue siendo una asignatura pendiente. Aunque el 84 % de los directivos identifica la continuidad del negocio como una prioridad, solo un 10 % de las empresas es capaz de estimar los costes reales de un ciberataque, y casi la mitad de las organizaciones no ha probado su plan de recuperación ante desastres. Este dato es especialmente preocupante en un contexto en el que los presupuestos destinados a la ciberseguridad continúan creciendo, pero las empresas aún carecen de una visión clara sobre el retorno de estas inversiones. De hecho, el 28 % de los CISO considera que la alta dirección no entiende cómo se estructuran ni cómo medir la efectividad de las inversiones en ciberseguridad. Además, un 40 % de las organizaciones desconoce cuánto tiempo tardarían en recuperarse tras una caída total de sus sistemas.

Uno de los mayores desafíos estructurales que enfrenta el sector de la ciberseguridad en España es la escasez de talento especializado. La creciente competencia internacional ha dificultado la atracción y retención de perfiles cualificados, lo que ha intensificado este problema en un 188 % con respecto al año anterior. Esta falta de profesionales afecta directamente a la capacidad de las empresas para gestionar amenazas y desarrollar estrategias

de seguridad sólidas. Deloitte concluye que, a pesar de los avances, las organizaciones españolas siguen enfrentando retos clave que requieren una mayor conciencia, inversión efectiva y una apuesta decidida por el talento. 



nuevos sistemas, lo que deja a las organizaciones expuestas a riesgos derivados de la implementación de tecnologías emergentes. Deloitte advierte que el enfoque tradicional de ciberseguridad "ya no es suficiente" para

# Lidera cloud

Powered by  V-Valley

## TU PLATAFORMA MSSP AUTOMÁTICA Y DESATENDIDA

La plataforma de gestión de servicios de suscripción MSSP, que ofrece la posibilidad de provisionar servicios de ciberseguridad de fabricantes mundialmente reconocidos, de manera automática y desatendida.



## ÚNETE A LAS VENTAJAS DE LIDERA CLOUD

 Modelo de suscripción

 Atención comercial

 Pago por uso

 Proceso de onboarding

 Mayor margen por volumen

 Servicio integral de soporte

 API de provisión

 Beneficios económicos

¿Quieres saber cómo integrar nuestras soluciones para acelerar tu negocio?  
¡Contacta con nuestros especialistas!

[www.v-valley.com](http://www.v-valley.com)

"Para combatir las amenazas contamos con talento, información y tecnología; lo que conforma una excelente combinación"



### Security Report Iberia

El pasado mes de marzo se anunciaban los resultados del

Security Report Iberia en el que Check Point Software detallaba el panorama de la ciberseguridad en España y en Portugal. A semejanza de lo que ocurre en el mundo, las amenazas también se incrementaron en ambos países. Según el fabricante, en los últimos seis meses en el territorio ibérico se registró un promedio de 1.919 ciberataques semanales por empresa, una cifra que es superior a la media mundial (1.845). Mario García señala al uso de la inteligencia artificial como el factor principal que explica este crecimiento general. "En Iberia, además, hay que recordar que, aunque muchos ataques utilizan el inglés, los atacantes aprovechan el peso que tienen el español, y también el portugués, para lanzar las amenazas". En cualquier caso, "con la inteligencia artificial, los ciberdelincuentes llevan a cabo sus ataques con un menor coste y en cualquier idioma".

Según el estudio, entre los ataques permanecen los clásicos, como es el caso del *ransomware* (España ocupó la octava posición a nivel mundial en esta amenaza) o del *phishing*, con correos electrónicos y suplantaciones de identidad. Con la IA como la tecnología que les hace más complejos y los automatiza a un coste cero. Mario García cree que, en su uso, los fabricantes van un paso por delante de los *hackers*. "Llevamos más tiempo usándola, con muchos medios y con muy buena información de los ataques: cuántos se producen, de qué tipo, cómo se llevan a cabo, con qué herramientas, etc. Una información que utilizamos después, aplicando la inteligencia artificial, para elaborar la defensa. Contar con una buena base de datos es esencial". Una tarea en la que el concurso del equipo humano se torna esencial. "Gracias a la expansión del teletrabajo, es



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

Tras un buen cierre en 2024, en el que la filial ibérica de Check Point Software creció por encima del ascenso de la corporación, en este 2025 el negocio sigue apuntando al crecimiento. El ecosistema de *partners*, como recuerda Mario García, director general de la oficina ibérica, sigue siendo pieza fundamental en un negocio que abarca cualquier tipo de empresa y de organismo público.

Marilés de Pedro

posible contar en cualquier país con los mejores especialistas, lo que nos permite atraer talento". En España disfrutaron del desempeño de varios profesionales que forman parte del departamento de I+D del fabricante. "Tenemos talento, información y tecnología; lo que conforma una excelente combinación".

### Buenos números

La filial ibérica cerró un excelente 2024 en el que su crecimiento fue entre tres y cuatro veces superior al que exhibió la corporación. "El equipo es la clave", señala. Este 2025 ha empezado de manera positiva. "Los ataques son, cada vez, mayores y tienen un componente glo-

bal, afectando a todo el mundo. Las empresas deberían ser conscientes de esta situación".

El pasado año el fabricante renovó su programa de canal y el pasado mes de marzo Ricardo de Ena se incorporó como nuevo responsable de la estrategia indirecta. García recuerda que el mercado presenta una enorme complejidad. "Nuestra cobertura abarca desde las grandes cuentas y los organismos del sector público, hasta las empresas medianas y pequeñas. Cada una de ellas exige una estrategia diferente. Nuestro propósito es la búsqueda de la mayor simplificación".

García señala al área de la mediana cuenta como un apartado de enorme crecimiento.

## Panorama de amenazas

El panorama de amenazas que pintó el Security Report Iberia observó algunos cambios de tendencia. Uno de ellos, el modelo de ataque: si en 2023 el 90 % utilizaba el *phishing*, en 2024 se ha incrementado el uso de los *info stealers* (un 58 % prefería esa vía) basados, por ejemplo, en la navegación web, en el robo de ficheros, la recogida de contraseñas, etc.

También se asistió a un cambio en el panorama del *ransomware*, con la caída de los dos grupos principales que se dedicaban a este tipo de extorsión (que llevaron a cabo, a pesar de todo, dos grandes ataques que lograron 75 y 22 millones de dólares, respectivamente). Se pintó un panel, más fragmentado, con grupos más pequeños, que realizaron menos ataques pero mucho más activos, prefiriendo, en lugar de técnicas de cifrado, la exfiltración o robo de datos. El *ransomware* como servicio siguió creciendo. EE.UU. se posicionó como el país más atacado, seguido de Canadá y el Reino Unido.

Los ataques provocados desde los estados (ciberguerras) siguieron creciendo con las naciones exhibiendo más recursos para desplegar sus amenazas. Cada país diseña estrategias particulares, haciendo uso del *hacktivismo* (*malware* destructivo) en los con-

flictos bélicos. Hasta en un tercio de los procesos electorales que se han celebrado en el mundo entre septiembre y diciembre de 2024, han existido campañas de desinformación para tratar de influir en la opinión pública a través, por ejemplo, de *deep fakes*, con China, Rusia e Irán como ejemplos de estas prácticas.

Las vulnerabilidades de los dispositivos *edge* y de IoT son otra vía de ataque, tanto para *botnets* como para estos actores estado. Atacar estos dispositivos es relativamente sencillo y Check Point recomienda una higiene cibersegura, cambiando siempre la configuración estándar que traen por defecto.

La nube sigue siendo un reto ya que este entorno cambia el paradigma de la computación, por lo que hay que conocer técnicas diferentes para su protección. El control de la administración está en manos de los programadores y, aunque está cambiando, no son especialistas en ciberseguridad. Su responsabilidad es que el sistema funcione, pero no se cuida, de igual modo, qué partes están expuestas a Internet y cuáles no.

Por último, se alertó de la brecha que abren las vulnerabilidades: el año pasado uno de cada 25 ataques las aprovechó, lo que pone de relieve lo importante que es el parcheo.

"Hay muchas empresas, con este tamaño, que están preocupadas por la ciberseguridad".

Para cubrir las necesidades de protección, la estrategia de Check Point Software está basada en una plataforma que ofrece una respuesta, unificada, capaz de cubrir todos los entornos. Una filosofía que alivia la escasez de talento y el conocimiento de los profesionales encargados de aplicar la tecnología. "No es posible que un ingeniero conozca, de manera profunda, todas las tecnologías; lo que complica la instalación y el mantenimiento de los sistemas de protección. Sin embargo, si solo tiene que aplicar una plataforma, la complejidad y el riesgo se minimizan", aporta como ventaja. "Ahora bien, una empresa no suele tener todos sus sistemas protegidos con un solo proveedor; pero, si en lugar de contar con una decena de fabricantes, apuesta por dos o tres, para el *partner* va a ser mucho más sencilla la instalación y el soporte".

### Normativas

La regulación europea trata de fortalecer los sistemas de protección. En la actualidad el protagonismo corresponde a DORA y a NIS2. Mario García, en el caso de la primera, cree

"En el uso de la IA, los fabricantes vamos un paso por delante de los *hackers*"

que las entidades financieras tienen muy bien trabajado, en general, el área de la ciberseguridad. "Todo es mejorable, por supuesto, y siempre habrá una evolución, pero es un segmento

que cuenta con una enorme regulación".

En relación a la Directiva NIS2, que aún no cuenta con su transposición en España, García cree que es una normativa muy válida para que las empresas analicen dónde tienen los problemas de ciberseguridad y si cumplen con niveles de protección suficientes. "Y, si no lo están, tomar las decisiones adecuadas para protegerse". Una directiva que cree que va a poner la máxima atención en la cadena de suministro de las empresas. "Va a ser el área crítica".

Acceda al vídeo desde el siguiente código QR



<https://newsbook.es/actualidad/ciberseguridad-ataques-20250504116673.htm>

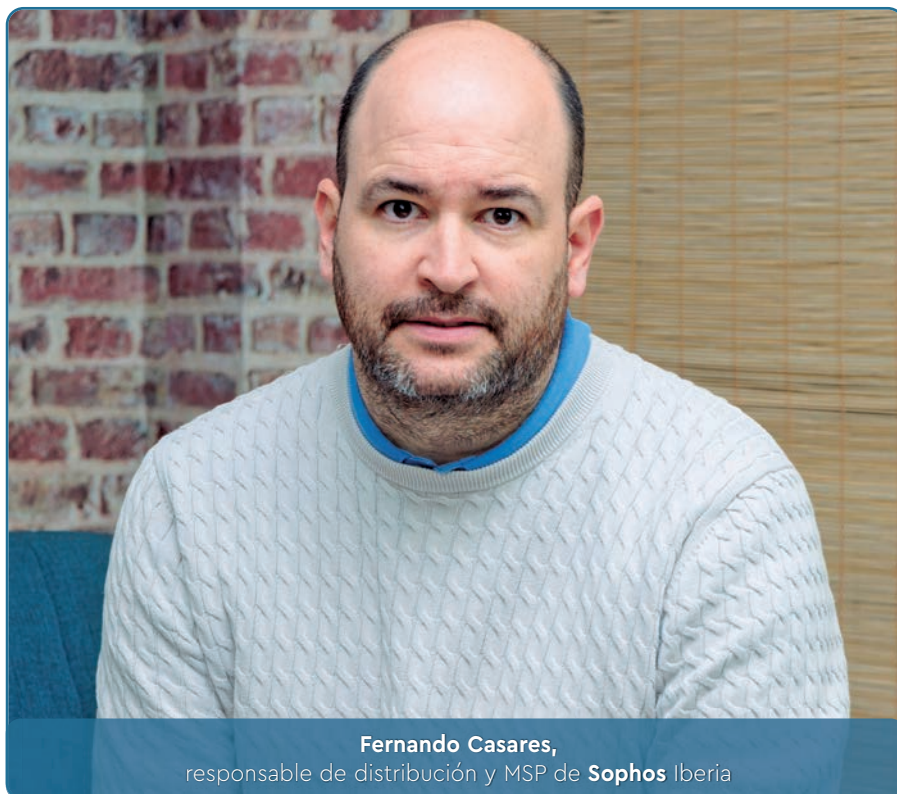


Casi 30.000 empresas disfrutan del servicio MDR de Sophos

"Una empresa de 10 usuarios, por menos de lo que cuesta un teléfono móvil, puede contar con un completo servicio de ciberseguridad"

Objetivos de negocio cumplidos por Sophos en su último año fiscal concluido el pasado 31 de marzo. Un ejercicio en el que la compra de Ajoomal por parte de TD Synnex introdujo novedades en su canal mayorista que se han saldado manteniendo los buenos números en su facturación. "El canal genera el 100 % de nuestro negocio. Sin el ecosistema de *partners* no es posible el negocio", recuerda Fernando Casares, responsable de distribución y MSP de Sophos Iberia. Un negocio en el que el modelo de servicios gestionados de detección y respuesta (MDR), accesible para todo tipo de empresas, es foco estratégico.

