

#DEBATE IT



El mercado de la ciberseguridad en España se encuentra en un punto de inflexión marcado por la rápida irrupción de la inteligencia artificial, la sofisticación de las amenazas y la necesidad de proteger identidades y entornos remotos. Analizamos la evolución que se está produciendo en el mercado, el comportamiento de los presupuestos destinados a seguridad y los retos del canal de distribución en su transición hacia el modelo de prestación de servicios gestionados de seguridad (MSSP).

EVOLUCIÓN DE LAS CIBERAMENAZAS Y CLAVES PARA LA PROTECCIÓN DE LAS ORGANIZACIONES



DEBATE IT >> Analizamos cómo está evolucionando el panorama de las ciberamenazas en la segunda mitad de 2026, y cómo los proveedores y el canal se están adaptando para garantizar la protección de las organizaciones, con la colaboración de expertos de ADM Cloud & Services, Samsung, SonicWall, Stormshield y V-Valley.

El panorama de la ciberseguridad afronta una profunda transformación impulsada por la inteligencia artificial, la sofisticación de los ataques y la desaparición del perímetro tradicional. Pese a un comportamiento tímido a comienzos de año, la ciberseguridad mantiene un crecimiento a doble dígito apoyado en la concienciación de los directivos, la presión regulatoria y la necesidad urgente de proteger las identidades, los datos y los dispositivos. Analizamos estas tendencias de mercado y la evolución que está viviendo el canal los servicios gestionados junto a Víctor Orive, CEO de ADM Cloud & Services; Enrique Martín, head of Large Enterprise de Samsung Iberia; Sergio Martínez, regional manager Iberia e Italia de SonicWall; Juan Manuel Granda, key account manager para Defensa y Seguridad de Stormshield Iberia; y David Gasca, director de Marketing y Operaciones de Ciberseguridad de V-Valley.

RADIOGRAFÍA DEL SECTOR

Tras un inicio de año contenido, el mercado de ciberseguridad ha demostrado que continúa ganando tracción y, según Context, el canal europeo creció cerca del 10% en in-



gresos en el segundo trimestre, y las perspectivas son positivas de cara a la segunda mitad de 2026.

David Gasca, de V-Valley, destaca la inercia positiva del mercado impulsada por la adopción tecnológica y el repunte de proyectos. En su opinión, “la IA lo está acelerando todo”, y añade que la visibilidad de las brechas de seguridad que se están detectando está reactivando el gasto de las empresas, porque “no hay capacidad de inversión hasta que no pasa algo cerca”.

Desde Stormshield Iberia, Juan Manuel Granda coincide en este plan-

teamiento, porque las organizaciones vinculan cada vez más la ciberseguridad a la continuidad de negocio. En su opinión “está habiendo un cambio de percepción en los clientes sobre la importancia de la ciberseguridad, ligado al impacto de negocio que realmente puede tener”. Asimismo, anticipa un último trimestre muy fuerte en España, que podría elevar la previsión de crecimiento hacia el 14%.

Por su parte, Sergio Martínez, de SonicWall, confirma el buen comportamiento del primer semestre y el empuje que se ha visto tras el verano. A pesar de ello, basándose



en su último informe sobre ciberseguridad, afirma que “no hay cosas nuevas, lo que pasa es que nadie hace los deberes”, y añade que los problemas persisten en la gestión de identidades y la vulnerabilidad del acceso remoto SSL VPN.

Aportando una visión centrada en la seguridad del dispositivo, Enrique Martín, de Samsung Iberia, pone el foco en la creciente preocupación por proteger las flotas de dispositivos móviles. “Lo que sí estamos viendo es que antes la parte de movilidad no preocupaba y cada vez preocupa más”, apunta, señalando que la aparición de ciberataques con suplantación de voz por IA está impulsando la demanda de más control.

Finalmente, Víctor Orive, de ADM Cloud & Services, también confirma crecimientos a doble dígito, explicando que las nuevas superficies de ataque que abre la IA y la regulación

El ransomware ya no espera. ¿Y tu recuperación?

Los atacantes de 2026 ya no cifran y esperan: primero borran tus copias de seguridad. Cove DRaaS pone tu recuperación fuera de su alcance y te devuelve la operatividad en menos de 15 minutos.

Descubre cómo funciona





“ MUCHOS QUIEREN SER MSP, PERO POCOS SABEN HACERLO; DAR EL SALTO NO ES FÁCIL ”

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

la administración pública muestra una inversión más contenida tras gastar los presupuestos anteriores, sectores como Defensa, Industria y las pymes están actuando como motores del mercado.

