it Digital MAGAZINE

Nº 37 · ABRIL 2026

Descarga esta revista y ábrela con Adobe Acrobat Reader para aprovechar sus opciones de interactividad

LOS PORTÁTILES CON IA IMPULSAN EL PUESTO DE TRABAJO INTELIGENTE

FORO ITDS: CONSOLIDANDO LA RESILIENCIA OPERATIVA

DESAFÍOS Y OPORTUNIDADES DE LA CIBERSEGURIDAD PARA EL MSP EN 2026

PRINCIPALES TENDENCIAS EN TORNO A LA CIBERSEGURIDAD EN 2026

PRESENTE Y FUTURO DEL SECTOR DE LAS REDES EMPRESARIALES

#CONTENIDOS IT

REVISTAS DIGITALES

DEBATES

>> Principales tendencias en torno a la ciberseguridad en 2026

>> Presente y futuro del sector de las redes empresariales

ÍNDICE DE ANUNCIANTES

IT Digital MAGAZINE
Nº 37 · ABRIL 2026

ACTUALIDAD

>> ASLAN2026 se consolida como la gran cita anual de la innovación digital y la IA en España

ENTREVISTA

>> Paolo Mioli y Álvaro Verdeja, CEOS de Lutech España

NO SOLO IT

N-ABLE authorized distributor

ADM Cloud & Services

Convierte el riesgo de Microsfot 365 con resiliencia

Una solución completa, fácil de vender y difícil de sustituir.

Cove Data Protection™ for Microsoft 365 + ITDR email protection

Descubre la promoción

ASLAN2026 SE CONSOLIDA COMO LA GRAN CITA ANUAL DE LA INNOVACIÓN DIGITAL Y LA IA EN ESPAÑA

El Congreso ha cerrado su edición con 9.000 asistentes y tres días de actividad centrada en IA, innovación digital y ciberresiliencia. Con 135 proveedores especializados y más de 200 ponentes, el evento se afianza como punto de encuentro imprescindible para responsables TI de empresas y administraciones públicas.

HILDA GÓMEZ Y MIGUEL A. GÓMEZ

El Congreso&EXPO ASLAN2026 ha reunido a 9.000 profesionales, consolidándose como la cita anual más relevante en España para conocer las tecnologías que están definiendo el futuro de las organizaciones. Bajo el lema “Agentes IA, Resiliencia, Activos digitales...? Evolucionamos”, el evento ha ofrecido tres días de ponencias, demostraciones y networking de alto nivel entre empresas tecnológicas, CISO, CIO, CDO y responsables públicos.

La inauguración estuvo presidida por el ministro para la Transformación Digital y de la Función Pública, Óscar López, quien subrayó que “la sobe-

ranía digital se ha consolidado como una prioridad estratégica para España y Europa" en un contexto marcado por la aceleración tecnológica y la expansión de la inteligencia artificial. También destacó que "uno de cada tres euros" de los fondos europeos en España "ha ido a la transformación digital", con una inversión total de 30.000 millones de euros.

Alberto Pascual, presidente de la Asociación @aslan, señaló que la IA y la robótica serán esenciales para impulsar la productividad en un contexto de envejecimiento demográfico. También advirtió sobre retos como la escasez de talento, la ciberseguridad, la resiliencia empresarial y la soberanía tecnológica, defendiendo la colaboración público-privada como vía para mantener la competitividad. "Necesitamos entornos que, como este Congreso ASLAN2026, faciliten el establecimiento de alianzas estratégicas y redes de colaboración de alto impacto", afirmó.

IA, CIBERRESILIENCIA Y AGENTES INTELIGENTES, PROTAGONISTAS DEL ENCUENTRO

El evento ha puesto el foco en los retos actuales de las organizaciones, marcados por tensiones geopolíticas, incertidumbre económica y cambios sociales. Según la asociación, pocas épocas han concentrado tanta presión sobre las organizaciones como la actual, lo que exige decisiones rápidas y fundamentadas.

Con 135 proveedores especializados y más de 200 ponentes, ASLAN2026 ha conectado tendencias globales con soluciones reales en inteligencia artificial, agentes de IA, innovación digital, ciberseguridad y ciberresiliencia.

El Congreso se ha organizado como una experiencia en tres etapas: la visión estratégica de CISO, CIO y CDO de grandes empresas del IBEX35; los fórums de Tendencias Tecnológicas: Cybersecurity & AI y Digital Innovation & AI, con expertos del sector; y la Zona Expo y Stages, donde los asistentes han podido conocer productos y soluciones concretas de los 135 expositores. Este diseño ha buscado transmitir todo el conocimiento tecnológico de los miembros de la Asociación @aslan para afrontar con garantías los retos actuales.

AMPLIA REPRESENTACIÓN EMPRESARIAL Y PÚBLICA

El ecosistema empresarial ha estado representado por responsables de compañías como Iberdrola, Santander, Exolum, Naturgy, Repsol, Cruz Roja Española, Bankinter, AECC, CaixaBank, Randstad España o Tendam.

El sector público también ha tenido una presencia destacada, con representantes del Ayuntamiento de Madrid, Gobierno de Cantabria, Policía Nacional, Comunidad de Madrid, red.es, CSIC, Centro Criptológico Nacional, Agència de Ciberseguretat de Catalunya, Junta de Extremadura, Ministerio de Defensa y la Agencia Digital de Andalucía.

El cierre del Congreso estuvo presidido por Miguel López-Valverde, consejero de Digitalización de la Comunidad de Madrid, quien destacó avances como la personalización de contenidos en EducaMadrid; la automatización de trámites con reducciones del 60% en tiempos; la evolución de Cuenta Digital, con un millón de usuarios; el despliegue del Escudo Digital de ciberseguridad en todos los municipios; y el futuro laboratorio 6G, operativo antes del verano. ■

MÁS INFO +

- ASLAN2026 se consolida como la gran cita anual de la innovación digital y la IA en España
- Entrevista a Alberto Pascual, presidente de la Asociación @aslan

COMPARTIR EN REDES SOCIALES

Alberto Pascual, presidente de la Asociación @aslan

"EL CONGRESO YA NO ES UN EVENTO SOLO DE TECNOLOGÍA, ES UN EVENTO DE NEGOCIO"

El presidente de la Asociación @Aslan, Alberto Pascual, analiza el crecimiento del Congreso Aslan y defiende la necesidad de conectar tecnología, negocio y estrategia en un contexto marcado por la inteligencia artificial, la ciberseguridad y los desafíos geopolíticos.

Las cifras de cierre del evento dan muestra del impacto del Congreso, pero, para Alberto Pascual, es algo más que un dato cuantitativo, "es un termómetro de lo cualitativo", asegura. El evento, que reúne a más de 150 expositores y a los principales actores del ecosistema tecnológico, refleja una evolución que va mucho más allá del crecimiento en asistencia.

Ese cambio tiene que ver con una transformación profunda del propio concepto del Congreso. Lo que durante años fue "una conversación de tecnólogos para tecnólogos" se ha convertido en un espacio donde convergen perfiles estratégicos. "Hemos sabido involucrar a quienes marcan la estrategia y deciden las inversiones, tanto en el sector privado como en el público", explica Alberto Pascual. La presencia de miembros de consejos de administración y representantes políticos ha enriquecido el debate y ha ampliado el impacto del encuentro.

Este viraje responde, según el presidente de @Aslan, a una obsesión clara: dotar de sentido práctico a la tecnología. "Todo acto debe tener una estructura: visión, para anticipar tendencias; retos, para entender el contexto; y solución, para aplicar la tecnología a problemas reales", subraya. En este enfoque, la innovación deja de ser un fin en sí mismo y se convierte en una herramienta para transformar el negocio.

UN NODO CLAVE PARA EL ECOSISTEMA

El Congreso Aslan se posiciona así como un nodo clave en un ecosistema cada vez más complejo. Alberto Pascual describe un escenario en el que la tecnología, aunque más sencilla para el usuario final, es cada vez más sofisticada en su arquitectura interna. "Ese puzzle tecnológico es tan complejo que resulta inviable que una única compañía tenga todas las capacidades necesarias", afirma. De ahí "la importancia de generar espacios de colaboración donde las empresas puedan identificar socios complementarios bajo un marco de confianza".

En este contexto, los grandes ejes del Congreso reflejan las preocupaciones globales. La productividad emerge como una prioridad estratégica, especialmente en Europa. "El estado de bienestar es insostenible si no somos capaces de aumentar la productividad", advierte nuestro interlocutor, quien señala a la inteligencia artificial, más allá de su vertiente generativa, como una palanca clave para lograrlo.

Junto a ello, el entorno geopolítico introduce nuevas capas de riesgo. La ciberseguridad sigue siendo esencial, pero ya no es suficiente. "No basta con prevenir; hay que ser resilientes y capaces de recuperarse rápidamente tras un ataque", señala. A este debate se suma el de la soberanía tecnológica, en un mundo cada vez más multipolar, donde evitar dependencias críticas se convierte en una prioridad estratégica.

La administración pública, por su parte, avanza, pero aún con recorrido por delante. Pascual reconoce progresos, aunque apunta a un desfase respecto al sector privado. "Todavía hablamos de digitalización cuando las empresas ya están en transformación digital", indica. La complejidad estructural del sector público exige, en su opinión, una reingeniería de procesos que acompañe a la adopción tecnológica.

#ENTREVISTA

“Más allá de los servicios que ofrecemos, nuestro gran valor es la capacidad de innovar”

PAOLO MIOLI, ÁLVARO VERDEJA, CEOS, LUTECH EN ESPAÑA

MIGUEL ÁNGEL GÓMEZ

El cierre de 2025 marcó un hito en el proceso de expansión internacional y crecimiento de Lutech que, en el caso del mercado español, se tradujo en el cierre definitivo de la adquisición del negocio de Cloud y Ciberseguridad de Making Science. Para conocer de primera mano cómo queda la organización en España y cuáles son sus retos y objetivos, hemos hablado con sus máximos responsables, Paolo Mioli y Álvaro Verdeja, quienes han analizado el presente y el futuro de la organización en nuestro país.

> "NO SE TRATA DE PENSAR EN UN NEGOCIO TRADICIONAL Y EN OTRO INNOVADOR, SINO DE ESTAR DISPUESTOS A EVOLUCIONAR EN UN ENTORNO TAN CAMBIANTE COMO EL TECNOLÓGICO Y SER MEJORES CADA DÍA"
>
> **PAOLO MIOLI,**
> CEO, **Lutech en España**

¿Cómo queda estructurada la compañía en nuestro país y en qué punto está la reorganización?

Paolo Mioli. Lutech en España nace en 2023 y desde esa fecha hemos tenido un crecimiento tanto orgánico como inorgánico. La de Making Science ha sido última adquisición que hemos hecho, y hemos decidido mantener entidades legales distintas por diversas razones, principalmente administrativas, pero, a nivel organizativo, somos una única organización. Álvaro y yo lideramos áreas distintas, yo más orientado al negocio SAP/Salesforce, mientras Álvaro tiene el foco en negocios más innovadores, pero realmente ante el cliente somos solo uno, con diversas líneas de negocio, pero una única empresa. Hemos consolidado un ecosistema único de capacidades donde compartimos recursos, conocimiento especializado y estructura. Hemos apostado por un modelo de comercialización transversal que elimina silos, permitiéndonos ser mucho más ágiles y ofrecer una respuesta integral y eficiente a los desafíos de nuestros clientes.

Álvaro Verdeja. Cuando pensamos en el futuro, esa visión compartida es que nosotros tenemos que ser Lutech en España, y hacer lo mismo que ha conseguido Lutech en Italia: convertirse en los principales jugadores del mercado, y para eso necesitamos ser una única marca.

¿Esto se ha trasladado ya al día a día de las operaciones?

P.M. Tenemos una única responsable de marketing, un departamento de RR.HH. común para todas las sociedades que tenemos en España, y lo mismo en el departamento de administración e, incluso, en la fuerza de venta, que se establece en una única organización, aunque sea transversal a las diferentes entidades legales, necesarias administrativamente, pero no de cara al mercado. Y esto se traslada también a Álvaro y a mí, no se trata de cargos, sino de hacer crecer la compañía de la mano de los servicios".

¿Cómo queda dividido el negocio?

P.M. Sustancialmente, lo que era la antigua SAPIMSA se ocupa del negocio SAP y del mundo Salesforce, lo que podríamos definir como el negocio tradicional.

A.V. En nuestro caso, tenemos el foco en el mundo cloud y en la inteligencia artificial, principalmente de la mano de Google Cloud, pero lo cierto es que, en apenas tres meses, ya tenemos equipos cruzados trabajando juntos, porque nos centramos en proyectos, personas y clientes.

Partiendo del plan de ser en España un jugador relevante como ya es la compañía en Italia, ¿cuáles son los

objetivos cuantitativos y cualitativos que se han planteado para este primer ejercicio?

P.M. Nuestro primer objetivo es buscar el posicionamiento correcto en el mercado español. Por nuestro tamaño, nos sentimos muy cómodos en el segmento medio del mercado, y nuestra idea para este año es definir un claro posicionamiento de marca y una oferta de servicios integrados para las organizaciones. Queremos ayudar a los clientes eficientando proyectos y procesos a través de la IA y de un uso inteligente de los datos, y por eso no descartamos seguir creciendo de forma inorgánica con nuevas adquisiciones con empresas que nos ayuden a complementar la propuesta de servicios o mercados que cubrimos actualmente. Un ejemplo podría ser el área de Banca y Seguros, donde podríamos buscar empresas que nos ayuden a crecer con servicios complementarios. Tenemos mucho conocimiento y buscamos tener una masa crítica suficiente para ser capaces de atender las necesidades de los clientes, que no quieren tener una nómina interminable de proveedores, sino uno que les ayude a consolidar, y ese debe ser nuestro objetivo: poner sobre la mesa del cliente todos los servicios que necesiten.

A nivel numérico, cerramos el año con una facturación alrededor de los 50 millones de euros, y el objetivo es incrementar esta cifra en un porcentaje de doble dígito. Es un reto importante, y para alcanzarlo tenemos que ser capaces de potenciar nuestra oferta de servicios, orgánica o inorgánicamente.

A.V. Tenemos muy claro lo que somos hoy y lo que queremos ser mañana, y sabemos quién es nuestro cliente, el segmento Corporate, sin olvidar que ya contamos con clientes del IBEX35; ya trabajamos con un tercio de las empresas de este índice, y queremos crecer tanto en el número de estos clientes como en los servicios que les ofrecemos a cada uno de ellos. En definitiva, sabemos cuál es la realidad del mercado y de la compañía en 2026, pero nuestro proyecto es muy ambicioso".

¿Cómo se divide el negocio entre las diferentes unidades?

P.M. El negocio tradicional de SAP es muy importante para nosotros actualmente, mientras que el negocio Salesforce es una línea de negocio muy nueva. Salesforce es una plataforma en continuo desarrollo y, en nuestro caso, para establecerlo en España,

> "LAS INVERSIONES TIENEN QUE SER SOSTENIBLES TANTO PARA EL CLIENTE COMO PARA NOSOTROS, Y PARTE DE ESTA SOSTENIBILIDAD DESCARGA EN LAS PERSONAS, QUE SON NUESTRO VERDADERO VALOR"
>
> **ÁLVARO VERDEJA**, CEO, **Lutech en España**

hemos utilizado importantes contratos de Italia con filiales locales de estas empresas, lo que no ha permitido apalancar cierto nivel de crecimiento en los últimos meses. Se trata de un mercado muy competitivo, donde es importante demostrar tu experiencia y contar con referencias de clientes ayuda a ganar contratos. Nuestra idea es hacer lo que sabemos hacer, y prepararnos para adquirir las capacidades necesarias para asumir cualquier proyecto en el momento es que se presente, porque, repito, nuestra idea es crecer y reforzar nuestras capacidades y probabilidades y, cuando estemos en un cliente, ser capaces de ofrecerle todo aquello que pueda necesitar más allá de la propuesta de servicios que tengamos para ellos. Y para ello es fundamental tener la capacidad de innovar y reinventarse uno mismo frente a su cliente.

A.V. Más allá de las cifras de negocio, las organizaciones son muy simi-

lares, hablamos de números, beneficios, personas... Y en este contexto, nosotros apostamos por consolidar nuestras capacidades y ofrecer la mejor opción posible. De hecho, podemos pensar en mejorar servicios SAP con piezas de tecnología cloud que nos permitan generar, incluso, algo totalmente nuevo. No se trata de pensar en un negocio tradicional y en otro innovador, sino de estar dispuestos a evolucionar en un entorno tan cambiante como el tecnológico y ser mejores cada día. Y, para ello, necesitamos a las personas adecuadas para liderar este cambio.

P.M. Creo que el activo principal que tenemos como empresa no es lo que vendemos, quiero decir el servicio, sino las personas que crean la innovación. Por eso queremos trabajar como una sola organización, porque desde el conocimiento y las experiencias nace el crecimiento. Ofrecer un servicio determinado y tener tecnología cloud de forma separada, es algo bueno, pero cuando integras ambas obtienes un valor exponencial. Y algo similar ocurre cuando integras profesionales con muchos años de experiencia con talento joven e innovador, se crea nuevo valor, y no olvidemos que ese valor es lo que tenemos que poner sobre la mesa para nuestros clientes.

Clica en la imagen para ver la galería completa

¿En qué verticales tienen una posición consolidada para seguir desarrollando negocio y cuáles quieren reforzar?

P.M. En el ámbito SAP, estamos muy consolidados en Administración Pública. Tenemos clientes desde hace 20 años, con lo que podemos decir que tenemos una posición afianzada. Otro sector en el cual somos potentes es en Utilities, porque en España no hay muchas empresas que tengan competencia en SAP IS-U, y nosotros sí la tenemos. Tenemos gran experiencia, hemos hecho implantaciones importantes, y hemos ganado clientes en este terreno. Son dos sectores donde estamos bien posicionados, mientras que en otros, como Manufacturing creo que podemos seguir creciendo.

A.V. El negocio cloud es un reflejo más de cómo la unión de las dos empresas nos está dando algo más potente. Somos complementarias, y no solo en la parte de las capacidades técnicas, sino también en las diferentes verticales. Si pensamos en las grandes verticales del mercado, podemos pensar en Telco, Media, Moda y Retail, Viajes o Inmobiliaria. En cuatro de ellas estamos bien posicionados, y a las otras dos podemos acercarnos con una propuesta conjunta que nos ayude a entrar en posibles clientes cruzados.

¿Esta integración les convierte en un proveedor diferente y les abre nuevas oportunidades?

P.M. Sí, a lo que podemos añadir otra ventaja competitiva: la cercanía. Tenemos un tamaño y una flexibilidad que nos permiten estar cerca de los empleados y de los clientes, y esto les da confianza. Queremos fortalecer esto con los clientes, porque es un valor muy destacado.

A.V. La transparencia con los clientes será clave en un futuro marcado por la innovación y la cercanía con los socios y los clientes. La capacidad de adaptación de los equipos será esencial para poder estar cerca de los clientes y definir juntos la relación.

¿Cuáles son sus prioridades a la hora de desarrollar las capacidades y el talento de los equipos?

P.M. Tenemos diferentes líneas de trabajo en este sentido. El talento joven es muy importante, pero no suficiente. También lo es la experiencia, por lo que es fundamental conciliar ambas líneas. Y esto es un reto, porque no es lo mismo lo que espera y demanda un profesional experimentado que un profesional recién llegado al mercado. Hay que ofrecer la flexibilidad adecuada a cada persona, implicando, más allá de la remuneración, otros factores, como la gestión del tiempo, y para eso, la cercanía a las personas es esencial. Hemos desarrollado un plan, de la mano de Recursos Humanos, para que todos los empleados tengan su propio crecimiento profesional.

A.V. En esta situación intervienen diferentes factores, y la realidad del mercado es un reto que necesitamos asumir las organizaciones. Evidentemente, el sueldo es un elemento importante, pero hay mucho más: la flexibilidad, la motivación, la integración con las personas y los proyectos... y, por supuesto, juntar personas con experiencia con talento más joven para que siga desarrollándose. Hay que apostar por las personas, escucharlas, entenderlas...

¿El incremento de personal es un objetivo para este año?

A.V. No queremos fichar por fichar, pero queremos crecer sí o sí, y para eso, hablaremos de tecnología, de proyectos, pero, sobre todo, de personas.

P.M. En nuestro caso, el número de profesionales no asignados a un proyecto es muy bajo, lo que significa que para seguir creciendo necesitaremos más personas que nos ayuden a llevar a cabo más proyectos. Y parte de este crecimiento llegará de la incorporación de talento joven, aunque ya somos una empresa con una edad media muy baja.

En el caso del mercado español, ¿cuál es la realidad del estado de la IA?

P.M. Para nosotros, y así lo trasladamos a los clientes, la IA es una vía para aportar valor. Miramos un proceso y tratamos de mejorarlo, y la automatización nos lo permite, porque ayuda a potenciarlo tomando ciertas decisiones de manera más rápida y eficiente. Pero no se trata de desarrollar proyectos muy grandes, sino proyectos que permitan ver el valor y el ROI lo antes posible. Nuestra idea es construir juntos, el cliente y nosotros, con un acercamiento sostenible y desarrollando proyectos rentables, para el cliente y para nosotros.

A.V. La situación global plantea un cierto nivel de incertidumbre en torno a la IA, la energía, la soberanía... Y en eso es en lo que mejor podemos ayudar a los clientes. Llevamos casi 10 años publicando casos de éxito donde estamos demostrando el impacto de la IA en diferentes organizaciones.

¿Demandan los clientes la IA para avanzar en sus proyectos?

P.M. Depende mucho de la madurez de cada sector, porque no están en el mismo punto algunos sectores privados, donde ha habido importantes inversiones, que en el Sector Público, por ejemplo. Aspectos como la normativa, y su impacto en la innovación, son muy relevantes a la hora de desarrollar un proyecto en un cliente. Hay sectores menos regulados donde el despliegue de estos proyectos es más rápido que en otros. En todo caso, es importante seguir creando pequeños proyectos que nos permitan avanzar y crecer rápidamente.

A.V. Ningún cliente quiere un proyecto de IA por ser de inteligencia artificial. Quieren saber cómo la IA va a impactar en el negocio, y ahí es donde tenemos que posicionarnos, en ayudarles a entender cómo la inteligencia artificial va a ayudarles.

P.M. En todo caso, es innegable que la IA va a tener un claro efecto en el negocio y en el mercado laboral, pero se trata de una transformación como otras que ya hemos visto a lo largo de la historia. Nosotros no podemos prever el futuro, pero sí ayudar a los clientes a adecuarse al entorno actual. La palabra clave, en cualquier caso, es la sostenibilidad. Las inversiones tienen que ser sostenibles tanto para el cliente como para nosotros, y parte de esta sostenibilidad descarga en las personas, que son nuestro verdadero valor. ■

MÁS INFO +

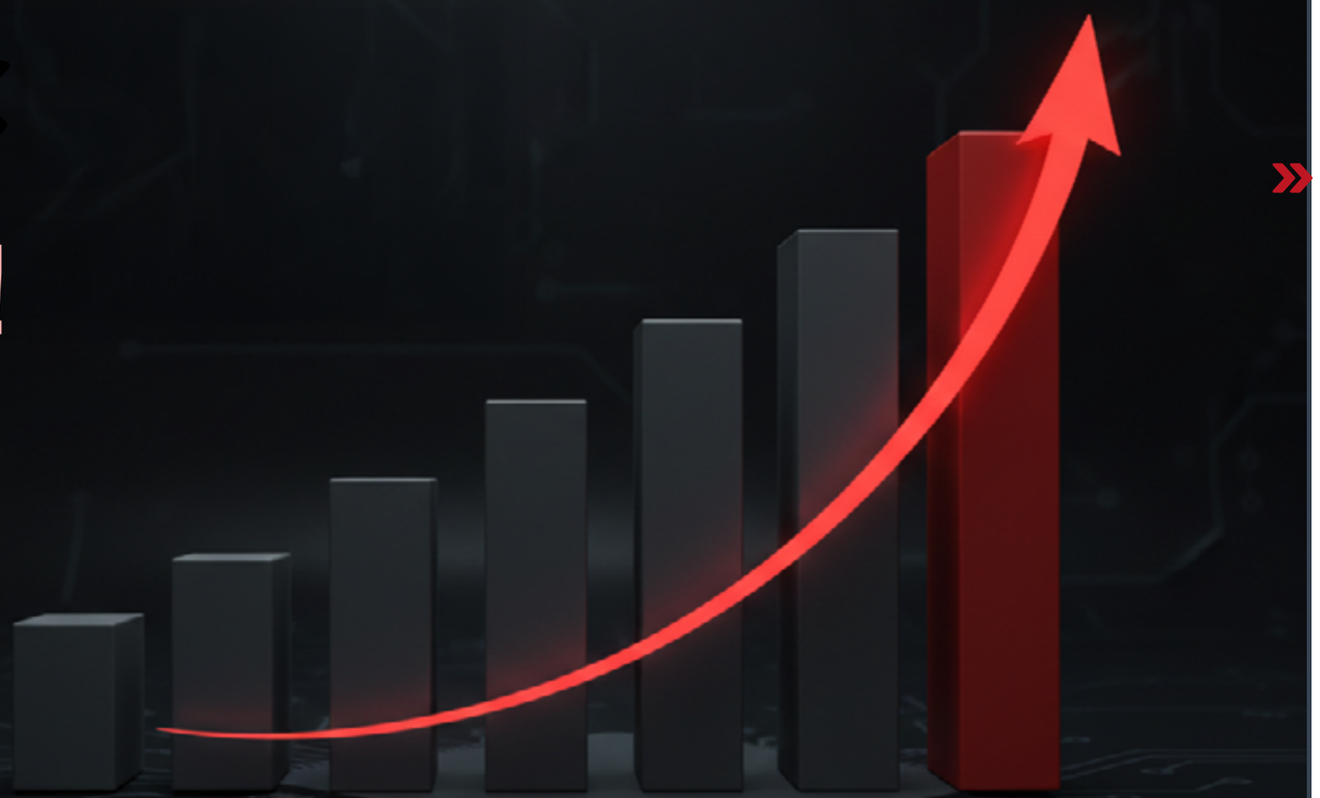
» Lutech acelera su expansión europea con nuevas adquisiciones y una apuesta por el talento

DESCUBRE POR QUÉ
SOMOS TU SOCIO ESTRATÉGICO

35 AÑOS

En un mercado que no se detiene, tu stock tampoco debería hacerlo. En DMI Computer combinamos logística inteligente y marcas líderes para que tu única preocupación sea seguir creciendo.

