ENCUENTROS IT RESELLER

EL ROL DEL PROVEEDOR DEL SERVICIOS GESTIONADOS ANTE EL ESTADO DE LA CIBERSEGURIDAD EMPRESARIAL

ORGANIZA

it Reseller TECH&CONSULTING

PATROCINADOR

ESET Cybersecurity
Progress. Protected.

LA IA ACELERA LA DISRUPCIÓN DEL MSP Y SITÚA LA CIBERSEGURIDAD EN EL CENTRO DEL NEGOCIO

#ENCUENTROSITRESELLER

La irrupción de la IA está transformando el negocio de los proveedores de servicios gestionados, automatizando tareas clave y obligando a los proveedores a replantear su propuesta de valor. La ciberseguridad emerge como el pilar más estable para sostener ingresos y diferenciarse en un mercado cada vez más competitivo.

El mercado de los proveedores de servicios gestionados (MSP) vive un punto de inflexión. La inteligencia artificial se ha convertido en la variable que más está transformando la operativa, la oferta de servicios y la relación con los clientes. De hecho, el 48% de los MSP identifica la IA y la automatización como la principal necesidad de sus clientes, por encima incluso de la seguridad o el backup.

Pero esta demanda llega en un contexto de presión creciente, con el 71% de los MSP que afirma que captar nuevos clientes es su mayor desafío. El tamaño medio de los contratos se ha reducido drásticamente, pasando del 75% al 41% en acuerdos superiores a 25.000 dólares anuales. La competencia aumenta, los márgenes se estrechan y demostrar valor rápido se ha convertido en una exigencia crítica.

En este escenario, la IA aparece como la palanca para escalar operaciones sin aumentar plantilla. El 53% de los MSP ya utiliza IA para automatizar ticketing, parcheo y monitorización, con mejoras visibles en tiempos de respuesta y eficiencia técnica. Sin embargo, la mayoría apenas ha automatizado una cuarta parte de su carga de trabajo, lo que evidencia que el recorrido es amplio, pero también complejo.

LA AUTOMATIZACIÓN REDEFINE EL VALOR DEL MSP

A pesar del entusiasmo, la realidad es que la IA está generando menos impacto del esperado. Un análisis de Boston Consulting Group (BCG) revela que solo el 5% de las organizaciones obtiene valor real de la IA a escala, mientras que un 60% reconoce que el impacto es escaso o inexistente. La causa no es tecnológica, sino organizativa.

Las empresas están desplegando IA sin preparar los cimientos, tales como la gobernanza del dato, la calidad y accesibilidad de la información, el impacto en los equipos, la definición de métricas de éxito, y la alineación con los procesos reales del negocio. Este vacío entre expectativas y resultados abre una oportunidad clara para que los MSP se conviertan en los actores que traduzcan la IA en impacto tangible.

Históricamente, el negocio MSP se ha sustentado en soporte, mantenimiento, monitorización y gestión de dispositivos. Pero la IA está automatizando gran parte de estas tareas de bajo nivel. Esto implica que el modelo tradicional basado en ho-

LOS MSP DEBEN SITUARSE EN EL CORAZÓN DE LOS PROCESOS DEL CLIENTE. YA NO BASTA CON GESTIONAR INFRAESTRUCTURA, HAY QUE ENTENDER CÓMO SE TRABAJA, DÓNDE SE PRODUCEN LOS CUELLOS DE BOTELLA Y QUÉ CASOS DE USO PUEDEN GENERAR VALOR INMEDIATO

ras, tickets y mantenimiento pierde peso. Facilitar acceso a herramientas es la parte fácil, pero ayudar a lograr resultados tangibles es el verdadero reto, y eso exige un cambio profundo en el rol del MSP.

La oportunidad de negocio no está en vender acceso a IA, sino en traducir la tecnología en impacto real. Los MSP que abracen este rol ayudarán a sus clientes a pasar del interés al impacto, y se posicionarán como actores esenciales en la próxima década de transformación digital.

Para generar impacto real, los MSP deben situarse en el corazón de los procesos del cliente. Ya no basta con gestionar infraestructura, hay que entender cómo se trabaja, dónde se producen los cuellos de botella y qué casos de uso pueden generar valor inmediato.

El nuevo modelo exige mapear workflows críticos y detectar ineficiencias, priorizar casos de uso simples y visibles para demostrar valor rápido; involucrar a COO, responsables de negocio y líderes de procesos, no solo a TI; definir métricas claras de éxito desde el primer día; acompañar al cliente en gobernanza, formación y adopción; y medir y optimizar de forma continua para sostener el impacto. Este enfoque consultivo convierte al MSP en un socio estratégico, no en un proveedor de soporte.