En cuanto al sector público, David Gasca (V-Valley), aclara que las entidades gubernamentales no dejan de ejecutar, sino que son conservadoras al migrar al cloud. Y advierte que “la IA es ahora mismo el eslabón más débil de la cadena, tiene acceso a nuestros dispositivos y datos”, facilitando el acceso sin la debida supervisión de TI.

Para Juan Manuel Granda (Stormshield) la administración opera de forma contraria al sector privado, concentrando sus inversiones en ci-



“ EL NEGOCIO FÁCIL ESTÁ EN LA GRAN CUENTA, PERO EL VOLUMEN Y LA OPORTUNIDAD ESTÁN EN LA PYME ”

ENRIQUE MARTÍN,
head of Large Enterprise de **Samsung Iberia**

infraestructuras para ponerse al día. A esto, añade, “sectores que están 'on fire' son Defensa e Industria, y las pymes están tirando bastante haciendo los deberes”, con previsiones de que la implantación de NIS2 estimulará aún más la demanda.

Sobre el marco regulatorio, Enrique Martín (Samsung) aconsejó a las corporaciones anticipar sus presupuestos para dar cumplimiento a las exigencias legales. “Yo me prepararía asumiendo que esto va a ocurrir y empezaría a pensar en los presupuestos del año que viene para adaptarse a esta nueva regulación”, comenta, previniendo sobre los riesgos de actuar a última hora.



impulsan la demanda. En su opinión, “las normativas ahora no solamente afectan a TI, sino que afectan al nivel directivo, a los directores generales”.

VARIACIONES POR SECTORES

El análisis por sectores que aportan los expertos refleja ritmos desiguales en la apuesta de las organizaciones por la ciberseguridad. Mientras



berseguridad al final del año. Afirma que “en España el último trimestre supone alrededor de un tercio del negocio anual de los fabricantes”, aunque destaca el auge de Defensa y de los entornos industriales OT/IoT, donde ya hay proyectos millonarios.

En esta misma línea, Sergio Martínez (SonicWall) enfatiza la fuerza del segmento pyme, que está renovando



“ HAY QUE PONER MUCHO FOCO EN MODERNIZAR EL ACCESO REMOTO, SOBRE TODO EN LAS PYMES ”

SERGIO MARTÍNEZ,
regional manager Iberia e Italia de **SonicWall**



“ LA SEGURIDAD DE LAS IDENTIDADES, HUMANAS Y NO HUMANAS, ES UNA ASIGNATURA PENDIENTE ”

JUAN MANUEL GRANDA,
key account manager para Defensa y Seguridad de **Stormshield Iberia**



Por último, Víctor Orive (ADM Cloud & Services) señala que la IA ha democratizado los ataques, convirtiendo a las pymes en un blanco directo. Y alerta sobre que “la inteligencia artificial ha democratizado el ataque; antes las pymes no eran conscientes, pero ahora cualquiera puede ser objeto de ataque”.

IMPULSORES DEL MERCADO

En el ámbito de la ciberseguridad, la gestión de identidades y accesos (IAM) está creciendo por encima del 20%, liderando la demanda junto a la observabilidad y la seguridad del dato. Ante la madurez de soluciones tradicionales, existe la duda de si el canal está asumiendo con la necesaria agilidad el concepto de ciberresiliencia y la importancia de los SOC.

Según Sergio Martínez, de SonicWall, el canal evoluciona hacia la gestión proactiva mediante SOC e IA, y señala la urgencia de actualizar los activos existentes, porque “la mayor parte de los ataques se



producen un viernes a las 4 de la madrugada para explotar esas 48 horas críticas”, y para combatir esto recomienda migrar a EDR y desplegar capacidades de detección temprana.

Por su parte, David Gasca, de V-Valley, sitúa la observabilidad como la tecnología estrella para los despliegues corporativos durante lo

que resta de año. “Es lo que nosotros estamos percibiendo más”, explica, a lo que añade que el almacenamiento en data lakes y la orquestación SOAR ya están llegando a la mediana empresa.

Desde Stormshield Iberia, Juan Manuel Granda defiende que la identidad es hoy el objetivo prioritario de los ciberdelincuentes, afirmando que “la seguridad de las identidades, humanas y no humanas, es una asignatura pendiente”. Por ello, opina que la identidad debe viajar con el usuario en arquitecturas flexibles ligadas a la protección del dato.