Tu stock, a un clic de distancia



¡ESCALAMOS TU NEGOCIO!

DMI Computer

LOS PORTÁTILES CON IA IMPULSAN EL PUESTO DE TRABAJO INTELIGENTE

RICARDO GÓMEZ

©freepik

El futuro de la informática está ligado a la inteligencia artificial, pero no solo a la basada en la nube o las grandes infraestructuras para IA, sino también en los Copilot+ PC. Estos dispositivos permiten ejecutar cargas de trabajo de IA sin depender de servicios o recursos externos, y en 2026 llegan al mercado nuevos modelos equipados con los chips más potentes hasta la fecha. Hablamos con representantes de la industria para conocer las últimas novedades en este campo y para conocer su punto de vista sobre el futuro de este tipo de ordenadores.

La expansión de la inteligencia artificial en el puesto de trabajo cuenta con varios aliados, comenzando por la nube, que actúa como base para ejecutar numerosas aplicaciones y servicios basados en IA. Pero también con los nuevos equipos informáticos capaces de ejecutar cargas de trabajo de inteligencia artificial en local, sin depender de conectividad o recursos externos: los Copilot+ PC.

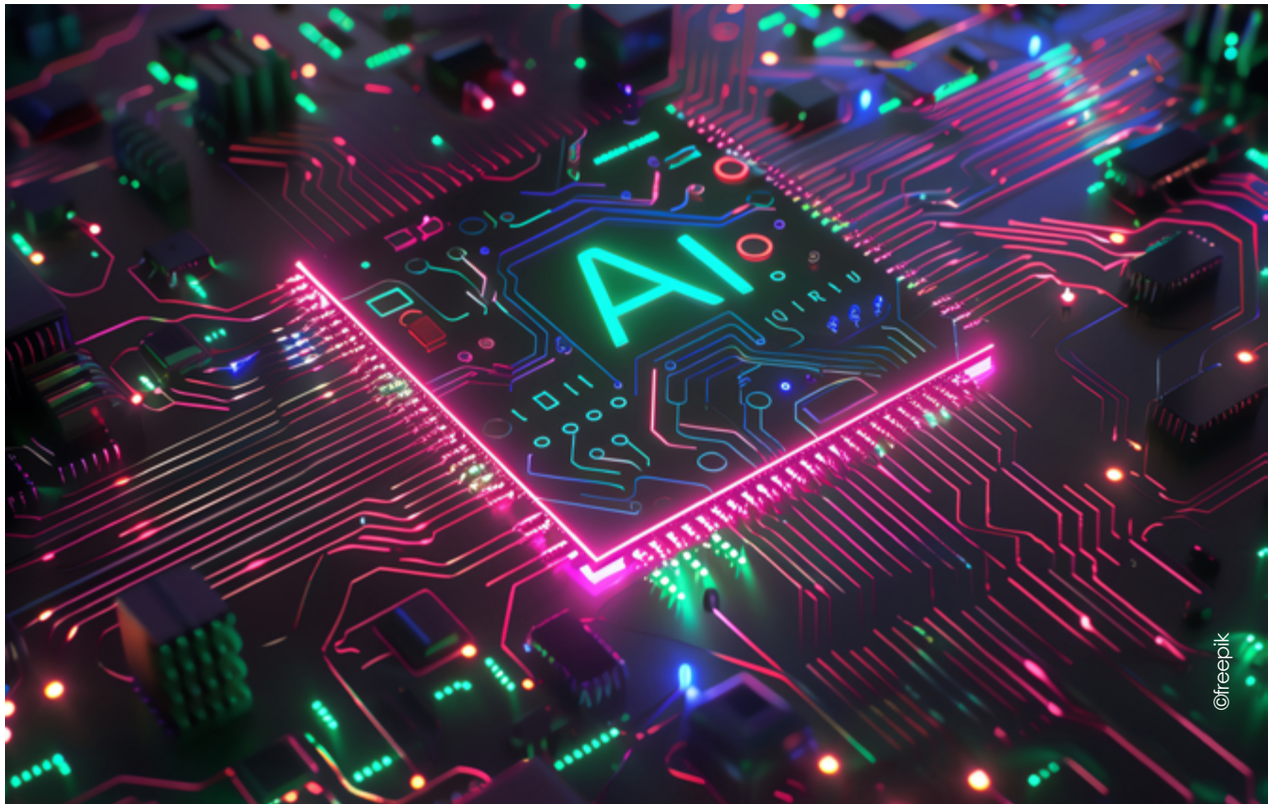
Esta categoría de equipos, impulsada inicialmente por Microsoft y los principales fabricantes de CPU (Intel, AMD y Qualcomm), se basa en la inclusión en el hardware de una NPU (Neural Processing Unit), un procesador diseñado específicamente para ejecutar operaciones vinculadas a la inteligencia artificial. Esto permite usar herramientas basadas en IA de forma local, contribuyendo a mejorar la productividad en diversos entornos de trabajo.

Actualmente, para que un portátil sea considerado Copilot+ PC, su combinación de CPU+NPU+GPU (si cuenta con una) debe ser capaz de alcanzar un mínimo de 40 TOPS (Tera Operations Per Second). Hasta el momento, solo eran ordenadores portátiles, porque el concepto incluía cuestiones propias de estos equipos, como la eficiencia y la autonomía. Pero con la nueva generación de CPU-NPU de Intel y AMD, el concepto se extenderá a los ordenadores de sobremesa.

¿CÓMO ESTÁN EVOLUCIONANDO LOS CHIPS?

Los fabricantes de PC ofrecen desde hace relativamente poco tiempo una amplia gama de Copilot+ PC que rondan esa cifra de 40 TOPS, y que han ido ganando peso en el mercado. Pero con las nuevas generaciones de procesadores que llegan este año al mercado, la industria pretende ofrecer un rendimiento superior, de unos 50 TOPS, que se amplían en modelos que cuentan con una GPU dedicada. Los nuevos chips de Intel son los Core Ultra Series 3, mientras que AMD ha presentado los Ryzen AI Serie 400 y Qualcomm los Snapdragon X2.

En opinión de Siquem González, SYS product manager lead de Asus España, se está viendo “una evolución muy rápida y clara en este segmento”, con “un salto significativo de capacidad de procesamiento de IA local, especialmente gracias a la integración de NPU más poten-



tes y a arquitecturas más eficientes". Esto, opina, "está permitiendo que funciones que antes dependían exclusivamente de la nube, ahora puedan ejecutarse directamente en el dispositivo, con ventajas claras en latencia, privacidad y eficiencia energética".

Coincide en esta visión Marcos Manzano, field product manager, Client Solutions de Dell Technologies, quien añade que, "en solo unas pocas generaciones, los PC han pasado de no tener apenas aceleración específica para IA a integrar NPU capaces de decenas o incluso cientos de TOPS, junto con GPU cada vez más potentes". Señala que esto está cambiando la forma de diseñar los ordenadores, situando la capacidad de ejecutar IA en un primer plano, afectando a la refrigeración, la autonomía, la seguridad y la experiencia de usuario. Y aclara que "lo más importante no es solo la potencia bruta en TOPS, sino la madurez de la capa de software y la integración con el sistema operativo".

La capacidad de superar los 40 TOPS es un hito importante para la industria, como señala Elena Pérez, responsable de go to market de Surface para Empresas, en Microsoft. Considera que este avance ha permitido introducir experiencias clave basadas en IA, que requieren una arquitectura optimizada y un procesamiento eficiente directamente en el dispositivo".

DEMANDA EN CRECIMIENTO

Para Siquem González, de Asus, "la acogida [de los Copilot+ PC] está siendo positiva y, sobre todo, progresiva". Tras una primera etapa de "descubrimiento", comenta, "durante este último año hemos visto un aumento claro del interés tanto en el segmento profesional como en el educativo y en el de creadores de contenido". Además, señala que "cada vez más empresas valoran la capacidad de ejecutar la IA en local, especialmente en escenarios donde la privacidad de los datos o la eficiencia operativa son importantes", y cree que la adopción va a crecer en los próximos ciclos de renovación de PC.

En Dell Technologies, como explica Marcos Manzano, tienen una percepción similar sobre el interés creciente en los Copilot+ PC, especialmente en los segmentos empresarial y de consumo premium. Relaciona esta tendencia con la existencia de aplicaciones potenciadas por IA que ya contemplan el uso en local, y comenta que "vemos una demanda más clara desde el usuario final", tanto por parte de las empresas como de los propios trabajadores, que quieren sacar más partido de la IA en su día a día.

Aunque cabe señalar que el aumento de costes y la baja disponibilidad de componentes de memoria y almacenamiento para ordenadores está impactando mucho en el mercado, repercutiendo en el PVP final de los portátiles. Y los analistas prevén un impacto negativo en las ventas, como indican los últimos datos de IDC, que anticipan una fuerte caída del mercado de PC en 2026.

¿MODA PASAJERA O EL FUTURO DEL PC?

Esta lógica pregunta se plantea cada vez que una tecnología llega al mercado prometiendo ser una revolución, pero la capacidad de ejecutar IA en local parece estar ganando adeptos rápidamente. Para Siquem González, de Asus, "va a convertirse en un elemento fundamental del PC moderno. No creemos que vaya a sustituir a la nube, sino que ambos modelos van

> "CADA VEZ MÁS EMPRESAS VALORAN LA CAPACIDAD DE EJECUTAR LA IA EN LOCAL"
>
> **SIQUEM GONZÁLEZ,** SYS product manager lead, **Asus España**

a convivir", ya que hay tareas que pueden beneficiarse de la capacidad local, mientras que los servicios en la nube suplirán capacidades de IA con mayores requisitos técnicos, para modelos más grandes o más volúmenes de datos.

En Dell Technologies, como explica Marcos Manzano, consideran que "la IA en local es una capacidad fundamental y a largo plazo del PC, no una moda pasajera". Los motivos principales estarían en la necesidad de mejorar la latencia y la experiencia de uso, los requisitos de privacidad y cumplimiento normativo, y también por cuestiones de coste de los servicios en la nube. Por ello, esperan que se instale el modelo híbrido, convirtiendo al PC en "un endpoint inteligente que puede preprocesar, personalizar y filtrar datos en local, mientras aprovecha la nube para modelos grandes o cargas muy pesadas".

Elena Pérez, de Microsoft, coincide con sus homólogos y destaca la rápida evolución que están viviendo las NPU, y también las ventajas del modelo híbrido. En este sentido, señala que "la combinación de modelos locales (SLM) y capacidades híbridas con la nube permite aprovechar lo mejor de ambos mundos".

¿PODRÁN LOS FABRICANTES SEGUIR EL RITMO DE EVOLUCIÓN DE LA IA?

Esta es otra de las grandes dudas que suscita el rápido avance de las tecnologías basadas en IA. Pero Siquem González (Asus) afirma que "tanto Intel como AMD y Qualcomm están acelerando sus hojas de ruta en torno a la IA", y sí considera que "el ecosistema -hardware, software y desarrolladores- está evolucionando de forma bastante coordinada".

De forma similar opina Marcos Manzano (Dell Technologies), quien asegura que "el rendimiento de NPU y GPU crece más rápido que el de la CPU tradicional, y los fabricantes se centran también en la eficiencia por vatio, que es crítica en formatos móviles". Opina que "el reto no será tanto la potencia absoluta en TOPS como encajar el acelerador adecuado con la carga adecuada y lograr que el software use de forma transparente el mejor motor disponible".

Elena Pérez (Microsoft) también opina de forma similar, y destaca los grandes avances en las últimas generaciones de CPU-NPU de Intel, AMD y Qualcomm, que han apostado fuerte por superar los 40 TOPS que requiere la experiencia Copilot+ PC. Además, dice, "Microsoft trabaja estrechamente con cada fabricante para optimizar Windows 11 y las experiencias de IA sobre estas arquitecturas, garantizando que el hardware evolucione al ritmo del software y de los escenarios reales de uso".

¿QUÉ CHIPS PREFIEREN LOS FABRICANTES?

Con cada generación de CPU-NPU surgen las dudas sobre qué plataforma es más potente, eficiente o adecuada para según qué casos de uso o perfiles de dispositivo. Siquem González comenta que en Asus analizan varios factores a la hora de elegir el chip para cada producto. "Evidentemente, el rendimiento es clave, pero también valoramos la eficiencia energética, el tipo de experiencia que queremos ofrecer, el diseño del equipo, el perfil del usuario y, por supuesto, aspectos como la disponibilidad o el posicionamiento de precio". Y señala que "cada fabricante de procesadores tiene fortalezas concretas, y nuestro objetivo es aprovecharlas para ofrecer el mejor equilibrio posible en cada gama de producto".

En Dell Technologies, según Marcos Manzano, adoptan "un enfo-

> "LA IA EN LOCAL ES UNA CAPACIDAD FUNDAMENTAL Y A LARGO PLAZO DEL PC, NO UNA MODA PASAJERA"

MARCOS MANZANO,
field product manager, Client Solutions, **Dell Technologies**

que holístico, guiado por el caso de uso", teniendo en cuenta que "diferentes familias y arquitecturas de CPU tienen puntos fuertes que encajan mejor con determinados segmentos". Por ello, independientemente del precio, el rendimiento o la disponibilidad de componentes, dice, "partimos sobre todo del perfil de uso y el punto de diseño (factor de forma, térmicas, batería, gestionabilidad, seguridad, capacidades de IA). A partir de ahí, elegimos el silicio que mejor encaja con la misión de ese producto".

¿HACIA DÓNDE SE DIRIGE EL SOFTWARE BASADO EN IA?

Para que la ejecución de IA en local tenga sentido es necesario contar con aplicaciones que contemplen un escenario de uso desconectado de la nube, y los fabricantes de equipos tienen un papel clave en este campo. Siquem González, de Asus, señala que la capacidad de correr IA localmente "abre la puerta a nuevas experiencias, tanto dentro del sistema operativo como en nuestras propias aplicaciones". Y precisamente están trabajando en funciones de optimización inteligente de rendimiento, gestión energética adaptativa, y mejoras en videoconferencia. Además, cuentan con "herramientas que ayudan a personalizar la experiencia del usuario en función de su forma de trabajar o crear contenido".

El punto de vista de Dell Technologies es similar, y Marcos Manzano destaca que sus últimos Copilot+ PC integran NPU y GPU de alta eficiencia, diseñadas específicamente para cargas de IA sostenidas en el dispositivo. Sobre estas capacidades, ofrecen mejoras inteligentes de seguridad y privacidad y una serie de herramientas propias, como "utilidades de gestión, soporte y optimización, tanto para los profesionales de TI como para los usuarios finales". Y señala que "nuestro objetivo es que el cliente no solo compre hardware de IA, sino que perciba un valor real aportado por Dell en forma de endpoints más inteligentes, resilientes y fáciles de gestionar".

Por su parte, Microsoft tiene mucho que decir en cuanto a las capacidades de inteligencia artificial en local, y Elena Pérez destaca las funcionalidades exclusivas de los Copilot+ PC: Recuerdos, una línea de tiempo inteligente que captura de forma local, privada y cifrada lo que ocurre en el PC, para su posterior consulta. También Cocreador, una herramienta de generación de imágenes con IA; Subtítulos en directo con traducción en tiempo real; Efectos de Windows Studio; Búsqueda semántica; o Click to Do, una serie de acciones instantáneas inteligentes, basadas en lo que aparece en pantalla. Además de esto, explica que "en los próximos meses, veremos más experiencias impulsadas por IA local, nuevas capacidades en Windows AI Foundry, mejoras en la optimización de modelos locales y una expansión del ecosistema de apps nativas para NPU".

Otro tema a tener en cuenta es cómo está abordando la industria de software el aumento de capacidades de ejecución de IA localmente en los portátiles. Elena Pérez afirma que el desarrollo de aplicaciones capaces de aprovechar esta característica es clave para el futuro de la industria de software, y que "el soporte de ejecución local significa menor latencia y experiencias más naturales, opciones de mayor privacidad, al gestionar todo localmente, mayor autonomía y costes más bajos al reducir necesidades de computación en la nube.

> "EN LOS PRÓXIMOS MESES, VEREMOS MÁS EXPERIENCIAS IMPULSADAS POR IA LOCAL"

ELENA PÉREZ,
responsable de go to market de Surface para empresas, **Microsoft**

Destaca que “el ecosistema se está moviendo hacia modelos híbridos, donde la IA local (SLM) cubre gran parte de las tareas del día a día y la nube se reserva para cargas complejas”, algo que desde Microsoft apoyan con “herramientas como Windows ML, ONNX Runtime, Windows AI Foundry y soporte para chips de Intel, AMD y Qualcomm que facilitan el desarrollo optimizado para NPU”. ■

MÁS INFO

» IDC alerta de una fuerte caída del mercado de PC en 2026

» Nuevos portátiles con IA

©freepik

LA IA LOCAL ACELERA LOS CICLOS DE RENOVACIÓN DE PC

Con el rápido avance de la inteligencia artificial se plantea la cuestión de cuánto tiempo serán capaces los Copilot+ PC de ejecutar en local las aplicaciones de IA para las que se han adquirido, y si no será necesario actualizarlos con más frecuencia que los portátiles convencionales. En este sentido, Siquem González, de Asus, ve “posible que los ciclos de renovación sean más dinámicos en determinados perfiles de usuario, especialmente en profesionales que dependen de herramientas avanzadas de productividad, desarrollo o creación de contenido”. Pero cree que el ritmo de actualización continuará basándose en una combinación de capacidades de software, mejoras significativas de eficiencia y rendimiento, y cambios en el ecosistema, como el soporte del sistema operativo.

Por su parte, Marcos Manzano, de Dell Technologies, se muestra más convencido de que las capacidades de IA local sí acelerarán los ciclos de renovación de equipos. Especialmente en segmentos de productividad basada en generación de contenidos y en “organizaciones que buscan una seguridad y un gobierno del dato más robustos, apoyados en IA local en el endpoint”. Aunque asegura que no todos los usuarios necesitarán contar con la última generación de CPU-NPU, y anticipan estrategias de actualización de equipos más fragmentadas que en la actualidad.

De forma similar opina Elena Pérez, de Microsoft, para quien “a medida que más aplicaciones incorporen IA local -desde productividad hasta seguridad o creatividad- la brecha entre dispositivos con y sin NPU será aún mayor, acelerando de forma natural los ciclos de actualización”.

FORO it Digital Security

CONSOLIDANDO LA RESILIENCIA OPERATIVA

@freepik

ORGANIZA

PATROCINADORES GOLD

PATROCINADORES SILVER

COLABORA

UNA TORMENTA PERFECTA PARA LA CIBERSEGURIDAD

EN LA X EDICIÓN DEL FORO DE IT DIGITAL SECURITY HEMOS VISTO CÓMO ORGANIZACIONES DE PERFILES MUY DIFERENTES AFRONTAN RETOS MUY SIMILARES, EN UN MOMENTO EN QUE LA PROTECCIÓN DEL ENDPOINT Y EL NUEVO PERÍMETRO DILUIDO Y LA CAPACIDAD DE RECUPERARSE TRAS UN CIBERATAQUE EXITOSO SE HAN CONVERTIDO EN ELEMENTOS FUNDAMENTALES DE LA SEGURIDAD CORPORATIVA.

Una digitalización acelerada que no ha dado tiempo al personal a interiorizar nuevos procesos laborales; la implantación de nuevos modelos de trabajo que incluyen constantes conexiones remotas; la multiplicación de los dispositivos conectados a las redes corporativas; el despliegue de la IA, en muchos casos con riesgos añadidos para la seguridad de los datos; la mayor sofisticación de las ciberamenazas y su constante aumento; una situación geopolítica que no para de tensarse...

Un combinado muy explosivo, una tormenta perfecta para la ciberseguridad.

En la X edición del Foro IT Digital Security, bajo el eslogan “Consolidando la resiliencia operativa”, hemos querido abordar la compleja situación de la ciberseguridad desde dos perspectivas. Por un lado, cómo se trabaja en la protección del endpoint con esa superficie ampliada y de perímetro diluido, en el observatorio “El endpoint y la

movilidad segura como piezas fundamentales de la resistencia digital". Por otro, cómo se aborda el elemento fundamental de las estrategias de seguridad corporativas, la ciberresiliencia, con el observatorio "Desde Zero Trust hasta los planes de recuperación: las claves de la ciberresiliencia".

LA CAPACIDAD PARA RECUPERARSE TRAS UN ATAQUE, FUNDAMENTAL PARA EL FUTURO

La ciberresiliencia es fundamental en una estrategia de ciberseguridad corporativa que parte de minimizar la posibilidad de que el ataque se produzca... Pero tiene un principio básico: esperar que, antes o después, un ciberataque tenga éxito. La adopción de la resiliencia cibernética depende de factores como el tamaño de la empresa, su sector o sus características propias, como el número de proveedores externos, la presencia de tecnología operativa o la cantidad de colaboradores que acceden a sus sistemas. Pero, en todos los casos, la ciberseguridad y la resiliencia han pasado a formar parte de los imprescindibles que permiten el crecimiento corporativo.

El cambio en las dinámicas de trabajo combina elementos como la IA, la digitalización y el trabajo a distancia, entrelazados entre sí y combinados con los desafíos propios de cada organización. La transformación de la superficie de ataque ha llevado a modelos de ciberseguridad corporativa en constante evolución, en paralelo a la transformación a largo plazo que está suponiendo la digitalización. El puesto de trabajo vive un proceso que no tiene vuelta atrás, en el que se intenta sacar el mayor partido a su propia evolución.

Además de los dos observatorios centrales de la jornada, el X Foro de IT Digital Security ha contado con entrevistas destacadas a Marc Rivero, coordinador del Máster de Ciberseguridad en La Salle; Viktor Kijaško, IT Resiliency director de DHL IT Services; César de la Serna, Cybersecurity lead de Sener; Modesto Álvarez, CISO en el Grupo TSK; y Virginia Vicente, manager de CyberMadrid.

Las presentaciones individuales del foro corrieron a cargo de Javier Sanz, presales manager de Kaspersky; Víctor Pérez de Mingo, presales manager de Veeam; Melchor Sanz, CTO de HP; Daniel Gascón, head of B2B en Motorola Iberia; Miguel López, regional sales director para el sur de Europa en Barracuda; Sergio Martínez, country manager para Iberia de SonicWall; y Tomás Saiz, business project manager para Iberia de Synology. ■

MÁS INFO +

» X Foro de IT Digital Security: Consolidando la resiliencia operativa

Kaspersky Next
XDR Optimum

Amplía las capacidades, no los «presupuestos»

Mejora tu ciberseguridad con
Kaspersky Next XDR Optimum

kaspersky

DESDE ZERO TRUST HASTA LOS PLANES DE RECUPERACIÓN: LAS CLAVES DE LA CIBERRESILIENCIA

Hablamos de cómo reforzar la capacidad de ciberresiliencia de las organizaciones, un elemento básico para su supervivencia en el contexto actual, con líderes de tecnología y ciberseguridad de **Ávoris, DHL IT Services, EADA Business School, Embou, Grupo TSK, MPO** y **Sener**, en un observatorio que ha contado también con la perspectiva de representantes de **Kaspersky** y **Veeam**.

#FOROITDS

DESDE ZERO TRUST HASTA LOS PLANES DE RECUPERACIÓN: LAS CLAVES DE LA CIBERRESILIENCIA

CON CONSTANTES INCREMENTOS EN EL VOLUMEN DE LAS AMENAZAS, CON TIPOS DE ATAQUE CADA VEZ MÁS SOFISTICADOS Y TENSIONES GEOPOLÍTICAS QUE NO PARECE QUE VAYA A AMAINAR, LOS PLANES DE CIBERRESILIENCIA SE HAN EMPEZADO A INCORPORAR EN LAS POLÍTICAS CORPORATIVAS COMO UN ELEMENTO BÁSICO PARA LA ESTRATEGIA DE SUPERVIVENCIA Y DE CRECIMIENTO DE LAS EMPRESAS.

La capacidad de recuperarse tras un incidente de seguridad marca no solo la postura de seguridad de las empresas, sino su futuro. Según los datos del Instituto Nacional de Ciberseguridad (INCIBE), un 60% de las empresas de tamaño pequeño o mediano que sufre un incidente de seguridad grave se ve obligada a echar el cierre en los seis meses siguientes al ciberataque. Para una gran empresa, verse obligada a detener sus operaciones unos días o semana puede ser un golpe duro, pero para la mayor parte de las pymes es definitivo.

La ciberresiliencia es un concepto relativamente nuevo. Hay que tener en cuenta que la propia práctica de la ciberseguridad se ha transformado en la última década, en línea con la transformación de las empresas y los modelos de trabajo hacia entornos más fluidos y menos rígidos. Con muchas empresas digitalizadas, la resiliencia no tiene sentido

“La resiliencia y la continuidad de las operaciones no son una cuestión técnica sino estratégica, y deben estar lideradas desde negocio, conjuntamente con ciberseguridad”
Jesús Dorado, CISO, **Ávoris**

“En ciberresiliencia no todas las soluciones deben ser caras: hay que pensar cómo podemos ayudar con los recursos que hay”
Viktor Kijasko, IT Resiliency director, **DHL IT Services**

“Hay que trabajar mucho en la cultura de la ciberresiliencia para que sea una idea que se asimile y pueda nacer desde dentro”
Marco Peña, CIO, **EADA Business School**

sin la parte ciber y cada vez más compañías están avanzando hacia estrategias de resiliencia que contemplan la parte física y la lógica como un todo.

Como es habitual, el modo en que las compañías se van adaptando a estas nuevas realidades depende de los factores concretos en los que se desarrolla su actividad. En el primero de los observatorios del X Foro de IT Digital Security hemos podido hablar sobre los usos y las claves de la ciberresiliencia con representantes de **Ávoris**, **DHL IT Services**, **EADA Business School**, **Embou**, **Grupo TSK**, **MPO**, **Sener**, en una mesa redonda que ha contado con el apoyo de **Kaspersky** y **Veeam**.

¡SIMULACROS, SIMULACROS, SIMULACROS!

Uno de los grandes consensos de la ciberseguridad es el de la formación. Una formación que tiene más sentido cuanto más práctica es. En el caso de la ciberresiliencia, los planes se tienen que poner a prueba con cierta frecuencia para asegurarse no solo de que funcionan los elementos técnicos, sino los procesos y el reparto de responsabilidades en caso de incidente. Por más claros que estén los conceptos sobre el papel, la realización de simulacros es un elemento básico que no puede faltar en la planificación de la resiliencia.