LA CIBERSEGURIDAD COMO PILAR DEL NEGOCIO

Mientras la IA automatiza tareas y redefine el modelo operativo, la ciberseguridad se consolida como el área donde los MSP pueden aportar más valor inmediato y medible. Los datos lo confirman: el 71% de los MSP reporta crecimiento interanual en servicios de ciberseguridad, la cifra más alta de todas las categorías, seguida por continuidad de negocio y recuperación ante desastres.

En un mercado donde demostrar valor rápido es cada vez más difícil, con un 19% de los MSP que reconoce problemas para hacerlo, casi el doble que el año anterior, la seguridad ofrece métricas claras, impacto directo, urgencia real, una narrativa comprensible para el cliente y un retorno inmediato.

La ciberseguridad se convierte así en el refugio del MSP, el área donde los clientes siguen invirtiendo, donde el valor es evidente y donde la competencia es menos sensible al precio. ■

EL ROL DEL PROVEEDOR DE SERVICIOS GESTIONADOS ANTE EL ESTADO DE LA CIBERSEGURIDAD EMPRESARIAL

ASAC, Excelia, Inforges, INSSIDE Ciberseguridad, Minery Report y Secure&IT analizaron en un nuevo Encuentro IT Reseller, apoyado por ESET, cómo está evolucionando la ciberseguridad empresarial y por qué el modelo de servicios gestionados se ha convertido en una pieza clave para proteger a las organizaciones. En un escenario marcado por la presión regulatoria, la escasez de talento y el aumento de amenazas, los proveedores coinciden en que el mercado demanda acompañamiento experto y relaciones de largo plazo.

La ciberseguridad ha dejado de ser una conversación reservada a los departamentos técnicos para instalarse de lleno en los comités de dirección. El incremento de

ENCUENTRO COMUNIDAD IT >> ASAC, Excelia, Inforges, INSSIDE Ciberseguridad, Minery Report y Secure&IT analizaron en un nuevo Encuentro IT Reseller, apoyado por ESET, cómo está evolucionando la ciberseguridad empresarial y por qué el modelo de servicios gestionados se ha convertido en una pieza clave para proteger a las organizaciones.

#ENCUENTROSITRESELLER

Clica en la imagen para ver la galería

amenazas, la presión regulatoria, la escasez de profesionales especializados y la creciente dependencia digital están obligando a las empresas a revisar sus estrategias de protección. En ese nuevo escenario, los modelos de servicios gestionados ganan peso porque ofrecen acceso inmediato a conocimiento experto, capacidad operativa continua y una estructura flexible que muchas organizaciones no pueden desarrollar por sí solas.

Esa fue una de las principales conclusiones del Encuentro IT Reseller, celebrado con el apoyo de ESET España y Ontinet, y en el que participaron directivos de ASAC, Excelia, Inforges, INSSIDE Ciberseguridad, Minery Report y Secure&IT. A lo largo del debate, los asistentes analizaron cómo está evolucionando el panorama de riesgos, qué demandan hoy los clientes y por qué la confianza, más que la tecnología en sí misma, se ha convertido en el verdadero factor diferencial dentro del mercado de la ciberseguridad.

ESTADO DE LA CIBERSEGURIDAD EN ESPAÑA EN LA PRIMAVERA DE 2026

Josep Albors, head of Awareness and Research de ESET España, arrancó el debate explicando que el mercado vive una continuidad de amenazas tradicionales que ahora se ven reforzadas por nuevas capacidades tecnológicas. En su opinión, el phishing sigue siendo el gran protagonista del panorama criminal, ya sea mediante correo electrónico, mensajes SMS, redes sociales o campañas más sofisticadas.

“Vemos no tanto una evolución, sino una continuidad de amenazas clásicas”, señaló. A su juicio, la inteligencia artificial ha permitido además que actores con escasa preparación técnica puedan lanzar ataques con mayor facilidad.

El directivo de ESET también puso el foco en el ransomware y en la posición de España dentro del mapa de riesgo europeo. El dato preocupa especialmente porque una gran parte de los ataques se dirige a compañías medianas y pequeñas, donde la resistencia suele ser menor y la recuperación, más costosa.

EL ESLABÓN MÁS PRESIONADO SIGUE SIENDO LA PYME

La pequeña y mediana empresa ocupó buena parte del debate. El motivo es evidente. Y es que España mantiene un tejido productivo ampliamente apoyado en este segmento y muchas de estas organizaciones operan con recursos limitados, plantillas reducidas y una capacidad tecnológica muy desigual.

Ricardo Martínez, Director de Desarrollo de Negocio de Ciberseguridad de Excelia, defendió que el retraso acumulado en muchas pymes las ha convertido en un objetivo prioritario para los atacantes. “Las pymes no han puesto tanto cuidado y llevan mucho retraso”, afirmó.