 Marilés de Pedro



Fernando Casares,  
responsable de distribución y MSP de Sophos Iberia

**L**a red de distribuidores de Sophos reúne a cerca de 1.500 socios, con alrededor de 800 activos cada año, repartidos en las distintas categorías (Autorizado, Silver, Gold y Platinum). Casares explica que la mejor oportunidad para este ecosistema es que ponga su foco en el cliente. "Deben ser *partners* capaces de proteger, de manera completa, a sus clientes. La confianza de la empresa es la clave para hacer crecer el negocio del ecosistema". Casares reconoce que la amplia cobertura de negocio de Sophos, que cuenta con una oferta que da respuesta desde la pequeña empresa a las grandes compañías, exige una red de distribución mayor. "El reto es cubrirlo todo".

Una red a la que el año pasado se le presentó Partner Care, como un único punto de contacto para que los *partners* puedan resolver cualquier duda y recibir asistencia operativa 24 horas del día, los 7 días de la semana. A través de este servicio, Sophos ayuda a sus *partners*

"El ecosistema debe poner su foco en el cliente"

a resolver cualquier cuestión no relacionada con las ventas con el fin de agilizar sus tareas administrativas y operativas para que puedan centrarse en vender y atender a sus clientes.

Es un soporte para realizar presupuestos, navegar por el portal de *partners*, resolver dudas sobre licencias o realizar solicitudes de no reventa (NFR). "Es un punto de referencia para que los *partners* mejoren su comunicación directa con la compañía y que puedan solucionar cualquier incidencia", explica Casares. Este año Sophos va a incorporar un servicio de renovaciones para que los *partners*, de forma directa, puedan contratar con el fabricante, lo que les permitirá una mayor agilidad para preparar sus propuestas a sus clientes.

El pasado año la compra de Ajoomal, mayorista de Sophos, por parte de TD Synnex supuso una novedad en el grupo de grandes distribuidores encargados de comercializar las solucio-

# EDR detecta. XDR conecta. MDR protege.

Las ciberamenazas están evolucionando.  
¿Y tu?

La prevención es importante pero la detección es clave. Una detección es efectiva cuando cuenta con el respaldo de un equipo experto.

[sophos.com](https://sophos.com)

**SOPHOS**  
Defeat Cyberattacks

© Copyright 2025, Sophos Ltd. Todos los derechos reservados. Registrado en Inglaterra y Gales No. 2096520, The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, UK. Sophos es una marca registrada de Sophos Ltd.

“Está claro que la venta de un producto no es suficiente”



nes de Sophos, del que también forman parte ALSO e Ingram Micro. “Supone una operación que nos concede un enorme beneficio por el potente perfil de TD Synnex”, valora. Para Sophos, reconoce, ha sido un cambio muy sencillo. “TD Synnex ha incorporado a su plantilla a todo el personal que trabajaba en el ecosistema de Sophos en Ajoomal”.

## Modelos MDR

Uno de los ejes estratégicos de Sophos es su propuesta de ciberseguridad como servicio, basada en el modelo MDR. En 2024, a nivel mundial, la base de clientes se incrementó en un 37 % y en la actualidad el número de empresas que han

apostado por este servicio roza las 30.000. Casares valora de manera muy positiva la adopción de este modelo por parte de los *partners* y de las empresas españolas. “Está claro que la venta de un producto no es suficiente. Es muy importante que el ecosistema de *partners* incorpore el servicio a su oferta. Se trata de un modelo completamente diferenciador”, explica. Un servicio que sirve especialmente a las empresas más pequeñas. “La labor del *partner* es esencial para hacer que las pymes sean capaces de entender que, por un coste no muy elevado, puedan disfrutar de un servicio 24/7 de ciberse-

guridad”. Casares apela a una democratización de un modelo que antes solo se planteaban las grandes corporaciones. “Una empresa de 10 usuarios, por menos de lo que cuesta un teléfono móvil, puede contar con un completo servicio de ciberseguridad”.

Un modelo que, entre otros beneficios, rebaja los incidentes. Un reciente estudio de Sophos revela que el importe medio de las indemnizaciones reclamadas por las empresas que utilizan servicios gestionados de detección y respuesta (MDR) es un 97,5 % inferior con respecto a aquellas que utilizan soluciones para *endpoints*. La media de las reclamaciones de los usuarios de servicios MDR es de 75.000 dólares frente a los 3 millones de dólares para aquellas empresas que solo utilizan seguridad para *endpoints*. En definitiva, cuando son víctimas de un ataque, los usuarios que solo utilizan soluciones para *endpoints* suelen reclamar 40 veces más que aquellos que utilizan servicios MDR. Las menores reclamaciones de los clientes de MDR se deben a la capacidad de estos servicios para detectar y bloquear rápidamente la actividad maliciosa, y repeler a los atacantes antes de que puedan causar daños graves. 

Acceda al vídeo desde el siguiente código QR



<https://newsbook.es/actualidad/servicios-mdr-20250504116667.htm>



## Amenazas y protección

A mediados del pasado mes de marzo, INCIBE ofrecía las cifras de ciberataques del año pasado en España: en 2024 los incidentes de ciberseguridad han aumentado un 15%. Las pérdidas económicas derivadas de estos ataques alcanzaron los 10.000 millones de euros a nivel global, duplicando las cifras del año anterior. Además, España ocupa el quinto lugar en el ranking mundial de incidentes de *ransomware*, con 58 grandes ataques registrados en solo seis meses, lo que supone un incremento del 38 %.

INCIBE señala que en el terreno de las empresas la suplantación de identidad ha sido la temática más relevante durante el pasado año por el duplicado de las páginas web de las empresas y la suplantación de sus redes sociales. En la segunda mitad de 2024 se detectó el incremento de las campañas de dirigidas a empresas y

otros organismos, el fraude BEC (*Business Email Compromise*).

Fernando Casares asegura que no es un panorama positivo, aunque recuerda que las exigentes normativas vigentes obligan a comunicar todos los ataques. “Ahora se conoce realmente lo que está pasando, lo que explica este incremento en los números”.

Las previsiones son que las empresas españolas sigan invirtiendo en sistemas y soluciones de ciberseguridad. Normativas como NIS2, recuerda, obligan, no solo a las empresas, también a toda la cadena de producción. “Cualquier empresa que quiera trabajar con las grandes compañías necesita estar cubierta y cumplir con ella”. DORA, normativa específica para el sector bancario, también va a empujar la inversión. “Las directrices europeas son importantes y estrictas; y para cumplirlas, se necesita una protección profesional”.

## La gestión e implementación efectiva de Zero Trust; un desafío para el canal

A medida que las organizaciones expanden su huella digital en entornos híbridos y multinube, la necesidad de adoptar una arquitectura de seguridad flexible que proteja los datos y las aplicaciones es cada vez mayor. Zero Trust ofrece el enfoque adecuado ya que permite gestionar el acceso a recursos en la nube de manera precisa y bajo estrictos controles, sin importar desde dónde se realice este.

**A**

este respecto, y aunque cada vez son más las empresas que deciden aprovechar y formarse sobre las ventajas y beneficios que Zero Trust proporciona, aún existe cierta disparidad entre el nivel de conciencia y de comprensión real.

Zero Trust protege contra las amenazas, mientras mejora la visibilidad, la eficiencia y el control de acceso en la red. Sin embargo, no se trata de una tecnología o herramienta aislada, sino de un modelo integral que requiere cambios en toda la arquitectura de seguridad y en la forma en la que se gestionan los accesos y permisos. Tampoco debe ser confundido con otras prácticas de ciberseguridad como la segmentación de red o la implementación de *firewalls* avanzados. Estos equívocos pueden llevar a una adopción incompleta o errónea bajo la suposición de que lo que se está adoptando es Zero Trust.

### Otros problemas a solventar

Si bien muchas organizaciones comprenden los principios generales de Zero Trust, como el acceso basado en el contexto y la autenticación continua, la transición hacia esta arquitectura de seguridad representa un reto significativo a nivel cultural. Al eliminarse la confianza implícita y establecerse políticas de ac-



ceso mucho más restrictivas y basadas en permisos mínimos, su ejecución involucra un cambio en cómo los empleados conciben la seguridad.

Otro problema tiene que ver con el alcance de su implementación. Algunas empresas que inician la adopción de Zero Trust no son plenamente conscientes de que no se trata de un plan puntual, sino de un proyecto continuo. Desplegar un modelo de Zero Trust implica una revisión exhaustiva de la arquitectura de red, la integración de herramientas avanzadas de autenticación y monitorización, y una gestión constante de permisos y accesos.

La dificultad para medir el Retorno de la Inversión (ROI) o la falta de capacitación es-

pecífica son otras importantes barreras. Sin un conocimiento profundo de los principios de Zero Trust, es difícil ejecutar y mantener una estrategia coherente y efectiva a este respecto.

### Un distribuidor de valor

Para ayudar a las empresas en su camino hacia la adopción de Zero Trust, el papel de un Distribuidor de Valor Añadido (VAD) es esencial para cualificar y formar al canal. Un VAD especializado en ciberseguridad que colabore con fabricantes líderes en soluciones alineadas con el modelo Zero Trust, será un gran aliado en la implementación eficaz y a medida de proyectos de Confianza

Cero en los clientes.

Exclusive Networks y su ecosistema de *partners* juegan un papel muy relevante en la difusión de Zero Trust en España. A través de programas de educación, demostraciones prácticas y consultoría estratégica, los proveedores han ayudado a las empresas a comprender cómo Zero Trust puede integrarse en sus entornos de manera efectiva. Esto ha sido clave en la adopción, ya que muchos líderes empresariales requieren asesoría para implementar Zero Trust de forma efectiva y aprovechar al máximo sus beneficios. 

**Javier Jurado,**  
director de desarrollo de negocio  
de Exclusive Networks Iberia

"Vender a precio no tiene futuro, vender valor sí; y la percepción del cliente varía muchísimo"

Con un excelente crecimiento del 19 % concluyó la oficina ibérica de Kaspersky su último año fiscal. Un buen balance que ha tenido su continuidad en el inicio de este 2025, en el que también ha exhibido crecimiento en su primer trimestre. Unos números de los que el ecosistema de *partners* es protagonista. José Antonio Morcillo, director de canal de la filial ibérica, señala el desarrollo de los servicios gestionados como el mejor camino de rentabilidad para este ecosistema. "Las perspectivas de negocio son buenas para este 2025 que cuenta con un pronóstico muy interesante", prevé.

 Marilés de Pedro



José Antonio Morcillo,  
director de canal de Kaspersky

**P**rograma de canal

El lanzamiento de Kaspersky Next, el pasado año, fue un punto de inflexión en la estrategia de la marca, primando la solución por encima del producto. "El canal ha percibido su valor", analiza. "Hemos tratado, desde el principio, de promover la migración, con diferentes bonificaciones, desde el producto clásico a esta nueva línea de soluciones. La respuesta ha sido muy positiva". El fabricante ya ha programado el fin de vida de algunos productos clásicos. "Si se trata de nuevo negocio hay ciertas soluciones que ya no se pueden ofrecer. Mantenemos solo las renovaciones aunque esto será durante un periodo limitado de tiempo". El programa de canal, Kaspersky United, acoge diferentes figuras y modelos de negocio. En el área de la "venta" (*Sell*) se ubican *resellers*, integradores de sistemas y VAR, repartidos en cuatro escalones (*Registered*, *Silver*, *Gold* y *Platinum*) mientras que el modelo "*Build*" está identificado con ISV, OEM y CSP. Los modelos de "*Deploy*" y de "*Managed*" completan el cuadro.