Javier Sanz, presales manager de Kaspersky, explica que “ya no hablamos de perímetro como hace algunos años, sino que hemos pasado a hablar de identidades. Creo que es fundamental involucrar al comité de dirección en toda la parte de seguridad para que sean conscientes del peligro que supone. No siempre somos capaces de aprender

“Los planes de recuperación y resiliencia son maravillosos sobre el papel, pero hay que probarlos recurrentemente para asegurarse de que no son papel mojado”
Alejandro Velilla, CTO, **Embou**

“Es mucho más difícil conseguir que se cambien procesos de negocio o la cultura de trabajo, que lograr mayores inversiones tecnológicas”
Modesto Álvarez, CISO, **Grupo TSK**

“Lo más importante para la ciberresiliencia es que el consejo de dirección se implique al 100%, tanto personal como económicamente”
Miguel Quintela, CIO/CISO, **MPO**

de situaciones que nos hemos encontrado. Nosotros realizamos simulacros en los que utilizamos casos reales que nos hemos encontrado en Kaspersky. Explicamos, entre otras cosas, cómo tienen que reaccionar. Llevamos los simulacros un poco al límite, apretando a nivel de tiempo y de todo lo que supone, involucrando a todos los equipos, desde el de marketing al de recursos humanos, obviamente a la parte de IT y seguridad. Pero no solo es cosa de tecnología: tu eslabón más débil es el usuario por falta de conocimiento. La concienciación es clave en temas como proteger el dato, las redes sociales, la detección de phishing o las passwords”.

Esos simulacros recurrentes permiten ver los puntos débiles que tienen los planes de ciberresiliencia. También permiten que los consejos de dirección entiendan los riesgos que pueden entrañar los ciberataques que tienen éxito y comprendan que una parte muy importante de la postura de seguridad es la capacidad de recuperarse que tenga la empresa. Una capacidad medible en elementos como el tiempo que puede estar con las operaciones detenidas o sin acceso a determinados datos o servicios. Pero lo que definitivamente contribuye a sensibilizar a una empresa es pasar por la mala experiencia de un ciberataque real.

LA CAPACIDAD DE SOBREVIVIR COMO CASO DE ÉXITO

Miguel Quintela, CIO y CISO de MPO, explicó el impacto que tuvo un ciberataque sobre su compañía en 2019: “Nosotros cambiamos nuestra mentalidad, como empresa, cuando sufrimos un ataque de

“En español, safety and security son lo mismo: un concepto muy bueno, porque la seguridad física y la lógica en estos momentos van de la mano”
César De la Serna Sánchez, Cybersecurity lead, **Sener**

“La seguridad perfecta no existe y seguramente no existirá nunca: lo que tienes al alcance es reducir la superficie de ataque a la que estás expuesto”
Javier Sanz, presales manager, **Kaspersky**

“Solos no podemos resolver nada, somos cada vez más conscientes de que todos necesitamos ayuda y es necesario hablar de ciberseguridad”
Víctor Pérez de Mingo, presales manager, **Veeam**

ransomware. Nos encriptaron todos los sistemas y nos pidieron rescate. Desde entonces hemos tomado conciencia y se ha trabajado mucho porque descubrimos que el plan de continuidad de negocio no funcionó correctamente. El ataque se inició por una factura que ni siquiera era de una empresa con la que trabajábamos. Un usuario abrió el fichero Excel por simple curiosidad. Llevaba una macro que se ejecutó y lo primero que hacía era preguntar si el teclado estaba en cirílico, porque los rusos no pueden atacar a empresas rusas. El ataque nos obligó a montar una empresa nueva, desde cero, en paralelo. Fue un mes y medio muy duro, pero logramos recuperar el 97% de toda la información y sistemas. Es de agradecer la colaboración y apoyo de todos los clientes durante el periodo de la reconstrucción de MPO”.Se trata, sin duda, de un caso de éxito. La compañía fue capaz de sobrevivir a un ataque muy duro gracias a su creatividad y desde entonces ha adquirido un nivel de madurez en ciberseguridad y resiliencia mucho mayor. El ransomware sigue siendo una de las principales amenazas para las empresas. Se va transformando, como todas las ciberamenazas, y va cambiando sus comportamientos, pero un tipo de ataque que no va a desaparecer.

La ciberresiliencia es fundamental en una estrategia de ciberseguridad que parte de minimizar la posibilidad de que el ataque se produzca. Marco Peña, CIO de EADA Business School, señala que, “aparte de proteger toda la parte de cloud, tenemos también mucha infraestructura on-premise. Estamos trabajando, por supuesto, en aportar todas las medidas técnicas posibles: protección

del endpoint, protección del correo electrónico, el firewall o el backup. Pero, sobre todo, estamos trabajando en la detección, en ganar visibilidad, en saber en un momento dado qué está pasando. Cuando pasa algo, cada segundo cuenta. Cuanto antes te des cuenta de que está pasando algo, mucho mejor. Entonces ese es el foco en el que estamos ahora. Pero, obviamente, eso es para luego generar el siguiente paso, que es cómo respondemos lo más rápidamente posible a cualquier eventualidad".

Víctor Pérez de Mingo, presales manager de Veeam, recuerda que "más del 30% de las compañías creen tener un nivel de ciberresiliencia mayor del que tienen. El desconocimiento es algo muy peligroso. La ciberseguridad efectivamente es un proceso de maduración. También se habla de detección temprana y de inmutabilidad. De hecho, una de las primeras cosas que suelen atacarnos es el backup, en el que además en muchos casos todavía no se encripta la información. Otra cosa en la que incidimos mucho es el entrenamiento. Los bomberos no se lanzan a apagar fuego sin haber tenido un entrenamiento previo: ellos entrenan con fuego real. Debemos intentar simular las condiciones de un ataque lo máximo posible. El mayor problema que hay, en todo caso, no es tecnológico, sino de personas, de organización. Y además la IA ha generado una superficie de exposición distinta y requiere una protección distinta. Necesitamos algo que sea capaz de ponerse en medio y revisar lo que hace la IA".

PRESENTACIÓN >> Javier Sanz, presales manager de Kaspersky, explica las capacidades de su solución de detección y respuesta gestionada y extendida. La propuesta de la compañía abarca desde la protección del endpoint hasta la concienciación y la formación de los equipos, reforzando la reducción de la superficie de ataque con el soporte del SOC de Kaspersky y sus motores de IA.

PREPARÁNDOSE PARA LA RESILIENCIA

Viktor Kijasko, IT Resiliency director en DHL IT Services, pone un ejemplo muy práctico del desarrollo de la resiliencia: "Tenemos un equipo dedicado a IT Resiliency y a la gestión de la continuidad de negocio. Con los servicios críticos de todo el grupo. Hemos empezado por identificar qué servicios son los más críticos que tenemos, 13 en total. Después, los equipos de operaciones hacen su Business Impact Analysis y definen qué necesitan para recuperar sus operaciones críticas. Tenemos miles de operaciones, pero no todas son críticas. ¿Qué necesitas recuperar? ¿En qué tiempo? ¿Cuál es el período máximo de caída? Si dicen que es necesario que una operación funcione, ¿qué sistemas críticos la soportan? Y, después, ¿cuáles son las dependen-

cias que tiene? Es difícil gestionar las instancias de automatización. Tienes algo pequeñito que, si no funciona y no se soporta, va a provocar que todo falle. Por eso hay que identificar las dependencias y las consecuencias de un fallo".

El modo en que se afronta la ciberresiliencia depende de factores como el tamaño de la empresa, el sector en el que trabaja y elementos que forman parte de su propia idiosincrasia, como el número de proveedores externos con el que trabaja, la presencia de tecnología operativa o la cantidad de colaboradores que acceden a sus sistemas. Pero, en todos los casos, la ciberseguridad y la resiliencia han pasado a formar parte de los imprescindibles que permiten el crecimiento corporativo.

Alejandro Velilla, CTO de Embou, explica que han vivido "una fase de crecimiento exponencial en la que hemos tenido que ir adaptándonos reactivamente a cómo ha ido el negocio. La parte de IT y de ciberseguridad son elementos muy importantes en el crecimiento, sobre todo cuando está basado tanto en el crecimiento orgánico de tus empresas como en la adquisición de otras que ya tienen un punto de madurez. Cada uno de los terrenos en los que nos metemos es una brecha potencial de seguridad, un nuevo desafío con un tercero. Con la fusión con Orange hemos pasado a una posición de ciberseguridad sólida, con un SOC muy potente. Algo muy importante para controlar y proteger la nueva barrera digital y la IA. No solo con las telecomunicaciones, sino con todas las verticales que tenemos en diferentes entornos, somos de las empresas que más clientes tienen en España. Y eso son datos que, al fin y al cabo, hay que proteger, pero que también se explotan".

PRESENTACIÓN >> Víctor Pérez de Mingo, presales manager de Veeam, detalla el modelo de madurez en la resiliencia de datos de la compañía, que lleva los principios Zero Trust a este elemento clave para la ciberseguridad. El especialista recuerda que buena parte de las organizaciones tienen una confianza en su resiliencia de datos que no se corresponde con sus capacidades reales

Por su parte, Modesto Álvarez, CISO en Grupo TSK, señala que realizan "instalaciones industriales para los clientes, yendo desde el diseño hasta la puesta en marcha y entrega; y, a veces, seguimos con operación y mantenimiento. Tenemos la ventaja de que cada una es independiente respecto a las demás. Pero tenemos dos desafíos de cara a la ciberresiliencia: la visibilidad y la gestión del cambio. Trabajamos en diferentes países y hay diferentes legislaciones, diferentes aproximaciones normativas, diferentes culturas. Esto entra dentro de lo previsible, pero te encuentras también, en algunas ocasiones, con una visibilidad muy limitada de una sola parte. Y los problemas pueden venir de

todas. Respecto a la gestión del cambio, creo que al final tiene que ver con personas y procesos, elementos más complicados que la propia tecnología".

César De la Serna Sanchez, Cybersecurity lead en Sener, explica que en su caso trabajan "principalmente en un mundo muy físico, donde nuestra mayor preocupación son tres elementos: primero las personas, luego los procesos y luego las tecnologías. Protegiendo las tres cosas estamos llegando a un ecosistema amplio, en el que la ciberseguridad parte desde el diseño, desde la concepción. Como ingeniería, nos gusta mucho el dato, nos gusta mucho recoger información para tratarla y buscar puntos de mejora. En el mundo de la ingeniería, antes se decía que, si funciona, no lo toques. Eso ya acabó. Ahora hay que preguntarse: ¿y es seguro? Tenemos unos programas de formación bastante potentes, también para el tema de la resiliencia. No solo los procesos de comunicación internos, sino también ejercicios de simulación de ataques por sector. Otra cosa que nos preocupa es la gestión de la cadena de suministro, porque no todo el mundo tiene la misma conciencia de la ciberseguridad".

UN BÁSICO PARA LA SUPERVIVENCIA

Sea cual sea el sector en el que se mueven las empresas, las interconexiones entre unas y otras son cada vez mayores. No es casualidad que una buena parte de los ciberataques exitosos de los últimos años se hayan generado en las cadenas de suministro. No es casualidad tampoco que las últimas normativas de ciberseguridad se hayan basado en una mejora de la postura de ciberresiliencia. Es el caso de DORA en el sector financiero y de NIS2 en muchos otros entornos.

Pero, por si fuera poco, además de estos marcos normativos en la Unión Europea tenemos la Ley de Ciberresiliencia. Entró en vigor a finales de 2024 y será obligatoria de forma general a finales de 2027, pero ya este año afectará a las obligaciones de información de los fabricantes y a los organismos de evaluación de conformidad, estableciendo unos requisitos de ciberseguridad obligatorios para todos los productos que tengan elementos digitales en su ciclo de vida. Estos marcos normativos en ocasiones se ven como punitivos, pero contribuyen a mejorar la postura de seguridad de todo el tejido productivo.

Jesús Dorado, CISO de Ávoris, recuerda que trabajan "en un amplio ámbito regulatorio, desde NIS2 o el Esquema Nacional de Seguridad hasta las directivas europeas en el ámbito de la seguridad operacional. Lo que intentamos es enfocar la ciberresiliencia y la confianza cero desde la perspectiva de la garantía de funcionamiento facilitando usabilidad y operativa. Para nosotros son muy importantes tanto ZTNA como la resiliencia activa que en conjunto permiten ofrecer al viajero una experiencia ágil, eficiencia y segura. Optamos por un enfoque integral de garantía de funcionamiento asumiendo que vamos en algún momento tendremos que asumir una disrupción para la que estaremos mejor preparados. En definitiva, lo enfocamos desde un punto de vista de negocio, de importancia de las operaciones para cada unidad, intentando homogeneizar las principales acciones de la continuidad de negocio. Y, dentro de esa continuidad, llevamos a cabo acciones tanto de concienciación como de sensibilización".

En 2025, INCIBE gestionó un 26% más de incidentes que el año anterior. Con la mejora de la IA y las tensiones geopolíticas no parece que el volumen de ciberamenazas vaya a disminuir. Solo queda adaptarse. Ya se sabe: no se trata de si te van a atacar sino de cuándo. O incluso de si ya lo han hecho y no te has dado cuenta. La ciberresiliencia es, simplemente, imprescindible para sobrevivir. ■

MÁS INFO +

- Cuándo actualizar de EDR a XDR
- Consolidar la resiliencia operativa: de Zero Trust a la recuperación cibernética
- Cómo anticipar los ciberataques del mañana con Inteligencia Contextual de Amenazas
- Modelo de Madurez de Resiliencia de Datos de Veeam (DRMM)
- Desarrollo de una estrategia de recuperación de datos ciberresiliente

COMPARTIR EN REDES SOCIALES

¿No sabes qué hacer ante los desafíos de la protección de datos?

veeam

Descubre lo nuevo de Veeam Data Platform

Descargando la versión de prueba gratuita

Descarga Aquí

Observatorio IT Digital Security

EL ENDPOINT Y LA MOVILIDAD SEGURA COMO PIEZAS FUNDAMENTALES DE LA RESISTENCIA DIGITAL

Hemos querido conocer de primera mano cómo diferentes empresas afrontan el cambio en su perímetro de seguridad. Para ello hemos tenido ocasión de hablar sobre la transformación de la ciberseguridad corporativa con responsables de tecnología y ciberseguridad de **Capital Energy, EADA Business School, Embou, Holcim** y **Sener**, en un observatorio que ha contado con el apoyo de **HP** y **Motorola**.

#FOROITDS

EL ENDPOINT Y LA MOVILIDAD SEGURA COMO PIEZAS FUNDAMENTALES DE LA RESISTENCIA DIGITAL

CON MODELOS HÍBRIDOS DE TRABAJO BIEN ASENTADOS Y UNA DIGITALIZACIÓN CORPORATIVA EXTENDIDA EN TODO TIPO DE SECTORES, LA PROTECCIÓN DEL PUESTO DE TRABAJO SE HA TRANSFORMADO, OBLIGANDO A LAS ORGANIZACIONES A REFORZAR SUS ESTRATEGIAS DE PROTECCIÓN DEL ENDPOINT.

No hace mucho tiempo, el modelo de la ciberseguridad corporativa se basaba en el llamado bastión: una fortaleza protegida por altos muros, dentro de la cual todo se consideraba protegido. Un perímetro seguro y más o menos fácil de defender. Sin embargo, en la última década, especialmente a partir del 2020, diferentes elementos han contribuido a transformar el paradigma de la seguridad corporativa, hasta el punto de que la palabra perímetro ha empezado a perder su sentido.

El último de esos elementos diferentes es la inteligencia artificial, en sus variantes generativa y agéntica. Dejando de lado la utilización que se hace de ella en la creación de diferentes tipos de ciberataques, el uso interno que hacen las organizaciones de esta tecnología ha ampliado el tipo de riesgos a los que se enfrentan, como el aumento

“Hacemos sesiones de formación departamentales y también píldoras de información más personales, lo que ha mejorado el porcentaje de éxito”
Jorge Crespo, responsable de Operaciones IT, **Capital Energy**

“Las herramientas del endpoint de algún modo son sondas, distribuidas en muchos entornos, con información sobre el comportamiento de los usuarios”
Marco Peña, CIO, **EADA Business School**

“Utilizamos una herramienta de formación interactiva, es una especie de escape room con el que nos aseguramos un mínimo de seguimiento”
Alejandro Velilla, CTO, **Embou**

de las identidades de máquina o las herramientas de IA en la sombra. Pero estos nuevos tipos de IA han llegado en un momento en que el perímetro ya había sufrido una enorme transformación.

La digitalización de numerosos sectores y la expansión de los modelos de trabajo remotos e híbridos ya había hecho su trabajo para transformar la forma en que se gestiona la ciberseguridad en las empresas. Entre otras cosas, cambió el volumen y la tipología de los endpoints que se tienen que gestionar. Hemos hablado sobre la transformación de la ciberseguridad corporativa con responsables de tecnología y ciberseguridad de **Capital Energy, EADA Business School, Embou, Holcim** y **Sener**, en un observatorio que ha contado con el apoyo de **HP** y **Motorola**.

LA TRANSFORMACIÓN DE LA SEGURIDAD DEL ENDPOINT

El cambio en las dinámicas de trabajo combina esos tres elementos: la IA, la digitalización y el trabajo a distancia, elementos entrelazados entre sí. Y, de igual manera que cada organización ha adoptado su modelo de trabajo o las estrategias de IA y digitalización que convenían a su negocio, la adaptación al nuevo escenario de la seguridad ha sido diferente en cada caso. Un buen ejemplo lo pone Jorge Crespo, responsable de Operaciones IT en Capital Energy:

“Hace 7 años, nuestro principal interés era el portátil de la empresa, que tuviera el antivirus o que esté en el directorio activo, entre otras cosas. Y ahora estamos viviendo un cambio. Las

Con las herramientas adecuadas, el trabajo no tiene por qué parecer trabajo

Redefine el futuro del trabajo

“Los ERP antiguos en red son los futuros legacy: en unos 20 años quizá no existirán las redes internas en muchas organizaciones medianas”

Daniel Fernández, global IT security officer, **Holcim**

oficinas se están convirtiendo en espacios de coworking privados; los usuarios pueden trabajar en ellos o donde quieran, con los ordenadores de la compañía. Nosotros nos apoyamos mucho en el acceso condicional. También estamos viviendo los cambios en la convergencia de IT y OT. Antes teníamos un castillo que protegíamos; veías que los aldeanos empezaban a salir cada vez más fuera del castillo. Se llevaban cosas y, al final, se quedaban a vivir ahí”.

“Le estamos quitando el peso de la seguridad al usuario y lo pasamos a la infraestructura, protegiendo toda la superficie de trabajo”

César De la Serna Sánchez, Cybersecurity lead, **Sener**

En mayor o menor medida, todos los expertos en ciberseguridad han vivido este cambio. Esa transformación de la superficie de ataque no es un hecho anecdótico. Siguiendo el ejemplo de la digitalización, el nuevo modelo de la ciberseguridad corporativa no es algo estático, sino que está vivo, sujeto a un proceso de constante evolución. Y, más que otra cosa, las circunstancias propias de cada compañía son las que marcan esa evolución.

PROTECCIÓN DEL PUESTO DE TRABAJO ADAPTADA A LA REALIDAD CORPORATIVA

Marco Peña, CIO de EADA Business School, explica que “traer dispositivos a nuestro entorno está a la orden del día, aunque tenemos una problemática un poco mixta. En la parte corporativa, tienes un cierto nivel de control, con tus herramientas, tu supervisión, tu visibilidad, etc. La otra parte es diferente, es una especie de BYOD un poco más asilvestrado. Para nosotros es capital la supervisión de todos esos dispositivos constantemente en nuestras redes. Son redes de servicio, separadas de la red corporativa, con todos los niveles de segmentación y la supervisión. Y tenemos en marcha políticas de aislamiento de dispositivos: si detectamos un comportamiento sospechoso, podemos aislarlo”.

Por su parte, Alejandro Velilla, CTO de Embou, incide en que “uno de los grandes desafíos que tenemos es que la superficie de ataque incluye a mucha gente que no es de la organización. Nosotros tenemos un gran número de tiendas, con vendedores y comerciales que no son de la casa. Un reto constante porque hemos seguido creciendo. El otro reto es el de IoT, que también se ha ampliado con el despliegue de medio millón de antenas que hay por el mundo, sensores, etcétera, con nuestras SIM. Se calcula que más de un 60% de las incidencias entran por equipos de IoT no gestionados, que no están en una red corporativa. Securizar esos dispositivos es otro de los grandes retos”.

César De la Serna, Cybersecurity lead de Sener, señala que, “al crear, fabricar y desarrollar infraestructuras críticas, requerimos que nuestros empleados tengan un importante grado de movilidad. Por ello estamos cambiando para proteger no solo el dispositivo, sino todo lo que es la superficie del puesto de trabajo. Esto es, entender al usuario en su contexto, con su rol y el riesgo asociado a esa persona. En muchos de los casos, hay que adaptar las reglas a ese empleado que lo necesita. Hay departamentos que sí tendrán reglas comunes, pero eso también requiere por nosotros una agilidad para entender ese escenario. Por ejemplo, cuál es la interacción de entornos industriales y entornos IT, cuál es la gestión de la cadena de suministro. No es lo mismo el equipamiento que se le da a uno de marketing que el que está allí o el que esté probando en campo tecnologías de defensa avanzadas. Proteger la superficie de trabajo con la gestión de la identidad es una de las cosas que más nos importa”.

PROTECCIÓN END TO END

Todos estos cambios en los planteamientos de la ciberseguridad también han afectado a los proveedores tecnológicos, y no solo a los que se dedican específicamente a la ciberseguridad. El trabajo que realizan tiene dos ámbitos: por un lado, el trabajo

PRESENTACIÓN >> Melchor Sanz, CTO de HP, muestra la visión de la seguridad de la compañía en la presentación “Ciberseguridad: los desafíos en los puestos de trabajo híbridos con IA”. Entre otras cosas, detalla la importancia de incorporar una capa de ciberseguridad en el hardware, concibiendo la seguridad no solo desde el diseño sino desde el propio proceso de fabricación”.

“Los ordenadores profesionales tienen características de securización que protegen la cadena de suministro hasta su puesta en marcha: diseño, fabricación y distribución”

Melchor Sanz, CTO, **HP**

interno de su propia seguridad; y, por otro, la protección inherente que deben ofrecer en los dispositivos que fabrican, especialmente los dirigidos al trabajo en los entornos corporativos.

Melchor Sanz, CTO de HP, explica que tienen "una consola que ubica el equipo desde el momento en que se fabrica, aunque no tenga el sistema operativo, haya cambiado o esté guardado en un sótano sin encender... Incluso estando apagado puedes localizar el equipo, borrarlo o bloquearlo. Y es algo que se hace desde el hardware, no con el sistema operativo o el MDM. No se puede ceder el control de la seguridad a una de las capas. Si se cede el control de la gestión de la seguridad al software, pero la capa del hardware está comprometida entonces, ¿para qué sirve? Por eso, llevamos muchos años haciendo securizaciones desde el hardware. Ahora hemos incorporado la herramienta Workforce Experience Platform, que hace muchas cosas más, como medir la experiencia del usuario. No es intrusiva, pero permite controlar el equipo y también ver cómo se está usando. Facilita la seguridad del equipo y la gestión de la información, dando al departamento de IT ese poder sobre el hardware como base sobre la cual se sustentan

PRESENTACIÓN >> Daniel Gascón, Head of B2B en Motorola Iberia, detalla la propuesta de ThinkShield y Motorola for Business para lograr el endpoint ultra seguro. La compañía ha llevado a los móviles corporativos una completa propuesta de seguridad integral, a nivel de hardware y de software, así como una versátil capacidad de gestión y control remoto de la flota de dispositivos corporativos.

"Estamos democratizando el uso de herramientas de productividad y seguridad como MotoSecure, que añaden una capa de seguridad extra"
Daniel Gascón, head of B2B, **Motorola**

el resto de capas, que son el sistema operativo, el antivirus y las aplicaciones".

Por su parte, Daniel Gascón, head of B2B en Motorola, comenta que "ha habido una preocupación alta en el entorno B2B por todo lo relacionado con la seguridad de los dispositivos. Nosotros tenemos un equipo de desarrollo deslocalizado, que hace que evolucionen todas estas soluciones que luego están por encima del sistema operativo. Llevamos cuatro años y medio desarrollando ThinkShield, un nivel de seguridad por encima del que proporciona Android. También creamos nuestro propio MDM, por supuesto, además de una herramienta para controlar actualizaciones de software; la herramienta predictiva Motoanalytics para que, según la salud de los dispositivos, se decidan las actuaciones a futuro que se deben tomar; o Antena Performance, que muestra cómo se comportan los dispositivos, cómo está la batería, el consumo de las aplicaciones, etc".

De cara al futuro, es difícil evaluar los cambios en la ciberseguridad, aunque hay conceptos que parecen claros. Daniel Fernández, global IT security officer de Holcim, destaca "la identidad es un elemento clave para identificar todos los dispositivos y con eso orquestar la defensa de lo que está gestionando el usuario. Independientemente del dispositivo, sea de empresa o no, habrá que incorporar la mayoría de la seguridad de manera transparente. Pero también con prohibiciones serias, dependiendo del dispositivo. En general, o empezamos a controlar todo inventariándolo o va a ser un descontrol. El futuro pasa por prohibir dispositivos personales no securizados. Si quieren utilizar, por ejemplo, el correo corporativo, viene con una serie de implicaciones de seguridad. Y, si no, no podrían utilizarlo".

En todo caso, el puesto de trabajo ha experimentado una transformación que, sea como sea el camino que vaya a tomar, no tiene vuelta atrás. Nadie se plantea, en ningún caso, volver a un escenario anterior. Lo que está sobre la mesa, más bien, es aprovechar el escenario actual, utilizando incluso el endpoint como un sensor capaz de recabar todo tipo de información contextual útil para la organización. ■

MÁS INFO +

- X Foro de IT Digital Security: Consolidando la resiliencia operativa
- HP for Business
- Motorola Business
- Construyendo un endpoint ultra seguro
- Entrevista César De la Serna Sanchez, Cybersecurity Lead de Sener

COMPARTIR EN REDES SOCIALES

motorola

FOR BUSINESS

edge 60 NEO

DISEÑO PREMIUM. DURABILIDAD COMPROBADA.

