

#DEBATE IT

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.

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-



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.

NIS-2



P - Property

R - Rent

D - Occupancy

P - Maintenance

E - Eviction

R - Repairs

T - Tenants

Y - Yield

M - Management

A - Accounting

N - Negotiation

A - Advertising

G - Guidelines

E - Expenses

M - Marketing

E - Efficiency

N - Inspection

T - Transactions

¿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

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.

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 anterior-

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

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

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 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**

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



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







la cadena de suministro y proporcionando más previsibilidad.

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



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

Hacer negocios con Exclusive Networks ahora es más fácil.

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



¡Únete hoy y descubre Exclusive Access!



“ 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 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

“ 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**

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,



Clica en la imagen para ver la galería

implementar estrategias de Fin-Ops 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”.



Clica en la imagen para ver la galería

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

Tu negocio
+ nuestra
plataforma
= una experiencia
más fluida

INGRAM MICRO[®]

Distributing Simplicity



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”.

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 ten-

“ LOS ATAQUES SON CADA VEZ MÁS INTELIGENTES Y POR ESO LAS DEFENSAS DEBEN SERLO TAMBIÉN ”

SERGIO MARTÍNEZ,
country manager de
SonicWall Iberia

dencias 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



Kaspersky Next
XDR Optimum

Amplía las capacidades, no los presupuestos

Mejora tu ciberseguridad con
Kaspersky Next XDR Optimum

kaspersky



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 auto-

matización 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 plataforma, 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. ■

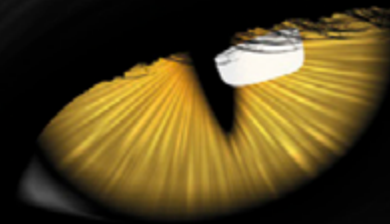
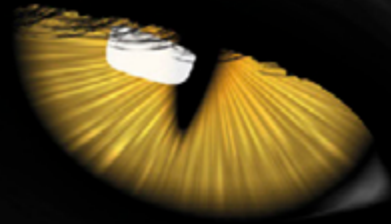
MÁS INFO +

» [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](mailto:serval@servalsales.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.

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



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

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, seguri-

dad 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 escribanos a spain@sonicwall.com.