El ecosistema identificado como "*Deploy*" está conformado por 7 *partners* en Iberia. Cuentan con 6 especializaciones (Industria, EDR, Networking Security, Security Education, Cloud Workload Protection y Threat Intelligence). La región ibérica es la zona de Europa con un mayor número de *partners* Deploy. Morcillo no se plantea lograr ningún número concreto en esta categoría. "El reto es contar con lo que necesitamos: tener un *partner* Deploy en todas las especializaciones y conseguir una adecuada cobertura geográfica". Unos *partners* que cuentan con un *rebate* extra, que se abona de manera trimestral, por sus ventas vinculadas con su especialización.

### Servicios gestionados

El área de los servicios gestionados señala la mayor oportunidad para el canal. El pasado año este apartado creció un 46 % en el nego-

cio ibérico. Morcillo reconoce que no todo el ecosistema será capaz de ofrecer un servicio. "Contamos con *partners* muy pequeños, que atienden al mercado de la pequeña y mediana empresa, que no tienen la capacidad para desplegarlos". Sin embargo, su vocación es dirigir al ecosistema hacia un modelo de prestación de servicios; no a fórmulas de reventa mensualizada. "Hay que promover la transformación y que los *partners* vean el valor que aporta la prestación de servicios", insiste. "Vender a precio no tiene futuro, vender valor sí; y la percepción del cliente varía muchísimo. Si se vende a precio y aparece un *partner* con una oferta más barata, la operación se pierde. Por el contrario, si el *partner* aporta valor, a pesar

# Especial Seguridad en el canal

de que sea más caro, se mantiene la oportunidad. En este caso el cliente percibe lo que ofrece, no el precio".

En el área de los mayoristas de valor añadido, el fabricante ha mejorado el programa VAD, con una mayor sincronización con la iniciativa vinculada con los Deploy. Unas figuras a las que se las exige, entre otros requisitos, algunas certificaciones, un plan de negocio y un entorno demo. En la actualidad solo hay un mayorista, V-Valley, que cumple con este perfil en Iberia. Morcillo explica que la intención no es promover que todos cuenten con este perfil. "Cada uno de nuestros mayoristas cumple su misión. Conta-

o a los teléfonos inteligentes. "Las empresas creen que son entornos aislados, que no se pueden atacar, y no es así. Hay que evangelizar en este sentido".

"Hay que dirigir al ecosistema hacia un modelo de prestación de servicios; no a fórmulas de reventa mensualizada"

## La IA, la tecnología "de moda"

La IA es uno de los temas más en boga. Según un estudio de Kaspersky, de principios de este

inteligencia real: la que permite conocer lo que va a ocurrir".

## Panorama de amenazas

El pasado año, Kaspersky bloqueó un 26 % más de intentos de *phishing* en todo el mundo en comparación con 2023. España ocupa la tercera posición entre los países que reciben estos archivos maliciosos adjuntos. En el caso del *ransomware*, la principal amenaza, España ocupa, en el ranking de los países más atacados, el octavo lugar.

En relación al panorama de este 2025 Morcillo asegura que "no aparecen amenazas nuevas aunque sí son más sofisticadas". El *phishing* se mantiene como una de las principales. "Es una fácil forma de acceder". También el robo, la compra de credenciales y un *ransomware* cada vez más complejo. "Antes el ataque penetraba y tras un tiempo, se descifraban los datos o llevaba a cabo algún tipo de acción. Ahora, asistimos a alguna variación y, una vez que está dentro, no es pasivo, y afecta, por ejemplo, al *backup* o a todos los datos".

Morcillo alerta de la desprotección de los dispositivos móviles. "Es uno de los vectores más fáciles de atacar". Las empresas "siguen sin tomar conciencia de lo peligroso que es tener un móvil desprotegido". Antes, el software debía requerir convencer al usuario objetivo de que haga clic en un enlace o archivo comprometido para que se instale en su teléfono, tableta u ordenador. "Sin embargo, con un ataque de clic cero, el software puede instalarse en un dispositivo sin que la víctima tenga que hacer clic en ningún enlace. Este *malware* es mucho más peligroso".

Por último, recuerda lo fácil que les resulta a los *hackers* acceder a ciertas herramientas para generar ataques. "Están a su disposición a un precio razonable, con lo cual el número de ataques será mayor". 



mos, por ejemplo, con alguno, enfocado en el desarrollo del mercado de la pyme, que lleva a cabo un trabajo excelente".

Una de las áreas con más oportunidades para el canal es el segmento de la protección industrial; un negocio que el pasado año experimentó un crecimiento del 155 %. Buena muestra de esas excelentes perspectivas es que la especialidad en protección industrial es la que cuenta con más *partners* Deploy. "Tiene un enorme recorrido y para Kaspersky es una apuesta clara", asegura. Una protección industrial que especifica que no solo se refiere a los entornos industriales, sino también a entornos con dispositivos vulnerables, diferentes a los PC

año, el 83 % de los encuestados españoles prevé un aumento significativo en los ataques potenciados por IA en los próximos dos años. José Antonio Morcillo puntualiza que no se trata de una inteligencia autónoma. "Es cada vez más sofisticada y en la que Kaspersky lleva trabajando muchos años, con el *machine learning* como precursor". Una tecnología que permite automatizar un volumen mayor, tanto de ataques como de defensas. "Facilita muchísimo tanto unos como otros". Lo más importante de la IA, explica, es la inteligencia de amenazas. "Tener un conocimiento previo de lo que va a ocurrir permite armar la defensa. Esa es la

Acceda al vídeo desde el siguiente código QR



<https://newsbook.es/actualidad/servicios-gestionados-de-ciberseguridad-20250504116670.htm>



El área de servicios gestionados es una de las grandes apuestas de V-Valley para este año

## V-Valley aboga por la especialización para crecer en el mercado de la ciberseguridad

El panorama de la ciberseguridad en 2025 está marcado por un crecimiento constante en el gasto de las empresas, la adopción de tecnologías como la inteligencia artificial y la automatización, y una clara tendencia hacia los servicios gestionados. V-Valley está desempeñando un papel esencial en el apoyo a los integradores y *partners* para que puedan ofrecer soluciones especializadas y mantenerse competitivos en un mercado cada vez más exigente y en constante evolución.

✚ Bárbara Madariaga



David Gasca, responsable de operaciones de ciberseguridad, y Alberto López, consejero delegado de V-Valley

empresas de las crecientes amenazas. David Gasca, responsable de operaciones de ciberseguridad en la compañía, explica cómo las grandes empresas están consolidando su gasto en ciberseguridad. "Estamos viendo que cada vez más la ciberseguridad está en el foco principal del gasto de las grandes empresas. Esto está llevando a una mayor visibilidad del mercado, lo que también está impulsando a las medianas empresas a invertir en áreas que antes no protegían".

### El impacto de las ciberamenazas

Entre las principales amenazas que están afectando a las empresas, el *ransomware* sigue siendo una de las más devastadoras. En 2024, España ocupó el octavo puesto en el ranking mundial de países más atacados por este tipo de *malware*. En este sentido, David Gasca explica que "estamos viendo que cada vez hay más ataques al *endpoint*. Cada día se generan 500.000 nuevas amenazas".

Para hacer frente a esta ola de ataques, la inteligencia artificial se ha convertido en un aliado imprescindible, ya que las soluciones basadas en IA permiten detectar y mitigar amenazas con una efica-

cacia mucho mayor que los sistemas tradicionales. "La inteligencia artificial es lo que va a venir. Los atacantes también están utilizando inteligencia artificial. La optimización de los procesos para detectar y remediar los ataques de manera automática es lo que necesitamos", afirma David Gasca.

**E**l mercado de la ciberseguridad sigue siendo uno de los sectores con mayor crecimiento. Con un incremento previsto del 8 % en el gasto para 2025 en España, según datos de IDC, las empresas, cada vez más conscientes de los riesgos digitales, están destinando una parte considerable de su presupuesto a reforzar sus defensas contra las ciberamenazas. Este aumento en la inversión refleja un cambio significativo en las prioridades empre-

sariales, donde la ciberseguridad se ha convertido en un área crítica.

En este contexto, V-Valley se posiciona como un actor clave en la distribución y gestión de soluciones tecnológicas que ayudan a proteger a las

"La especialización en una tecnología concreta es lo que garantizará el éxito.

Cuanto más estés metido en una tecnología, más valor aportarás como *partner*"

# Especial Seguridad en el canal

Sin embargo, tal y como explica el directivo de V-Valley, la innovación en ciberseguridad no se limita únicamente a la inteligencia artificial, sino que también se amplía a otros campos como la orquestación de soluciones y la ciberinteligencia. "La inteligencia artificial en ciberseguridad está orientada a la automatización de procesos, pero

también estamos viendo una mayor interconexión entre las soluciones, lo que nos permite tener un enfoque más proactivo".

Además, la capacidad de obtener visibilidad sobre lo que ocurre en otras partes del mundo es fundamental para anticipar los ataques. "La ciberinteligencia es esencial para ir un paso por delante de los atacantes".

## V-Valley y su apuesta por la ciberseguridad

El crecimiento de V-Valley en el sector ha sido constante. Alberto López, consejero delegado de la compañía, señala que 2024 cerró de manera excelente y el comienzo de 2025 ha seguido la misma tendencia positiva. "Terminamos el año pasado muy bien, con un comienzo de 2025 muy potente. Hemos seguido creciendo en la cuota de mercado de los fabricantes que representamos", explica Alberto López, quien destaca que V-Valley ha organizado su cuarto evento de ciberseguridad, el V-Valley Cybersecurity Summit, reuniendo a más de 180 clientes y más de 30 fabricantes en La Granja (Segovia).

Alberto López también recuerda que las inversiones en ciberseguridad no solo provienen de grandes empresas, sino que las medianas también están cada vez más comprometidas con la protección de sus sistemas. "Es un principio positivo, a pesar de la situación política mundial. Las empresas están invirtiendo más debido a las crecientes amenazas, que ahora son más diversas que nunca".

## La especialización como clave del éxito

A medida que el mercado de la ciberseguridad se diversifica, tanto los integradores como los mayoristas deben encontrar un equilibrio entre



la ampliación de su oferta y la especialización. Alberto López señala que en V-Valley han logrado mantener este equilibrio entre la expansión de su cartera de productos (ya trabajan con más de 40 fabricantes) y el desarrollo de cada marca, lo que les permite proporcionar soluciones altamente especializadas. "Al final, no firmamos con una compañía solo para aumentar nuestra facturación. Siempre buscamos que el nuevo fabricante encaje bien en nuestra oferta y aporte algo único". Esta estrategia les ha permitido seguir creciendo, especialmente en servicios profesionales, una de las áreas más demandadas en el sector. David Gasca añade que, además de continuar ampliando su portafolio, "la parte de servicios profesionales es esencial para complementar las soluciones que ofrecemos a nuestros clientes". A medida que las empresas abordan proyectos más complejos, contar con expertos en la materia se convierte en una ventaja competitiva crucial.

En este sentido, el área de servicios gestionados es una de las grandes apuestas de V-Valley para este año. Alberto López destaca que la compra de Lidera ha sido un paso estratégico fundamental para ofrecer un apoyo más sólido a los *partners* que aún no están preparados para brindar estos servicios de manera autónoma. "El negocio de los servicios gestionados es fundamental para nuestro crecimiento. Cada vez más, las empresas optan por modelos de servicio en lugar de adquirir productos físicos".

## Evolución del ecosistema de *partners*

Alberto López resalta la transformación del ecosistema de *partners*, donde los fabricantes han ganado protagonismo en España, estableciendo equipos de preventas y comerciales.