Diseño compacto pero resistente con protección IP68/69, Gorilla® Glass 7i y certificación militar MIL-STD 810H

50 MP

Cámara principal de de 50MP Sony LYTIA™ y moto ai

Batería de 5000 mAh y carga rápida de 68W

A

MIGUEL LÓPEZ, REGIONAL SALES DIRECTOR PARA EL SUR DE EUROPA DE BARRACUDA

ESCALANDO ZERO TRUST: IDENTIDAD Y CADENA DE SUMINISTRO COMO NUEVO PERÍMETRO

MIGUEL LÓPEZ, REGIONAL SALES DIRECTOR PARA EL SUR DE EUROPA DE BARRACUDA, EXPLICA LA EVOLUCIÓN DE LAS POLÍTICAS ZERO TRUST EN TORNO A LA IDENTIDAD, LOS DISPOSITIVOS, LOS ENTORNOS DE RED, LAS APLICACIONES Y LOS DATOS, DESTACANDO EL RETO OPERATIVO DE ESCALAR ZERO TRUST DE FORMA CONSISTENTE Y COHERENTE EN ENTORNOS HÍBRIDOS.

En la actualidad, la ciberseguridad ha dejado de centrarse en el perímetro tradicional, los límites físicos de la oficina, para enfocarse en los ecosistemas híbridos y distribuidos. Así lo explica Miguel López, regional sales director para el Sur de Europa de Barracuda, quien señala que muchas organizaciones cometen el error de pensar que Zero Trust es simplemente una cuestión de sustituir VPN o reforzar la autenticación. Para el directivo, “el verdadero reto es escalar Zero Trust de una forma coherente en un entorno híbrido” en el que deben convivir infraestructuras on-premise, nubes, usuarios remotos y terceros.

El concepto de seguridad basado en muros, en un modelo de bastión, ha quedado obsoleto.

Como señala el experto, “el perímetro tradicional ya no existe” y se ha desplazado de forma definitiva hacia la identidad digital. Esta identidad no se limita únicamente a las personas; hoy abarca dispositivos, cargas de trabajo y, de forma creciente, las API. En este nuevo escenario, cada acceso debe ser evaluado bajo una verificación que debe ser “continua, no puntual”, analizando quién accede, desde qué dispositivo y en qué contexto.

GRANDES AMENAZAS A LA CIBERSEGURIDAD MODERNA

López destaca como uno de los peligros más críticos detectados en entornos híbridos es la creación de “islas de seguridad”, debidas habitualmente a implantaciones parciales. Por ejemplo, proteger la identidad en la nube pero no en entornos locales genera brechas que los atacantes pueden explotar con facilidad. “Probablemente, una de las mayores amenazas que puede haber a la ciberseguridad es precisamente esta falsa sensación de seguridad”, pues deja múltiples huecos abiertos mientras la organización cree estar protegida.

Otro de los grandes desafíos lo representa la cadena de suministro. La superficie de ataque se ha expandido exponencialmente a través de terceros. En un modelo interconectado, “los ataques a la cadena de suministro ya no requieren vulnerar directamente a la víctima; basta con comprometer un proveedor, un software o una API de tercero”. Si estas identidades externas no se gobiernan bajo los principios de mínimo privilegio y verificación continua, se convierten irremediablemente en el eslabón más débil de la defensa.

Miguel López concluye que “Zero Trust no es un producto, es una estrategia operativa”, concebida en torno a la seguridad de cinco elementos: la identidad, los dispositivos, los entornos de red, las aplicaciones y los datos. Para escalar esta estrategia de manera sostenible, las empresas deben centrarse en tres aspectos clave: tratar la identidad, humana y no humana, como el nuevo perímetro; aplicar el modelo Zero Trust de forma coherente en entornos híbridos, eliminando los silos entre cloud y on-premise; e integrar la gestión del riesgo de la cadena de suministro dentro de todas las políticas de acceso. Al consolidar estas capacidades en una plataforma unificada, las organizaciones no solo reducen su superficie de ataque, sino que mejoran su resiliencia frente a un ecosistema cada vez más complejo e interconectado. ■

MIGUEL LÓPEZ, DE BARRACUDA, CONSIDERA QUE UNA DE LAS MAYORES AMENAZAS QUE HAY PARA LA CIBERSEGURIDAD ES PRECISAMENTE UNA FALSA SENSACIÓN DE SEGURIDAD

MÁS INFO +

- Guía para construir una estrategia de ciberresiliencia
- Por qué una plataforma integral de ciberseguridad supera a las soluciones puntuales
- Zero Trust en entornos híbridos: cuando la identidad y la cadena de suministro se convierten en el nuevo perímetro
- X Foro de IT Digital Security: Consolidando la resiliencia operativa

Barracuda

PROTECCIÓN COMPLETA FRENTE A LOS « CIBERATAQUES »

Managed XDR, protección de email, datos, aplicaciones y redes.

SERGIO MARTÍNEZ, COUNTRY MANAGER DE SONICWALL

CÓMO SABER QUÉ SUCEDE EN TU RED Y SISTEMAS

SERGIO MARTÍNEZ, COUNTRY MANAGER DE SONICWALL, OFRECE UN DETALLADO ANÁLISIS DEL PANORAMA DE AMENAZAS ACTUAL Y LAS NECESIDADES DE PROTECCIÓN DE LAS EMPRESAS, FRENTE A LAS QUE LA COMPAÑÍA OFRECE UNA AMPLIA PROPUESTA DE DETECCIÓN Y RESPUESTA AMPLIADA Y GESTIONADA.

Uno de los mayores retos actuales es gestionar la ingente cantidad de información que generan los sistemas. Sergio Martínez, country manager de SonicWall, utiliza una analogía clara: una casa llena de sensores (cámaras, humo, ventanas) donde, de repente, “el perro ladra y no sabes por qué”. Las organizaciones se enfrentan a una fatiga de alertas donde no siempre es fácil distinguir qué eventos son críticos.

Además, los atacantes aprovechan los momentos de menor vigilancia, como recuerda Martínez: “Casi ocho de cada 10 ciberataques se producen fuera del horario laboral y los fines de semana, típicamente la madrugada del viernes al sábado, porque tienen así 48 horas para explotar”. Una complejidad a la que se suma la inteligencia artificial, utilizada para revitalizar viejos ataques.

En efecto, la IA generativa y agéntica permiten crear phishing extremadamente convincen-

te, localizar sistemas no parcheados (legacy) y automatizar el encadenamiento de exploits. Lo más preocupante es su capacidad para evadir la detección mediante técnicas de ofuscación, esperando el momento oportuno para actuar. Estos elementos crean un escenario con unos niveles de exigencia muy altos, habitualmente fuera del alcance de las pymes.

UN SERVICIO A LAS PYMES A TRAVÉS DEL CANAL

El desarrollo de SonicWall está, de hecho, muy ligado a las pymes, trabajando siempre a través de una red de decenas de miles de socios de canal. Para este segmento la compañía ofrece los servicios de seguridad gestionada soportada desde su SOC europeo situado en Frankfurt. Desde este centro de operaciones de seguridad proporcionan, entre otros, servicios de detección y respuesta gestionados y servicios NOC.

Sergio Martínez recalca la necesidad urgente de modernizar las VPN tradicionales basadas en SSL, que son un vector de ataque frecuente debido a fallos de diseño. La propuesta de la compañía para por evolucionar hacia arquitecturas de Zero Trust (ZTNA) y el uso de Cloud Secure Edge, integrando múltiples factores de autenticación para garantizar un acceso remoto seguro y moderno.

En cuanto a la inteligencia artificial utilizada en tareas defensivas, no se trata de una moda pasajera sino de algo que lleva mucho tiempo nutriendo a las empresas de ciberseguridad. Martínez explica que “hace más de 25 años que utilizamos la IA con nuestros sandboxes avanzados para detectar comportamientos, atípicos dentro de la infraestructura”.

El mensaje final de SonicWall es la democratización de la ciberseguridad avanzada. Su estrategia de “defensa por capas” busca que la capacidad de detectar lo desconocido y responder ante amenazas complejas sea algo asequible, “que todo esto lo pueda pagar una pyme”, permitiendo que cualquier organización, sin importar su tamaño, sea resiliente en el entorno hostil actual. ■

MÁS INFO

- Informe SonicWall Cyber Protect 2026
- Cómo saber qué sucede en tu red y sistemas
- X Foro de IT Digital Security: Consolidando la resiliencia operativa

COMPARTIR EN REDES SOCIALES

TOMÁS SAIZ, BUSINESS PROJECT MANAGER EN SYNOLOGY

BACK-UP & GESTIÓN DEL DATO: NUEVOS RETOS EN LA CONTINUIDAD DE NEGOCIO

TOMÁS SAIZ, BUSINESS PROJECT MANAGER EN SYNOLOGY, DETALLA LOS DESAFÍOS Y LOS RIESGOS DE UN ELEMENTO CLAVE PARA LA CAPACIDAD DE CIBERRESILIENCIA DE LAS ORGANIZACIONES: EL BACKUP. DESDE LA COMPAÑÍA REFUERZAN LA PROTECCIÓN DE LAS COPIAS DE SEGURIDAD CON INMUTABILIDAD, SEPARACIÓN GRANULAR DE PERMISOS Y CREDENCIALES O UNA CAPACIDAD DE RESTAURACIÓN VERSÁTIL, ENTRE OTROS ELEMENTOS.

En un entorno empresarial marcado por la incertidumbre digital, la gestión del dato se ha consolidado como el pilar fundamental de la resiliencia corporativa. Tomás Saiz, business project manager en Synology, detalla en esta presentación la visión integral de la compañía sobre cómo las organizaciones deben afrontar los retos actuales, subrayando que la continuidad de negocio no se limita a responder ante desastres físicos, sino que exige una estrategia proactiva y coordinada.

Uno de los puntos clave que desgrana la ponencia es la necesidad de entender la interrelación entre tres pilares: el backup, la gestión del dato y la continuidad de negocio. El éxito de estos sistemas no reside únicamente en la infraestructura técnica, sino en un concepto humano y organizativo. Saiz destaca que "backup, gestión del dato y continuidad de negocio, son tres conceptos que van muy muy ligados. Y uno de los más relevantes es la orquestación, que no tiene nada que ver con la tecnología, sino que es la inclusión de toda la compañía en esta gestión".

EL ALTO RIESGO DE NO RECUPERARSE TRAS UN CIBERATAQUE

La realidad actual presenta amenazas sofisticadas como la inteligencia artificial en la sombra o los ataques de phishing altamente dirigidos que comprometen la integridad de los datos.

Las consecuencias son severas: se estima que, además del propio incremento en el volumen de los ciberataques el 60% de las pymes españolas no logran recuperarse totalmente tras un ataque, y aquellas que lo hacen tardan una media de 100 días en restablecer su actividad. A esto se suman los riesgos legales, ya que el 32% de estos incidentes terminan en multas y sanciones administrativas.

Frente a este escenario, Synology aboga por una restauración versátil y granular, huyendo de la idea de duplicar infraestructuras completas de forma ineficiente. La clave reside en identificar qué unidades de negocio son críticas y qué datos necesitan realmente para seguir operando. Tal como explica Tomás Saiz, "no se trata de restaurar todo el ecosistema, sino que tenemos que ir a cada una de esas unidades y darles las herramientas que sean necesarias para continuar con su trabajo".

La estrategia de protección del backup se completa con la adopción de la inmutabilidad del dato y la realización de pruebas constantes. La preparación es la única garantía de éxito ante un incidente real, lo que obliga a las empresas a pasar de la teoría a la práctica. En palabras de Saiz: "hay que ensayar de manera que cuando ocurra un incidente todos sepamos lo que tengamos que hacer y quién tiene que intervenir para poder restaurar en tiempo y forma". Esta capacidad de respuesta, sumada a una visibilidad clara del estado de los sistemas, es lo que permite reducir los tiempos de recuperación al mínimo posible, asegurando que el negocio no se detenga ante los riesgos del ecosistema digital actual. ■

MÁS INFO +

- X Foro de IT Digital Security: Consolidando la resiliencia operativa
- Soluciones ActiveProtect
- Contacta con Synology
- De la copia de seguridad a la ciberresiliencia real
- Seguridad en el Dato: Custodia, Confianza y Compliance

COMPARTIR EN REDES SOCIALES

Synology® | DP SERIES

Dispositivos con ActiveProtect 1.2

Impulse la protección de los datos de su empresa al más alto nivel, mientras simplifica su gestión y reduce la carga del equipo.

Fácil de usar

Interfaz intuitiva para empezar en minuntos.

Escalable

Facilita la evolución del sistema y reduce costes.

Seguridad avanzada

Inmutabilidad, WORM y protección completa.

Gestión centralizada

Supervise todas sus cargas desde una única consola.

*Hable con un experto de Synology:

“La protección de la identidad y la higiene digital son básicos para pyme y gran empresa”

Marc Rivero, La Salle

“Necesitamos asegurar que nuestras operaciones siempre están funcionando”

Viktor Kijaško, DHL IT Services

“La ciberseguridad será cada vez más transversal y estará más unida al negocio”

César de la Serna, Sener

“Tenemos que prepararnos para responder, pero tiene que hacerlo toda la empresa”

Modesto Álvarez, Grupo TSK

“Las mujeres no se pueden quedar atrás en un sector que es estratégico para la economía”

Virginia Vicente, CyberMadrid

Consolidando la resiliencia operativa

En la X edición del Foro de IT Digital Security hemos visto cómo organizaciones de perfiles muy diferentes afrontan retos muy similares, en un momento en que la protección del endpoint y la capacidad de recuperarse tras un ciberataque se han convertido en elementos fundamentales de la seguridad corporativa.

FORO it Digital Security

CONSOLIDANDO LA RESILIENCIA OPERATIVA

¡Ver todos los contenidos!

ORGANIZA

PATROCINADORES GOLD

PATROCINADORES SILVER

COLABORA

ENCUENTROS **IT RESELLER**

DESAFÍOS Y OPORTUNIDADES DE LA CIBERSEGURIDAD PARA EL MSP EN 2026

ORGANIZA

it Reseller TECH&CONSULTING

PATROCINADORES

Acronis

ADM Cloud & Services

LOS MSP SE CONSOLIDAN COMO EL EJE DE LA NUEVA CIBERSEGURIDAD EUROPEA

La ciberseguridad vive un reajuste profundo, en el que la inversión se desplaza hacia modelos basados en identidad, plataformas integradas y servicios gestionados. En este escenario, los MSP se convierten en el motor operativo que permite a las organizaciones cumplir, responder y sostener su seguridad en entornos híbridos cada vez más complejos.

La ciberseguridad europea ha entrado en 2026 con un cambio de rumbo evidente. Según los últimos datos de Context, el mercado ha registrado una caída del 4,6% interanual en las primeras semanas del año, un frenazo que no responde a una pérdida de interés, sino a una reorientación del gasto. Las organizaciones están dejando atrás herramientas aisladas para apostar por plataformas integradas, seguridad centrada en la identidad y servicios gestionados capaces de absorber la complejidad operativa y regulatoria que marca el nuevo entorno digital.

El canal corporativo es el que más acusa esta desaceleración, mientras que los resellers pequeños y medianos mantienen el crecimiento. Esta divergencia se produce porque la demanda ya no se mueve por volumen de producto, sino por capacidad de acompañamiento, especialización y servicio continuo. En paralelo, segmentos tradicionales como la seguridad de red o el endpoint retroceden —con caídas del 8% y un descenso sostenido, respectivamente—, presionados por la transición hacia modelos XDR y soluciones SaaS unificadas. Incluso la seguridad del dato, tras años de inversión impulsada por GDPR y eIDAS, cae un 33% al completarse los grandes ciclos de cifrado y cumplimiento.

Frente a este retroceso, emergen áreas de crecimiento. La identidad crece un 25% impulsada por Zero Trust y por la necesidad de proteger identidades humanas y no humanas, mientras que SIEM, SOAR y la gestión de vulnerabilidades avanzan al ritmo que marcan las nuevas obligaciones de reporte y la presión regulatoria.

LA CIBERSEGURIDAD ENTRA EN UNA FASE DE CAMBIO ESTRUCTURAL

Context apunta que Europa está entrando en una fase de “realineamiento estructural”, en la que la seguridad deja de ser un conjunto de capas aisladas para convertirse en un ecosistema integrado, automatizado y profundamente condicionado por la regulación. La combinación de sanciones cibernéticas de la UE, el impulso del Cybersecurity Act 2 y las iniciativas de soberanía digital está empujando a las organizaciones hacia modelos más controlados, auditables y basados en plataformas que integren, automaticen y reduzcan la carga operativa. Quieren seguridad que se gestione, no que se acumule.

En este nuevo tablero, los proveedores de servicios gestionados (MSP) se han convertido en el actor más dinámico del mercado. Mientras el conjunto del sector se con-

trae, los MSP crecen con fuerza: un 72% en Alemania, un 42% en Reino Unido e Irlanda y un 6% en Italia, según Context.

Este crecimiento no es coyuntural, sino que responde a dos fuerzas que se han vuelto estructurales. La primera es la regulación. NIS2, DORA, GDPR, eIDAS y las nuevas normativas nacionales están obligando a las organizaciones a operar con niveles de trazabilidad, reporte y respuesta que solo pueden sostenerse con operaciones 24/7. La externalización ya no es una opción táctica, sino una necesidad para cumplir.

La segunda es la escasez de talento. La brecha de profesionales en ciberseguridad sigue ampliándose, y las empresas no pueden competir en un mercado donde los perfiles especializados son escasos y caros. Los MSP, en cambio, pueden escalar equipos, procesos y plataformas para ofrecer resultados medibles.

Este auge del modelo gestionado encaja de lleno con las conclusiones del estudio global de Westcon-Comstor, que revela que los MSP están encontrando oportunidades de crecimiento sostenido en cloud, seguridad y datos a medida que el modelo híbrido se convierte en el estándar operativo de las empresas. Según el informe, el 23% de los partners identifica la migración y gestión cloud como su mayor oportunidad de ingresos, seguida muy de cerca por la seguridad y la gestión de amenazas (22%).

LAS ORGANIZACIONES ESTÁN DEJANDO ATRÁS HERRAMIENTAS AISLADAS PARA APOSTAR POR PLATAFORMAS INTEGRADAS, SEGURIDAD CENTRADA EN LA IDENTIDAD Y SERVICIOS GESTIONADOS CAPACES DE ABSORBER LA COMPLEJIDAD OPERATIVA Y REGULATORIA QUE MARCA EL NUEVO ENTORNO DIGITAL

Los MSP que mejor están capitalizando esta oportunidad son aquellos capaces de estandarizar, gobernar y empaquetar sus servicios, convirtiendo la integración, la identidad y la automatización en capacidades repetibles y escalables. No se trata solo de implementar tecnología, sino de convertirse en asesores estratégicos. Un 31% de los encuestados afirma que su función más crítica es actuar como guía en la estrategia híbrida del cliente, y un 28% destaca la importancia de la gestión end-to-end de los sistemas.

En suma, la ciberseguridad europea no está en retroceso, sino que está redefiniéndose. Y en esa redefinición, los MSP se han convertido en el pilar que sostiene la operación, el cumplimiento y la resiliencia. La transición hacia modelos basados en identidad, plataformas y servicio no es una tendencia pasajera, sino la nueva normalidad. Las organizaciones que se adapten rápido y los partners que sepan acompañarlas, serán quienes lideren la próxima etapa de este mercado en transformación. ■

DESAFÍOS Y OPORTUNIDADES DE LA CIBERSEGURIDAD PARA EL MSP EN 2026

La ciberseguridad ha dejado de ser un servicio añadido para convertirse en el eje del modelo MSP, tal y como quedó patente en el primer Encuentro IT Reseller Tech & Consulting junto a ADM Cloud & Services, Acronis y ocho de los principales MSP del país. El MSP evoluciona hacia un socio esencial capaz de anticipar riesgos, guiar decisiones y sostener la continuidad del negocio.

ENCUENTRO COMUNIDAD IT >> Hablamos con A3Sec, Grupo Aelis, DICOP Consulting, IaaS365, MR Informática, Serval Networks, TUYÚ Technology y Viewnext, con el apoyo de ADM Cloud & Services y Acronis, para analizar cómo la ciberseguridad está redefiniendo el modelo de negocio de los proveedores de servicios gestionados (MSP).

El primer Encuentro IT Reseller Tech & Consulting reunió a ADM Cloud & Services, Acronis y a A3Sec, Grupo Aelis, DICOP Consulting, IaaS365, MR Informática, Serval Networks, TUYÚ Technology y Viewnext para analizar cómo la ciberseguridad está redefiniendo su modelo de negocio de los proveedores de servicios gestionados (MSP).

La conversación dejó claro que la seguridad ya no es un complemento, sino el núcleo del servicio gestionado. La presión regulatoria, la irrupción de la inteligencia artificial, la escasez de talento y la necesidad de hablar el lenguaje del negocio están transformando el rol del MSP. En este nuevo escenario, la proactividad, la especialización y la honestidad se convierten en los pilares de un mercado que exige criterio y capacidad de anticipación.

LA SEGURIDAD COMO PUNTO DE PARTIDA

La mesa redonda arrancó con una idea que todos compartieron: la seguridad ha dejado de ser un añadido para convertirse en el eje central del modelo MSP.

La demanda del mercado, la sofisticación de las amenazas y la presión normativa han empujado a los proveedores hacia un enfoque más maduro y estratégico. Para Alejandro Agudelo, director Global de Operaciones y Ciberseguridad en A3Sec, “es un momento bastante crítico para el MSP. Se está consolidando en servicios, pero las estrategias de hiperescala y la necesidad de integrar todo nos están empezando a consumir”.

Agudelo insistió en que la presión operativa es real, ya que “a seguridad se le exige que sepa de todo, y que sepa de todo más que nadie”. Esta visión resume bien el punto de inflexión del sector, donde el MSP ya no puede limitarse a operar herramientas, sino que debe sostener una visión global del riesgo, del negocio y de la continuidad.

Uno de los cambios más profundos del mercado es que el cliente final ya no busca tecnología, sino orientación. Quiere entender qué riesgos tiene, cómo afectan a su negocio y qué decisiones debe tomar. Como explicó Óscar Vierge, director de ventas de cuentas estratégicas y director de marketing en Serval Networks, “el cliente ya no te pide que seas reactivo ni que le des logs. Te pide que seas proactivo, que le hables de riesgos y de negocio.”

Clica en la imagen para ver la galería completa

“LA OPERACIÓN DE SEGURIDAD NO PUEDE BASARSE EN INTUICIONES”

ALEJANDRO AGUDELO
Director Global de Operaciones y Ciberseguridad en **A3Sec**

“NUESTRO VALOR ESTÁ EN LA CONSULTORÍA. SOMOS SU DEPARTAMENTO TI”

ÓSCAR CARRILLO
Director Comercial en **DICOP Consulting**

Clica en la imagen para ver la galería completa

Clica en la imagen para ver la galería completa

Gabriel Rus, Sales Manager IT Specialist en Grupo Aelis, reforzó esta idea al recalcar que “la comunicación es la clave. Hay que transmitir a alguien sin conocimientos de ciberseguridad por qué necesita una estructura sólida”. Este giro obliga a los MSP a desarrollar habilidades consultivas, a adaptar el discurso al nivel de madurez del cliente y a convertirse en traductores entre tecnología y negocio.

LA REGULACIÓN COMO MOTOR Y COMO PRESIÓN

La normativa se ha convertido en uno de los grandes aceleradores del mercado. NIS2, ENS, DORA y otras regulaciones están obligando a empresas de todos los tamaños a tomarse la seguridad en serio.

Giacomo Brambilla, Distributor Operations Account Manager en Acronis, destacó cómo la ciberseguridad ha dejado de ser un asunto puramente técnico para convertirse en un elemento central del negocio. “La ciberseguridad ya no es un tema tecnológico, es gestión de riesgo medible. Ya no vale decir tengo esta tecnología para cumplir, sino que, tienes que medir hasta dónde lo estás cubriendo.”

Víctor Orive, CEO de ADM Cloud & Services, desmontó un mito habitual asegurando que “es un error pensar que las pymes no están obligadas. Todas están en la cadena de suministro”. Óscar Vierge añadió un matiz clave, y es que “la regulación es una obligación. Las multas no han llegado aún, pero llegarán”.

Por su parte, José Andrés Félix, director de servicios de ciberseguridad en Viewnext, recordó que el marco regulatorio ya no es negociable y que “la NIS2 no habla solo de sectores críticos. Habla de proveedores esenciales. La seguridad pasa a ser estratégica”.

La regulación está empujando a los MSP a profesionalizarse, certificarse y estructurar sus servicios con mayor rigor, convirtiéndolos en actores imprescindibles para garantizar cumplimiento y resiliencia.

“EL CLIENTE NO QUIERE TECNOLOGÍA, QUIERE QUE TODO FUNCIONE”

GABRIEL RUS,
Sales Manager IT Specialist en **Grupo Aelis**

“EL VALOR SE LO DA EL SERVICIO”

FERNANDO CALVO
Director de Desarrollo de Negocio en **IaaS365**

Clica en la imagen para ver la galería completa

LA IA ACELERA EL CAMBIO

La inteligencia artificial apareció en la conversación como un factor doble: potencia las capacidades defensivas, pero también multiplica la sofisticación de los ataques. Según José María Díaz-Canel, responsable de crecimiento en MR Informática, “la IA condiciona comportamientos que afectan a la seguridad y a la estrategia del negocio”.

La mesa coincidió en que la IA está generando un nuevo tipo de amenaza, más rápida, adaptable y difícil de anticipar. Como señaló Díaz-Canel, “la IA no solo amplifica el riesgo técnico, sino que altera la forma en que las organizaciones toman decisiones”.

Óscar Vierge, recalcó que “con la velocidad de la IA es imposible que un cliente gestione esto solo. La gestión será externa sí o sí”. José Andrés Félix, de Viewnext, añadió que “la IA no es solo un riesgo técnico. Es un riesgo operativo y estratégico que debe estar en la mesa del comité de dirección”.

La IA obliga a los MSP a revisar sus modelos operativos, reforzar su capacidad de análisis y comunicar con claridad qué es realista en un entorno donde la predictibilidad es cada vez más difusa.

Los participantes coincidieron en que la IA también está transformando la demanda del cliente. Muchas empresas buscan orientación para entender qué modelos pueden desplegar, cómo evaluar su impacto en la seguridad y qué implicaciones tiene para la continuidad del negocio. En palabras de Félix, “los clientes no piden tecnología. Piden capacidad experta para pilotarla.”

