Desde 2020 el mercado de la ciberseguridad acumula un crecimiento del 70 %

No hay fin para el crecimiento de la ciberseguridad: identidad, normativas, IA y servicios gestionados señalan la oportunidad

El mercado de la ciberseguridad seguirá creciendo de forma sostenida. A pesar de la madurez que ha alcanzado en las inversiones de las empresas y las administraciones públicas, sigue impulsada por un ramillete de factores que no deja de crecer: la protección de la identidad, el cumplimiento de las normativas, el uso de la inteligencia artificial o el despliegue de los servicios gestionados. Pero también con un mensaje claro para el canal: el verdadero valor estará cada vez más en la especialización, la capacidad de integración y la prestación de servicios de alto valor añadido.

ADM Cloud & Services, Arrow, Exclusive Networks, Ingram Micro, TD SYNNEX y V-Valley analizan las tendencias que están transformando el negocio de la ciberseguridad y estas múltiples oportunidades.

Marilés de Pedro

Identidad, observabilidad e IA, ejes de la inversión

El mercado de la ciberseguridad mantiene su condición de ser uno de los segmentos más dinámicos del sector TIC. Tras alcanzar en 2024 los 2.500 millones de euros en España —con un crecimiento del 14,2 % y una subida acumulada cercana al 70 % desde 2020—, el ecosistema del canal afronta 2026 con nuevas prioridades: identidad, observabilidad, automatización, protección del dato y servicios gestionados impulsados por inteligencia artificial.

Los mayoristas aseguran que el mercado está entrando en una fase de madurez. Ángel García, director del área de ciberseguridad de Arrow, señaló que "la inversión de las empresas se orienta menos a incorporar nuevas soluciones y más a optimizar, integrar y obtener un valor real de sus sistemas". En este contexto, destaca como focos prioritarios "la gestión de la identidad, la protección y la monitorización del dato, y el Zero Trust". No olvidó apelar a la inteligencia artificial. "Va a ser clave saber gestionar y sacar el máximo rendimiento a esta tecnología". Las empresas están "invirtiendo con un criterio más claro y más maduro, apoyándose en plataformas y en la búsqueda de resultados concretos".

> "Las herramientas centradas en la formación y en la concienciación del usuario son cada vez más importantes"

Para David Gasca, director de marketing y operaciones del área de ciberseguridad de V-Valley, el crecimiento alcanza a todas las áreas del mercado: no solo el negocio que aportan fabricantes especializados, con un menor recorrido en el mercado y con mayores tasas de crecimiento; también los proveedores más maduros y consolidados que incorporan nuevas tecnologías a la oferta. "Es el caso, por ejemplo, del área de la observabilidad, donde estamos viendo grandes proyectos", puntualizó.

También los mayoristas acceden a nuevas áreas de especialización: "En V-Valley hemos incorporado soluciones de automatización de ataques, con fabricantes que cuentan con una oferta en torno a la visibilidad de red y a los ataques externos", explicó. "Es otro nicho de crecimiento para este año".

Javier Jurado, director de desarrollo de negocio para el mercado ibérico de Exclusive Networks, insistió en el auge de la identidad como el nuevo perímetro de seguridad, del que la adquisición de CyberArk por parte de Palo Alto es claro ejemplo. "Es un claro vector de crecimiento". Además de áreas más "tradicionales" como la protección del *cloud* y del SASE, destacó el crecimiento de soluciones ligadas a la exposición continua al riesgo y la automatización de los ataques desde el punto de vista defensivo.

La desaparición del perímetro tradicional fue otro de los elementos de consenso de la mesa. Martín Trullás, director del área de Advanced Solutions de Ingram Micro, insistió en que "ya no hay perímetro" y que, en consecuencia, "lo más importante es la gestión de la identidad, la gobernabilidad y cómo nos movemos ahora en un entorno abierto". La persona, por tanto, es el punto débil de la cadena y alertó sobre el efecto de la IA en la sofisticación de los ataques: "Los malos van por delante de nosotros: hacen que la gente cometa muchos errores".