Esto ha modificado el papel del integrador, que a menudo se ve desplazado en proyectos grandes donde el cliente final tiene un contacto directo con el fabricante. Sin embargo, los integradores siguen necesitando el apoyo cercano del mayorista, como el que ofrece V-Valley, que ha reforzado su relación no solo con el cliente *enterprise*, sino también con el mercado más comercial, mediano y SMB. "Eventos como el Cybersecurity Summit o el Tech Summit en Ávila estrechan la relación con nuestros clientes, presentándoles a más miembros del equipo y conectándoles más directamente con nuestros fabricantes. Al final, esto ayuda a que nuestros *partners* se sientan más cómodos ofreciendo más tecnologías".

En cuanto al futuro del canal de distribución, Alberto López comenta que "cada vez es más importante especializarse en algo concreto. En ciberseguridad, el canal debe centrarse en una tecnología o un área específica donde pueda ser el mejor, y luego asociarse con otros para complementar su oferta".

David Gasca reafirma esta postura, señalando que la especialización será la clave para que los *partners* sigan creciendo en un mercado cada vez más competitivo. "La especialización en una tecnología concreta es lo que garantizará el éxito. Cuanto más estés metido en una tecnología, más valor aportarás como *partner*".

El canal de distribución tiene ante sí grandes oportunidades para expandir su oferta, siempre que se enfoque en la especialización y la adopción de nuevas soluciones innovadoras. "Poner foco en una especialidad es lo que llevará al canal al éxito. Es imposible vender de todo, pero si te conviertes en el mejor en algo, el éxito está asegurado", finaliza Alberto López. 

El canal de distribución tiene ante sí grandes oportunidades para expandir su oferta, siempre que se enfoque en la especialización y la adopción de nuevas soluciones innovadoras.

"Poner foco en una especialidad es lo que llevará al canal al éxito. Es imposible vender de todo, pero si te conviertes en el mejor en algo, el éxito está asegurado", finaliza Alberto López. 

Acceda al vídeo desde el siguiente código QR



<https://newsbook.es/actualidad/videos/especial-seguridad-canal-v-valley-20250505116637.htm>



## Del riesgo a la resiliencia

En el panorama actual de ciberseguridad, las amenazas no se limitan a intentos aislados de intrusión; son campañas sofisticadas, adaptativas y persistentes. Frente a este desafío, la seguridad ya no puede ser reactiva ni fragmentada. Requiere una estrategia integral que combine inteligencia, operación y colaboración. En este contexto, los Proveedores de Servicios de Seguridad Gestionada (MSSP) juegan un papel esencial, y en Kaspersky entendemos que su éxito está intrínsecamente ligado a una asociación sólida y estratégica.



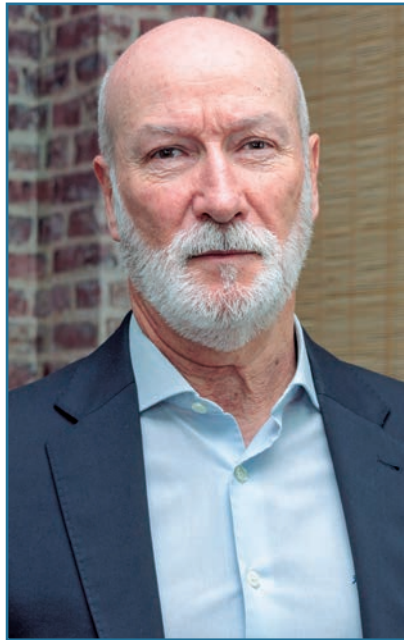
Los datos hablan por sí solos ya que según el último informe de análisis de Kaspersky Managed Detection and Response (MDR), se han detectado amenazas persistentes avanzadas (APT) en el 25 % de las empresas, un 74 % más en comparación con 2023. No pensemos que en España estamos libres ya que nos encontramos entre los países europeos con mayor cobertura del servicio de MDR (15 %).

Contar con información sobre amenazas es fundamental, pero lo que realmente marca la diferencia es cómo se interpreta y se aplica esa información. Tener visibilidad sobre amenazas emergentes ya no es una ventaja, es una condición mínima. Lo verdaderamente diferenciador es saber qué hacer con esa información.

En el contexto actual, caracterizado por un entorno digital en constante evolución y amenazas cada vez más sofisticadas, implementar, mantener y gestionar un modelo avanzado de ciberseguridad se ha convertido en una tarea compleja, costosa y, en muchos casos, fuera del alcance de las capacidades internas de muchas organizaciones.

### Inteligencia de amenazas y delegar con control, la combinación perfecta

La creciente presión regulatoria, la necesidad de proteger datos sensibles y la proliferación de ataques dirigidos obligan a las



empresas a replantear su estrategia de defensa. En este escenario, apoyarse en socios estratégicos como los proveedores de servicios de seguridad gestionada deja de ser una opción para convertirse en una necesidad para muchas empresas.

Colaborar con un MSSP permite a las empresas acceder a modelos de ciberseguridad más flexibles, escalables y adaptados a sus necesidades particulares. Desde soluciones de inteligencia de amenazas hasta Centros de Operaciones de Seguridad (SOC), los MSSP ofrecen capacidades especializadas que muchas veces no son viables de desarrollar internamente, especialmente para organizaciones que no cuentan con grandes equipos de seguridad o presupuestos extensos.

En este sentido, los MSSP dejan de ser simples proveedores de servicios para consolidarse como verdaderos aliados estratégicos en la ciberdefensa. En Kaspersky valoramos profundamente estas colaboraciones y nos comprometemos a fortalecerlas con soporte técnico especializado, formación continua y acceso a nuestras soluciones más avanzadas. Sabemos que solo a través de una relación sólida y bidireccional es posible enfrentar los retos actuales de ciberseguridad, desde el cumplimiento normativo hasta la protección frente a amenazas persistentes avanzadas.

La ciberseguridad moderna requiere un enfoque integral, donde inteligencia, tecnología, personas y procesos se alineen para construir una defensa resiliente y adaptable. En Kaspersky creemos firmemente que la colaboración con MSSP es clave para alcanzar ese objetivo. Juntos, transformamos los desafíos en oportunidades, respondemos con eficacia a los incidentes y ayudamos a garantizar la continuidad del negocio en un entorno digital cada vez más complejo.

Esta visión compartida es la que nos permite avanzar hacia un ecosistema más seguro, donde la prevención y la reacción convivan en equilibrio, asegurando no solo la protección del presente, sino también la preparación para el futuro. 

**José Antonio Morcillo**  
director de canal en Kaspersky Iberia

The Industry's Best  
Prevention Rate:

99.9%

***Miercom***

Miercom Enterprise and Hybrid Mesh  
Firewall Benchmark 2025

AI-Driven Threat Prevention.  
That's **Security in Action.**

[checkpoint.com/action](https://checkpoint.com/action)



# De la táctica a la estrategia: por qué la ciberseguridad debe tener un papel relevante en el consejo de administración

En el pasado, la seguridad de la información en las organizaciones se administraba desde los departamentos de tecnología, sin incluirse en las conversaciones estratégicas de los consejos de dirección. Sin embargo, este enfoque ha cambiado radicalmente.

**E**n el actual contexto geopolítico y con el avance acelerado de la digitalización, las empresas se enfrentan a una exposición a riesgos cada vez más sofisticados y globales. Hoy en día, cualquier compañía (independientemente de su tamaño o sector) está sujeta a consecuencias que van más allá del ámbito técnico: los ciberataques pueden generar impactos reputacionales, legales, económicos e incluso amenazar su propia supervivencia.



## Una obligación normativa que impulsa el cambio

La Directiva NIS2 marca un antes y un después en la gestión de la ciberseguridad corporativa. Por primera vez, los consejos de administración y la alta dirección serán responsables de garantizar la seguridad digital. Este mandato no trata solo de evitar sanciones económicas significativas (que pueden alcanzar hasta el 2 % de la facturación global o hasta 10 millones de euros), sino también fomentar un papel activo en la gestión del ciberriesgo.

La directiva exige que los consejeros estén informados, capacitados y participen activamente en la toma de decisiones en materia de seguridad. Este cambio normativo refuerza la tendencia observada en informes recientes. Por ejemplo, el Instituto Nacional de Ciberseguridad (INCIBE) reportó más de 96.000 incidentes en España en 2024, lo que

“La ciberseguridad ya no es únicamente un asunto técnico, es una cuestión decisiva que requiere liderazgo”

representa un incremento del 15 % en comparación al año anterior.

## Seguridad como ventaja competitiva: ¿está preparado su consejo?

Las compañías más resilientes han entendido que la ciberseguridad no es un costo, sino una inversión. Están incorporando la seguridad en el diseño de sus procesos, productos y servicios. También están formando a sus directivos, revisando sus planes de continuidad y, muy especialmente, están incorporando perfiles expertos en seguridad de la información en sus órganos de gobierno.

Un consejo de administración que lidere la es-

trategia de seguridad proyecta robustez, confianza y transparencia frente inversores, clientes y socios. Los interrogantes que deberían plantearse incluyen:

- ¿Existe una estrategia de seguridad alineada con los objetivos de negocio?
- ¿Se han protegido los activos y procesos críticos de la organización?
- ¿Dispone el consejo de información acerca de los riesgos actuales y emergentes?
- ¿Reciben los consejeros formación para entender el contexto de amenazas?
- ¿Cómo se mide y reporta la efectividad de

las políticas de ciberseguridad al consejo?

Si todavía no se han tenido en cuenta algunos de estos factores, es momento de me-

ditar: la ciberseguridad ya no es únicamente un asunto técnico, es una cuestión decisiva que requiere liderazgo.

En conclusión, la ciberseguridad se ha transformado en un componente fundamental de la estrategia corporativa. Evolucionar lo táctico a estratégico significa ir más allá de la protección de sistemas: implica construir confianza, prestigio y resiliencia.

Contar con una estrategia de negocio se da por sentado. ¿Por qué no ocurre lo mismo con la de seguridad? La verdadera pregunta es: ¿está su consejo preparado para transformar la seguridad en una ventaja competitiva? 

Ana Sáez

Security strategy expert

# La sostenibilidad, ¿en el centro del negocio?



# La sostenibilidad como clave para el futuro

Las empresas españolas están reconociendo cada vez más la importancia de integrar la sostenibilidad en su modelo de negocio, no solo como una obligación normativa, sino como una herramienta clave para mejorar su competitividad y fortalecer su reputación. Sin embargo, los desafíos normativos y la falta de recursos siguen siendo obstáculos importantes para muchas de ellas.

➡ Bárbara Madariaga

**E**n un mundo cada vez más centrado en la sostenibilidad, las empresas están reconociendo la importancia de adoptar prácticas responsables con el medio ambiente, no solo como un cumplimiento normativo, sino como una oportunidad para mejorar su competitividad, fortalecer su reputación y alcanzar sus objetivos comerciales. Así lo destaca en un informe Grant Thornton, que asegura que las compañías están apostando por áreas que abarcan desde las energías renovables hasta la digitalización, pasando por la gestión de residuos y la reducción de emisiones.

Uno de los principales motivos que mueve a las empresas a invertir en sostenibilidad es el impacto positivo sobre su reputación de marca y su capacidad para ser más competitivas en un mercado cada vez más consciente del medio ambiente. Aproximadamente el 48 % de las empresas españolas tiene previsto invertir en energías renovables, una apuesta que supera la media de la Unión Europea (43 %) y la global (42 %). Este compromiso con las energías limpias responde a una necesidad urgente de reducir la huella de carbono y ser más responsables con los recursos naturales.

Pero la sostenibilidad no solo se trata de energías renovables. La digitalización para impulsar la eficiencia es otra de las áreas de inversión. Además, el desarrollo de productos sostenibles y la reducción de emisiones de carbono son prioridades para el 30 % de las empresas.

El estudio revela que la sostenibilidad no solo es vista como una inversión financiera, sino como una parte de la estrategia empresarial. Cuatro de cada 10 directivos españoles aseguran haber

puesto en marcha o tener previsto implementar una estrategia de sostenibilidad en los próximos 12 meses. Otros esfuerzos incluyen la elaboración de informes y memorias (32 %), la evaluación de criterios ESG (33 %) y el cumplimiento de objetivos en materia de sostenibilidad (38 %). No obstante, aunque España está alineada con



## La adopción de criterios sostenibles se ve frenada por la falta de recursos humanos y tiempo

la media europea, el informe destaca que las empresas españolas aún se encuentran por debajo del compromiso global en sostenibilidad. Mientras que, a nivel mundial, más de la mitad de las empresas (51 %) ya cuenta con estrategias de sostenibilidad implantadas, en España esta cifra se reduce considerablemente.

