Ciberseguridad: negocio sin límite

A pesar de los progresos persisten los déficits en talento, gobernanza y resiliencia

España avanza

en ciberseguridad empresarial

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

Bárbara Madariaga

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

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

La ciberseguridad en terceros y la IA

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

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

Uno de los mayores desafíos estructurales que enfrenta el sector de la ciberseguridad en España es la escasez de talento especializado. La creciente competencia internacional ha dificultado la atracción y retención de perfiles cualificados, lo que ha intensificado este problema en un 188 % con respecto al año anterior. Esta falta de profesionales afecta directamente a la capacidad de las empresas para gestionar amenazas y desarrollar estrategias de seguridad sólidas. Deloitte concluye que, a pesar de los avances, las organizaciones españolas siguen enfrentando retos clave que requieren una mayor conciencia, inversión efectiva y una apuesta decidida por el talento.

Lidera cloud

Powered by V-Valley

TU PLATAFORMA MSSP AUTOMÁTICA Y DESATENDIDA

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

ÚNETE A LAS VENTAJAS DE LIDERA CLOUD

- Modelo de suscripción
- Pago por uso
- Mayor margen por volumen
- API de provisión
- Atención comercial
- Proceso de onboarding
- Servicio integral de soporte
- Beneficios económicos

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

www.v-valley.com

Buen arranque del año para la filial ibérica de Check Point Software

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

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

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

Marilés de Pedro

Security Report Iberia

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

Según el estudio, entre los ataques permanecen los clásicos, como es el caso del *ransomware* (España ocupó la octava posición a nivel mundial en esta amenaza) o del *phishing*, con correos electrónicos y suplantaciones de identidad. Con la IA como la tecnología que les hace más complejos y los automatiza a un coste cero. Mario García cree que, en su uso, los fabricantes van un paso por delante de los *hackers*. "Llevamos más tiempo usándola, con muchos medios y con muy buena información de los ataques: cuántos se producen, de qué tipo, cómo se llevan a cabo, con qué herramientas, etc. Una información que utilizamos después, aplicando la inteligencia artificial, para elaborar la defensa. Contar con una buena base de datos es esencial". Una tarea en la que el concurso del equipo humano se torna esencial. "Gracias a la expansión del teletrabajo, es posible contar en cualquier país con los mejores especialistas, lo que nos permite atraer talento". En España disfrutan del desempeño de varios profesionales que forman parte del departamento de I+D del fabricante. "Tenemos talento, información y tecnología; lo que conforma una excelente combinación".

Buenos números

La filial ibérica cerró un excelente 2024 en el que su crecimiento fue entre tres y cuatro veces superior al que exhibió la corporación. "El equipo es la clave", señala. Este 2025 ha empezado de manera positiva. "Los ataques son, cada vez, mayores y tienen un componente global, afectando a todo el mundo. Las empresas deberían ser conscientes de esta situación".

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

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

Panorama de amenazas

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

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

Los ataques provocados desde los estados (ciberguerras) siguieron creciendo con las naciones exhibiendo más recursos para desplegar sus amenazas. Cada país diseña estrategias particulares, haciendo uso del *hacktivismo* (*malware* destructivo) en los conflictos bélicos. Hasta en un tercio de los procesos electorales que se han celebrado en el mundo entre septiembre y diciembre de 2024, han existido campañas de desinformación para tratar de influir en la opinión pública a través, por ejemplo, de *deep fakes*, con China, Rusia e Irán como ejemplos de estas prácticas.

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

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

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

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

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

Normativas

La regulación europea trata de fortalecer los sistemas de protección. En la actualidad el protagonismo corresponde a DORA y a NIS2. Mario García, en el caso de la primera, cree que las entidades financieras tienen muy bien trabajado, en general, el área de la ciberseguridad. "Todo es mejorable, por supuesto, y siempre habrá una evolución, pero es un segmento que cuenta con una enorme regulación".