Trullás alertó de que la escasez de componentes está empezando a impactar en el mercado de la ciberseguridad, lo que se notará en el segundo semestre. "Muchos proyectos se van retrasando y va a seguir fortaleciéndose un modelo híbrido en el que, ante las dificultades de suministro, haya empresas que opten, de manera temporal, por un hiperescalar, con un modelo *cloud*, hasta que se alivie esta falta de componentes.

Víctor Orive
CEO de **ADM Cloud & Services**

Víctor Orive, CEO de ADM Cloud & Services, insistió en la vulnerabilidad y la fragilidad de las personas, lo que señala otra área de oportunidad. "Las herramientas centradas en su formación y en su concienciación son cada vez más importantes".

Ángel García
director del área de ciberseguridad de **Arrow**

"Las empresas están invirtiendo con un criterio más claro y más maduro, apoyándose en plataformas y en la búsqueda de resultados concretos"

NIS2 y DORA: del cumplimiento a la supervivencia

La entrada en vigor de las nuevas normativas europeas está teniendo un impacto directo en el mercado. Es el caso, por ejemplo, de DORA o de NIS2, cuya trasposición, que debía haberse aprobado en octubre de 2024, se prevé que se produzca a finales de este año. Carlos Serra, *technical practices manager* de TD SYNNEX España, señaló su papel tractor para impulsar inversiones en ciberseguridad. En el caso del mayorista el portavoz aseguró que lo están notando en el negocio. "Estamos realizando formaciones específicas para ayudar al canal a entender y aplicar estos marcos regulatorios".

Claude Mythos y el nuevo escenario de amenazas

Uno de los ejemplos que salió a relucir durante el debate fue el impacto de nuevas herramientas basadas en IA, como Claude Mythos, el modelo experimental de Anthropic especializado en detección de vulnerabilidades, muchas de ellas existentes desde hacía años en áreas como los sistemas operativos, las bases de datos o los navegadores. Javier Jurado aprovechó para insistir en la oportunidad que supone proteger todas ellas. "Con que los *hackers* encuentren una ya es suficiente".

El debate puso sobre la mesa cómo la IA está acelerando tanto la capacidad defensiva como ofensiva. En el caso de Claude Mythos, pensada para encontrar vulnerabilidades y alertar de ello, si cae en las manos equivocadas, el fin puede ser otro. Por ello Anthropic ha decidido restringir el acceso "solo" a unos cuantos fabricantes (Apple, Amazon o Microsoft entre ellos).

David Gasca destacó el auge de las soluciones ligadas a la exposición al riesgo en la cadena de suministro, clave en normas como NIS2, "lo que denota la preocupación que tienen las empresas". Recordó el portavoz de V-Valley que en el mercado conviven fabricantes con herramientas específicas para cumplir con las normativas en el nivel de auditoría y para saber con qué aplicaciones cuentan, junto con proveedores con una oferta que permite una mayor automatización y visibilidad. "Hemos visto muchos ataques dirigidos a la cadena de suministro", alertó, lo que hace especialmente atractivas herramientas y fabricantes vinculados con su protección.

Javier Jurado alertó de que el comportamiento del mercado está siendo muy distinto, atendiendo a si la norma está vigente o no. En el caso de DORA, normativa en vigor, el mercado está tremendamente activo. "El segmento de la banca y de las aseguradoras está a pleno rendimiento", aseguró. "Los comités de dirección son muy conscientes del riesgo y de las multas que acarrea en el caso de un incumplimiento". En cambio, con NIS2, pendiente la transposición, la actividad es menor aunque, desveló, algunas empresas ya se están dando cuenta de que van a tener que prepararse. Y, el primer paso, puntualizó, es tener control. "Los *partners* están lanzando iniciativas relacionadas con el aumento de la visibilidad y la priorización de vulnerabilidades ya que no se puede proteger lo que no se ve".

Víctor Orive corroboró que, en relación a NIS2, muchas empresas se están anticipando a la llegada de la transposición. La preocupación ya no se limita a las sanciones económicas sino también a cómo afecta a la dirección y a la continuidad del negocio. "Las empresas pueden perder credibilidad y confianza; además de hacer frente a las consecuencias que puede tener en su negocio una parada". Incluso, alertó, "para una pequeña empresa puede suponer su cierre".