Desde la experiencia de Excelia, el esfuerzo criminal necesario para comprometer una pyme suele ser menor que el exigido por una gran

“LA CIBERSEGURIDAD ES CONFIANZA Y TRANQUILIDAD PARA EL CLIENTE”

MARIO CORPAS
consultor TIC en **ASAC**

“AHORA LOS CLIENTES BUSCAN MÁS LO QUE LE VAS A DAR CON EL PRODUCTO QUE LO QUE EL PRODUCTO HACE”

RICARDO MARTÍNEZ
director de Desarrollo de Negocio de Ciberseguridad en **Excelia**

Clica en la imagen para ver la galería completa

corporación, mientras que las probabilidades de monetización son elevadas. Esa ecuación explica por qué el foco de los delincuentes se ha desplazado con tanta claridad hacia este colectivo. “Es un segmento al que deberíamos poner foco dentro de nuestras estrategias de ciberseguridad”, recalcó.

Germán Sánchez, responsable de línea de negocio de Sistemas y Ciberseguridad de Inforges, recordó además que el 90% del tejido empresarial español está formado por pymes, lo que convierte cualquier debilidad estructural en un problema sistémico para la economía. “El problema que tenemos es tratar de que un gerente vea la necesidad y la importancia”, señaló. En muchas pequeñas compañías, explicó, la inversión en seguridad sigue posponiéndose hasta que se produce un incidente real.

También Miguel Ángel Romero, CEO y socio fundador de Minery Report, explicó que están detectando un fuerte incremento de necesidades entre pequeñas empresas industriales, alimentarias y organizaciones que tradicionalmente habían quedado fuera del radar de los grandes integradores. “No encuentran proveedores directamente que sean capaces de ayudarles”, indicó al referirse a compañías que necesitan apoyo tanto en entornos IT como OT. Según explicó, muchas de ellas sí disponen de cierta gestión informática, pero siguen muy perdidas en todo lo relacionado con protección industrial.

Por su parte, Lautaro Fernández, Chief Information Security Officer & Cybersecurity Advisor de INSSIDE Ciberseguridad, apuntó que “las pymes y las startups, que para mí son dos conceptos diferentes, están teniendo un gran problema”. En su opinión, muchas grandes compañías están trasladando exigencias regulatorias a su cadena de suministro sin tener en cuenta la capacidad real de sus proveedo-

“LA CIBERSEGURIDAD YA NO ES UNA CUESTIÓN TÉCNICA, ES UNA CUESTIÓN DE NEGOCIO”

GERMÁN SÁNCHEZ,
responsable de línea de negocio de Sistemas y Ciberseguridad en **Inforges**

Clica en la imagen para ver la galería completa

res más pequeños para asumirlas en plazo.

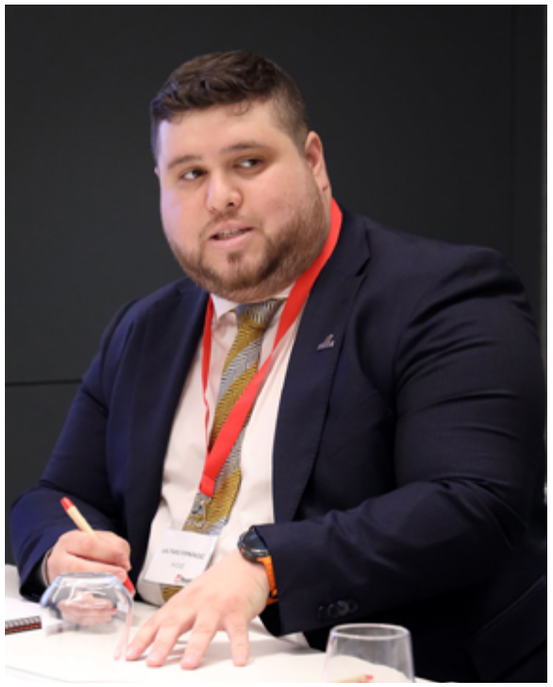
LA CIBERSEGURIDAD ENTRA DE LLENO EN LA AGENDA DEL NEGOCIO

La conversación sobre ciberseguridad ya no pertenece exclusivamente a los departamentos técnicos. Esa fue una de las ideas más compartidas durante el encuentro. Los incidentes afectan a la continuidad operativa, a la reputación, a la capacidad de facturación y, en muchos casos, a la viabilidad misma de una compañía cuando no existe preparación previa.

En esa línea se pronunció Germán Sánchez, de Inforges, quien recordó que la ciberseguridad ya no puede tratarse como una partida aislada. “La ciberseguridad ya no es una cuestión técnica, es una cuestión de negocio”, indicó. Cuando una fábrica se detiene, cuando un ERP queda bloqueado o cuando una operación logística se interrumpe, el problema deja de pertenecer al área tecnológica y pasa a la cuenta de resultados.