En este sentido, Enrique Martín, de Samsung, puntualiza que la identidad no puede desvincularse del estado de seguridad del terminal porque “no es solo quién eres, sino también desde dónde accedes y si el dispositivo está en condiciones”, ya que la autenticación falla si el dispositivo está vulnerado.

VECTORES DE ATAQUE

« España se mantiene entre los países europeos más afectados por ciberataques. La explotación de protocolos tradicionales, las campañas de ingeniería social mejoradas con IA y el robo de credenciales están concentrando el riesgo, por lo que los expertos ponen el foco en las vulnerabilidades recurrentes y en la necesidad de aplicar una IA defensiva.

Sergio Martínez (SonicWall) alerta sobre el riesgo crítico de las conexiones remotas tradicionales porque “el protocolo SSL VPN es un protocolo vulnerable; más de la mitad de las brechas se producen por culpa de esa vulnerabilidad”. Y detalla patrones donde el robo de credenciales deriva en cifrado, para lo que defiende el uso de IA agéntica local en los dispositivos.

Desde su punto de vista, Víctor Ori-ve (Cloud & Services), percibe que el



factor humano sigue siendo un vector muy explotado, y explica que “son los mismos empleados los que buscan la alternativa de poder seguir accediendo, saltándose las reglas”, mientras la IA permite crear engaños hiperrealistas que se le escapan al usuario.

Frente a estas amenazas, Juan Manuel Granda (Stormshield) apuesta por aplicar principios de Zero Trust de forma integral. “No nos creemos nada de nadie ni de nada; todo tiene que ser verificado en todo momento, viajando con el dato y con la identidad”, y por ello aboga por esquemas donde la encriptación asegure la información de punta a punta.

“ LA IA ES AHORA MISMO EL ESLABÓN MÁS DÉBIL DE LA CADENA ”

DAVID GASCA,
director de Marketing y
Operaciones de Ciberseguridad
de **V-Valley**



Coincidiendo con sus homólogos Enrique Martín (Samsung), resalta la conveniencia de adoptar la IA de forma segura para potenciar la productividad, ya que opina que “tienes que poder utilizar la inteligencia artificial para hacer cosas porque aumenta la productividad, no puedes bloquear todo”, un contexto en el que apuesta por el procesamiento local en dispositivos con NPU.

HACIA EL MODELO DE MSSP

Los servicios gestionados crecen a un ritmo superior al 40% en España y se están consolidando como la vía de futuro para el canal. Sin embargo, pasar de la venta transaccional a la suscripción recurrente acarrea desafíos operativos y de capacitación que no se están resolviendo a la velocidad esperada.

En este sentido, Víctor Ori-ve, de ADM Cloud & Services, pone de relieve las barreras que frenan a los distribuidores tradicionales, observando que “muchos quieren ser MSP, pero pocos saben hacerlo; dar el salto no es fácil y requiere estandarizar la propuesta”. Además, critica la falta de herramientas en algunos fabricantes para integrar aprovisionamiento y facturación.

David Gasca explica cómo V-Valley facilita la transición mediante soluciones flexibles de marca blanca, comentando que “habilitamos al partner más pequeño, o que no quiere invertir, para ofrecer servicios de manera mensual y flexible”, lo que les permite comercializar servicios para pymes sin asumir riesgos de infraestructura.

Asimismo, Sergio Martínez, de SonicWall, alerta sobre la obsolescencia del parque instalado de cortafuegos en Europa, diciendo que “el tiempo me-»

dio de parchear cualquier dispositivo de red en general es alto y, en el caso de los firewalls, es de más de 180 días”, lo que en su opinión demuestra que tiene sentido su estrategia de ofrecer servicios de SOC y parcheo gestionado al canal.

Por su parte, Enrique Martín, de Samsung, incide en que atender a las pymes requiere industrializar los procesos de servicio con políticas estandarizadas. Comenta que “el negocio fácil está en la gran cuenta, pero el volumen y la oportunidad real está en la pyme”.

En último lugar, Juan Manuel Granda, de Stormshield, asegura que la migración hacia el servicio exige planificación estratégica de largo recorrido. “Es una transición que exige una visión estratégica”, señala, “tienes que invertir ahora para obtener un retorno que no es inmediato”, por lo que recomienda comprometerse con acompañar a los distribuidores en su necesaria capacitación.