Ángel García añadió otro factor crítico: la necesaria obligación de que toda la cadena de suministro cumpla la normativa, lo que incluye a las pymes. "Estas empresas trabajan para las grandes corporaciones y pueden ser un foco de ataque, por lo que también ellas deben estar adecuadamente protegidas y cumplir con NIS2". ¿El riesgo en caso de ser atacadas? Quizás ser expulsadas de la cadena.

Ataques más sofisticados... y "democráticos"

La ciberdelincuencia sigue "reposando" en estructuras organizadas, distribuidas y con un claro enfoque económico. El año pasado, en España, el Instituto Nacional de Ciberseguridad (INCIBE) gestionó, a través de su CERT, un 26 % más de incidentes de ciberseguridad, en comparación con 2024, alcanzando un total de 122.223 incidentes. "La ciberdelincuencia está cada vez más profesionalizada", recordó Martín Trullás. "El *ransomware*, con su variante como servicio, ya está industrializado, y está al servicio de estados y empresas". La IA, insistió, está facilitando ataques más complejos, personalizados y orientados también al daño reputacional.

> "La protección de la identidad, como el nuevo perímetro, es un claro vector de crecimiento"

Ángel García coincidió en que la IA ha profesionalizado todos los ataques, que son mucho más sofisticados y dirigidos, buscando un fin económico. "Los ciberdelincuentes tienen claro cuál es el retorno de inversión del ataque".

Javier Jurado habló de una "democratización del ataque": "Alguien que no sabía programar pero que tenía una motivación y una información privilegiada, ahora tiene capacidad para llevar a cabo determinados ataques gracias a la IA: no hace falta ser un súper *hacker* para encontrar alguna grieta". Claude Mythos, el modelo experimental de Anthropic, puede ser un "buen" ejemplo. Aunque la compañía restringió el acceso al código fuente a algunas empresas, la cadena de suministro ha dejado al descubierto algunos caminos. "Ha sido a través de una de las librerías que se alimentan para entrar en el modelo lo que permitió a algunas empresas, que no estaban en ese grupo selecto, acceder a las credenciales y a la URL en la que Anthropic publica sus modelos".

David Gasca, por último, alertó del cambio en el foco del ataque. "Ahora el objetivo es conseguir una credencial válida dentro de la red. Antes el objetivo era cifrar los datos de la compañía y pedir por ellos un rescate". Una realidad que explica el crecimiento de tecnologías PAM, IAM, MFA y de modelos de autenticación reforzada.

Plataformas frente al *"best of breed"*

La "convivencia" en el mercado de fabricantes con una propuesta, global, centrada en el concepto de plataforma con los proveedores más especializados centró una parte del debate. Una dicotomía que también se traslada al canal. "Hay dos arquetipos de *partners*", recuerda Carlos Serra. "Uno, muy focalizado en cierto tipo de soluciones, ya sea en una tecnología o en un fabricante; y, por otro lado, compañías que van adquiriendo volumen y que han decidido apostar por fabricantes con una oferta global".

Javier Jurado
director de desarrollo de negocio para el mercado ibérico de **Exclusive Networks**

A juicio de Ángel García esa elección debe tener en cuenta el talento y los profesionales de los que dispone el *partner* para abordar el despliegue de determinadas tecnologías. "Cuando cuenta con una plantilla más limitada, con un conocimiento de un número reducido de tecnologías, la opción más natural es optar por fabricantes que apuestan por la plataforma".

Por otro lado, aquellos *partners* que prefieren un modelo *"best of breed"* apuestan por una mayor especialización. "Aunque las marcas con un modelo de plataforma siguen creciendo mucho, seguirá existiendo espacio para fabricantes especializados", pronostica el director del negocio de ciberseguridad en Arrow.

Martín Trullás apunta que la orientación del canal tiene que ver con el perfil de sus clientes: "Si se trata del segmento de la pyme o del *midmarket* se apuesta más por las opciones de plataforma", explica. "En las grandes cuentas, que cuentan con un CISO y que tienen que hacer frente a la gestión de entornos más complejos, se opta muchas veces por soluciones diversas y especializadas".