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

Acceda al vídeo desde el siguiente **código QR**

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

Casi 30.000 empresas disfrutan del servicio MDR de Sophos

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

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

Marilés de Pedro

Fernando Casares,
responsable de distribución y MSP de **Sophos** Iberia

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

Una red a la que el año pasado se le presentó Partner Care, como un único punto de contacto para que los *partners* puedan resolver cualquier duda y recibir asistencia operativa 24 horas del día, los 7 días de la semana. A través de este servicio, Sophos ayuda a sus *partners* a resolver cualquier cuestión no relacionada con las ventas con el fin de agilizar sus tareas administrativas y operativas para que puedan centrarse en vender y atender a sus clientes.

> "El ecosistema debe poner su foco en el cliente"

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

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

EDR detecta.
XDR conecta.
MDR protege.

Las ciberamenazas están evolucionando. ¿Y tu?

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

sophos.com

SOPHOS
Defeat Cyberattacks

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

Modelos MDR

Uno de los ejes estratégicos de Sophos es su propuesta de ciberseguridad como servicio, basada en el modelo MDR. En 2024, a nivel mundial, la base de clientes se incrementó en un 37 % y en la actualidad el número de empresas que han apostado por este servicio roza las 30.000.

Casares valora de manera muy positiva la adopción de este modelo por parte de los *partners* y de las empresas españolas. "Está claro que la venta de un producto no es suficiente. Es muy importante que el ecosistema de *partners* incorpore el servicio a su oferta. Se trata de un modelo completamente diferenciador", explica. Un servicio que sirve especialmente a las empresas más pequeñas. "La labor del *partner* es esencial para hacer que las pymes sean capaces de entender que, por un coste no muy elevado, puedan disfrutar de un servicio 24/7 de ciberseguridad". Casares apela a una democratización de un modelo que antes solo se planteaban las grandes corporaciones. "Una empresa de 10 usuarios, por menos de lo que cuesta un teléfono móvil, puede contar con un completo servicio de ciberseguridad".

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

Acceda al vídeo desde el siguiente **código QR**

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

Amenazas y protección

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

INCIBE señala que en el terreno de las empresas la suplantación de identidad ha sido la temática más relevante durante el pasado año por el duplicado de las páginas web de las empresas y la suplantación de sus redes sociales. En la segunda mitad de 2024 se detectó el incremento de las campañas de dirigidas a empresas y otros organismos, el fraude BEC *(Business Email Compromise).*

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

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

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

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

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

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

Otros problemas a solventar

Si bien muchas organizaciones comprenden los principios generales de Zero Trust, como el acceso basado en el contexto y la autenticación continua, la transición hacia esta arquitectura de seguridad representa un reto significativo a nivel cultural. Al eliminarse la confianza implícita y establecerse políticas de acceso mucho más restrictivas y basadas en permisos mínimos, su ejecución involucra un cambio en cómo los empleados conciben la seguridad.

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

La dificultad para medir el Retorno de la Inversión (ROI) o la falta de capacitación específica son otras importantes barreras. Sin un conocimiento profundo de los principios de Zero Trust, es difícil ejecutar y mantener una estrategia coherente y efectiva a este respecto.

Un distribuidor de valor

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

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

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

Buen inicio de año para la filial ibérica de Kaspersky

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

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

Marilés de Pedro

José Antonio Morcillo, director de canal de **Kaspersky**

Programa de canal

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

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

Servicios gestionados

El área de los servicios gestionados señala la mayor oportunidad para el canal. El pasado año este apartado creció un 46 % en el negocio ibérico. Morcillo reconoce que no todo el ecosistema será capaz de ofrecer un servicio. "Contamos con *partners* muy pequeños, que atienden al mercado de la pequeña y mediana empresa, que no tienen la capacidad para desplegarlos". Sin embargo, su vocación es dirigir al ecosistema hacia un modelo de prestación de servicios; no a fórmulas de reventa mensualizada. "Hay que promover la transformación y que los *partners* vean el valor que aporta la prestación de servicios", insiste. "Vender a precio no tiene futuro, vender valor sí; y la percepción del cliente varía muchísimo. Si se vende a precio y aparece un *partner* con una oferta más barata, la operación se pierde. Por el contrario, si el *partner* aporta valor, a pesar