### Obstáculos y retos normativos

¿Por qué no se invierte? Según el informe, dos de cada tres líderes de medianas empresas

(65 %) consideran que el cumplimiento de los criterios ESG constituye un obstáculo para el desarrollo de sus negocios y limita su expansión internacional.

La adopción de criterios sostenibles también se ve frenada por la falta de recursos humanos y tiempo, siendo este el principal temor del 44 % de los empresarios españoles. La velocidad de actualización de las normativas es otro desafío, con un 43 % de los directivos señalando que la rapidez con la que las instituciones modifican las reglas dificulta la planificación a largo plazo.

Las empresas españolas están navegando por un "tsunami normativo" cada vez más complejo, con nuevas regulaciones europeas que requieren una adaptación urgente. Entre las más relevantes se encuentra la Directiva de Información Corporativa sobre Sostenibilidad (CSRD), que obliga a las empresas a ampliar los informes de sostenibilidad y aumentar la transparencia con sus grupos de interés. Además, deben cumplir con el Reglamento de Taxonomía (UE) 2020/852, que exige a las empresas reportar actividades medioambientales elegibles, y con la nueva Directiva de Diligencia Debida

en Sostenibilidad, que entró en vigor en abril de 2024, imponiendo obligaciones para garantizar el respeto a los derechos humanos y al medio ambiente, con sanciones de hasta el 5 % del volumen de negocio en caso de incumplimiento. Aunque el proceso de adaptación no es fácil y presenta obstáculos, la sostenibilidad se está convirtiendo en una ventaja competitiva que no solo impacta en la imagen de las empresas, sino también en su rentabilidad y eficiencia operativa.

# Cambiamos el modo de vender tecnología

---

## SOLUCIONES alquiler, renting, financiación



Asesoramiento  
sin costes de  
gestión



Cualquier  
producto  
tecnológico puede  
ser financiable



Buscamos la  
solución que  
mejor se adapte  
a cada  
operación

**Contacta con nosotros**

[Serviciosfinancieros@esprinet.com](mailto:Serviciosfinancieros@esprinet.com)

# HP: liderando el camino hacia un futuro sostenible



**David Ortega,**  
responsable de asuntos gubernamentales  
y políticas públicas de HP

# H

P es una de las compañías más comprometidas con la sostenibilidad y así lo resalta David Ortega,

responsable de asuntos gubernamentales y políticas públicas de la firma, quien explica que la estrategia de HP se fundamenta en tres pilares: acción climática, equidad digital y derechos humanos. En relación con el primero, la compañía ha implementado medidas concretas para reducir su huella de carbono. "Nuestro objetivo es ser neutrales en 2040 y reducirla en un 50 % para 2030. Actualmente, con respecto a 2018, ya hemos reducido un 27 %". Además, HP se ha comprometido a utili-

zar únicamente energía 100 % renovable y a avanzar en la circularidad de sus productos, destacando la importancia de un modelo de negocio que sea tanto rentable como respetuoso con el medio ambiente.

## "HP Amplify Impact ha sido clave en la integración de la sostenibilidad en nuestra red de *partners*"

El segundo pilar de la estrategia de HP es la equidad digital, un aspecto fundamental para la compañía que busca cerrar la brecha digital global. David Ortega afirma que "el acceso a la tecnología es esencial para que nadie se quede atrás", subrayando que la digitalización debe ser inclusiva. Con este fin, HP ha desarrollado programas como HP Life, que proporciona formación a millones de per-

sonas en todo el mundo, y el Acelerador de Equidad Digital, que busca capacitar a 100 millones de personas para 2030. España es uno de los países prioritarios para este programa, como indica David Ortega. "Este año, España se beneficia directamente de esta ini-

ciativa, con programas de capacitación dirigidos a diversas comunidades".

El respeto por los derechos humanos es el tercer pilar en la estrategia de HP. Ortega subraya que la compañía trabaja activamente para asegurar que sus productos se fabriquen bajo los estándares laborales más rigurosos y con el más alto respeto por los derechos fundamentales. "El 67 % de los cargos directivos en España están ocupados por mujeres", resalta el directivo, lo que refleja el compromiso de HP con la diversidad y la inclusión en sus operaciones locales. Además, la compañía se enfoca en fomentar una cultura inclusiva, asegurando que las prácticas laborales sean éticas y responsables a lo largo de su cadena de suministro.

### Sostenibilidad y negocio

Para HP, la sostenibilidad no solo es una cuestión ética, sino también una palanca para el crecimiento del negocio. "Para nosotros está muy claro que sostenibilidad y negocio van de la mano", afirma David Ortega, quien asegura que el 60 % de las ventas de HP en 2023 estuvieron vinculadas a productos y servicios sostenibles. Esta sinergia entre sostenibilidad y rentabilidad es una de las claves de la

compañía. "La sostenibilidad es un motor de innovación que impulsa el desarrollo de nuevos materiales, productos y procesos, creando al mismo tiempo oportunidades comerciales que no solo benefician al planeta, sino que también fortalecen nuestra posición en el mercado".

Bárbara Madariaga



Además, esta apuesta por la sostenibilidad ha tenido un impacto directo en el talento. "Un 91 % de los empleados de HP está muy orgulloso de trabajar para una empresa que tiene unos compromisos tan firmes en materia de sostenibilidad". Este factor contribuye a la atracción y retención de talento, demostrando que los valores sostenibles son un elemento básico en la cultura corporativa de HP.

## Economía circular: HP Renew Solutions

En este contexto, HP ha lanzado recientemente en España su programa HP Renew Solutions, que forma parte de su estrategia de economía circular. Esta iniciativa permite a las empresas adquirir productos reacondicionados que han pasado por un riguroso proceso de reacondicionamiento certificado, garantizando la calidad y durabilidad de los equipos. Entre los modelos que la compañía ha incorporado al mercado español se encuentran los populares EliteBook 8040 G7 y los modelos EliteBook 8040 y 8050 G8. Estos dispositivos reacondicionados no solo son una alternativa más económica, sino también más sostenible, ya que su impacto ambiental es considerablemente menor al de los productos nuevos. "El reacondicionamiento de estos equipos reduce la huella de carbono en un 60 % en comparación con los productos

nuevos", subraya David Ortega, que también destaca el importante rol que esta estrategia juega en la lucha contra el cambio climático. Además de los beneficios medioambientales, HP también ofrece garantías adicionales para asegurar la satisfacción de los clientes. "Lo que buscamos es que el reacondicionado no sea solo una opción más barata, sino una opción que también esté alineada con las mejores prácticas en términos de rendimiento y fiabilidad". Todos los productos reacondicionados cuentan con una garantía de un año, con la posibilidad de extenderla hasta tres años, incluyendo soporte técnico *in situ*.

## La IA jugará un papel crucial en la evolución de la sostenibilidad en HP

### HP Amplify Impact: impulsando la sostenibilidad en el canal

Mención especial merece la estrategia de canal de HP en materia de sostenibilidad. Desde 2021, la compañía cuenta con el programa HP Amplify Impact, que busca que sus *partners* integren la sostenibilidad en sus negocios. David Ortega califica este programa de "muy exitoso", con más del 60 % de los socios globales participando activa-

mente. En España, más de 100 *partners* se han sumado al programa, superando las expectativas de la compañía.

"HP Amplify Impact ha sido clave en la integración de la sostenibilidad en nuestra red de *partners*, proporcionando formación, materiales de marketing y auditorías personalizadas para ayudarles a integrar la sostenibilidad en su estrategia", explica David Ortega. Este programa no solo beneficia a HP, sino que también contribuye al crecimiento de sus *partners*. Según los datos de la compañía, un 53 % de los *partners* en España han aumentado sus ventas y un 55 % ha ampliado su base de clientes gracias a su implicación en la sostenibilidad. "Esto es un negocio redondo, por no llamarlo circular, pero redondo", asegura Ortega, destacando que la sostenibilidad es una fuente directa de beneficios tanto para HP como para su red de venta indirecta.

### El futuro de la sostenibilidad en HP

Mirando hacia el futuro, David Ortega menciona que la IA jugará un papel crucial en la evolución de la sostenibilidad en HP. "La IA ha venido para quedarse", afirma el directivo de HP, quien destaca la capacidad de esta tecnología para transformar la forma en que la compañía gestiona sus procesos y productos. "La inteligencia artificial nos permitirá optimizar nuestras operaciones de forma más eficiente, reduciendo aún más nuestra huella de carbono y mejorando la sostenibilidad de nuestros productos y servicios", explica Ortega.

Además, HP espera que el programa HP Amplify Impact se expanda a más países en el futuro. "Nuestro objetivo es seguir ayudando a nuestros *partners* en todo el mundo a integrar la sostenibilidad en sus negocios, no solo a nivel de productos, sino también en sus procesos internos y operaciones diarias".

Acceda al vídeo desde el siguiente código QR



<https://newsbook.es/actualidad/videos/especial-sostenibilidad-hp-2025-20250430116641.htm>



En nuestro país la concienciación de todo el ecosistema de *partners* y clientes es prioritaria

## "Los mayoristas son los que están más concienciados a seguir el camino con Acer en el tema de la sostenibilidad"

Acer mantiene un fuerte compromiso con la conservación del planeta y la sostenibilidad. Una responsabilidad que ha recogido en su estrategia *Earthion*, que articula los pasos que sigue para contribuir a la conservación del planeta a través de la ejecución de prácticas sostenibles desde el diseño del producto hasta que llega al final de su vida útil. En este trabajo su red de socios juega un papel principal llevando al mercado su mensaje de conservación de la naturaleza y respeto al medio ambiente.

 Rosa Martín

**A**cer lleva varios años trabajando para contribuir a la protección medioambiental y a fomentar las prácticas sostenibles. Un esfuerzo que se ha intensificado desde hace cuatro años y que lidera la dirección mundial de la compañía, según explica Emilio Dumas, director de ventas de Acer Ibérica. Este compromiso con la sostenibilidad se plasma en la estrategia *Earthion*, una combinación de las palabras en inglés *Earth* y *Mission*, tierra y misión, que ejemplifica la vocación de la compañía por un mundo más sostenible. "La misión en la tierra de Acer es un compromiso absoluto con la sostenibilidad", recalca Dumas.

Este compromiso, que le supuso la distinción Platinum de la organización EcoVadis en 2022 por su actividad en este terreno, se traduce en una visión sostenible en toda su operativa, desde el diseño del producto y la fabricación hasta que llega a manos del usuario, sin olvidar todas las fases por las que pasa en la cadena de suministro, incluido su reciclaje al final de su vida útil.

Acer Ibérica, como indica Dumas, sigue las pautas que marca la central y trabaja para seguir con este modelo de producción sostenible en todas las fases de desarrollo, producción, logística y entrega al usuario. Además, sus oficinas centrales en España, ubicadas en la localidad barcelonesa de Gavá, están diseñadas con criterios de sostenibilidad, siguiendo las directrices de otras oficinas europeas. "En España la central la tenemos en Gavá y es una oficina 100 % sostenible y, además, contamos con paneles solares para disponer de energía limpia".



Emilio Dumas,  
director de ventas de Acer Ibérica

"La misión en la tierra de Acer es un compromiso absoluto con la sostenibilidad"



## Cero emisiones netas

Dentro de su estrategia de sostenibilidad, Acer se ha marcado un objetivo ambicioso que es alcanzar cero emisiones netas en 2050, una meta en la que está trabajando intensamente. El fabricante, según explica Dumas, forma parte de la iniciativa Science Based Targets Initiative (SBTI), de la que forma parte el Pacto Mundial de las Naciones Unidas, que ayuda a las empresas a conseguir sus objetivos de cero emisiones a través de distintas herramientas. "Tenemos la previsión de que en 2030 lleguemos al 50 % de emisiones hacia ese objetivo de que sean cero", detalla. Su intención es trabajar para que este porcentaje sea del 70 % en 2035 y alcanzar el de cero emisiones netas en 2050. "Estamos cumpliendo los objetivos", recalca el directivo.