Una convivencia que corroboró Javier Jurado: "Hay *partners* muy orientados a la prestación de servicios que necesitan una plataforma, lo que les permite una mayor estandari-

Martín Trullás,
director del área de Advanced Solutions de **Ingram Micro**

> "La IA está facilitando ataques más complejos, personalizados y orientados al daño reputacional"

zación; y otros que apuestan por un modelo *best of breed* y que buscan acercar al cliente las últimas innovaciones". Por último, a juicio de David Gasca el crecimiento de las plataformas también responde a la "presión" de los fabricantes que apuestan por este modelo: "Cada vez incorporan más tecnologías y soluciones, lo que les ha permitido incrementar su posicionamiento y sus ventas". Una realidad que, corroboró, también deja espacio para aquellos proveedores "disruptivos, que cuentan con tecnologías muy innovadoras".

Incluso es posible la colaboración. Víctor Orive asegura que en su oferta, compuesta por fabricantes de tamaño mediano, que están incorporando funcionalidades a sus plataformas para seguir creciendo, "están muy abiertos a colaborar con otros proveedores e integrar sus tecnologías para complementar su plataforma".

Proyectos más grandes

El mercado de la ciberseguridad también está experimentando un importante incremento en el volumen y dimensión de los proyectos: si hace apenas unos años un gran pedido se identificada con un montante de un millón de euros, ahora es frecuente observar proyectos en los que los millones se cuentan con un doble dígito.

Un crecimiento que está permitiendo igualar el peso his-

OT: un mercado aún en desarrollo

El mercado de protección de entornos OT (Operational Technology) en España todavía es relativamente pequeño frente al conjunto de la ciberseguridad, pero es uno de los segmentos con mayor potencial de crecimiento por la convergencia IT/OT, la presión regulatoria y el aumento de ataques sobre infraestructuras críticas.

A nivel internacional, el mercado mundial de seguridad OT crecerá a ritmos cercanos al 20 % anual durante la próxima década, impulsado por la digitalización industrial y la necesidad de proteger infraestructuras críticas. "Debería ser una oportunidad", declaró Carlos Serra. En su análisis del mercado señaló que mientras que la inversión en el área TI no deja de crecer en el segmento OT "siguen con diodos muy básicos para cortar la comunicación entre ambas áreas y evitar los problemas". El portavoz de TD SYNNEX alertó de la complejidad que supone proteger estos entornos industriales. "Se trata de máquinas, con un alto coste, gestionadas por dispositivos obsoletos, que no cuentan con sistemas de ciberseguridad adecuados".

Sin embargo, los ataques sobre los entornos industriales están aumentando con fuerza. Según NCC Group entre abril de 2025 y marzo de 2026, las organizaciones industriales concentraron el 30 % de todos los incidentes globales de *ransomware*. En España, el crecimiento de OT está especialmente ligado a la industria manufacturera, las empresas de *utilities* y energía, el segmento de los transportes y la sanidad.

El canal, poco a poco, está empezando a ver proyectos relevantes. David Gasca aseguró que se están desplegando proyectos de cierta entidad en este apartado, con soluciones especializadas para proteger entornos OT, con un tamaño similar al que tenían los grandes proyectos de *firewall* o EDR de hace unos años, aunque con ciclos de venta mucho más largos.

Uno de los grandes frenos sigue siendo el legado tecnológico. Muchos entornos industriales operan con PLC, SCADA y maquinaria crítica diseñada hace décadas y sin capacidades nativas de seguridad. Eso complica tanto la protección como la actualización de sistemas. "Se trata de tecnologías obsoletas que hay que emigrar", señaló Ángel García, que recordó que las áreas primigenias fueron la industria, las *utilities* y la energía. "Esperamos un boom en el mercado de la sanidad para el control de dispositivos de OT".

También hay un déficit importante de talento especializado. El perfil OT exige conocimientos industriales y de ciberseguridad al mismo tiempo, algo todavía escaso en el mercado.