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

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

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

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

La IA, la tecnología "de moda"

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

Panorama de amenazas

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

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

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

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

Acceda al vídeo desde el siguiente **código QR**

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

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

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

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

Bárbara Madariaga

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

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

En este contexto, V-Valley se posiciona como un actor clave en la distribución y gestión de soluciones tecnológicas que ayudan a proteger a las empresas de las crecientes amenazas. David Gasca, responsable de operaciones de ciberseguridad en la compañía, explica cómo las grandes empresas están consolidando su gasto en ciberseguridad. "Estamos viendo que cada vez más la ciberseguridad está en el foco principal del gasto de las grandes empresas. Esto está llevando a una mayor visibilidad del mercado, lo que también está impulsando a las medianas empresas a invertir en áreas que antes no protegían".

El impacto de las ciberamenazas

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

Para hacer frente a esta ola de ataques, la inteligencia artificial se ha convertido en un aliado imprescindible, ya que las soluciones basadas en IA permiten detectar y mitigar amenazas con una eficacia mucho mayor que los sistemas tradicionales. "La inteligencia artificial es lo que va a venir. Los atacantes también están utilizando inteligencia artificial. La optimización de los procesos para detectar y remediar los ataques de manera automática es lo que necesitamos", afirma David Gasca.

> "La especialización en una tecnología concreta es lo que garantizará el éxito. Cuanto más estés metido en una tecnología, más valor aportarás como *partner*"

Sin embargo, tal y como explica el directivo de V-Valley, la innovación en ciberseguridad no se limita únicamente a la inteligencia artificial, sino que también se amplía a otros campos como la orquestación de soluciones y la ciberinteligencia. "La inteligencia artificial en ciberseguridad está orientada a la automatización de procesos, pero también estamos viendo una mayor interconexión entre las soluciones, lo que nos permite tener un enfoque más proactivo".

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

V-Valley y su apuesta por la ciberseguridad

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

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

La especialización como clave del éxito

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

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

Evolución del ecosistema de *partners*

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

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

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

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

Acceda al vídeo desde el siguiente **código QR**

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

Del riesgo a la resiliencia

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

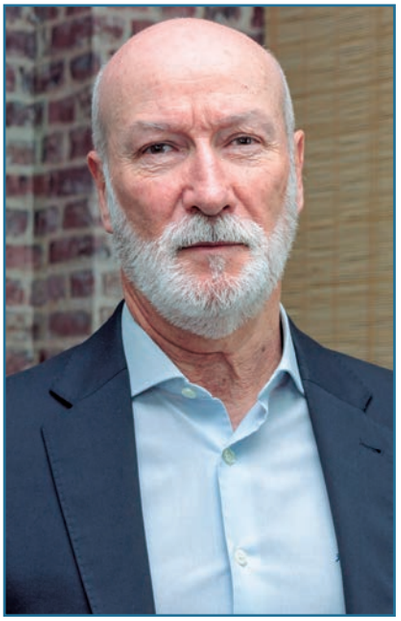
Los datos hablan por sí solos ya que según el último informe de analistas de Kaspersky Managed Detection and Response (MDR), se han detectado amenazas persistentes avanzadas (APT) en el 25 % de las empresas, un 74 % más en comparación con 2023. No pensemos que en España estamos libres ya que nos encontramos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

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

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

Inteligencia de amenazas y delegar con control, la combinación perfecta

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



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

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

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

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

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

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

The Industry's Best Prevention Rate:

99.9%

Miercom

Miercom Enterprise and Hybrid Mesh Firewall Benchmark 2025

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

checkpoint.com/action

CHECK POINT™