## Productos ecológicos y economía circular

Acer está impulsando la fabricación sostenible introduciendo en sus productos materiales reciclados y nuevos componentes respetuosos con el medio ambiente. La gama Vero es el principal exponente de esta categoría de productos ecológicos, aunque desde el año pasado la gama Swift también ofrece características sostenibles. "Son dos gamas que queremos que estén en el top de la tecnología".

Los productos que integran estas gamas incluyen plástico reciclado post consumo en su chasis. Por ejemplo, el modelo Aspire Vero 16 ya cuenta con un 70 % de este tipo de plástico y la intención es que este porcentaje ascienda al máximo que se pueda incluir técnicamente. Y otro rasgo diferencial de este modelo es que incluye un material hecho con caparzones de ostra. "Cada vez hay más componentes limpios dentro de la producción de esta gama", recalca el directivo.

## Más datos

- La energía que utiliza es 100 % renovable.
- Ha reducido el consumo de energía un 45 % en los últimos ocho años.
- Ha fabricado 40 millones de ordenadores y monitores utilizando plástico reciclado post consumo de 2020 a 2023.
- Mantiene un acuerdo con Plastic Bank para la recogida de los desechos plásticos con el fin de evitar que acaben en el océano.
- Está considerada como una de las empresas tecnológicas más sostenibles del mundo.
- Forma parte del índice Dow Jones Sustainability (DSI) desde 2024.

Al mismo tiempo que incorpora nuevos materiales y prácticas sostenibles en la fabricación, está trabajando para cumplir la normativa europea que fomenta la comercialización de equipos reacondicionados. Dumas señala que, a pesar que en otros países esta actividad está más desarrollada, a través de su servicio técnico ubicado en las oficinas centrales en España está preparado para reacondicionar equipos para lanzarlos a la venta.

Acer también está trabajando en el reciclaje eficiente de los productos al final de su vida útil para cumplir con la normativa y seguir contribuyendo a reducir los residuos electrónicos. Dumas aporta un dato significativo: el 22 % de las emisiones residuales electrónicas están recicladas, frente al 0 % de años anteriores, lo que demuestra el compromiso y el trabajo hecho en pos de la sostenibilidad.

## Alianzas y acciones

Para desarrollar su estrategia cuenta con una red de aliados que le ayudan a conseguir sus metas de sostenibilidad y transmitir a los usuarios finales los beneficios de sus productos ecológicos. En esta red de socios destacan las figuras de sus mayoristas, sobre todo los paneuropeos, porque "son los que están más concienciados

para seguir el camino con Acer en todo este tema de sostenibilidad", destaca Dumas.

La compañía tiene un programa de incentivos para que sus *partners* puedan alinear sus estrategias con las de Acer en lo relativo a la sostenibilidad. Y, además, los distribuidores que forman parte de su programa de canal profesional están adoptando esta visión. "Más del 50 % de los *resellers* que tenemos están en sintonía con el programa de sostenibilidad de Acer".

La colaboración con sus socios forma parte de las acciones que Acer Ibérica está poniendo en marcha para impulsar las buenas prácticas en materia de sostenibilidad, una actividad que comienza con la concienciación interna. "Tenemos una serie de *trainings* constantes dentro de la empresa para que todos sepamos qué es lo que hay a hacer y qué es lo que queremos transmitir", señala el responsable de ventas de Acer Ibérica.

La concienciación a sus clientes es otra de las acciones que está ejecutando para que sepan los esfuerzos que está realizando para ser más eficientes en materia energética y reducir la huella de carbono. "Si somos capaces de evangelizar no solamente a nuestros empleados, sino a todo nuestro entorno, de que este es el camino correcto y que las pautas que seguimos son las adecuadas, pensamos que esto va a ser beneficioso para nosotros, nuestros clientes y para todo el planeta", insiste Dumas. 



Acceda al vídeo desde el siguiente código QR



<https://newsbook.es/actualidad/videos/entrevista-acer-sostenibilidad-20250429116633.htm>



# "La sostenibilidad está en el ADN de los centros de datos"

La sostenibilidad sigue calando en el sector tecnológico. Muestra de ello es la reflexión de Miguel del Moral, director de canal de España, Portugal y Francia de Vertiv, que cree que resulta obsoleto asegurar que aquella empresa que no se suba en el barco de la sostenibilidad se quedará fuera del mercado. Ya parece estar claro: "La sostenibilidad debe estar en el centro de la estrategia de negocio de nuestros *partners*". Un camino que el ecosistema puede recorrer con Vertiv. "Nos sentimos protagonistas en el mercado de la sostenibilidad y de la eficiencia energética. Nuestros productos, ya sean de alimentación eléctrica, de refrigeración o de gestión de la infraestructura, ofrecen mejoras en el consumo energético, con un menor gasto de agua, y permiten ocupar un menor espacio a la tecnología".

Marilés de Pedro

**C**uestión de todos

En un estudio de Accenture de finales de 2022, realizado a 2.000 grandes empresas públicas y privadas de todo el mundo, se reflejaba el incremento del compromiso de las empresas con la eficiencia: el 83 % de las empresas españolas consultadas tenía como objetivo cero emisiones netas, un 33 % más que en 2021. "El quid de la cuestión es que la sostenibilidad es tarea de todos", resume del Moral. "Se trata de un objetivo que alcanza a la sociedad civil, a la empresa privada y a la Administración pública; son los tres ejes, activos, que se articulan para conseguir los retos que presenta la sostenibilidad".

Una ola de concienciación que empezó en las grandes compañías y "que está arrastrando a todas". La necesidad de que todos los colectivos se impliquen en este reto es el punto clave. "Primero, la concienciación; y, luego, la actuación y el compromiso de todas las empresas". El gran reto que tiene España es "amoldar la economía a los retos que plantea la sostenibilidad. Ese es el quid de la cuestión".

### Centro de datos

Un sector que está realmente comprometido con la sostenibilidad es el de los centros de datos. Hace un par de años Vertiv lanzó una guía para ayudar a este sector, el cual de-



Miguel del Moral,  
director de canal de España, Portugal y Francia de Vertiv

"El gran reto que tiene España es amoldar la economía a los retos que plantea la sostenibilidad"

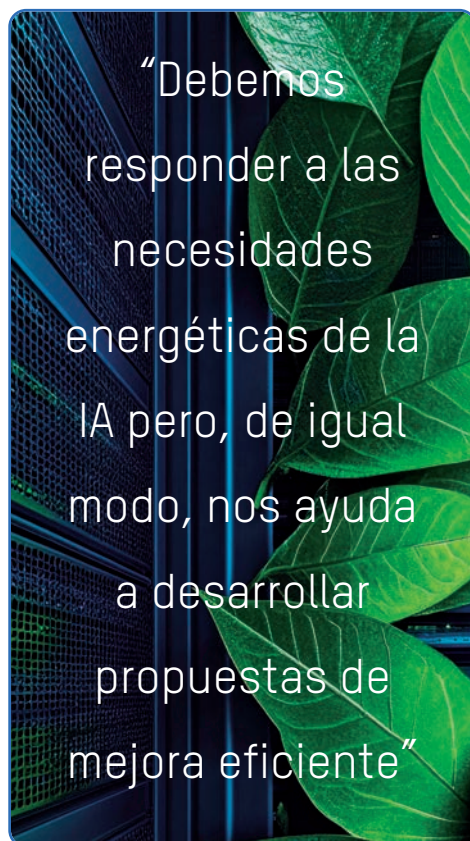
manda el 1 % de la electricidad mundial, a reducir su impacto medioambiental a través de la reducción de las emisiones de carbono y el uso del agua. "El sector de los centros de datos, mucho más que otros, es punta de lanza en materia de sostenibilidad".

La juventud del sector en España permite que los grandes centros de datos sean nativos sostenibles. "Cuando se gestaron ya había un claro compromiso en cuanto a sostenibilidad. Todos están trabajando para conseguir una mayor eficiencia energética y están investigando nuevas fórmulas, trabajando, por ejemplo, en entornos de microrredes o con pilas de combustible. También están viendo cómo aprovechar el calor sobrante. En definitiva, están trabajando en todas las direcciones para ser más sostenibles y dejar una huella prácticamente nula". Una labor en la que, completa, "es clave la coordinación entre entes privados y públicos".

## El concurso de la IA

Una de las tecnologías por las que Vertiv apuesta es la refrigeración líquida. "Es una respuesta a una necesidad tecnológica que tienen los centros de alta computación y, sobre todo, al uso intensivo de la inteligencia artificial".

La infraestructura sobre la que reposa la inteligencia artificial exige nuevas capacidades. "Ya no trabajamos con CPU: estamos



Acceda al vídeo desde el siguiente código QR



<https://newsbook.es/actualidad/sostenibilidad-en-los-centros-de-datos-20250504116664.htm>



empezando a trabajar con GPU que requieren unos consumos energéticos muy altos", recuerda. "Refrigerar un armario con un consumo de 40 o 50 kilovatios exige otro tipo de tecnología. Con la refrigeración por aire no es suficiente, lo que exige implantar una refrigeración líquida o, incluso, combinar el aire y el líquido". El futuro marca niveles de consumo energético mucho mayores: Nvidia ya ha anunciado una nueva GPU con un consumo por rack de 600 kilovatios. "Es increíble la velocidad con la que se está incrementando el consumo energético; lo que exige tecnologías con una eficiencia mucho más alta. Es el caso de la refrigeración por líquido, que ofrece un rendimiento mucho más alto. También se trabaja con otras como la de puertas frías, la inmersión o la inyección directa al chip".

La inteligencia artificial "juega" un doble papel: exige nuevas prestaciones a la infraestructura y, a la vez, su uso da respuesta a algunos retos. Una completa paradoja. "Los proveedores debemos responder a sus necesidades energéticas pero, de igual modo, esta tecnología nos ayuda a desarrollar propuestas de mejora en términos de sostenibilidad", analiza. En el caso de Vertiv ya están aplicando la inteligencia artificial en algunos servicios alrededor de los centros de datos, para una mejor toma de decisiones en relación al uso de la infraestructura. 

## Los centros de datos, en la Unión Europea

En Europa, el sector de los centros de datos tiene un acuerdo firmado a través del cual se compromete a alcanzar la neutralidad de carbono a través de fuentes de energía 100 % renovables en 2030. "Es bastante ambicioso", asegura. "En un principio, la Unión Europea, cuando trataba temas de sostenibilidad, solo ponía el foco en los equipos de consumo y en el reciclado de los mismos. Posteriormente percibió que los centros de datos y la economía digital, incluyendo las telecomunicaciones y los nodos de redes, suponían un consumo energético suficientemente importante para tenerlos en consideración", explica.

La última novedad es la Directiva Europea de Eficiencia Energética (UE) 2023/1791, que se ha visto complementada por el Reglamento Delegado (UE) 2024/1364, y que establece nuevas obligaciones para los centros de datos, con el objetivo de reducir el consumo energético y avanzar aún más en la sostenibilidad en el sector. Una directiva que establece, por ejemplo, que aquellos centros de

datos con una potencia igual o superior a 500 kW deberán reportar anualmente datos claves sobre su rendimiento energético. Unos informes que deben incluir indicadores como el consumo total de energía, la eficacia del uso de la energía (PUE), el uso de agua (WUE), el factor de reutilización de energía (ERF), el factor de energía renovable (REF), el uso de calor residual y el uso de energía renovable. En el caso de las instalaciones con una potencia total superior a 1 MW, deben aprovechar el calor residual para calefacción u otras aplicaciones de recuperación de energía, a menos que puedan demostrar que no es técnica o económicamente viable.

"Todos los centros de datos van a tener que forzarse en virtualizar servidores o en sacar mejores prestaciones a sus equipos de refrigeración utilizando tecnologías más avanzadas. Se les está empujando a conseguir una mayor eficiencia", analiza. "De cualquier manera, la palabra sostenibilidad ya está en su ADN".

# La sostenibilidad aplicada a la innovación y al producto cuenta con el respaldo del mercado

En Canon tenemos un compromiso muy claro con la sostenibilidad. Esto emana de nuestra propia filosofía corporativa a nivel global, *"Kyosei"*, que significa "vivir y trabajar por el bien común" y se une también con otro de nuestros principios básicos como compañía, la innovación.