"Estamos realizando formaciones específicas para ayudar al canal a entender y aplicar los marcos regulatorios como DORA o NIS2"

Carlos Álvarez
technical presales consultant para **TD SYNNEX** España

tórico de otras áreas del negocio TIC. "Antes los grandes proyectos solo se trabajaban en el área de los centros de datos. Ahora los fabricantes de ciberseguridad también son capaces de llevar a cabo grandes despliegues", subrayó Ángel García.

Un crecimiento que no solo beneficia a los grandes fabricantes. "Hay grandes proyectos con grandes fabricantes de ciberseguridad, pero los fabricantes más pequeños también están alcanzando cifras que hace años habríamos considerado inverosímiles", señaló Javier Jurado. Además, destacaron que muchos de esos proveedores especializados, pese a contar con menor volumen de negocio, "están creciendo a un ritmo mayor que los grandes".

IA: oportunidad de negocio y riesgo

En la mesa quedó claro que la inteligencia artificial exhibe una gran dicotomía: es, a la vez, una gran oportunidad y también un riesgo.

David Gasca se mostró especialmente contundente: "La IA es el mayor riesgo al que nos enfrentamos en el mundo de la ciberseguridad". Frente a la afirmación, muy repetida, de que el usuario es el eslabón más débil de la cadena, Gasca señaló a la IA como tal. Gasca alertó sobre implementaciones inseguras y modelos con acceso masivo a los datos corporativos. "Si antes un *hacker* tenía que esforzarse en hacer un ataque de *phishing* o un *malware* complejo, ahora la IA va a abrir las puertas de las compañías". Las empresas están implementando modelos de IA que les ayudan a

David Gasca,
director de marketing y operaciones del área de ciberseguridad de **V-Valley**

> "Ahora el objetivo es conseguir una credencial válida dentro de la red. Antes era cifrar los datos de la compañía y pedir por ellos un rescate"

ser más ágiles y eficientes "pero que no están protegidos". De nada vale, insistió, en formar al usuario, "si las empresas hacen uso de una IA que no cuenta con una correcta gestión de permisos". Gasca insistió en la dicotomía. "Es un nuevo frente, con un enorme riesgo, que no está protegido, lo que supone una gran oportunidad para el ecosistema de ciberseguridad".

Javier Jurado puso el foco en el *shadow AI*, en el uso real que se está haciendo de esta tecnología en las organizaciones y en los riesgos de filtración de datos. Incluso alertó del *jailbreaking*, el proceso de explotar los defectos de un dispositivo electrónico bloqueado para instalar software distinto al que el fabricante ha puesto a disposición del dispositivo. "El eslabón más débil son aquellos usuarios que disfrutan de ciertos privilegios. La IA se está utilizando en muchas partes de la empresa porque lo está adoptando el usuario desde abajo".

> La IA es el mayor riesgo al que se enfrenta el mundo de la ciberseguridad

Proteger la IA es una oportunidad que está siendo observada por los *partners* que prestan servicio para desarrollar sus propias soluciones: "Hay *partners* que están creando herramientas para automatizar el diagnóstico o la orquestación y acuden a los mayoristas para ayudarles a distribuirlas", explicó Jurado.

Para Orive la IA es más oportunidad que riesgo y en relación a la incorporación de la IA que han hecho los fabricantes a sus propias soluciones, muchos *partners* "lo observan como una gran oportunidad, sobre todo para abarcar más mercado y más clientes con los mismos recursos".

MSP y servicios gestionados: oportunidad con barreras

El desarrollo de servicios gestionados de seguridad sigue creciendo. Es una de las áreas de mayor ascenso dentro del sector de la seguridad en España y Europa. La combinación de escasez de talento, aumento de ataques, presión regulatoria y complejidad tecnológica está acelerando la externalización de servicios de seguridad.