EL TALENTO SIGUE SIENDO EL GRAN CUELLO DE BOTELLA

Si hubo un punto donde todos coincidieron fue en la dificultad para atraer y retener talento especializado. La rotación, la inflación salarial y la escasez de perfiles senior están tensionando a los MSP.

> “SI EL CLIENTE TE MARCA LA SOLUCIÓN Y TÚ NO PUEDES OFRECERLA, NO TE ESCOGERÁ”

JOSÉ MARÍA DÍAZ-CANEL
Responsable de Crecimiento en **MR Informática**

> “CON LA VELOCIDAD DE LA IA ES IMPOSIBLE QUE UN CLIENTE GESTIONE ESTO SOLO. LA GESTIÓN SERÁ EXTERNA SÍ O SÍ”

ÓSCAR VIERGE
Director de Ventas de Cuentas Estratégicas y Director de Marketing en **Serval Networks**

Clica en la imagen para ver la galería completa

Vierge fue tajante al afirmar que “formas a un joven, lo certificas tres veces y se va al día siguiente porque le pagan el doble.”

La conversación dejó claro que la falta de talento no solo afecta a la operación diaria, sino también a la capacidad de los MSP para escalar servicios, asumir nuevos proyectos y mantener la calidad en un mercado cada vez más exigente.

Además, varios participantes coincidieron en que la presión regulatoria y la complejidad tecnológica están elevando el nivel de exigencia sobre los equipos. Ya no basta con tener técnicos capaces de operar herramientas: se necesitan profesionales que entiendan negocio, normativa, continuidad y riesgo. Como apuntó Vierge, “el MSP tiene que hablar con CIO, CTO y CISO en un lenguaje que entiendan”, lo que obliga a los equipos a desarrollar habilidades híbridas que combinan lo técnico con lo estratégico. Esta evolución del perfil profesional añade una capa más de dificultad a la ya complicada tarea de atraer y retener talento.

¿AGNÓSTICOS O ESPECIALIZADOS?

Uno de los debates más interesantes fue el del agnosticismo tecnológico. ¿Debe un MSP ser neutral o apostar por un conjunto limitado de soluciones? Pues bien, Vierge, afirmó que “nadie es agnóstico. Probamos, comparamos y elegimos líderes.”

Por su parte, José María Díaz-Canel añadió un matiz clave al recalcar que “los partnerships son importantes. Lo que vendemos es nuestra compañía y nuestras personas”. Para él, la confianza del cliente no se construye sobre la promesa de ser

> NUESTRO GRADO DE CONOCIMIENTO LLEGA HASTA UN PUNTO Y A PARTIR DE AQUÍ TIRAMOS DEL FABRICANTE

RAMÓN GARCÍA,
Socio Director en **TUYU Technology**

> NOSOTROS APORTAMOS EL CONTEXTO. EL FABRICANTE APORTA LA VISIÓN TECNOLÓGICA

JOSÉ ANDRÉS FÉLIX
Director de Servicios de Ciberseguridad en **Viewnext**

Clica en la imagen para ver la galería completa

agnóstico, sino sobre la capacidad de demostrar criterio y experiencia real en las soluciones que se recomiendan.

Sobre este respecto, Fernando Calvo, director de Desarrollo de Negocio en IaaS365, aclaró que “si queremos dar un servicio excelente, tenemos que dominar lo que ofrecemos. No podemos permitirnos trabajar con herramientas que no conocemos en profundidad”.

Aun así, la mesa coincidió en que la especialización no debe confundirse con rigidez. Esto implica que, aunque el MSP tenga preferencias tecnológicas, debe ser capaz de adaptar su propuesta al nivel de madurez, presupuesto y necesidades reales del cliente.

Además, varios participantes señalaron que el cliente cada vez llega más informado, o cree estarlo, y que esto obliga a los MSP a justificar sus recomendaciones con datos, comparativas y pruebas de concepto. Como recordó Vierge, la honestidad es clave: “Hay que ser honesto con el cliente. Si tienes dos soluciones en tu porfolio, explícale por qué una es líder y por qué la otra es más accesible”.

Varios MSP coincidieron en que cada vez es más habitual que el cliente llegue con una solución ya elegida. A este respecto, Ramón García, socio director en TUYÚ Technology, comentó que “nos encontramos herramientas ya decididas y algunas no están bien instaladas. En esos casos tenemos que hacer el papel de mediador entre el cliente y el fabricante para conseguir que se parametrice bien la herramienta”.

José María Díaz-Canel añadió que “si el cliente te marca la solución y tú no puedes ofrecerla, no te es-

cogerá". Este fenómeno obliga a los MSP a equilibrar flexibilidad y criterio profesional, actuando como mediadores entre expectativas, capacidades y realidad técnica.

EL SERVICIO COMO VERDADERO VALOR

En un mercado saturado de soluciones, plataformas y fabricantes, el consenso fue unánime: el valor del MSP está en el servicio, no en la tecnología. Como dijo Fernando Calvo, de IaaS365, "el valor se lo da el servicio."

Su afirmación refleja una realidad que todos los participantes reconocieron, y es que la tecnología es importante, pero no es lo que fideliza. Lo que realmente diferencia a un MSP es su capacidad para acompañar al cliente, entender su contexto y sostener su operación en el día a día. Como recalcó Alejandro Agudelo, de A3Sec, "la operación de seguridad no puede basarse en intuiciones. Si no priorizamos bien y no damos contexto al dato, el cliente no entiende el riesgo y nosotros no podemos demostrar el valor del servicio".

Oscar Carrillo, director comercial en DICOP Consulting, reforzó esta idea desde la perspectiva de la pyme, al apuntar que "nuestro valor está en la consultoría. Somos su departamento TI." En su caso, la cercanía y la capacidad de traducir necesidades en soluciones realistas es lo que mantiene la relación con clientes que, de otro modo, no podrían gestionar su infraestructura ni su seguridad.

Clica en la imagen para ver la galería completa

> "LA CIBERSEGURIDAD YA NO ES UN TEMA TECNOLÓGICO, ES GESTIÓN DE RIESGO MEDIBLE"
>
> **GIACOMO BRAMBILLA**
> Distributor Operations Account manager en **Acronis**

Para muchas pymes, el MSP no es un proveedor: es la única estructura tecnológica de la que disponen. "Nuestro trabajo es analizar, recomendar y acompañar. El cliente toma decisiones basadas en nuestra confianza, no en el nombre del fabricante", enfatizó Carrillo.

En la misma línea, Gabriel Rus, de Grupo Aelis, manifestó que "el cliente no quiere tecnología, quiere que todo funcione. Y para eso necesita un MSP que esté encima."

Óscar Vierge, director de ventas de cuentas estratégicas y director de marketing en Serval Networks, añadió que "no se trata de que el cliente compre la mejor solución, sino la que necesita. La fidelización está en la especialización."

Su reflexión apunta a un elemento crítico, y es que el servicio no consiste en desplegar herramientas, sino en saber cuándo, cómo y por qué desplegarlas. La especialización permite al MSP ofrecer un acompañamiento más profundo, anticipar problemas y evitar que el cliente invierta en tecnologías sobredimensionadas o mal ajustadas a su realidad.

En lo que también coincidieron es en que el servicio implica también honestidad y transparencia. Ramón García, de TUYÚ Technology, señaló que "no podemos saber de todo. Nuestro grado de conocimiento llega hasta un punto y a partir de aquí tiramos del fabricante". Esta sinceridad, lejos de restar valor, refuerza la confianza del cliente, que percibe al MSP como un socio que no improvisa ni promete lo que no puede cumplir.

LA RELACIÓN ENTRE FABRICANTES, MAYORISTAS Y MSP SE REDEFINE

Por lo que respecta a la relación entre fabricantes y MSP, también está cambiando, y ya no es una relación

> “LA PYME ESTÁ DENTRO DE LA CADENA DE SUMINISTRO, Y ESO LA OBLIGA IGUAL QUE A CUALQUIER GRAN EMPRESA”

VÍCTOR ORIVE
CEO de **ADM Cloud & Services**

Clica en la imagen para ver la galería completa

jerárquica ni unidireccional, sino un ecosistema interdependiente donde cada actor aporta una pieza crítica. José Andrés Félix, de Viewnext, fue claro al afirmar que “nosotros aportamos el contexto. El fabricante aporta la visión tecnológica”. Esa complementariedad es hoy imprescindible para que las soluciones lleguen al cliente con sentido, con criterio y con un modelo operativo que las sostenga.

La calidad del servicio, la especialización y la reputación del MSP se han convertido en factores decisivos para que los fabricantes seleccionen a sus partners. De hecho, como subrayó Óscar Vierge, de Serval Networks, “ahora muchas veces es el fabricante el que nos elige a nosotros.” Ya no basta con vender licencias: se exige capacidad de implantación, soporte, consultoría y acompañamiento real.

RESPONDIENDO A LOS RETOS DEL SECTOR

VÍCTOR ORIVE, ADM CLOUD & SERVICES

“El mayor desafío de los MSP hoy es incorporarse a las decisiones estratégicas de las empresas”

Según nos explica Víctor Orive, “el mayor desafío de los MSP hoy es incorporarse a las decisiones estratégicas de las empresas para aportarles continuidad de negocio y no incidir tanto en las tecnologías sino en el valor estratégico”.

“Evidentemente”, continúa, “el cumplimiento normativo creo que es el mayor desafío, el mayor reto porque, al final, va a implicar a cualquier tipo de cliente”.

Desde la perspectiva de ADM Cloud & Services, “creemos que la estandarización de los servicios es clave para poder llegar al mercado adecuadamente y nosotros ayudamos a nuestros partners a preparar esta propuesta de forma atractiva y adaptada a la tipología de sus clientes”.

En este punto, varios participantes destacaron también el papel del mayorista, especialmente en un mercado donde la complejidad tecnológica crece más rápido que la capacidad de los equipos para absorberla. El mayorista aporta soporte preventa, formación, acceso a laboratorios, acompañamiento en pruebas de concepto y, en muchos casos, una visión transversal del mercado que ayuda al MSP a tomar decisiones informadas. Su papel es especialmente relevante para proveedores medianos que necesitan acelerar la especialización sin disparar sus costes internos.

La mesa coincidió en que esta escucha activa es fundamental para evitar despliegues sobredimensionados, propuestas irreales o modelos comerciales que no encajan con la madurez del cliente. El MSP es quien está en primera línea, quien conoce el ritmo, las limitaciones y las prioridades reales de cada organización. “El partner conoce al cliente. El fabricante y el mayorista tienen que escucharnos”, recalcó Vierge.

Además, se destacó que la relación ya no se basa solo en la venta inicial, sino en la capacidad de construir un recurrente sostenible. En un modelo de suscripción, donde los márgenes son más ajustados, la fidelización depende de que fabricante, mayorista y MSP trabajen alineados, sin presionar al cliente con módulos innecesarios ni complejidades que no puede asumir. En definitiva, la relación entre fabricantes, mayoristas y MSP se está redefiniendo hacia un modelo más colaborativo, más equilibrado y orientado al valor. El MSP aporta el conocimiento del cliente, el fabricante aporta la tecnología y el mayorista aporta la estructura que permite que todo funcione. Y solo cuando estas tres piezas encajan, el cliente percibe el verdadero valor del servicio gestionado. ■

MÁS INFO +

» Encuentros IT RESELLER Desafíos y oportunidades de la ciberseguridad para el MSP en 2026

Clica en la imagen para ver la galería

Acronis

ADM Cloud & Services

El antivirus ya no es suficiente.

Evoluciona a EDR.

Descubre la promoción

PRINCIPALES TENDENCIAS EN TORNO A LA CIBERSEGURIDAD EN 2026

Analizamos con expertos de la industria cómo está evolucionando el mercado de ciberseguridad en España y otras cuestiones como el impacto que está generando la IA en este segmento y la evolución del canal hacia el modelo MSSP.

DEBATE IT >> Analizamos junto a expertos de ADM Cloud & Services, Exclusive Networks, Ingram Micro, Kaspersky, Serval Networks y SonicWall las principales tendencias del mercado de ciberseguridad en 2026 y los cambios que se están produciendo en este segmento del canal.

El panorama español de ciberseguridad es cada vez más complejo y las empresas deben enfrentar importantes retos relacionados con la sofisticación de los ataques, la adaptación a normativas como NIS2 o los riesgos asociados a infraestructuras más distribuidas. En este escenario, la inteligencia artificial y los servicios gestio-

nados se postulan como los grandes dinamizadores de un mercado que continúa creciendo con solidez. Analizamos estas claves junto a Javier Jurado, director de desarrollo de negocio en Exclusive Networks Iberia; Martín Trullás, director de la división Advanced Solutions en Ingram Micro España; Almudena Álvarez, enterprise partner account manager en Kaspersky España; Oscar Vierge, sales director strategic accounts de Serval Networks España; y Sergio Martínez, country manager de SonicWall Iberia.

Clica en la imagen para ver la galería

PERSPECTIVAS DE CRECIMIENTO EN 2026

El sector en España mantiene un crecimiento sostenido del 14%, con la perspectiva de alcanzar una facturación de 3.000 millones de euros en 2026, impulsado por la transformación de unas 1.800 empresas especializadas. Sergio Martínez, de SonicWall, señala que el mercado se está transformando rápidamente tras la dilución del perímetro durante la pandemia, moviéndose hacia entornos híbridos. Aunque el hardware de red como el firewall sigue siendo una pieza fundamental, Martínez observa que el crecimiento real se desplaza hacia la gestión de la identidad y ZTNA, a lo que se suma la expansión de los servicios gestionados por la escasez de talento. Y advierte que la situación es crítica porque “el campo de batalla ha cambiado totalmente, los ataques son cada vez más sofisticados”.

Por su parte, Javier Jurado, de Exclusive Networks, destaca que su compañía ha superado el hito de los 300 millones de euros de facturación en la región de Iberia. Explica que los clientes están abordando proyectos con un carácter más sistémico, buscando automatización y eficiencia integrada en la operativa del negocio, más que soluciones aisladas, y se muestra optimista para un 2026 en que las organizaciones “buscan más integración, automatización y eficiencia relacionada con la seguridad”.

Desde la distribución, Martín Trullás, de Ingram Micro, subraya que la ciberseguridad es uno de los principales motores de la industria TI, aunque advierte sobre la incertidumbre por la escasez de componentes en la cadena de suministro. Explica que los clientes demandan soluciones completas que abarquen infraestructura y plataforma, y pone en valor que, frente a las crisis que afectan a otros ámbitos, “el mundo de la ciberseguridad tiene unos números bastante robustos”.

Almudena Álvarez, de Kaspersky, posiciona a la ciberseguridad como un sector de valor estratégico dentro del mercado digital global, ante un entorno cada vez más complejo. Resalta que la adopción de la IA y el cloud ha ampliado la superficie de ataque, lo que está disparando la demanda de servicios gestionados y la inversión del canal en capacitación y especialización, ya que “el entorno es cada vez más complejo, vemos que los ciberataques son más sofisticados”.

Finalmente, Oscar Vierge, de Serval Networks, aporta la visión de una empresa que sostiene el crecimiento del mercado a pesar de ser de tamaño moderado. Apunta que España debe consolidar su crecimiento tras haber priorizado la digitalización sobre la protección en años anterio-

ADM
Cloud & Services

¿Tu empresa está lista para cumplir con la NIS-2?

Compruébalo con nuestra auditoría gratuita y además accede a la grabación del **webinar**

Auditoría gratuita

Webinar NIS-2

> LAS EMPRESAS BUSCAN MÁS INTEGRACIÓN, AUTOMATIZACIÓN Y EFICIENCIA RELACIONADA CON LA SEGURIDAD

JAVIER JURADO,
director de desarrollo de negocio en **Exclusive Networks Iberia**

> LA IA GENERATIVA, DEFENSIVA, DE CIBERSEGURIDAD, ES LO QUE AHORA MISMO TIENE MAYOR RELEVANCIA

MARTÍN TRULLÁS,
director de la división Advanced Solutions en **Ingram Micro España**

Clica en la imagen para ver la galería

res. Para él, la normativa es el gran motor de este ejercicio, ya que “la presión regulatoria ahora ya no es una amenaza, es una realidad”.

CIBERSEGURIDAD Y CLOUD

El debate continúa abordando problemas como el fin de los fondos Next Generation y la escasez en la cadena de suministro, que están forzando a las empresas a replantear sus modelos de inversión y acelerar el salto a la nube. Martín Trullás (Ingram Micro) analiza cómo la falta de componentes físicos está convirtiendo al cloud en el principal “salvavidas” para los clientes que no pueden esperar meses por el hardware, y opina que es “el segmento más beneficiado ahora mismo de todo este entorno; aparte de ciberseguridad, es cloud”.

En una línea similar, Javier Jurado (Exclusive Networks) comenta cómo el sector se ha movido significativamente hacia el software y los servicios SaaS, ayudando a mitigar los problemas de la cadena de suministro y proporcionando más previsibilidad.

Clica en la imagen para ver la galería

Sergio Martínez (SonicWall) pone el foco en la explosión de los servicios profesionales, un área donde las consultoras y las “Big Four” están creciendo significativamente. Advierte que la sofisticación de los ataques, potenciados por IA, obliga a las empresas a invertir en defensas que estén a la altura, y comenta que la evolución defensiva es obligatoria porque “los ataques son cada vez más inteligentes y, por eso, las defensas también deben serlo”.

Almudena Álvarez (Kaspersky) coincide en que la escasez de componentes está forzando a muchas compañías tradicionales de infraestructura física a diversificarse rápidamente hacia el software, un proceso que requiere tiempo y una adaptación técnica compleja, que en su opinión “va a hacer que se acelere más la adopción de cloud”.

Por su parte, Oscar Vierge (Serval Networks) introduce la necesidad de

> UNA DE LAS TENDENCIAS CLAVE PARA ESTE AÑO ES LA PROTECCIÓN DE ENTORNOS OT E IOT

ALMUDENA ÁLVAREZ,
enterprise partner account manager en **Kaspersky España**

> EL FUTURO DE LA CIBERSEGURIDAD SE DIRIGE HACIA LA GESTIÓN DE IDENTIDADES Y LA MICROSEGMENTACIÓN

ÓSCAR VIERGE,
sales director strategic accounts de **Serval Networks España**

Clica en la imagen para ver la galería

EL PAPEL DISRUPTIVO DE LA IA

2026 se plantea como el inicio de una nueva era en la ciberseguridad, en la que los agentes autónomos de IA entrarán a formar parte tanto de la ciberdefensa como de los ciberataques, potenciando el modelo de Ransomware as-a-Service. Almudena Álvarez, de Kaspersky, comenta que “ya hay grupos ciberatacantes que ya están utilizando la IA”, obligando a los fabricantes a integrar estas tecnologías en sus herramientas de prevención y análisis.

Sergio Martínez, de SonicWall, explica que “la IA permite hacer un descubrimiento muy rápido de los puntos vulnerables” y encadenar ataques virulentos que son difíciles de detectar para los sistemas tradicionales, lo que pone de relieve el potencial ofensivo de esta tecnología.

Para Oscar Vierge, de Serval Networks, el mayor riesgo proviene de que “la IA va a permitir que el Ransomware as-a-Service se transforme en el Ransomware 3.0”, que emplea la IA para hacer cambios selectivos en datos críticos, en lugar de una simple encriptación, lo que puede ser fatal en sectores como el sanitario. Ante esto, defiende la externalización de SOC que utilicen IA para filtrar el ruido y priorizar las amenazas reales.

Martín Trullás, de Ingram Micro, diferencia entre agentes de IA ofensivos y defensivos, señalando que los errores de configuración en IA de productividad pueden generar fugas de datos masivas accidentales. En este contexto, opina que “la IA generativa, defensiva, de ciberseguridad, implementar estrategias de FinOps para controlar los costes inesperados que puede generar la IA en la nube. Apunta que “el futuro de la ciberseguridad se dirige hacia la gestión de identidades y la microsegmentación”, y comenta que el foco ha cambiado, porque “ya no es el endpoint, es la persona que lo maneja, su identidad”.

EXCLUSIVE NETWORKS

Gestiona presupuestos, facturas, pedidos y compra materiales en un solo lugar.

Hacer negocios con Exclusive Networks ahora es más fácil.

EXCLUSIVE ACCESS

- Acceso a ofertas
- Disponibilidad de stock
- Gestión de usuarios
- Comprar materiales
- Seguimiento de pedidos
- Visor de facturas

¡Únete hoy y descubre Exclusive Access!

es lo que ahora mismo tiene mayor relevancia", y debe ser una prioridad.

A esto, Javier Jurado, de Exclusive Networks, añade un problema de escala demográfica, donde la capacidad para producir agentes de IA autónomos se va a disparar, multiplicando las identidades con potencial de filtración. Y advierte que "la capacidad para producir agentes de inteligencia artificial se va a disparar enormemente".

OTRAS TENDENCIAS A FUTURO

Más allá de la IA, en el sector están ganando fuerza otras tendencias en el ámbito de la ciberseguridad, como los avances en la computación cuántica o la consolidación definitiva del modelo Zero Trust vinculado a la gestión de privilegios. Oscar Vierge (Serval Networks) alerta sobre el potencial de los procesadores cuánticos para descifrar cualquier protección actual, lo que lleva a los atacantes a robar datos hoy para descifrarlos mañana, y dice que "todo lo que no esté cifrado cuánticamente será accesible como si fuera abrir una puerta".

Sergio Martínez (SonicWall) coincide en la aceleración tecnológica que se está produciendo en este campo, como ya se está viendo con la capacidad de la IA de acelerar los plazos de desarrollo. Y también apunta que "muchos ataques acaban robando datos cifrados con la esperanza de poder descifrarlos".

> "LOS ATAQUES SON CADA VEZ MÁS INTELIGENTES Y POR ESO LAS DEFENSAS DEBEN SERLO TAMBIÉN"
>
> **SERGIO MARTÍNEZ,** country manager de **SonicWall Iberia**

Una recomendación clave para Javier Jurado (Exclusive Networks) es la de implementar cuanto antes técnicas "post-quantum" para proteger la información de larga duración frente a esta estrategia de "robar ahora y descifrar después" ya que, en su opinión, estos riesgos exigen una respuesta proactiva por parte de las empresas.

Almudena Álvarez (Kaspersky) explica que en 2026 "una de las tendencias clave es la protección de entornos OT e IoT", extendiendo la seguridad a hospitales y centros de producción hiperconectados. Y subraya que, en este mundo hiperconectado, la concienciación humana sigue siendo el último baluarte defensivo.

A esto, Martín Trullás (Ingram Micro) añade la tendencia imparable hacia el Zero Trust, que considera especialmente necesaria para controlar los permisos que se ceden a los nuevos agentes de IA autónomos. Y cree que este modelo debe avanzar hacia una microsegmentación cada vez más automatizada y ágil.

LA TRANSFORMACIÓN DEL CANAL A MSSP

La evolución del canal hacia la figura del Proveedor de Servicios Gestionados de Seguridad (MSSP) se acelera porque, como comenta Oscar Vierge, de Serval Networks, para el partner el reto es que "crece mucho más rápido la necesidad de talento que la oferta en el mercado". Y señala que esta transformación requiere una eficiencia extrema y el uso de la IA para filtrar la fatiga de alertas, sin multiplicar los recursos humanos.

Almudena Álvarez, de Kaspersky, sugiere que los partners no necesitan construir sus propios SOC desde cero, pudiendo apoyarse en los recursos y analistas que ya ofrecen los fabricantes para dar un servicio global. En su opinión, los clientes valoran cada vez más la capacidad de respuesta ante incidentes por encima de la marca tecnológica utilizada, y les recomienda apoyarse en los fabricantes que ya tienen su SOC.

Por otra parte, Martín Trullás, de Ingram Micro, apunta a una oportunidad exponencial en el mercado pyme, donde el partner ejerce un papel de prescriptor fundamental ante clientes que carecen de conocimientos técnicos avanzados. Considera que la falta

Tu negocio
+ nuestra plataforma
= una experiencia más fluida

INGRAM MICRO®

Distributing Simplicity

de recursos en las pequeñas empresas convierte al proveedor de servicios en una pieza indispensable, y que “el crecimiento en MSP es exponencial porque falta el talento”.

Desde el punto de vista de Javier Jurado, de Exclusive Networks, se está conformando un modelo de servicios compartidos donde el mayorista complementa al partner en aquellas capacidades a las que este no puede llegar por sí solo. Y opina que esta colaboración es clave para que el canal pyme acceda a tecnologías disruptivas de forma rentable.

Finalmente, Sergio Martínez, de SonicWall, destaca el despliegue de SOC que ha hecho su compañía en diferentes geografías para empaquetar servicios de monitorización para el canal medio y pequeño, cuyo objetivo es “facilitar que este SOC esté a disposición de cualquiera, que sea multifabricante”, para que el partner pueda construir sus servicios desde esta base.

CONCENTRACIÓN DEL SECTOR

Tras un 2025 de récords, el mercado de ciberseguridad sigue viviendo un proceso de consolidación mediante adquisiciones estratégicas. Oscar Vierge (Serval Networks) pronostica que las empresas capaces de integrar ZTNA, microsegmentación y gestión de identidad bajo un paraguas de lo que en su compañía denominan “Zero Trust Extreme” serán las que lideren las próximas operaciones.

Para Javier Jurado (Exclusive Networks) las próximas operaciones de adquisición tendrán mucho que ver con la importancia estratégica que está adquiriendo la identidad para las grandes compañías, que quieren ofrecer plataformas unificadas que los clientes puedan absorber con facilidad. Y también señala la explosión de identidades gestionadas por IA como un factor que impulsa este proceso de consolidación.

Almudena Álvarez (Kaspersky) prevé una división clara entre fabricantes globales que adquieren porfolio externo y aquellos que apuestan por el desarrollo interno para la evolución de sus soluciones. Y cree que es estas operaciones “están yendo, en muchos casos, hacia fabricantes súper globales”.

Para Sergio Martínez (SonicWall) el objetivo de muchas de estas compras es el de entrar rápidamente en el segmento de servicios gestionados y captar talento experto que no existe en el mercado, ya que la tecnología es a menudo secundaria frente a la capacidad de servicio.

Y Martín Trullás (Ingram Micro) incide en que la necesidad de los partners de ser más competitivos y ganar capacidad técnica está detrás de este proceso de fusiones sin precedentes, lo que considera la respuesta natural a un mercado que exige especialización y volumen.