En Canon nos esforzamos por contribuir a crear un mundo y una sociedad mejores en los que vivir.

Esto es lo que manifiesta nuestra filosofía corporativa de origen japonés, *"kyosei"*, que es lo que nos lleva a apostar por la innovación y la sostenibilidad como dos importantes pilares de nuestro negocio.

Como fabricante, reconocemos la responsabilidad de limitar el impacto medioambiental de nuestras operaciones y del ciclo de vida de nuestros productos. Por este motivo, a nivel mundial, nos hemos propuesto alcanzar cero emisiones netas de carbono en

el ciclo de vida de nuestros productos para 2050. En la actualidad, nos encontramos en vías de lograr una reducción del 50 % en las emisiones de CO<sub>2</sub> por

producto para 2030, tomando como referencia los niveles de 2008. De hecho, hasta la fecha hemos conseguido una reducción acumulada del 43 %, alcanzando reducciones medias anuales del 4,1 % frente a un objetivo del 3 %.

## La fuerza de la innovación para un negocio más circular y sostenible

Este compromiso con la sostenibilidad es un viaje que iniciamos hace más de 30 años cuando implementamos por primera vez nuestro programa de reciclaje de cartuchos. Sin embargo, somos conscientes



## "Innovamos directamente en el diseño de nuestros productos teniendo en cuenta su impacto medioambiental"

de que el reciclaje por sí solo no basta para marcar la diferencia.

Por este motivo, innovamos directamente en el diseño de nuestros productos teniendo en cuenta su impacto medioambiental y trabajamos para que los nuevos modelos sean más compactos y ligeros, utilicen menos materias primas y demanden menor energía en su fabricación y transporte.

Así, este compromiso con la economía circular también se refleja en nuestro portfolio de soluciones de impresión. En este punto, destaca nuestra gama de equipos de impresión multifunción refabricados,

que incluye, por ejemplo, los dispositivos imageRUNNER ADVANCE ES, contruidos con hasta un 90 % en peso de piezas reutilizadas y recicladas, lo que se traduce en un menor uso de materias primas durante la fabricación. De esta forma, todos los componentes del nuevo dispositivo se someten a rigurosas pruebas para garantizar el mismo rendimiento que un dispositivo totalmente nuevo.

La gama también incluye nuevas características que mejoran aún más el rendimiento medioambiental, como la tecnología *"low melting point"* tóner, que contribuye a reducir el consumo de energía del dispositivo.

En Canon, comenzamos a producir este tipo de equipos refabricados en 1992 y España es uno de los mercados que han demostrado el interés que despiertan,

habiendo superado los más de 18.000 dispositivos vendidos. Esto constata la demanda existente por parte de las empresas del país por soluciones tecnológicas que contribuyen, a su vez, a mejorar la sostenibilidad de su actividad.

En definitiva, en Canon seguimos trabajando para reducir nuestro impacto medioambiental y ofrecer a nuestros clientes los dispositivos, soluciones y servicios que buscan y que les ayudan a avanzar hacia un negocio más circular. 

**M. Jesús Arroyo**

Office product manager de Canon España

# ¿NECESITAS RENOVAR? **ELIGE TRAVELMATE P4**

Acer lo mejor en IA, seguridad y diseño



RESOLUCIÓN



FINGERPRINT  
READER



SMART CARD



PURIFIEDVOICE  
WITH AI NOISE  
REDUCTION



TRUEHARMONY



DUSTDEFENDER



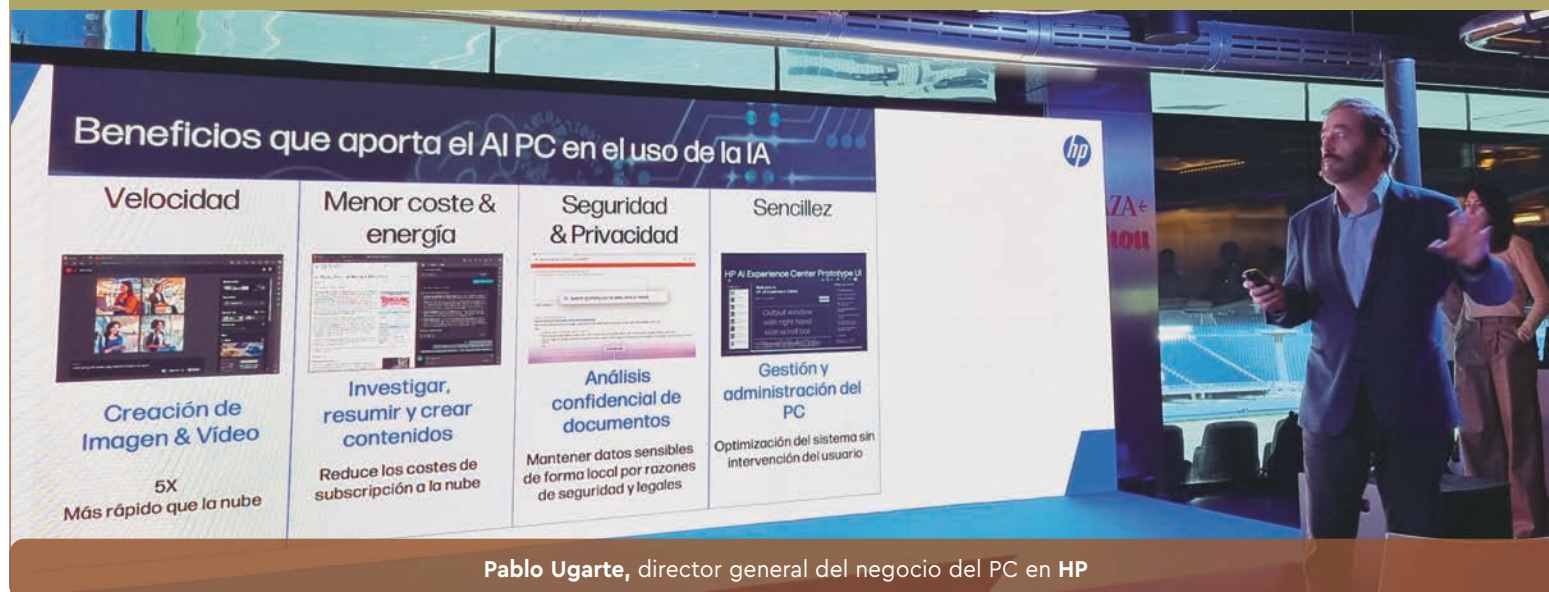
MIL-STD 810H  
CERTIFIED



POST  
CONSUMER  
RECYCLED

Disponible en:

## Nuevas gamas de equipos de HP con inteligencia artificial



Pablo Ugarte, director general del negocio del PC en HP

# HP sitúa al PC en el centro del desarrollo de la IA

**L**as razones, obvias: se trata de una tecnología hambrienta de energía, de procesamiento y de almacenamiento, lo que abre a la nube importantes desafíos a los que el PC puede contribuir a dar cumplida respuesta. "La nube es limitada, costosa y poco sostenible en su capacidad de computación. Contar con ordenadores repartidos por todo el mundo, y siendo el PC la herramienta más versátil para el trabajo diario, permite aprovechar su capacidad de cómputo", completó Melchor Sanz, CTO de HP. Basándose, de nuevo, en la apuesta por el modelo híbrido, extendió el protagonismo del desarrollo de la IA hasta el edge. "Se trata de democratizar la IA y llevar a cabo la computación, no solo en la nube, sino en las propias empresas y los usuarios". Una expansión hasta la periferia que permite notorias ventajas. "La velocidad y la latencia de una computación cercana al usuario, casi instantáneas, son mejores que en la nube", explicó Sanz. Además, los datos quedan menos expuestos. "Ejecutar la IA en local implica una experiencia más personalizada y garantiza la privacidad". Una ventaja amparada, recordó, por las leyes de la UE, "que prohíben el uso de ciertos datos fuera del ámbito del propio dispositivo". También hay una reducción del coste. "Cuando se ejecuta la IA en el dispositivo no hay coste: va incluido en la adquisición del mismo".

Mucho depende el desarrollo de la IA del PC. En un entorno en el que la nube parece que dirige cualquier innovación tecnológica, la "irrupción" de la IA ha devuelto una mayor dosis de protagonismo al PC. "El desarrollo de esta tecnología en el entorno de la nube necesita la capacidad de cómputo del PC, mucho más allá del punto de acceso que supone", explicó Pablo Ugarte, director general del negocio del PC en HP.

Marilés de Pedro

### Ecosistema IA en HP

Según los cálculos de HP más del 50 % de los PC integrarán esta tecnología en 2026 frente al 7 % de este 2025. Una tecnología identificada con una NPU por encima de 40 o 50 TOPS. En la empresa, esta integración crece 15 veces más rápido que el mercado global. Pablo Ugarte insistió en que, aunque el primero en llegar ha sido el hardware, "en el uso de la IA el punto crítico lo señala el software".

Por todo ello, la "IA va a suponer un cambio sustancial en el mercado del PC", aseguró. Hasta el momento, "todos los PC tenían parecidos criterios de diseño y utilizaban los mismos componentes; pero esto va a cambiar", explicó el máximo responsable del negocio de los PC. "Las arquitecturas, aún siendo estándares, van a permitir a los fabricantes diferenciarse". Defendió la riqueza de la oferta de HP, más allá del PC. "Vamos a incorporar la IA a las impresoras, a las soluciones de vídeo y audio, etc.". Una oferta, sincronizada, que "permite ofrecer una experiencia única".



## Gama de PC con IA

HP ha lanzado nuevas gamas de PC con IA, abarcando desde las gamas premium, que han incluido los procesadores de Intel como gran novedad tras integrar en sus primeras versiones AMD y Qualcomm; hasta los modelos ProBook. Clave es la inclusión de AI Companion, un asistente virtual de IA que permite, entre otras prestaciones, el análisis y consulta de archivos, priorizar la agenda, ayuda en el soporte y mantenimiento del PC, etc.

El buque insignia es el HP EliteBook Ultra G1. Equipado con procesadores Intel Core Ultra 5 y 7, ofrece hasta 48 TOPS de rendimiento NPU. Pesa menos de 1,2 kilogramos con una autonomía de 21

horas. Cuenta con una pantalla OLED 3K de 120 Hz, cámara de 9 megapíxeles, micrófonos duales y altavoces cuádruples.

Tanto para las pymes como para las grandes cuentas, gracias a su carta de configuraciones, se ha diseñado el HP EliteBook X G1i. Se trata de un portátil de 14", disponible en azul y plateado. Tiene una cámara de 5 megapíxeles

y capacidades de seguridad avanzada. Integra procesadores Intel o AMD.

HP EliteBook 8 es una opción convertible. Con opciones de NPU de hasta 50 TOPS, proporciona hasta un 224 % más de eficiencia energética y hasta 43 veces más velocidad en la generación de imágenes con IA. Ha modificado su diseño, que es más ligero, y se ha pensado para una larga vida

útil, por lo que incluye una garantía para los componentes que alcanza los 7 años. Integra procesadores Intel o AMD.

Otros modelos son el HP EliteBook X Flip G1i, convertible y de diseño ligero; con lápiz activo recargable; el HP EliteDesk 8 Series, que es la opción de sobremesa; o las estaciones de trabajo HP ZBook Ultra G1a, móvil de 14" y con

procesador AMD Ryzen AI Max PRO; y la mini HP Z2 Mini G1a, impulsada por el mismo procesador.

En la gama HP OmniBook se incluyen la serie HP OmniBook X con dispositivos convertibles de 14" hasta modelos clamshell de 17,3"; la familia HP OmniBook 7 y la serie HP OmniBook 5. 