PROPUESTAS PARA FINAL DE AÑO

Ante el panorama actual de ciberamenazas y teniendo en cuenta las previsiones de inversión empresarial para el resto de 2026, los portavoces de estas empresas resumen su propuesta en materia de ciberseguridad para



los próximos meses. Comienza Víctor Orive, de ADM Cloud & Services, anunciando la incorporación a su catálogo de tecnologías para la protección de aplicaciones, API y mitigación de bots maliciosos, mencionando acuerdos estratégicos para estructurar paquetes atractivos para el MSP.

En el ámbito de la movilidad, Enrique Martín, de Samsung, destaca la inclusión de protección criptográfica

avanzada en sus terminales de corte empresarial, y asegura que “en los últimos modelos hemos incorporado el cifrado postcuántico, pensando en que el dispositivo estará seguro durante años”, y que también han profundizado en la integración de la telemetría móvil con los SIEM y SOC.

Desde SonicWall, Sergio Martínez repasa sus novedades pensadas para acabar con las vulnerabilidades del acceso y, en este campo, comenta, “presentamos Cloud Secure Edge para sustituir la tecnología SSL VPN por acceso remoto ZTNA verdaderamente seguro”, y también su nuevo Endpoint integrado y ligero para blindar los puestos de trabajo.

En el caso de Stormshield, Juan Manuel Granda detalla los pilares de su hoja de ruta tecnológica, destacando que “Stormshield Encryption Platform permitirá al cliente mantener el control total sobre las claves de cifrado de sus datos en la nube”, y también adelanta el futuro lanzamiento de soluciones de comunicación mallada simplificada con cifrado postcuántico.

Finalmente, David Gasca aporta más detalles sobre las iniciativas de V-Valley para estrechar lazos con el ecosistema de socios de cara a final de año, y comenta que “lanzamos el R-Evolve AI Tour para acercarnos a los partners en distintas ciudades y reforzamos nuestro equipo con hasta casi 90 especialistas”, además de destacar su presencia en citas clave del sector como ENISE y Madrid Tech Show. ■

MÁS INFO +

» [Evolución de las ciberamenazas y claves para la protección de las organizaciones](#)



COMPARTIR EN REDES SOCIALES

SAMSUNG



Diseñado para proteger su negocio

Galaxy Z Fold8 for business

Samsung Knox



Víctor Orive, CEO de ADM Cloud & Services

“HAY QUE BASARSE EN PROTEGER LAS IDENTIDADES, EL DATO Y EL SERVICIO”

« El panorama actual de las ciberamenazas está experimentando una profunda transformación empujada principalmente por el desarrollo acelerado de la inteligencia artificial. Como comenta Víctor Orive, esta tecnología está abriendo constantemente nuevas superficies y vectores de ataque dentro de las organizaciones. A pesar de que muchas empresas sostienen la falsa creencia de que tienen todo su perímetro protegido y su círculo de seguridad totalmente cerrado, la realidad diaria demuestra que continuamente están surgiendo nuevas vulnerabilidades que ponen en riesgo la continuidad del negocio y la integridad de los datos corporativos.

Para hacer frente con éxito a esta compleja situación, Orive opina que la estrategia de protección de las organizaciones debe fundamentarse



en tres pilares: la salvaguarda de las identidades digitales de los usuarios, la protección exhaustiva y continua del dato corporativo y el despliegue de herramientas especializadas suministradas bajo el modelo as-a-Service. Estas soluciones deben garantizar una resiliencia adecuada y estructurada, permitiendo

a las empresas ejecutar una recuperación rápida, ágil y eficiente ante cualquier tipo de ciberataque, incidente de seguridad o desastre operativo que ponga en peligro sus operaciones.

Ante esto, señala Víctor Orive, “en ADM Cloud & Services estamos ampliando activamente nuestro

catálogo de soluciones avanzadas de ciberseguridad. Entre las incorporaciones más destacadas figura la integración de tecnologías especializadas en la mitigación y control del tráfico de bots a través de nuestra alianza con Black Wall, abordando un vector de riesgo crítico en la red. Asimismo, estamos cerrando el círculo de protección de aplicaciones clave mediante la incorporación de las soluciones avanzadas de Barracuda, fortaleciendo la defensa de los entornos corporativos”. Su estrategia, explica, está concebida con la meta de ponérselo fácil al proveedor de servicios gestionados (MSP), que es su cliente prioritario. Para ello, empaquetan y estructuran estas herramientas en soluciones listas para ser revendidas de forma sencilla, ágil y rentable por el canal de distribución.