ESTRATEGIAS PARA 2026

Para concluir, los participantes exponen sus hojas de ruta para el mercado de ciberseguridad en 2026. Oscar Vierge, de Serval Networks, destaca que su estrategia se centrará en la integración de ZTNA y microsegmentación para sus grandes clientes, buscando cerrar el círculo de la identidad, y afirma que la prioridad es el enfoque selectivo “porque no puedes abarcarlo todo”.

Desde Kaspersky, Almudena Álvarez explica cómo su compañía se ha diversificado hacia la detección y respuesta (EDR/XDR) y la protección de entornos industriales OT, superando su etiqueta tradicional de proveedor de antivirus, lo que facilita la gestión operativa a sus socios.

En Ingram Micro, como comenta Martín Trullás, continuarán con su estrategia de convertirse en un mayorista de plataforma, a través de xVantage, buscando la máxima eficiencia y automatización sin perder la especialización en proyectos complejos. Y resalta que el valor diferencial reside en “nuestro ADN de especialización, de proximidad, de trabajar en proyectos”.

Javier Jurado, explica que Exclusive Networks promoverá la plataformización, los servicios locales y globales, y la introducción de tecnologías disruptivas como la gestión de exposición de vulnerabilidades. Además, señala que “hay una apuesta clara de integración que vamos a promover”, porque la integración es la clave para que el canal absorba la innovación.

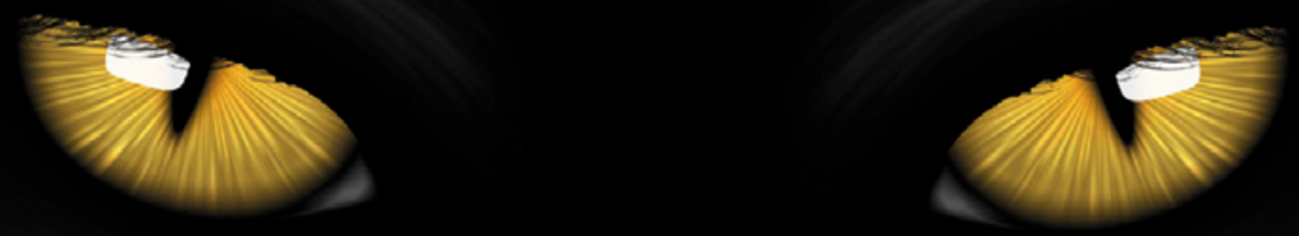
Por último, Sergio Martínez dice que, en SonicWall, “seguiremos impulsando la actualización a la nueva generación 8 de firewalls”, apostando por su plataforma de visibilidad unificada y por el modelo de SOC as-a-Service para el canal SMB. ■

MÁS INFO

» Principales tendencias en torno a la ciberseguridad en 2026

COMPARTIR EN REDES SOCIALES

Con nuestros Servicios de Ciberseguridad



serval NETWORKS

ponemos ojos en la oscuridad del Ciberespacio

www.servalnetworks.com
servalsales@servalnetworks.com

VÍCTOR ORIVE, CEO DE ADM CLOUD & SERVICES

“Estamos centrados en ofrecer plataformas de ciberprotección integrada”

Como parte del Debate IT Reseller Principales tendencias en torno a la ciberseguridad en 2026, conversamos con Víctor Orive, CEO de ADM Cloud & Services, sobre el desarrollo del mercado de ciberseguridad y las principales tendencias que se están desarrollando en este sector. Además, nos explica en detalle las claves de la propuesta de su compañía para este ámbito en 2026.

ENTREVISTA >> Víctor Orive nos habla sobre la evolución del mercado de ciberseguridad y comenta su propuesta para este ámbito en 2026.

EVOLUCIÓN DEL MERCADO

Para Víctor Orive “el crecimiento del mercado español en la ciberseguridad refleja una realidad muy clara”: que “la ciberseguridad ha pasado de ser una inversión tecnológica a una prioridad estratégica de negocio”. Liga este progreso a tres factores: “la adopción acelerada del cloud, el aumento de

la superficie de ataque y el endurecimiento del marco regulatorio".

Percibe que las pymes y medianas empresas "están migrando cada vez más de modelos reactivos a modelos de protección gestionada", y en ADM Cloud & Services se están centrando en "ofrecer plataformas de ciberprotección integrada, que combinan backup, XDR, EDR, protección de identidad, seguridad para el correo y continuidad de negocio, todo ello gestionado desde una plataforma cloud y muy orientada al canal MSP. Porque considera que la inversión de las empresas ya no se centra solo en infraestructuras, como en años anteriores, sino en la resiliencia digital, lo que está impulsando el mercado de plataformas unificadas de ciberprotección, que simplifican la gestión y reducen la complejidad operativa para los equipos de TI y los MSP".

AUGE DE LA IA Y LA IDENTIDAD

La inteligencia artificial es una tendencia destacada en el campo de la ciberseguridad, y Víctor Orive comenta que ya están viendo "campañas de phishing que utilizan IA para generar ataques más sofisticados, automatizar el reconocimiento de sistemas o escalar ataques de forma masiva". Pero también cree que "hay que considerar la IA como una herramienta fundamental para la defensa", aplicando la IA y el machine learning. En ADM Cloud & Services están siguiendo este camino, "incorporando estas capacidades dentro de nuestras soluciones de ciberprotección", permitiendo detectar esas amenazas antes de que afecten a la continuidad de negocio.

Otras tendencias que destaca son el avance de zero trust, el auge del ransomware como servicio, que está industrializando el cibercrimen, y la protección de identidades y accesos. A esto añade la convergencia entre el backup y la ciberseguridad, que considera la clave para la recuperación frente al ransomware; y las plataformas integradas de ciberprotección, que unifican seguridad, protección de datos y continuidad.

En cuanto al canal, ve cómo avanza la tendencia hacia "la consolidación del mercado alrededor de plataformas completas de seguridad", y anticipa que los próximos movimientos de fusiones y adquisiciones probablemente se concentrarán en la identidad y gestión de accesos, en la seguridad del cloud y el cloud nativo, la protección de datos, seguridad de API y aplicaciones, y la inteligencia artificial aplicada a seguridad.

ENFOQUE DE LA CIBERSEGURIDAD

De cara a este año, en ADM Cloud & Services se están centrando en ofrecer plataformas cada vez más integradas, que incluyan backup, protección de endpoint, seguridad cloud y recuperación de desastres en una sola plataforma. Y, como comenta Víctor Orive, tienen un enfoque muy centrado en los MSP, aportando herramientas no solo pensadas para el cliente final, sino también específicas para los MSP. Además, señala, "estamos incorporando capacidades avanzadas de automatización y análisis" de la mano de los fabricantes con los que trabajan. ■

MÁS INFO +

» Entrevista Víctor Orive, ADM Cloud & Services

COMPARTIR EN REDES SOCIALES

> "LAS EMPRESAS NECESITAN SEGURIDAD INTEGRAL EN CLOUD, AUTOMATIZACIÓN MEDIANTE IA, PROTECCIÓN DE IDENTIDADES Y CONTINUIDAD OPERATIVA"
>
> **VÍCTOR ORIVE,**
> CEO de **ADM Cloud & Services**

SONICWALL®

Nunca solo. Seguridad inquebrantable.

Soluciones de ciberseguridad para

- Red
- Nube
- Endpoint
- Servicios XDR gestionados

Descubra cómo impulsar sus ingresos: visite SonicWall.com o escríbanos a spain@sonicwall.com.

PRESENTE Y FUTURO DEL SECTOR DE LAS REDES EMPRESARIALES

El mercado de networking atraviesa una transformación sin precedentes, impulsada por el estándar WiFi 7, la gestión en la nube y la ciberseguridad integrada. Analizamos el progreso que está experimentando el sector, la evolución de este segmento del canal hacia los servicios gestionados y las perspectivas de la industria para este año, con algunos de los principales fabricantes de dispositivos de red.

DEBATE IT >> Analizamos cómo se ha desarrollado el mercado de redes empresariales durante el último año, qué perspectivas maneja la industria para 2026 y cómo están evolucionando el hardware, el software y los servicios de networking, con expertos de Cambium Networks, D-Link, Keenetic y QNAP.

Clica en la imagen para ver la galería

El progreso digital conlleva un uso creciente de las comunicaciones de red y las empresas demandan no solo más velocidad, sino más estabilidad, seguridad y mejores capacidades de gestión para sus redes, lo que está revitalizando el mercado, arrojando buenas perspectivas para el futuro. Aunque el hardware sigue siendo la base, el impulso real proviene de la gestión remota, la inteligencia artificial y los modelos de pago por uso, cuya consolidación está marcando un punto de inflexión en el sector. Debatimos sobre cómo está desarrollándose el mercado en 2026 junto a David Tajuelo, RSM Iberia de Cambium Networks; Anselmo Trejo, marketing manager para Iberia de D-Link; Luigi Salmoiraghi, head of Business Development Europe de Keenetic; y Guillermo Alcover, sales specialist Iberia en QNAP.

BALANCE DE UN 2025 DE CRECIMIENTO

Comenzamos el debate analizando el comportamiento que ha mostrado el mercado español de networking durante el año pasado, incluyendo hardware, software y servicios, cuyas previsiones indicaban que se cerraría el año con un crecimiento cercano al 2%.

David Tajuelo, de Cambium Networks, destaca que para su firma ha sido un año muy positivo, superando las medias del mercado. “Nosotros, en concreto, hemos crecido a doble dígito”. Según explica, el aumento de dispositivos conectados y la demanda de seguridad han sido los motores principales, una tendencia que espera ver reflejada también durante 2026.

Por su parte, Anselmo Trejo, de D-Link, califica el periodo como excepcional y señala que “para nosotros, el año pasado fue un año histórico en cuanto al número de lanzamientos, con más de 50”. Y comenta que la consolidación de su producción y su apuesta por la innovación les ha permitido cerrar el primer trimestre de 2026 con expectativas muy optimistas.

Desde Keenetic, Luigi Salmoiraghi aclara que “España ha crecido en 2025 por encima de la media de los otros mercados europeos”, en parte por la buena utilización de los fondos europeos. No obstante, advierte que parte del crecimiento pudo deberse a un aprovisionamiento preventivo de stock ante la subida de costes logísticos y de componentes, un problema que podría dar la cara en la segunda mitad de 2026.

Finalmente, Guillermo Alcover, de QNAP, subraya cómo el networking ha dejado de ser un accesorio para convertirse en una parte central de su estrategia de almacenamiento. “Es una línea de negocio que está creciendo dentro de la compañía”, y “cada vez ofrecemos más equipos y más grandes”. Y asegura que, para QNAP, la red es ahora el complemento indispensable para evitar cuellos de botella en el manejo de datos.

RETOS Y SUMINISTRO PARA EL 2026

Ante la incertidumbre geopolítica y la actual crisis en la cadena de suministro de ciertos componentes electrónicos, planteamos la cuestión de qué sectores impulsarán la demanda y cómo afectarán estas problemáticas a la disponibilidad y el precio de los equipos. Luigi Salmoiraghi (Keenetic) muestra su preocupación por el mercado de memorias, cuyo coste se ha multiplicado de forma alarmante en pocos meses. Y advierte que, aunque los fabricantes

> EL MODELO MSP NO ES SOLO UNA OPCIÓN, SINO UNA NECESIDAD DE SUPERVIVENCIA PARA EL PARTNER

DAVID TAJUELO,
RSM Iberia de
Cambium Networks

> LA CONMUTACIÓN MULTI-GIGABIT ES VITAL PARA EVITAR CUELLOS DE BOTELLA EN EQUIPOS CON WIFI 7

ANSELMO TREJO,
marketing manager para
Iberia de **D-Link**

Clica en la imagen para ver la galería

han amortiguado el impacto inicialmente, la subida llegará inevitablemente a la pyme y complicará las licitaciones públicas de precio cerrado.

David Tajuelo (Cambium Networks) coincide en que la situación es compleja porque a los ciclos habituales de escasez se suman otros factores que no estaban presentes en anteriores crisis. “En ese cóctel no había una guerra, no había un corte de un estrecho que ve pasar el 90% de todos esos componentes”, comenta, y afirma que esta incertidumbre global impide realizar pronósticos certeros a corto plazo.

Anselmo Trejo (D-Link) prefiere mantener una postura optimista apoyada en la capacidad de previsión de su canal de distribución, que “tiene esa buena costumbre, en cuanto al sell-in, de estocar”. Además, destaca las buenas previsiones de ventas para sectores como el hotelero, que tiene previsión de añadir más de 300 nuevos establecimientos este año, y donde la infraestructura WiFi y LAN será fundamental. A esto, suma el incremento de

Clica en la imagen para ver la galería

contrataciones en el sector tecnológico, que requerirán mayor conectividad y podrían contribuir a las ventas generales del mercado.

Guillermo Alcover (QNAP) advierte que el problema de los componentes no solo afecta al precio, sino a la viabilidad de proyectos a largo plazo, por falta de producto. Y señala que “aunque hayamos intentado provisionar, llega un momento que no hay producto y es un problema a largo plazo”. En su opinión, esto podría ralentizar la renovación de infraestructuras que dependen de estas memorias y soluciones de almacenamiento.

SERVICIOS DE GESTIÓN AVANZADA

Como ya está sucediendo en otros segmentos del mercado tecnológico, los servicios basados en la nube están revolucionando el mercado de redes empresariales. La mayor complejidad de la infraestructura tecnológica requiere una gestión avanzada que las empresas no siempre pue-

www.cambiumnetworks.com

ONE NETWORK

Conexiones fiables y seguras en todos los sectores empresariales

> LO QUE NECESITA LA PYME ES ESTABILIDAD DE CONEXIÓN, SEGURIDAD Y ACTUALIZACIÓN DE SU RED

LUIGI SALMOIRAGHI,
head of Business Development Europe de **Keenetic**

> LOS FABRICANTES DEBEMOS HACER QUE EL MENSAJE DE LA SEGURIDAD VAYA CALANDO

GUILLERMO ALCOVER,
sales specialist Iberia en **QNAP**

den lograr por sí solas, lo que pone el foco en las ventajas de los servicios gestionados, bajo el modelo de Networking as-a-Service.

Luigi Salmoiraghi, de Keenetic, observa un cambio profundo en la mentalidad del distribuidor, que ahora prioriza la gestión sobre el hardware, y prevé “un cambio de modelo... que en lugar de que se adquiera el bien físico, se disfrute de este bien a través de servicios MSP”. Y opina que la necesidad de capital circulante para estocar está empujando a muchos socios hacia este modelo.

En opinión de Anselmo Trejo, de D-Link, la administración de red como servicio es una demanda creciente, especialmente en pymes sin departamento informático propio. Comenta que “la administración de red se puede contratar como servicio añadido”, y que su plataforma Nuclias Unity permite a los partners gestionar redes de forma remota y cobrar por ese soporte, asegurando la continuidad del negocio del cliente final.

David Tajuelo, de Cambium Networks, sostiene que este modelo no es solo una opción, sino que “el partner debe migrar a un modelo de MSP, más que nada, por asegurar su propia supervivencia”. Y explica que la obsolescencia de gran parte de la infraestructura instalada hace años en España representa una oportunidad única para renovar, que podría impulsar este paradigma de servicios en la nube.

EL SALTO AL WIFI 7 Y MULTI-GIGABIT

La tecnología de redes continúa evolucionando para proporcionar no solo más ancho de banda, sino más estabilidad, seguridad y capacidad multidispositivo. En opinión de Guillermo Alcover, de QNAP, la convergencia entre red y seguridad, además de la necesidad de mayores anchos de banda para las nuevas modalidades de trabajo, están siendo importantes motores para el mercado. A esto, añade que “hay una integración cada

vez mayor de la ciberseguridad en las redes", y que los requisitos de latencia y volumen de datos están obligando a adaptar toda la infraestructura.

Anselmo Trejo, de D-Link, pone el foco en la necesidad de evitar cuellos de botella mediante el uso de conmutación multi-gigabit ya que, "si enchufas lo antiguo a un puerto gigabit... le estás creando un cuello de botella bastante grave". Y cree que la demanda de WiFi 7 y las conexiones 5G para zonas sin banda ancha fija son importantes tendencias que marcarán el devenir del mercado este año.

Desde su punto de vista, Luigi Salmoiraghi, de Keenetic, matiza que, más allá de la velocidad pura, "lo que necesita la pyme es estabilidad de conexión, seguridad y actualización de su red". Y opina que el cumplimiento de normativas como NIS2 obliga a mantener actualizados y convenientemente parcheados sus equipos, por lo que en su compañía se enfocan en ofrecer al cliente y al partner un sistema operativo que no solo permite sacar partido de todas las capacidades del hardware, sino que garantiza la seguridad y facilita la gestión de la red.

David Tajuelo, de Cambium Networks, añade la visibilidad como un factor crítico para poder remediar problemas antes de que afecten al servicio. Asegura que "la seguridad de la red empieza por la propia red" y aboga por proporcionar herramientas basadas en inteligencia artificial que aprendan de los patrones de tráfico y ayuden al administrador a reducir los tiempos de resolución de incidencias.

Clica en la imagen para ver la galería

SEGURIDAD Y GESTIÓN INTELIGENTE

La seguridad se ha convertido en un pilar fundamental de las redes empresariales, un ámbito en el que conceptos como zero trust han cobrado una importancia capital. David Tajuelo (Cambium Networks) propone integrar herramientas inteligentes directamente en las plataformas en la nube donde, en su opinión, "puedes montar pequeñas herramientas basadas en machine learning" para automatizar tareas como la segmentación de red según el tipo de dispositivo, mejorando la productividad y eficiencia del equipo técnico.

Anselmo Trejo (D-Link) incide en la importancia de la concienciación y la formación, ya que muchos fallos de seguridad provienen del factor humano. En su opinión, "no hace falta ser ingeniero informático para crear una segmentación de red", pero lamenta que todavía existan redes empresariales sin segmentar. Por ello, apuesta por la evangelización del canal a través de certificaciones y campañas para los partners.

Guillermo Alcover (QNAP) coincide en que el riesgo siempre estará presente debido al factor humano, por lo que los fabricantes deben simplificar la protección. "Es un trabajo que debemos hacer los fabricantes", apunta, "para que vaya calando cada vez más en el mercado", y considera que el objetivo es ofrecer soluciones que reduzcan al máximo el riesgo y lo hagan de forma transparente para la empresa.

HACIA REDES MÁS RÁPIDAS Y CON IA

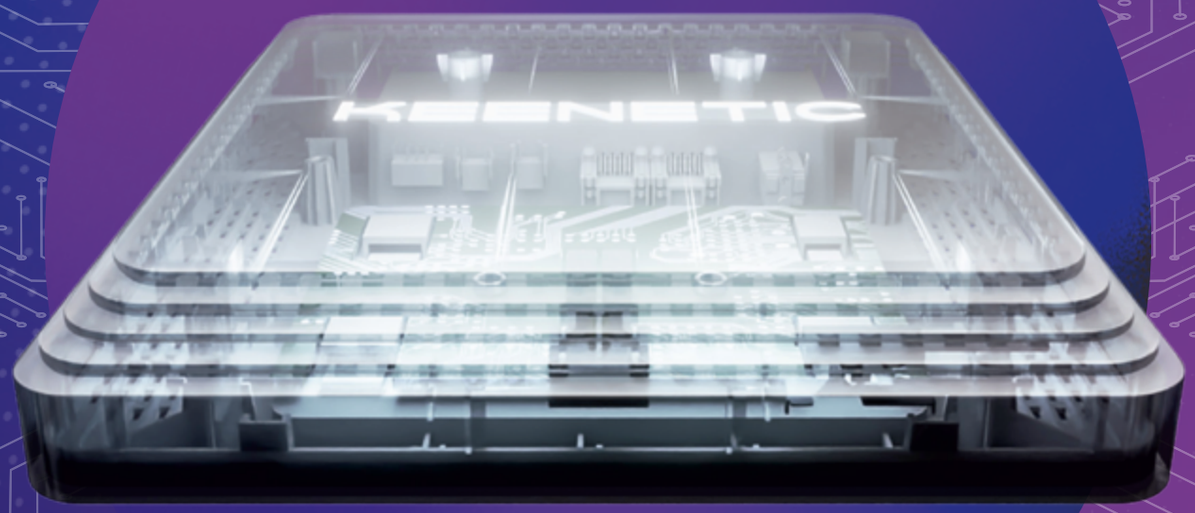
Otras tendencias clave en el sector de las redes de datos son la expansión de la inteligencia artificial en los ecosistemas tecnológicos y el crecimiento de los entornos IoT, dos factores que impulsarán el aumento

KeeneticOS

KeeneticOS: el corazón de una conexión fiable, hecho simple para todos, cada día

Sistema operativo modular con seguridad integrada, fiabilidad y control remoto

- Gestiona desde cualquier lugar
- Monitorización de tráfico DPI
- Conecta cualquier dispositivo fácilmente
- Rendimiento ultra fiable
- Preparado para TR-069
- Respaldo Multi-WAN
- Seguridad y control
- Simplicidad y eficiencia



KEENETIC

Más información en keenetic.com

del ancho de banda y la demanda de equipos multi-gigabit. Al mismo tiempo, la IA tiene su propio papel en la gestión y optimización de las redes.

Anselmo Trejo, de D-Link, recalca que el estándar Gigabit se ha quedado obsoleto para las demandas actuales de WiFi 6 y 7, que requieren más ancho de banda. Asimismo, opina que la IA ya está ayudando en procesos de gestión de red, optimizando canales y potencias de forma automática para reducir la carga de trabajo a los administradores.

Desde el punto de vista de Luigi Salmoiraghi, de Keenetic, muchas funciones que se atribuyen a la actual IA ya existían bajo otros nombres, pero reconoce que la evolución de esta tecnología hasta el nivel actual permite un análisis de patrones mucho más rápido y efectivo, y su impacto en las redes seguirá expandiéndose en el futuro.

Guillermo Alcover, de QNAP, confirma que el mercado ya está adoptando el estándar de 2,5 Gbps, incluso en gamas de entrada, y señala que "el gigabit no es un estándar. Estamos en dos y medio". Aunque aclara que actualmente nos encontramos en un periodo de transición complejo, debido a la convivencia de las tecnologías más avanzadas con infraestructuras legacy a las que todavía es necesario dar soporte.

Por su parte, David Tajuelo, de Cambium Networks, destaca que la red ha vuelto al primer plano porque es el cimiento de todo lo demás. En su opinión, "no solo se trata de dar esa velocidad, sino de gestionar esa densidad de usuarios", y cree que la llegada de dispositivos con IA integrada obligará a evolucionar no solo el WiFi, sino toda la capa de acceso y core hacia el multi-gigabit. También menciona la integración de satélites de órbita baja como un nuevo punto de comunicación clave para las redes en ciertos escenarios.

ESTRATEGIAS Y NOVEDADES PARA 2026

Para finalizar, los cuatro portavoces detallan los pilares de su estrategia y los lanzamientos que realizarán a lo largo de este año. Guillermo Alcover explica que en QNAP van a incorporar soluciones MDR en su gama de switching para elevar la seguridad de la red. También se enfocarán dispositivos de networking que apoyen a sus soluciones de almacenamiento, en funcionalidades a nivel de copia aislada y en "que nuestros switches y routers sean capaces de gestionar los puertos de los equipos para aislar otros equipos de la red y dar un plus de seguridad".

Luigi Salmoiraghi, de Keenetic, destaca el reciente lanzamiento de KeeneticOS 5, "que aporta mucha más seguridad y más servicios, sobre todo para profesionales y para mercado de consumo", y la ampliación de su catálogo de routers WiFi 7 con una gama más "entry level". Además, a mediados de año completarán su oferta con switches no gestionables diseñados específicamente para las necesidades de la pyme, a los que se sumarán modelos gestionables a comienzos de 2027.

Anselmo Trejo explica que en D-Link apuestan por la plataforma gratuita Nuclias Unity "que permitirá la gestión de todos los equipos, desde el extremo hasta el core, las capas de switching y wifi, con muchas herramientas, multisede, multitenant...". A esto se sumarán lanzamientos de nuevos equipos WiFi 7 y switches multi-gigabit, y un crecimiento de las soluciones machine to machine y 5G, categorías en las que están creciendo mucho. Además, quieren abordar el segmento Enterprise de micro data center, y seguirán "apostando por el canal, con "roadshows para acercarnos a nuestros clientes y presentarles todas estas novedades".

Por último, David Tajuelo destaca que en Cambium Networks seguirán haciendo hincapié en lo que denominan "red daltónica", con CN Maestro, que permite ver todo lo que sucede en la red, para "detectar, analizar y remediar absolutamente cualquier incidencia que pueda surgir". Además, van a ampliar su catálogo de WiFi 7 y switches, dando "mucha importancia al MLAG como solución para el stacking físico", reforzando la apuesta por el multi-gigabit y por las redes SD-WAN, que considera un importante foco de crecimiento para 2027. A esto suma la mejora de ciberseguridad, de servicios de internet y la integración con los servicios satelitales de Starlink y los de Kuiper, entre otros, cuando salgan al mercado. ■

MÁS INFO +

» Presente y futuro del sector de las redes empresariales, a debate

COMPARTIR EN REDES SOCIALES

Luigi Salmoiraghi, head of Business Development Europe de Keenetic

“NUESTRA PROPUESTA DE VALOR ESTÁ PENSADA PARA EL CLIENTE EUROPEO Y ESPAÑOL, FUNDAMENTALMENTE PYME”

Tras el debate de IT Reseller ‘Presente y futuro del sector de las redes empresariales, conversamos con Luigi Salmoiraghi, head of Business Development Europe de Keenetic, para conocer su punto de vista sobre la evolución del mercado de networking y las claves de su propuesta para el mercado en 2026.

Comenta que el mercado español de redes empresariales ha vivido un 2025 muy bueno, con cifras superiores a la media europea, y que los primeros meses de 2026 están siendo buenos para el canal, en cuanto a las ventas de infraestructura, de redes y servicios. Reconoce que existe preocupación a causa del creciente coste y la escasez de suministro de componentes informáticos, y que la incertidumbre ha aumentado en las últimas semanas por el conflicto el Oriente Medio. Pero aclara que el stock existente en el canal y las compras realizadas a precios antiguos harán que los posibles problemas no se manifiesten en el canal hasta la segunda mitad del año, y que en cualquier caso las perspectivas son buenas, ya que existe una fuerte demanda de conectividad en el mercado.