“La nube es limitada, costosa y poco sostenible en su capacidad de computación. Contar con ordenadores repartidos por todo el mundo permite aprovechar su capacidad de cómputo”

**Síguenos en LinkedIn  
y no te pierdas la  
actualidad del canal  
de distribución**



[linkedin.com/company/newsbook](https://www.linkedin.com/company/newsbook) 

[twitter.com/newsbook\\_tai](https://twitter.com/newsbook_tai) 

[facebook.com/newsbooktai](https://facebook.com/newsbooktai) 

**Newsbook.es** 

La venta indirecta, clave en el crecimiento de HPE

# "Mi primer objetivo ha sido que HPE continúe siendo el socio de referencia para el canal"

En un entorno empresarial en constante evolución, Hewlett Packard Enterprise continúa creciendo, alcanzando un incremento del 16 % en sus resultados económicos más recientes. Este éxito también se refleja en el mercado español, donde la venta indirecta ha sido clave para impulsar el crecimiento. Esta apuesta se ha traducido en una reorganización interna y una inversión significativa en recursos que comenzó el pasado mes de noviembre coincidiendo con el nombramiento de Alejandro Martín como director de canal y del ecosistema de *partners* de HPE España.

 Bárbara Madariaga



Alejandro Martín, director de canal y del ecosistema de *partners* de HPE España



Mi primer objetivo era tratar de seguir manteniendo que HPE fuera el socio de referencia para todos los *partners* en el mercado", asegura Alejandro Martín, quien explica que su equipo está compuesto por diversos segmentos: *solution providers*, distribuidores, *service providers* e integradores. En el caso de los *solution providers*, se ha incorporado a una persona dedicada a la captación de nuevos *partners*, tanto tradicionales como aquellos enfocados en áreas emergentes como la inteligencia artificial y la virtualización. "Vemos cada vez más *partners* que se están especializando en inteligencia artificial, y no necesariamente buscan la reventa de productos, sino que desempeñan una labor más consultiva".

### El impulso de la IA y las soluciones de nube privada

Uno de los pilares más relevantes en la estrategia de HPE es la inteligencia artificial, un sector en auge que la compañía está posicionando como una oportunidad de crecimiento para sus *partners*. En palabras de Alejandro Martín, la IA se ha convertido en un área clave para HPE, tanto a nivel global como en España. "La apuesta de la compañía por el canal, no solo a nivel mundial, sino a nivel país, es patente".

Una de las soluciones destacadas en este ámbito es el Private Cloud AI, desarrollado en colaboración con Nvidia. Descrita como una solución "llave en mano", permite a las empresas implementar inteligencia artificial en sus sistemas de manera sencilla y rápida. "Lo que nos permite es no dejar que la inteligencia artificial se convierta en un puzle que cada cliente tiene que intentar cuadrar, sino que ofrecemos una solución llave en mano que en tres clics puede llegar a ponerse en producción".

Además de la IA, HP GreenLake ha tenido un papel crucial en el crecimiento de la compañía. Martín resalta que, más allá de ser un modelo de pago por uso, "GreenLake es una plataforma de gestión de IT que permite incorporar todos los productos de HPE, productos de terceros, soluciones de virtualización, de inteligencia artificial, y manejarlo como si fuera una experiencia de nube".

### Desarrollando nuevas oportunidades con *partners* de inteligencia artificial

La integración de inteligencia artificial en la oferta de HPE ha supuesto un desafío para el canal, que a menudo encuentra dificultades a la hora de presentar casos de negocio concretos. Según Alejandro Martín, uno de los ma-

yores retos es "establecer un *business case* en el que se pueda concretar al cliente final cuál es el retorno de la inversión y cuándo nos va a venir ese retorno". No obstante, también destaca el potencial de los nuevos *partners* especializados en IA, que se centran en ofrecer servicios consultivos y no en la reventa de productos. "Nosotros podemos ponerles en contacto también con estos *partners* que son nativos en IA, y que les pueden guiar y aconsejar y convertirse en sus propios *partners* para ir a los clientes".

Para ayudar a los *partners* a capitalizar la oportunidad de la inteligencia artificial, HPE ha puesto en marcha programas de formación y apoyo. "Nuestra apuesta es formar y capacitar al canal para que esté preparado, pero a la vez ofrecer alternativas para poder ir al mercado".

### Partner Ready Vantage y Smart Choice

El programa Partner Ready Vantage se presenta como una de las principales iniciativas de HPE para apoyar a su canal de distribución en este proceso de transformación hacia la inteligencia artificial. A través de este programa, HPE permite a los *partners* integrar sus propios servicios con soluciones de la compañía, tanto en áreas como la IA, la virtualización o la computación en nube privada (PCI). Esta iniciativa no solo capacita a los *partners* en el uso de las tecnologías, sino que también les ofrece oportunidades para incrementar su rentabilidad, brindándoles el acceso exclusivo a la comercialización de soluciones innovadoras. Además, la posibilidad de ofrecer servicios gestionados a los clientes permite al canal abrir nuevas oportunidades de negocio, mejorando su competitividad y su capacidad para adaptarse a las nuevas demandas del mercado.

Por otro lado, una de las estrategias clave para impulsar el canal de distribución ha sido el programa Smart Choice, que ha sido fundamental para redefinir el modelo de negocio transaccional con los distribuidores. Este programa tiene como objetivo garantizar que los productos se vendan al precio adecuado desde el primer momento. Según Martín, se ha trabajado junto a los mayoristas para identificar los productos de mayor rotación en el mercado y establecer precios adecuados para mejorar el circulante y reducir los inventarios. Además, se implementó un seguimiento semanal de las ventas, permitiendo adaptarse rápidamente a las evoluciones del mercado y mejorar la eficiencia operativa para los distribuidores.

### Acuerdos con Nvidia y Deloitte

Durante la celebración de HPE Discover el pasado mes de noviembre, la firma anunció importantes colaboraciones con empresas como Nvidia y Deloitte.

En este sentido, y tal y como confirma Alejandro Martín, la firma ha integrado a Nvidia en su programa de formación dirigido al canal. Esta colaboración no solo busca familiarizar a los *partners* con las soluciones de HPE, sino también con las tecnologías avanzadas de Nvidia, como sus tarjetas gráficas, que son claves en la modernización de las infraestructuras tecnológicas.

Con relación a Deloitte, HPE mantiene una estrecha colaboración para introducir soluciones de infraestructura como PCI y abordar tendencias

emergentes como la repatriación de datos, que son fundamentales para el crecimiento de las aplicaciones de inteligencia artificial. Alejandro Martín recuerda que De-

loitte fue pionero en detectar la necesidad de ejecutar aplicaciones de IA donde están los datos, lo que les permite ofrecer soluciones más adaptadas a las necesidades de los clientes. Además, HPE y Deloitte han identificado el alto coste de ejecutar IA en la nube pública, lo que ha llevado a HPE a desarrollar alternativas más rentables y escalables para sus *partners*, ayudándoles a evitar sorpresas en los costes al poner en producción las aplicaciones de IA. Esta colaboración resulta ventajosa para su red de venta indirecta, ya que le permite acceder a soluciones de infraestructura más eficientes y adaptadas a las necesidades del mercado.

### Compromiso con la sostenibilidad y la eficiencia operativa

Además de la capacitación en IA, HPE también pone un énfasis importante en la sostenibilidad. En este sentido, la firma está comprometida con la reducción de su huella de carbono y ayuda a su canal a posicionarse como empresas responsa-

bles. El objetivo es que tengan "una ventaja competitiva al ofrecer soluciones que no solo son tecnológicamente avanzadas, sino también responsables con el medio ambiente".

Por último, HPE ha llevado a cabo una reorganización global de su canal con el objetivo de mejorar la colaboración con sus *partners* y optimizar sus operaciones. Según Martín, esta reorganización responde a las demandas del canal planteadas durante los últimos años. "Esta estrategia permite que los *partners* interactúen con HPE de manera más eficiente, simplificando las negociaciones y generando oportunidades conjuntas", señala Martín, quien remarca que "lo único que ha aportado son ventajas para el canal". Esta reorganización no solo refleja un compromiso con la eficiencia, sino que también representa una apuesta por el futuro del canal, ofreciendo a los *partners* la posibilidad de aprovechar sinergias y colaborar de forma más efectiva con HPE. 

## HPE GreenLake ha tenido un papel crucial en el crecimiento de la compañía



Está trabajando con una amplia red de *partners* para construir nuevas soluciones

# Vertiv, preparado para responder a los desafíos de los nuevos centros de datos

**M**iguel del Moral, director de ventas indirectas de España, Portugal y Francia de Vertiv, junto con José Alfonso Gil, director de venta de servicios para el sur de Europa, analizaron los retos que tiene que superar el sector de los centros de datos para responder a la demanda actual y explicaron cómo la compañía está afrontando estos desafíos. "Estamos en un momento transformador", recalcó Miguel del Moral. "El centro de datos es la columna vertebral de la economía digital y de la economía de este país", añadió. En este proceso de transformación la inteligencia artificial está generando un cambio en la infraestructura de la alimentación eléctrica y la refrigeración ya que los nuevos centros de datos requieren de un mayor consumo de energía. En la actualidad el consumo energético en España es del 1,2 pero es muy probable que se triplique. Este incremento implicará que la refrigeración líquida se combinará con la tradicional de aire e incluso se espera que esta última represente solo entre el 5 % y 10 % de los centros de datos del futuro. José Alfonso Gil destacó que los sistemas refrigerantes tendrán que estar conectados a los SAI, lo que supone un cambio de arquitectura.

Para ajustarse a estas necesidades Vertiv ha preparado su oferta con la ampliación de su familia de *chillers* o enfriadoras de alta capacidad con *free-cooling* y bajo GWP orientados a centros de datos de alta densidad. Y ha adquirido la tecnología de *chillers* de la empresa china BSE. Al mismo tiempo ha lanzado una nueva generación de SAI para atender la demanda de alimentación de la IA y ha puesto en marcha una nueva propuesta de servicios para realizar un mantenimiento preventivo. Gil destacó que Ver-



Miguel del Moral,  
director de ventas indirectas  
de España, Portugal y Francia de Vertiv

**Vertiv ha identificado las tendencias que están marcando el futuro de los centros de datos en un contexto en el que la inteligencia artificial está transformando su arquitectura y sus componentes y en el que la colaboración industrial está desempeñando un papel clave.**

 Rosa Martín

tiv ha preparado una guía para que los clientes sepan qué es lo que necesitan para la infraestructura para la IA.

Vertiv también destacó que las organizaciones están priorizando soluciones energéticas eficientes y alternativas, como microrredes y pilas de combustible para hacer frente al incremento del consumo energético. Además, se está observando que en algunos países se están empezando a utilizar pequeños reactores modulares para generar energía.

En esta búsqueda de energías alternativas se está trabajando también en las renovables que requieren un sistema BESS. Un ejemplo de este trabajo es el proyecto que desarrolló Vertiv con la empresa sueca Conapto.

## Colaboración

Otro aspecto importante que está marcando la evolución de la industria de los centros de datos es la colaboración entre empresas. Del Moral señaló que "las compañías que no tengan en su ADN la colaboración y la sostenibilidad y no las integren con la innovación tecnológica sufrirán". El directivo señaló que la única forma de ser líder

en esta nueva "ola de transformación digital es colaborando, innovando y poniendo como una prioridad la sostenibilidad". Vertiv está colaborando con otros jugadores de la industria como Nvidia e Intel. Un ejemplo de esta actividad es el programa Coolerships que desarrolló con Nvidia. También ha firmado acuerdos con ZincFive y con Tecnogen.

El proveedor también destacó que la ciberseguridad y las regulaciones son otras dos tendencias que están marcando el futuro de los centros de datos. 



# Motorola, la libertad de estar siempre conectado

DMI Computer Distribuidor Oficial



**DMI**  
Computer

[www.dmi.es](http://www.dmi.es)



# PUESTO de trabajo SEGURO

esprinet



## ¿Qué incluye la solución completa que te ofrecemos si eres agente digitalizador?



Configuración inicial



Protección de dispositivos



Justificación 1ª fase



Antivirus, formación  
y soporte 24x7



Justificación  
2ª fase



Acompañamiento  
auditorias

Esprinet y Microsoft te proporcionan **“materiales de marketing”** para que lances la campaña de Puesto de Trabajo Seguro del Kit Digital a tus clientes

Línea Exclusiva Kit Digital: 976 97 15 05 | [kitdigital@esprinet.com](mailto:kitdigital@esprinet.com)