A nivel global, el mercado de servicios gestionados de seguridad mantiene tasas de crecimiento superiores al 10 % anual. Según MarketsandMarkets, la demanda mundial alcanzará los 66.830 millones de dólares en 2030, frente a los 39.470 millones de 2025. En paralelo, Canalys/Omdia estima que el mercado global de servicios TI gestionados moverá 610.000 millones de dólares en 2025 y señala a la ciberseguridad como una de las áreas con mayor crecimiento y rentabilidad para el canal. Los segmentos que más están creciendo en España son aquellos vinculados con el MDR *(Managed Detection & Response)*, SOC *as a Service*, EDR/XDR gestionado, el SASE gestionado, la gestión de vulnerabilidades o la monitorización 24x7. Según Mordor Intelligence, MDR ya representa más del 27 % del mercado MSSP mundial y es la categoría que más crece.

Javier Jurado explicó que muchos fabricantes, para seguir creciendo y no solo en el ámbito de las grandes cuentas, están impulsando el modelo MSP para expandirse en la pyme y generar negocio recurrente. "Es un formato MSP perfecto porque el *partner* puede vender sus servicios y crecer a través de esta vía".

Sin embargo, no es un modelo exento de dificultades operativas: "Montar un servicio gestionado 24x7 es muy costoso y requiere mucho talento especializado", alerta Ángel García.

Aunque muchos fabricantes están impulsando modelos MSP y MSSP, todavía existen limitaciones identificadas con la integración *multitenant*, el *billing* automatizado, el aprovisionamiento, la automatización operativa o la necesaria coordinación con otros proveedores.

Por eso los mayoristas están ganando peso como habilitadores de este modelo suministrando al ecosistema de distribuidores plataformas de automatización, SOC compartidos, soporte técnico especializado o soluciones de financiación. "Estamos ayudando a los *partners* a dar ese tipo de servicio mediante plataformas automatizadas y servicios gestionados", señaló Martín Trullás. "Contamos con herramientas automatizadas para ofrecer la provisión y, después, la gestión y mantenimiento; lo que nos permite seguir creciendo en este negocio".

Asunción desigual

El modelo MSP/MSSP sigue evolucionando dentro del canal, aunque no todos los *partners* están afrontando esta transición de la misma manera. En el caso de ADM Cloud, se trata de un mayorista que nació bajo este modelo. "Continuamos muy ligados a este enfoque aunque cuesta mucho convertir", reconoce Orive. Actualmente, entre un 50 y un 60 % de su ecosistema de clientes opera parcialmente bajo este modelo. Un ecosistema conformado por un perfil de *partner* pequeño y mediano que trata de simplificar al máximo la gestión tecnológica. "De manera mayoritaria suele adoptar una sola tecnología o una sola plataforma", desvela. Esta estrategia les permite apoyarse en el SOC del propio fabricante para cubrir todo el entorno gestionado.

Orive advirtió de la complejidad que supone trabajar con múltiples plataformas en un entorno MSP: "Si tienes varias plataformas, se trata de distintos servicios, lo que obliga a agruparlos en un *hub* y a disponer de recursos internos para gestionarlo". Por ello, "el *partner* pequeño o mediano que se orienta al modelo MSP siempre utiliza una plataforma de referencia".

Ángel García recordó que el modelo MSP nació en el área del centro de datos hace muchos años. "El gran reto aparece cuando se introduce la ese de seguridad", un mercado que requiere de un conocimiento específico. "Muchos proveedores tradicionales de servicios gestionados, centrados en el desarrollo de otras áreas, no cuentan con él". En este escenario, considera que el papel del mayorista es clave para ayudar al *partner* allí donde no dispone del conocimiento o los recursos necesarios.

Una tendencia que corroboró Martín Trullás, destacando que algunos fabricantes están acelerando su entrada en este mercado mediante adquisiciones: "Está habiendo mucha compra de pequeñas empresas de servicios gestionados para incorporarlas a su catálogo".

No todos los fabricantes cuentan con el mismo desarrollo para trabajar bajo un modelo MSP. "Hay fabricantes que tienen mucho más interiorizado este modelo y ofrecen más facilidad para generar *tenants* o gestionar entornos multicliente", explicó Javier Jurado. Otros, sin embargo, cuentan con un desarrollo menor. A su juicio, un verdadero modelo MSP requiere capacidades específicas: "Se necesita una gestión *multitenant*, una segmentación clara por clientes y una facturación lo más automatizada posible".