El motivo es la necesaria actualización de las redes que las pymes compraron durante la pandemia, por lo que considera que “es el momento perfecto para actualizar la red e incorporar servicios que hace 5 años no estaban disponibles”, por ejemplo, tecnología WiFi 7 y mejoras de red que provienen de los nuevos sistemas operativos, como KeeneticOS 5.

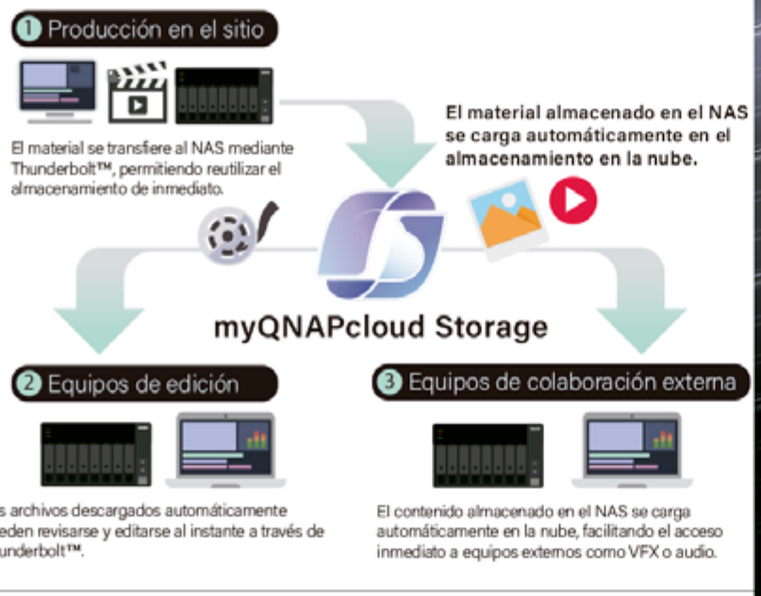
Precisamente, en Keenetic han puesto el foco en mejorar su sistema operativo que, en sus palabras, “garantiza una optimación de los componentes hardware y una gran estabilidad, sobre todo en router y access point”. Además, explica que este año van a ampliar la gama de router con equipos WiFi 7, tanto entry level como de una gama superior, así como puntos de acceso para exterior e interior, equipos pensados para hoteles y una nueva gama de WiFi 5, 6 y 7. Y destaca especialmente el hito de los switches no gestionables a finales del primer semestre, a los que añadirán switches gestionables a comienzos de 2027. En resumen, dice, “vamos a tener una propuesta de valor pensada para la tipología de cliente europeo y español, fundamentalmente pyme”, que constituye el 90% del tejido empresarial español.

QNAP

Cree un flujo de trabajo multimedia flexible con un solo NAS de QNAP

Comparta material de producción de forma remota y habilite la colaboración en tiempo real sin limitaciones de ubicación.

QNAP NAS permite a los equipos creativos capturar, editar y compartir contenido de manera eficiente en múltiples ubicaciones, desde la ingesta en el sitio hasta la colaboración remota.



Conectividad Thunderbolt™ de alta velocidad

Thunderbolt™ 4 ofrece velocidades de hasta 40 Gbps, incluso sin una infraestructura 10GbE.

Edición 4K en tiempo real con caché SSD NVMe

La caché SSD NVMe PCIe Gen 4 proporciona edición 4K fluida y de baja latencia.

Carga automática a la nube con HybridMount

Los archivos del NAS se cargan automáticamente a la nube sin intervención manual.

Compartición de medios basada en la nube

El contenido en la nube se descarga y almacena en caché automáticamente en cada NAS de edición.

QNAP

High Availability Manager

Maximice el tiempo de actividad del servicio con la conmutación automática por error

Menor costo total de propiedad (TCO)

Ofrece alta disponibilidad de nivel empresarial para pymes y entornos profesionales, sin la complejidad ni el costo de las infraestructuras HA tradicionales.

Gestión simplificada del clúster HA

Una interfaz de administración intuitiva permite a los administradores supervisar el estado del clúster, gestionar procesos de failover y mantener visibilidad total del entorno HA.

Sincronización de datos en tiempo real con SnapSync

Mediante SnapSync, los datos se sincronizan en tiempo real entre los nodos activo y pasivo, garantizando RPO = 0 y coherencia continua de los datos.

Tiempo de inactividad mínimo con failover rápido

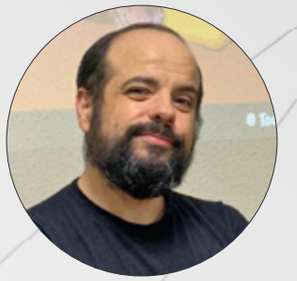
Ante una falla, los servicios se transfieren automáticamente al nodo pasivo en menos de un minuto, logrando un RTO inferior a 60 segundos y una disponibilidad casi continua.

Para más información, contáctenos en sales@qnap.com

JOSÉ MANUEL NAVARRO
experto en Marketing

LA "REARQUITECTURA" DEL ECOSISTEMA DE PAGOS: INSTANTÁNEO, SOBERANO Y AUTÓNOMO

LORENZO MARTÍNEZ RODRÍGUEZ
experto en ciberseguridad



JUANITO TIENE EL PODER (Y TÚ NO)

MANUEL LÓPEZ
asesor de Comunicación

DATOS SIN MEMORIA: CUANDO LA COMUNICACIÓN CORPORATIVA SABE QUIÉN ERES, PERO NO RECUERDA QUIÉN HAS SIDO

DANIEL PÉREZ LIMA
experto en ciberseguridad

ATENCIÓN: SPOOFING/PHISHING USANDO INVITACIONES ICS

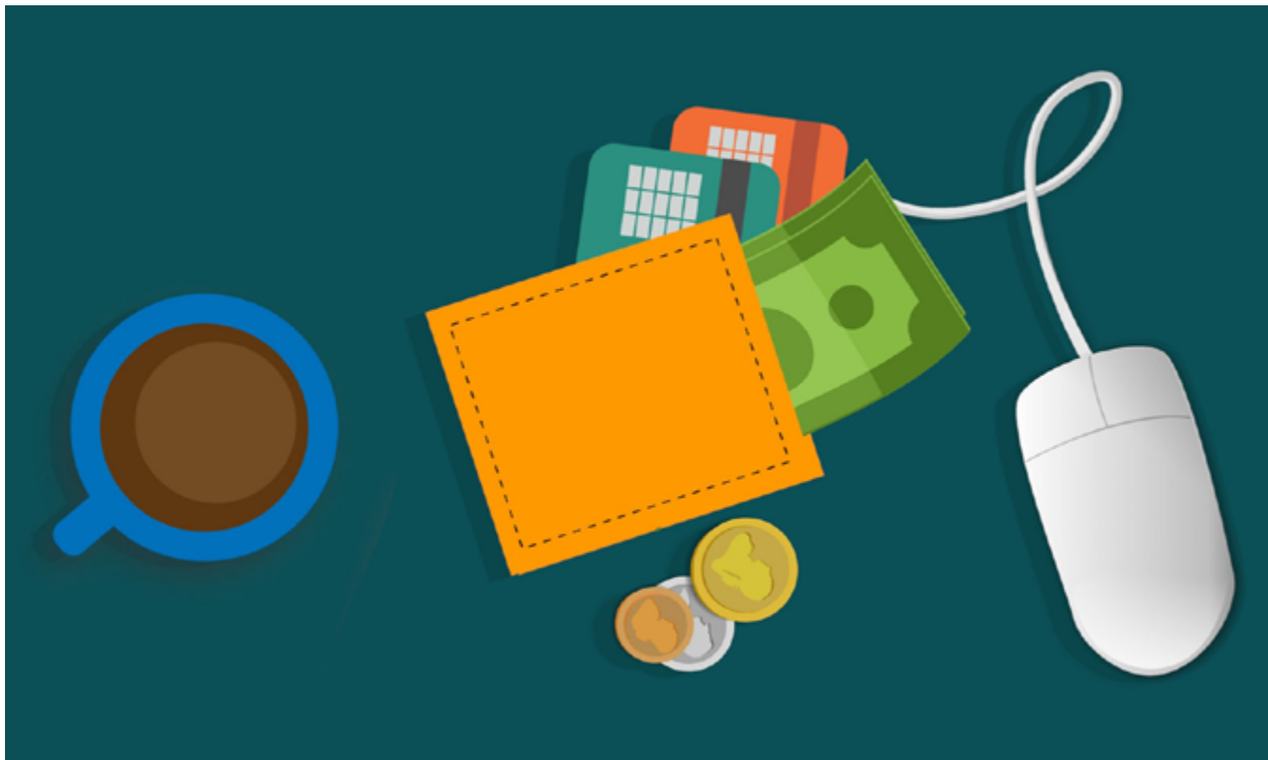
JOSÉ MANUEL NAVARRO
Experto en marketing

Su vida profesional la ha dedicado principalmente al sector financiero, donde ha desempeñado funciones como técnico de organización de procesos y como directivo de marketing. Y, basándose en su formación en Biología, ha profundizado en las neurociencias aplicadas a la empresa, lo que le ha permitido dirigir, coordinar e impartir formación en diferentes masters de neuromarketing en escuelas privadas y en universidades públicas nacionales e internacionales. Ha sido socio fundador de diversas empresas y de la entidad de dinero electrónico con licencia bancaria otorgada por el Banco de España SEFIDE EDE, de la que en la actualidad es director de Estrategia y Marca. Es autor de “El Principito y la Gestión Empresarial” y “The Marketing, stupid”.

LA “REARQUITECTURA” DEL ECOSISTEMA DE PAGOS: INSTANTÁNEO, SOBERANO Y AUTÓNOMO

El mercado de pagos en Europa atraviesa la transformación más disruptiva de su historia al experimentar, además de un acelerado proceso de innovación tecnológica, la “rearquitectura” completa de su infraestructura financiera. La convergencia del marco regulatorio europeo, el auge de la inteligencia artificial agentica, la consolidación de sector Fintech y la búsqueda de una soberanía estratégica frente a los gigantes tecnológicos está reconfigurando los cimientos de la economía digital del segundo cuarto de siglo. Mientras que los canales tradicionales de efectivo, tarjetas y transferencias definieron las siete décadas anteriores, el horizonte de 2026 a 2030 pertenece a los pagos instantáneos de cuenta a cuenta (A2A), las carteras digitales unificadas y los protocolos nativos de internet que permiten a las máquinas transaccionar de forma autónoma.

El comportamiento del consumidor europeo muestra una trayectoria clara hacia la desvinculación del dinero, aunque el ritmo de esta transición varía profundamente según la geografía y la cultura de adopción de los medios de pago. Según el estudio SPACE 2024 del Banco Central Europeo, el uso de efectivo en los puntos de venta físicos ha caído del 59% en 2022 al 52% en 2024 en términos de número de transacciones. A pesar de este declive, el efectivo sigue siendo una herramienta fundamental para la inclusión y la privacidad, especialmente en transac-



LA GRAN PREGUNTA PARA LOS PRÓXIMOS CINCO AÑOS ES SI LAS REDES DE TARJETAS PODRÁN MANTENER SU DOMINIO FRENTE AL ASCENSO DE LAS NUEVAS SOLUCIONES IMPULSADAS POR LOS PAGOS A2A

ciones de bajo valor y pagos entre personas, donde representa el 41% de los movimientos.

ENTORNOS HÍBRIDOS DE PAGO

La dualidad entre la eficiencia digital y la tangibilidad del efectivo ha creado un entorno de pagos híbrido en el que un 62% de los ciudadanos considera vital que los comercios sigan aceptando efectivo, una percepción que ha crecido ligeramente debido a las preocupaciones sobre la privacidad y la gestión del presupuesto doméstico en tiempos de incertidumbre económica. Sin embargo, la balanza del valor (volumen de €) se ha inclinado definitivamente hacia lo digital. En términos de valor total de las transacciones, las tarjetas ya superan al efectivo (45% frente al 39%), y las aplicaciones móviles están ganando tracción rápidamente, alcanzando ya el 7% del valor transaccionado, impulsadas por la adopción masiva en mercados como los Países Bajos, Finlandia e Irlanda.

Indicador de Pagos en el Punto de Venta UE	2022	2224	2026 (Proyectado)
Cuota de efectivo (n.º transacciones)	59%	52%	46%
Cuota de tarjetas (valor transacciones)	46%	45%	44%
Pagos mediante aplicaciones móviles (valor)	4%	7%	11%
Transacciones online (% del nº total diario)	17%	21%	25%

La digitalización, además de ser una cuestión de conveniencia, supone como consecuencia una integración profunda en el estilo de vida del ciudadano europeo. Las transacciones online representan ahora el 36% del valor total de los pagos diarios, un salto significativo desde el 28% registrado hace dos años. Este cambio estructural está forzando a los comercios a adoptar soluciones omnicanal, donde la distinción entre el entorno físico y el digital se difumina mediante tecnologías como el *Tap-on-Phone*, que convierte cualquier dispositivo móvil en un terminal de aceptación de pagos.

Por otro lado, la nueva columna vertebral de la innovación en pagos europeos es el Reglamento (UE) 2024/886 (RPI) de pagos instantáneos, que ha transformado las transferencias instantáneas de un servicio premium opcional a una obligación universal, y en iguales condiciones que las transferencias estándar. Para finales de 2025, prácticamente todas las instituciones financieras de la eurozona ya eran capaces de enviar y recibir fondos en menos de 10 segundos, operando las 24 horas del día, los 365 días del año.

El impacto de esta norma se ha transformado en sistémico al eliminar la fricción temporal del sistema bancario tradicional; con ello, Europa crea un ecosistema que rivaliza con las redes globales de tarjetas en términos de velocidad y con una estructura de costes significativamente menor para el comercio. El reglamento exige la igualdad de tarifas y la inmediatez como catalizador necesario para que los pagos de cuenta a cuenta (A2A) se conviertan en medio de pago prevalente en el comercio minorista.

Sin embargo, la implementación técnica no está exenta de desafíos. El 41% de las instituciones financieras identifican su infraestructura heredada como el obstáculo más crítico para la adopción total de los pagos en tiempo real. La necesidad de procesar transacciones de forma atómica en menos de 10 segundos choca con sistemas de back-office diseñados para el procesamiento por lotes (batch processing) de décadas pasadas. Esto ha provocado una migración masiva hacia soluciones de banca en la nube y modelos SaaS, donde el 51% de los bancos buscan mejorar su eficiencia operativa integral para sobrevivir en

el nuevo entorno regulatorio y para afrontar el crecimiento exponencial de los sistemas de pago instantáneo, impulsados por Wero en Europa (inicialmente Bizum en España).

INMEDIATEZ Y VULNERABILIDAD

Con la inmediatez en el envío de fondos surge una mayor vulnerabilidad ante el fraude. El RPI aborda esta problemática mediante la introducción obligatoria de la Verificación del Beneficiario (VoP). Este servicio permite al pagador confirmar que el nombre del destinatario coincide con el titular del IBAN introducido antes de autorizar la transacción. En países como el Reino Unido, donde sistemas similares (Confirmation of Payee) ya están operativos, se ha observado una reducción de hasta el 59% en ciertos tipos de fraude de pagos push autorizados (APP).

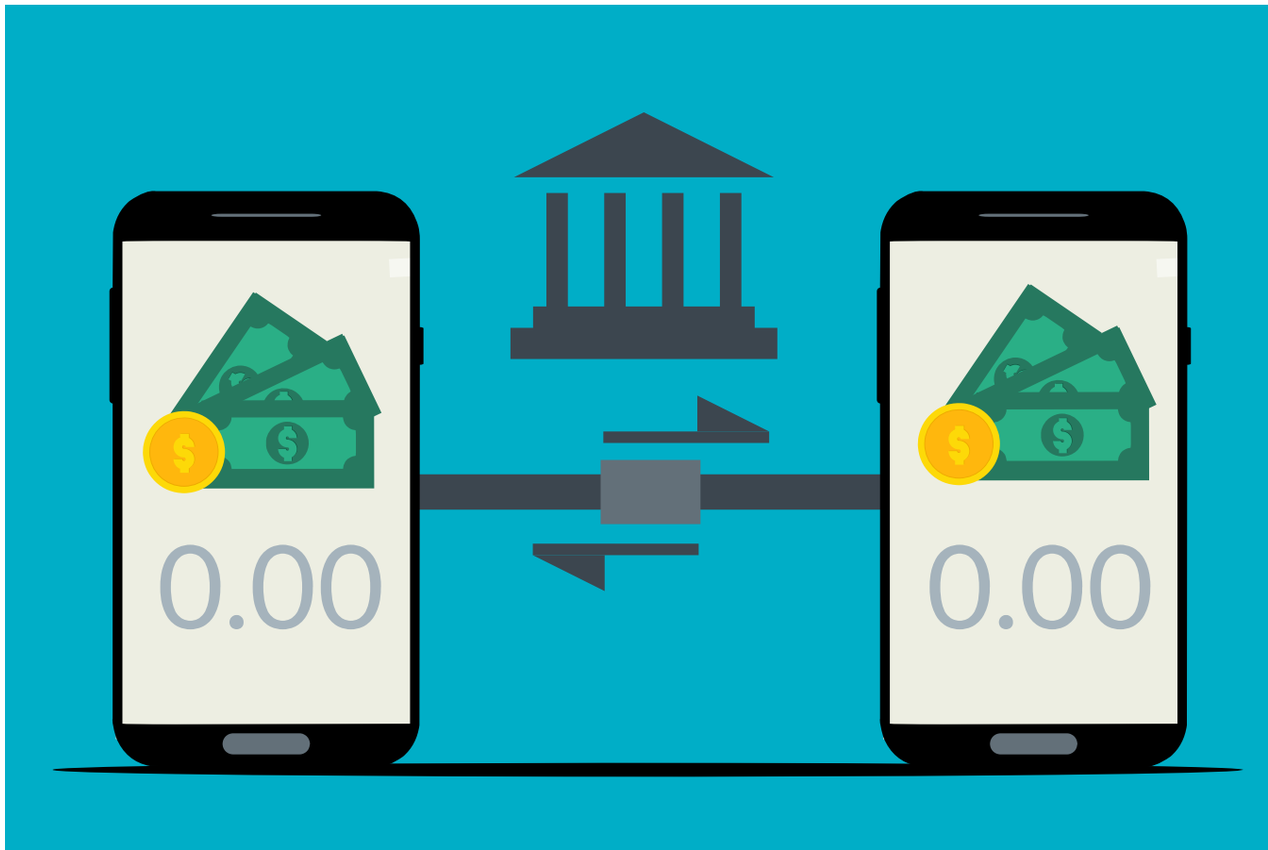
En este escenario de evolución acelerada, la Iniciativa de Pagos Europea (EPI) ha favorecido el lanzamiento de Wero, su propuesta de cartera digital unificada. Respaldada por 16 bancos europeos líderes, Wero tiene como objetivo explícito reducir la dependencia de las redes de tarjetas internacionales y ofrecer una solución de pago netamente europea. Con 43,5 millones de usuarios registrados para principios de 2026, Wero está demostrando que existe una preferencia real por una alternativa soberana.

La estrategia de Wero es pragmática: absorber infraestructuras nacionales exitosas y convertirlas en paneuropeas. El caso más paradigmático es el de iDEAL en los Países Bajos. A partir de 2026, iDEAL comenzará una fase de transición bajo la marca “iDEAL - Wero”, con el objetivo de ser absorbido totalmente por la plataforma europea para finales de 2027. Este movimiento no solo asegura una base de usuarios masiva desde el primer día, sino que también integra una red de comercios ya acostumbrados a los pagos A2A.

Uno de los hitos recientes más significativos es el memorando de entendimiento firmado entre EPI y la Alianza Europea de Pagos (EuroPA), que incluye a las empresas fundadoras Bizum (España), MB WAY (Portugal), Bancomat (Italia) y a las recién incorporadas Vipps MobilePay (países nórdicos), Blik (Polonia) e IRIS (Grecia). Este acuerdo no busca la fusión de las marcas, sino la creación de un hub de interoperabilidad técnica que permita pagos transfronterizos fluidos entre las diferentes aplicaciones nacionales.

Para el ciudadano español, esto significa que Bizum mantendrá su identidad y experiencia de usuario, pero ganará en interoperabilidad transfronteriza, lo que le permitirá enviar dinero a un contacto en Alemania que use Wero, o pagar en un comercio en Italia que acepte Bancomat, todo ello liquidado instantáneamente a través del canal de SEPA Instant. Se estima que para 2027, esta red conectará a más de 130 millones de usuarios en 13 países europeos, cubriendo el 72% de la población de la UE y Noruega.

En pocos años, Bizum ha pasado de ser una herramienta útil para compartir gastos a convertirse en el estándar de facto para los pagos directos en España. Con 30,6 millones de usuarios a finales de 2025, la plataforma procesa más de 3,4 millones de operaciones diarias. Lo más notable es su expansión hacia el comercio electrónico, con un crecimiento del 82% en volumen transaccionado durante el último año, alcanzando los 5.400 millones de euros. Para 2026, Bizum prevé alcanzar los 32,5 millones de usuarios



y superar los 1.400 millones de operaciones anuales. Su hoja de ruta para los próximos 24 meses incluye:

- **Pagos presenciales:** A mediados de 2026, Bizum lanzará su solución de pago en tiendas físicas, desafiando directamente a la tarjeta de débito en el punto de venta tradicional.
- **Interconexión europea:** El despliegue masivo de pagos P2P transfronterizos permitirá a los "bizumers" operar en todo el continente, reduciendo la fricción en viajes y comercio transfronterizo.

La relevancia de Bizum en el contexto europeo es tal que su modelo de éxito ha servido de inspiración para otros esquemas nacionales y para la propia concepción de Wero. La clave ha sido la simplicidad operativa; el número de teléfono como identificador universal ha eliminado las barreras técnicas para el usuario medio, una lección que la industria de pagos europea está aplicando ahora a escala continental.

La estrategia de EuroPA y EPI para impulsar Wero pasa también por aprovechar los movimientos del Banco Central Europeo para acelerar el proyecto del euro digital e incluir la nueva moneda en su modelo de billetera.

Tras concluir la fase de preparación en octubre de 2025, el BCE ha entrado en una fase técnica crítica para asegurar la emisión potencial de esta moneda hacia 2029. El euro digital no pretende reemplazar al efectivo ni al euro "bancario", sino complementarlos, llevando los beneficios de privacidad del primero y de accesibilidad al mundo digital del segundo. Con ello, se proporciona una infraestructura de pagos puramente europea que no dependa de entidades externas a la eurozona, se ofrecerá una privacidad similar al efectivo para transacciones offline y, por su usabilidad, se minimizará el impacto en sectores más vulnerables como los excluidos financieros, personas mayores o ciudadanos con discapacidades.

¿POSIBLE FUGA DE DEPÓSITOS?

El escepticismo de algunos actores financieros ante una posible fuga de depósitos bancarios a monederos digitales se contrapone al entusiasmo de los proveedores de servicios de pago, para los que el euro digital ofrece una oportunidad al poder utilizar sus estándares abiertos para expandir su alcance en la eurozona sin necesidad de construir redes de aceptación propias.

Todo ello ha implicado necesariamente dar el salto del Bizum y Wero pensado para los humanos, al protocolo x402 desarrollado para las máquinas. En lo que se ha denominado la Next Era of Payments, la inteligencia artificial agentica ya realiza transacciones de forma autónoma. El protocolo x402 activa el código de estado HTTP 402 ("Payment Required"), que ha estado reservado en los estándares de internet desde su creación, para permitir el intercambio de transacciones nativas en la web. De esta forma, una agente de IA puede iniciar operaciones de compra verificando previamente el precio, autorizar el pago en euro digital o en stablecoin y recibir la confirmación de envío en milisegundos, todo sin que un humano intervenga en el proceso de login o de autorización.

El protocolo x402 utiliza criptografía y redes blockchain de segunda capa para permitir pagos que mejoran los sistemas usados en los canales tradicionales, tanto por su menor coste (con independencia del valor de la transacción), como por

su usabilidad (interfaz de usuario invisible) o su sistema de autenticación (Wallet as ID).

Para 2026, se espera que el 82% de las organizaciones integren agentes de IA en sus flujos de trabajo, y el protocolo x402 se posiciona como el estándar financiero para los nuevos recursos laborales digitales. Empresas como Google Cloud, AWS y Anthropic ya han mostrado interés en la integración de máquinas que utilizan este estándar en sus flujos de trabajo.

La gran pregunta para los próximos cinco años es si las redes de tarjetas podrán mantener su dominio frente al ascenso de las nuevas soluciones impulsadas por los pagos A2A. Las tarjetas disfrutan de una ventaja de red masiva, con más de 150 millones de puntos de aceptación a nivel mundial. Sin embargo, los comercios ya comparan la presión de la comisión y los tiempos de liquidación (T+1 o T+2) en tarjetas con la gratuidad e inmediatez de los pagos A2A.

Por ello, Europa está liderando una “rebelión” contra el modelo de tarifas y la dependencia del conjunto de actores que intervienen en el esquema de tarjetas. Las soluciones basadas en SCT Inst, como Wero y Bizum, eliminan a múltiples intermediarios en la cadena de pago, lo que permite ofrecer costes mucho más bajos a los comercios. Además, la eliminación de los chargebacks (reversiones de pago) en los pagos A2A reduce la incertidumbre financiera para los vendedores, aunque esto traslade una mayor responsabilidad de seguridad al consumidor.

Por su parte, las redes de tarjetas no se están quedando quietas. Están evolucionando de ser “redes de tarjetas” a “redes de datos”. Visa y MasterCard están invirtiendo masivamente en infraestructura de banca abierta y pagos en tiempo real (ej. Mastercard Send) para ofrecer sus propios servicios A2A. Además, están introduciendo el Flexible Credential, que permite a una sola tarjeta actuar como débito, crédito o pago a plazos de forma dinámica, adaptándose a las preferencias del usuario en el momento de la compra.

Parece que el consenso entre los analistas es que Wero y las plataformas interoperables se convertirán en el rail por defecto para las transacciones domésticas y cotidianas de débito, mientras que Visa y Mastercard retendrán su papel dominante para el crédito, las compras internacionales de alto valor y los programas de fidelización premium.

PROFUNDA CONVERSIÓN DE LA INFRAESTRUCTURA

Pero para que toda esta innovación sea posible, los bancos han tenido que realizar una conversión profunda de sus sistemas internos. La adopción de la norma ISO 20022 ha sido el pilar de esta transformación. Al estandarizar el lenguaje de los mensajes financieros, la ISO 20022 permite que los pagos viajen con riqueza de datos securizados, facilitando la conciliación automática y reduciendo las intervenciones manuales. Se espera que, para 2026, el 80% de las compensaciones de alto valor en el mundo se realizará bajo este estándar.