Enrique Martín, head of Large Enterprise de Samsung Iberia

“DAMOS HERRAMIENTAS DE HARDWARE PARA GARANTIZAR LA SEGURIDAD A NUESTROS PARTNERS”

El entorno de la ciberseguridad empresarial se enfrenta actualmente a tres dinámicas fundamentales que condicionan la estrategia de protección. En primer lugar, según Enrique Martín, “asistimos a una aceleración sin precedentes de las ciberamenazas impulsada por la inteligencia artificial. Los ataques no solo se propagan a una velocidad mucho mayor, sino que resultan cada vez más sofisticados, novedosos y técnicamente elaborados”. En segundo lugar, destaca la gestión de la identidad como un factor crítico para certificar la autenticidad del usuario. En este contexto, opina que el dispositivo endpoint desde el que se accede a los sistemas corporativos está adquiriendo un rol estratégico como elemento clave de verificación y puerta de entrada a la red empresarial. Por último,



ante la creciente complejidad de este ecosistema, señala que las organizaciones se encuentran en el momento idóneo para delegar la gestión operativa de su seguridad en proveedores especializados de servicios gestionados (MSSP).

Frente a esta coyuntura, la propuesta de valor de Samsung

Iberia aborda la seguridad desde la propia arquitectura del hardware, garantizando que el dispositivo sea seguro por diseño. Sobre esta base física, explica, “facilitamos una completa suite de servicios para que nuestros partners del canal de distribución puedan implementar y operar la seguridad de manera

óptima en las empresas. Un claro ejemplo de este compromiso preventivo es la incorporación del cifrado postcuántico en nuestros dispositivos móviles más avanzados, como la serie S26, preparando a las organizaciones desde hoy para responder a los desafíos criptográficos del futuro”.

En el ámbito de los servicios, señala, “continuamos evolucionando nuestras soluciones para asegurar el pleno cumplimiento normativo de las flotas corporativas”. Esto abarca el control del inventario de equipos, la actualización constante del software y la telemetría en tiempo real, proporcionando las herramientas necesarias para asegurar el endpoint, además de capacitar al canal para gestionar eficazmente la ciberseguridad empresarial.

David Gasca, director de Marketing y Operaciones de Ciberseguridad de V-Valley

“LA IA ESTÁ ACELERANDO TODO A UN RITMO DEMASIADO RÁPIDO Y EXPONENCIAL”

La evolución reciente de las ciberamenazas discurre de manera paralela al avance acelerado de la inteligencia artificial. Si bien la IA es una herramienta indispensable para fortalecer las defensas de las empresas, también está siendo explotada masivamente por los ciberdelincuentes. David Gasca explica que los atacantes utilizan la IA para abrir nuevos vectores de agresión, como campañas de phishing automatizadas y ultra sofisticadas que desbordan la capacidad de respuesta de los Centros de Operaciones de Seguridad (SOC) a la hora de orquestar y analizar los datos. Esta velocidad de ataque está generando una presión inédita sobre las infraestructuras de protección tradicionales.

A esta amenaza externa se suma un desafío interno crítico: la proliferación del Shadow IT mediante el uso no

regulado de herramientas de IA por parte de los empleados. Gasca apunta que al subir información sensible a plataformas externas sin el control del departamento de TI, las organizaciones se hallan en una fase temporal de pérdida de control, y opina que esta situación solo comenzará a estabilizarse a

medida que se implemente un marco regulatorio adecuado y las empresas adapten sus políticas de gobernanza digital. Afortunadamente para el sector, comenta, los principales fabricantes del mercado están reaccionando con rapidez para desarrollar soluciones enfocadas en proteger los datos corporativos frente

a estas prácticas.

David Gasca termina destacando que “en V-Valley trabajamos estrechamente con nuestros aliados tecnológicos habituales para ofrecer soluciones de protección adaptadas a este nuevo escenario, incorporando además marcas especializadas para cubrir nichos específicos de mercado”. La mayoría de los fabricantes del sector están desplegando actualmente herramientas para asegurar la interacción con la IA y proteger la información de las organizaciones. No obstante, anticipa que el mercado experimentará una selección natural en los próximos años, en la que únicamente prevalecerán aquellas propuestas consolidadas que respondan con efectividad a las necesidades reales de las empresas y del canal de distribución tecnológico y sus clientes finales.



STORMSHIELD

« Una amplia propuesta y una seguridad óptima »

PROTECCIÓN DE LOS ENTORNOS SENSIBLES