PARA 2026, SE ESPERA QUE EL 82% DE LAS ORGANIZACIONES INTEGREN AGENTES DE IA EN SUS FLUJOS DE TRABAJO, Y EL PROTOCOLO X402 SE POSICIONA COMO EL ESTÁNDAR FINANCIERO PARA LOS NUEVOS RECURSOS LABORALES DIGITALES

En base a lo expuesto, la predicción que podemos deducir, para el mercado de los medios de pago que prevalecerán, se puede resumir en tres líneas fundamentales:

- **Dominio de los pagos A2A (dispositivos móviles):** para 2030, la mayoría de los pagos minoristas en tiendas físicas y online en Europa se realizarán a través de carteras digitales (como Bizum - Wero) interconectadas entre sí. La tarjeta física se convertirá en un objeto de nicho, mientras que el "pago por banco" será la experiencia estándar para el ciudadano medio, superando en volumen a las tarjetas de débito tradicionales.
- **Invisibilidad del pago y comercio autónomo:** gracias a protocolos como x402, una parte creciente de la economía (especialmente en servicios digitales y B2B) se moverá sin intervención humana. Los pagos se volverán "invisibles", integrados en el flujo de servicios de IA y dispositivos IoT, con liquidaciones inmediatas en monedas digitales reguladas.
- **El efectivo como reserva:** el efectivo no desaparecerá, pero su función cambiará. Dejará de ser un medio de pago diario para convertirse en un activo de resiliencia y una herramienta de privacidad para transacciones específicas.

En resumen, el éxito de iniciativas como Wero y la interconexión de Bizum (y del resto de wallets implicados) determinará si el continente sigue siendo un mercado de consumo para tecnologías externas o si logra establecer sus propias reglas del juego en la infraestructura más vital de la economía moderna: el sistema se pagos. La tecnología ya está disponible; ahora es una cuestión de adopción, confianza y ejecución operativa por parte de las instituciones financieras y de los ciudadanos. ■

MÁS INFO +

- SPACE 2024
- Tap-on-Phone
- Reglamento 2024/886 de pagos instantáneos
- Verificación del Beneficiario
- Next Era of Payments

JUANITO TIENE EL PODER (Y TÚ NO)

LORENZO MARTÍNEZ RODRÍGUEZ
Experto en ciberseguridad

Lorenzo Martínez Rodríguez es ingeniero en Informática por la Universidad de Deusto. Perito informático forense, actualmente es director de la empresa Securízame. Igualmente, es conferenciante habitual en congresos de Ciberseguridad.

A lo largo de 25 años dando servicios de ciberseguridad a empresas y participando en respuestas ante incidentes de toda índole, he tenido que interactuar con todo tipo de seres humanos y, a veces, con otros que no me lo han parecido tanto.

Con frecuencia he escrito y he contado en conferencias cómo las empresas (sobre todo pymes) confían de manera ciega en "su informático de toda la vida". Esa confianza, en ocasiones, las vuelve sordas ante lo que un externo que acaba de llegar para solucionar una papeleta más o menos compleja intenta advertirles.

En determinados incidentes se repite una escena conocida: la persona o pequeña empresa de sistemas, generalmente por negligencia o falta de diligencia, intenta esconder la basura debajo de la alfombra y tirar balones fuera para que "a mí no me echen la culpa". No han sido pocas las ocasiones (y últimamente llevo tres casos así en menos de cuatro meses) en las que el cliente no dispone de las credenciales administrativas de acceso a sus propios sistemas.

A veces ocurre por confianza absoluta en su informático (a quien llamaré cariñosamente "Juanito") o en la empresa de sistemas. El razonamiento suele ser sencillo: "Si quien accede como administrador a los equipos es Juanito, ¿para qué voy a tenerlas yo?".

En otras ocasiones es el propio "Juanito" quien impone que no exista coadministración. Así evita delimitar responsabilidades en caso de incidente y responder a la pregunta incómoda: ¿quién hizo qué para que un atacante montase la de San Quintín en la red de la empresa?.

Otras veces ni siquiera hay mala fe, sino falta de previsión. Nadie se detiene a pensar: ¿y si mañana le pasa algo a Juanito? Dios no lo quiera, pero ¿y si muere o queda incapacitado y las credenciales de administración solo las tenía él?

No es una hipótesis extravagante. En una ocasión real, tras las devastadoras inundaciones que azotaron varias localidades cercanas a Valencia, las contraseñas estaban físicamente en la empresa de sistemas y no existía copia en ningún otro lugar. En cualquiera de estos escenarios la pregunta es inevitable: ¿cómo continúo con mi actividad?

Y aún hay más.

¿Qué ocurre si la relación se deteriora? ¿Si me enfado con él o él conmigo? ¿Si decido sustituir a la empresa que gestiona mis sistemas?

Entiendo que, en circunstancias normales, Juanito es majo y honrado. Pero, en una situación desfavorable, ¿qué sucederá cuando le solicite un inventario completo de credenciales administrativas? ¿Actuará con ética profesional y facilitará la transición para que mi empresa continúe su actividad con otro proveedor o utilizará ese control como instrumento de presión?

En mi experiencia participando en respuestas ante incidentes he visto todas estas variantes. Y puedo asegurar que los momentos en los que aparecen son tensos, incómodos y, en ocasiones, abiertamente violentos.

Si Juanito se niega a entregar las credenciales y la empresa decide demandarlo, pueden pasar años hasta que un juez lo obligue a facilitar el acceso. Mientras tanto, quien queda inoperativa es la empresa. La actividad se paraliza. Los sistemas no esperan.

DELEGAR LA GESTIÓN ES RAZONABLE; PERDER EL CONTROL NO LO ES, PORQUE LA CONFIANZA NUNCA DEBERÍA SUSTITUIR A LA CUSTODIA DE LAS LLAVES

Recuerdo también el caso de un administrador interno que dejó de acudir a su puesto de trabajo sin previo aviso. La gerencia no logró contactar con él y, de repente, la organización se encontró sin credenciales de administrador. Tuvimos que aplicar distintas técnicas (según el sistema) para resetear accesos y recuperar el control. Se consiguió, pero no sin coste, estrés y riesgo.

Cuando a mi empresa le toca asumir el papel de “Juanito”, nuestra postura es clara. Creemos en la administración delegada de firewalls y sistemas; es razonable que solo nosotros operemos sobre ellos. Pero no creemos que el cliente deba quedar excluido del acceso a sus propias credenciales.

Los sistemas son suyos. Los datos son suyos. Y también debe ser suya la capacidad última de decidir quién los gestiona.

Si somos nosotros, perfecto. Si un día deciden sustituirnos, nos dará pena, pero no somos nadie para secuestrar el acceso administrativo. La relación profesional no puede sostenerse sobre la retención de las llaves.

Existen fórmulas intermedias: usuarios diferenciados, custodias compartidas, mecanismos que permitan incluso revocar accesos si la relación termina. Es, probablemente, el enfoque más equilibrado cuando técnicamente es viable.

Pero todos sabemos que ese modelo no encaja con quien aspira a ser el único amo y señor del entorno tecnológico.

Por eso mi recomendación es simple.

Clientes del mundo, no cedáis ante los “Juanitos” que no os permiten disponer de un usuario administrador o de la contraseña del administrador de cada sistema. Incluid en vuestros contratos una cláusula que establezca que solo haréis uso de esas credenciales en caso de emergencia o cuando decidáis prescindir del proveedor.

Y permitidme una advertencia clara: desconfía del Juanito que te prohíba tener las credenciales de administrador de tus propios sistemas.

Delegar la gestión es razonable; perder el control no lo es, porque la confianza nunca debería sustituir a la custodia de las llaves. ■

MÁS INFO +

» Backup a prueba de ransomware

EN CIBERSEGURIDAD CADA MOVIMIENTO CUENTA

¿LOGRARÁS SER EL HACKER QUE DESCUBRE LAS VULNERABILIDADES O EL DELINCUENTE TE GANARÁ LA PARTIDA?

FORMACIÓN DE HACKING ÉTICO 2026

https://www.securizame.com/hacking-etico

SECURIZAME

DATOS SIN MEMORIA:
CUANDO LA COMUNICACIÓN CORPORATIVA SABE QUIÉN ERES, PERO NO RECUERDA QUIÉN HAS SIDO

MANUEL LÓPEZ
Asesor de comunicación

Madrileño de nacimiento, horchano de adopción, informático de profesión, con más de 35 años de experiencia en el sector de TI, ha desarrollado la mayor parte de su carrera profesional en Hewlett-Packard, donde ocupó cargos de responsabilidad en diferentes áreas como consultoría, desarrollo de negocio, marketing, comunicación corporativa o PR. Actualmente dedica la mayor parte de su tiempo a asesorar a starups en temas relativos a la comunicación, desde su posición de partner en la plataforma de profesionales goXnext.

A comienzos de 2021, escribí para este mismo medio de comunicación un artículo titulado “Comunicación en tiempos difíciles. Las gafas de no ver”. Estábamos en momentos difíciles, saliendo del COVID y con Filomena en España. En él desarrollaba la idea de que cuando vienen tiempos difíciles tenemos la tendencia a meternos bajo tierra y olvidarnos de todo, poniéndonos las “gafas de no ver”. Hoy 5 años después podríamos publicar el mismo artículo cambiando COVID y Filomena por IA y Guerra de Irán, por ejemplo, y sería igual de válido que entonces.

Pero por no repetirme, voy a cambiar el enfoque y vamos a hablar del “olvido de la comunicación”, aplicando el síndrome de Capgras y el de Fregoli para poner marco a ciertas situaciones que se están dando en la comunicación actual. La idea me ha venido con la lectura del libro “El cielo que olvida sus estrellas”, del neuropsicólogo Saul Martínez-Horta, que explica como el mismo dice: las enfermedades del cerebro como nunca te las han contado; un libro altamente recomendable para sobrevivir en los tiempos actuales, conociendo algo del funcionamiento del cerebro en base a las enfermedades de éste.

Primero hablemos un poco de la enfermedad. En 1906, el neuropatólogo Alois Alzheimer describió por primera vez la enfermedad que llevaría su nombre. Entre sus síntomas más devastadores no está únicamente la pérdida de memoria, sino algo más sutil y cruel: la distorsión de la identidad ajena. El paciente

COMPARTIR EN REDES SOCIALES

no solo olvida; a veces sustituye, confunde o multiplica a quienes le rodean. La neurología tiene nombres precisos para estos fenómenos. La comunicación corporativa, lamentablemente, los practica sin saberlo y lo que resulta inquietante es la facilidad con la que se pueden proyectar sobre la forma en que muchas organizaciones se relacionan con sus propios clientes.

Repasemos brevemente dos síndromes que vamos a correlacionar con la Comunicación, copiando textualmente 2 párrafos de una página del libro:

"El síndrome de Capgras, en el que una persona está convencida de que su familiar, sea este su cónyuge, hijo o cuidador habitual, ha sido sustituido por un impostor idéntico. Lo ve, lo escucha, pero no logra conectar emocionalmente con esa imagen, y entonces, el cerebro, buscando una explicación que encaje con esa experiencia interna, elabora como mejor solución posible: 'este no es mi marido. Se parece pero no es.'

Otras manifestaciones, que si bien no son tan frecuentes en la enfermedad de Alzheimer, resultan muy llamativas, es por ejemplo cuando una persona cree que un mismo individuo adopta diferentes apariencias físicas para engañarla o perseguirla. Puede decir por ejemplo 'la enfermera es en realidad mi vecina, disfrazada'. Aqui el error es inverso al de Capgras, se reconoce erróneamente a diferentes personas como si fueran una sola constituyendo lo que conocemos como síndrome de Fregoli."

Antes de hablar de correlaciones, conviene establecer el diagnóstico general. Las empresas invierten cantidades ingentes de recursos en captar clientes: campañas de marketing, embudos de conversión, programas de onboarding, equipos de ventas entrenados para escuchar. Y sin embargo, en el momento en que el cliente firma, paga o activa su cuenta, algo se rompe. El interlocutor que le conocía desaparece. Las promesas quedan sepultadas bajo protocolos de soporte. La relación, que durante el proceso comercial fue cálida y personalizada, se vuelve fría, genérica e impersonal. Podríamos decir que el cliente existe, pero ya no le recuerdas.

El equivalente corporativo del síndrome de Capgras se manifiesta cuando una organización es capaz de identificar al cliente en sus sistemas, pero no de reconocerlo en la comunicación real. Este fenómeno no es nuevo, pero se ha agravado con la digitalización. Los CRM almacenan datos, sí, pero los datos no son memoria. El CRM contiene su nombre, su historial de compras, sus incidencias previas, sus preferencias declaradas. Pero cuando ese cliente interactúa con la empresa —abre un ticket, recibe una comunicación, habla con un agente— el sistema actúa como si fuera un desconocido.

La identificación es técnica; el reconocimiento es relacional. Una empresa puede tener perfectamente actualizada la ficha de un cliente de diez años y, al mismo tiempo, enviarle una comunicación de bienvenida al activar un nuevo canal de soporte, incluirle en una campaña de captación diseñada para nuevos usuarios, o pedirle que explique de nuevo un problema que ya resolvió

EL CLIENTE QUE HA PASADO POR UNA MIGRACIÓN, VARIAS RENOVACIONES DE CONTRATO Y CICLOS DE FORMACIÓN INTERNA NO ESPERA QUE SE LE TRATE COMO UN PRIMER CONTACTO

hace tres meses. El dato existe. La memoria, no.

En entornos IT, donde las relaciones entre proveedor y cliente son a menudo largas, complejas y técnicamente densas, este síndrome tiene consecuencias especialmente visibles. El cliente que ha pasado por una migración, varias renovaciones de contrato y ciclos de formación interna no espera que se le trate como un primer contacto. Cuando eso ocurre, la señal que recibe no es de un error puntual: es de que su historia con la empresa no importa.

En cambio, el síndrome de Fregoli es, en cierto sentido, el opuesto complementario del de Capgras. Aquí el paciente cree que diferentes personas son en realidad la misma, disfrazada. Donde hay diversidad, el cerebro proyecta una única identidad que cambia de forma. El error no es no reconocer, sino reconocer en exceso: ver a uno donde hay muchos.

En comunicación corporativa, este síndrome se llama segmentación única. O, más brutalmente, marketing de plantilla. Es la empresa que tiene cien mil clientes y les manda el mismo email de "oferta personalizada". Es el proveedor de servicios cloud que envía la misma newsletter de producto a un desarrollador independiente, a una pyme de logística y a un banco de inversión. Es la newsletter que empieza con "Sabemos que eres diferente" y termina con exactamente el mismo contenido para todos.

Los sistemas de automatización han democratizado el síndrome de Fregoli a escala industrial. Las herramientas de 'marketing automation' permiten segmentar, sí, pero también permiten no hacerlo y aparentar que sí. El resultado es una comunicación que tiene la forma de la personalización sin su sustancia. Un disfraz que el cliente detecta a la primera lectura.

La neurología distingue ambos síndromes porque sus mecanismos son distintos, aunque su origen comparta raíces. En la práctica corporativa, muchas organizaciones los padecen simultáneamente: tratan a cada cliente como si fuera el mismo (Fregoli) y a la vez como si no tuvieran historia compartida (Capgras). El doble fracaso: ni te diferencio de los demás, ni te recuerdo a ti.

El problema no es tecnológico. Las herramientas para evitarlo existen y son accesibles. El problema es de arquitectura comunicativa y, más profundamente, de cultura organizacional. ¿Qué datos recoge realmente

EL PROBLEMA NO ES TECNOLÓGICO, ES DE ARQUITECTURA COMUNICATIVA Y, MÁS PROFUNDAMENTE, DE CULTURA ORGANIZACIONAL

la empresa sobre el cliente y con qué propósito? ¿Quién en la organización es responsable de la coherencia de la experiencia comunicativa a lo largo del tiempo? ¿Existe un "hilo de memoria" que conecte el primer contacto con el décimo?

El olvido corporativo no se cura con más software. Se trata con intención. Con procesos que obliguen a preguntarse antes de cualquier comunicación: ¿quién es exactamente este cliente?, ¿qué hemos vivido juntos y qué necesita escuchar ahora de nosotros? No qué necesitamos decirle, sino qué necesita escuchar.

La diferencia entre una empresa que padece estos síndromes y una que no los padece no siempre es visible en un dashboard. Se nota en un email que llega en el momento justo con el contexto correcto. En un agente de soporte que abre la conversación sabiendo lo que ya no hace falta explicar. En una renovación de contrato que reconoce el recorrido compartido en lugar de empezar de cero.

En la enfermedad de Alzheimer, no es crueldad, es una lesión. Pero en las empresas no hay lesión que lo justifique. Solo decisiones, procesos y prioridades mal ordenadas. El cliente que lleva años contigo y siente que no lo conoces no va a llamarlo síndrome de Capgras. Lo va a llamar cancelación. Y tendrá razón.

Así pues, aprendamos a diagnosticar el Olvido Corporativo, pongámosle remedio y tengamos un Encuentro con la Comunicación, para evitar Desencuentros y Frustraciones con la Comunicación que nos llevarán sin duda a perder negocio. ■

MÁS INFO +

» El cielo que olvida sus estrellas

» Medallia + CXPA (2024). 2024 State of CX Personalization Report

» Nextiva (2026). 2026 Customer Service Statistics: Trends to Improve Experience

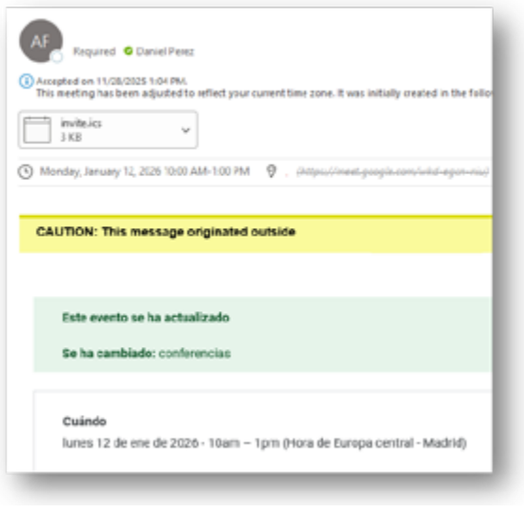
DANIEL PÉREZ LIMA
Experto en ciberseguridad

Ejecutivo de TI y ciberseguridad práctico y orientado a resultados, con amplia experiencia liderando gobernanza de seguridad, gestión de riesgos y operaciones de TI en entornos multinacionales.
Experto en alinear estrategias de TI y ciberseguridad con los objetivos empresariales y marcos de cumplimiento (NIST, ISO, COBIT, CMMC, PCI DSS...), asegurando una prestación de servicios de TI resiliente, eficiente y segura.
Cuenta con certificaciones CISM y CISSP de ISC2.

COMPARTIR EN REDES SOCIALES

ATENCIÓN: SPOOFING/PHISHING USANDO INVITACIONES ICS

Los archivos ICS son un formato estándar de archivo de calendario basado en el estándar iCalendar, que se utiliza para compartir eventos, citas y agendas entre distintas aplicaciones de calendario. Los habrás visto muchas veces. Recibes un correo para una reunión o evento, y ahí tienes un ICS que debes abrir.

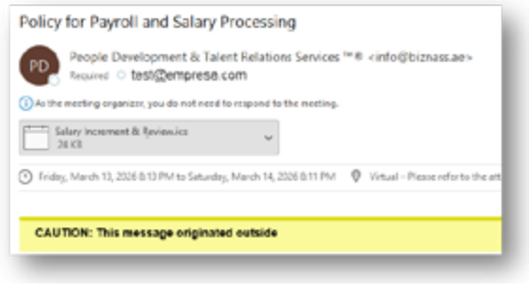


Y al abrirlo, te sale la invitación para agregarla al calendario. Aceptas, y listo. Lo que vamos a tratar es un nuevo método de spoofing/phishing basado en este funcionamiento.

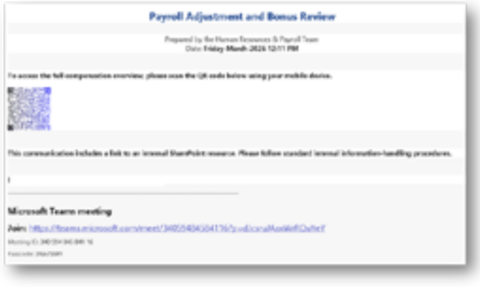
MÉTODO DE ATAQUE

La idea de los atacantes es aprovechar este flujo de trabajo normal y legítimo para saltar las defensas de los filtros de correos. Como sabemos, los filtros de correo miran muchos puntos para aceptar o no un mensaje. Reputación del dominio, autenticación del email, contenido de este, búsqueda de archivos o enlaces maliciosos... Entonces, ¿cómo hacen para saltarse las protecciones? Presta atención al flujo que utilizan:

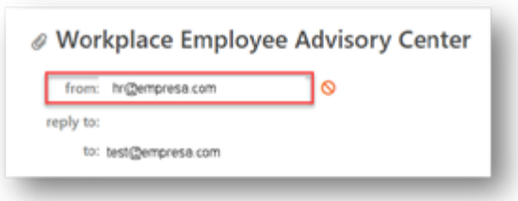
1. El atacante registra un dominio real, legítimo. Y abre una cuenta de correo en este nuevo hosting.
    a. Otra variante, más agresiva y peligrosa es que el atacante compromete una cuenta corporativa
2. En ambos supuestos, el atacante tiene acceso a una cuenta de correo corporativa, legítima y que pasa los principales bloqueos de los filtros de correo (reputación, autenticación...)
3. A partir de aquí, envía una invitación de calendario, con un fichero ICS adjunto.
4. El email es correcto. Emisor legítimo, no hay spoofing, no hay phishing, ningún enlace malicioso. Sólo un adjunto ICS que es una invitación de calendario.



5. Al abrir el adjunto ICS, aparece el contenido malicioso. Un phishing como una catedral con un código QR.



6. Y no sólo eso, sino que pueden poner como organizador el correo corporativo que están atacando (en nuestro caso, empresa.com) como organizador del evento.



7. Dado que el contenido malicioso y el spoofing suceden dentro del ICS, que no es un archivo adjunto habitual, y siempre se usa con fines legítimos para una reunión, puede pasar los filtros de protección sin problemas.

¿CÓMO PUEDES MITIGAR ESTE RIESGO?

La respuesta fácil es configurar tu filtro de correo para que elimine los adjuntos ICS. Pero claro, esto impactará negocio, dado que todas las reuniones externas legítimas que utilicen estos archivos no podrán enviarlos más. Otra opción es configurar tu sistema de correo para rechazar meetings externos. De nuevo, esto puede generar un impacto importante en negocio.

Así que quedan estas opciones:

- **Formación y concienciación:** Estamos ante un caso que puede depender del usuario detectarlo. Así que un buen plan de formación y concienciación ayudará a que detecten estos casos y los reporten para su análisis y bloqueo reactivo.
- **Sistema de reporte de emails funcional:** Construye confianza asegurando que cada email que reporta un usuario es analizado y revisado. Esto ayudará a que reporten más y más.
- **Mejorar el filtro de correo:** Al fin y al cabo, es un adjunto con un contenido malicioso. Debes intentar ajustar el filtro de correo para que sea capaz de detenerlos. Contacta con tu proveedor y soporte, y escala esta incidencia hasta que te confirmen que detendrán los nuevos casos.
- **Sistemas de filtrado web:** En el caso que el usuario haga click en el enlace, si tienes un filtrado web activo es posible que evite que el usuario acceda a esta web maliciosa.
- **Autenticación Multifactor:** Por supuesto, MFA es obligatorio, y puede ser un punto de defense clave si el usuario sigue adelante con el enlace malicioso.

- **Politicas de Acceso Condicional enlazadas con equipos corporativos:** En el supuesto que el usuario siga todo el camino del phishing, si tienes políticas de acceso condicional que fuercen a que los logins sean de equipos corporativos, actuará como defensa final. Esto te protegerá incluso ante el robo de token de sesión, que como estamos viendo está siendo un punto sangrante para las corporaciones (hablaremos de ello en próximos artículos).

CONCLUSIÓN

Este caso nos muestra cómo los atacantes siempre idearán formas nuevas de intentar saltar nuestras defensas. Y cómo un buen plan de formación, así como de análisis y reporte de correos sospechosos, puede ser fundamental para parar este tipo de ataques.

Por otra parte, como siempre, mejora continua: revisa tus defensas y controles, y busca asesoramiento en los equipos especializados de soporte para que este tipo de amenazas no pasen tus defensas. No lo dejes como algo aislado. Si un email de estos ha pasado tus defensas, otro lo hará. Y quizá en ese caso, el usuario no lo reporte. ■

MÁS INFO +

» ICS phishing

La documentación TIC, a un solo clic

Navegue por el “desordenado medio” de la transformación impulsada por IA

Este documento ofrece una visión honesta y basada en datos sobre cómo están afrontando las empresas esta etapa clave de la adopción de la IA. Descubrirás por qué la IA no solo acelera tareas, sino que transforma flujos de trabajo completos, exige nuevas habilidades, etc.

Cómo anticipar los ciberataques del mañana con Inteligencia Contextual de Amenazas

El panorama de amenazas evoluciona a un ritmo que supera la capacidad de respuesta de muchas organizaciones. Los atacantes innovan constantemente, automatizan sus campañas y perfeccionan sus tácticas para evadir las defensas tradicionales. Este whitepaper explica cómo la Inteligencia Contextual de Amenazas permite transformar señales fragmentadas en conocimiento accionable para anticipar ataques antes de que se produzcan.

Guía práctica para transformar la gestión de la información en tu empresa

La información es uno de los activos más valiosos de cualquier empresa, y también uno de los más difíciles de gestionar. Documentos dispersos, procesos manuales, riesgos de cumplimiento normativo y falta de visibilidad son desafíos habituales que impactan directamente en la productividad, los costes y la toma de decisiones.

Perspectivas de inversión en TI y tendencias tecnológicas para 2026

Advice Strategic Consultants ofrece en este informe un análisis del comportamiento del mercado tecnológico y las previsiones de inversión y demandas tecnológicas de las empresas. Descarga ahora este documento y conoce, con una mirada amplia, qué está sucediendo en el mercado tecnológico y qué deparará el próximo año.