“LA CIBERSEGURIDAD NO PUEDE ESTAR EXENTA DE LA MISIÓN Y VISIÓN DE LA COMPAÑÍA”

LAUTARO FERNÁNDEZ
Chief Information Security Officer & Cybersecurity Advisor en **INSSIDE Ciberseguridad**



Clica en la imagen para ver la galería completa

También Javier Martí, responsable de seguridad de Secure&IT, insistió en la velocidad a la que evoluciona el riesgo. “Antes cuando salía una vulnerabilidad teníamos semanas para parchearlo y ahora si tienes horas pues has tenido suerte”, afirmó. Esa aceleración obliga a revisar procesos internos, capacidad de respuesta y nivel real de vigilancia.

Desde ASAC, Mario Corpas, consultor TIC, añadió que muchas organizaciones todavía están en fases tempranas de madurez y necesitan orientación para priorizar inversiones. Según explicó, no siempre falta voluntad, sino conocimiento para decidir por dónde empezar y qué controles implantar primero. “El cliente lo que necesita ahora mismo es priorizar”, señaló. Esa necesidad de criterio está elevando el papel de los proveedores especializados como socios de decisión y no solo como suministradores tecnológicos.

> EL PRINCIPAL VALOR QUE APORTAMOS AL CLIENTE ES POSICIONARNOS A SU LADO Y QUITARLE PESO

MIGUEL ÁNGEL ROMERO
CEO y socio fundador en
Minery Report

> UN MSP TE DA LA POSIBILIDAD DE TENER UN EQUIPO MULTIDISCIPLINAR FORMADO EN UN ÁMBITO DE 24X7

JAVIER MARTÍ
responsable de Seguridad en
Secure&IT

REGULACIÓN Y CUMPLIMIENTO ACELERAN LAS DECISIONES

Si durante años muchas organizaciones aplazaron inversiones en protección digital, la llegada de nuevas normativas está actuando como catalizador. NIS2, DORA y otros marcos sectoriales están obligando a revisar procesos, proveedores y niveles reales de madurez.

Mario Corpas, de ASAC, explicó que una parte relevante de su actividad se concentra en administraciones públicas y entidades relacionadas con ellas. En esos entornos, el cumplimiento normativo se ha convertido en prioridad inmediata. “Nos piden acompañamiento para ‘compliance’ e implementar todas las medidas técnicas posibles”, señaló. Según explicó, muchas entidades necesitan apoyo tanto jurídico como operativo, además de un socio que les ayude a traducir la norma en medidas reales.

Clica en la imagen para ver la galería completa

Corpas añadió que, en numerosos casos, las organizaciones deben centrarse en su misión principal y no disponen de estructura suficiente para asumir internamente toda la carga que exige la nueva regulación.

También Miguel Ángel Romero, de Minery Report, confirmó un fuerte incremento de demanda vinculado al cumplimiento. “Este primer trimestre hemos tenido casi un 40% más de trabajo relacionado con la normativa NIS2 o similares”, aseguró.

Romero explicó que muchos responsables de TI ya han entendido que adaptarse no consiste en comprar una herramienta ni en redactar un documento. Requiere revisar procedimientos, medir riesgos, establecer controles y, sobre todo, generar cultura interna.

Clica en la imagen para ver la galería completa

Lautaro Fernández, Chief Information Security Officer & Cybersecurity Advisor de INSSIDE Ciberseguridad, introdujo asimismo una reflexión especialmente relevante. Para él, la seguridad no puede imponerse de forma artificial cuando

> VEMOS NO TANTO UNA EVOLUCIÓN, SINO UNA CONTINUIDAD DE AMENAZAS CLÁSICAS

JOSEP ALBORS,
head of Awareness and Research en **ESET**

> LOS CLIENTES YA NO QUIEREN SOLO EL PRODUCTO, SINO A ESA PERSONA QUE HAY DETRÁS

FRAN MOLLÁ
channel account manager en **Ontinet**

« Clica en la imagen para ver la galería completa »

la organización no ha desarrollado antes un nivel básico de orden y madurez. “La ciberseguridad es madurez. No puedes implementar herramientas sobre cosas que no tienen un nivel de madurez”, subrayó.

SOBERANÍA DIGITAL Y REVISIÓN DEL CLOUD

La geopolítica y la dependencia tecnológica también ocuparon una parte relevante del debate. Muchas organizaciones están revisando su relación con los grandes proveedores internacionales y replanteando la ubicación de cargas críticas.

Mario Corpas, de ASAC, aseguró que ciertos clientes públicos ya no solo buscan alternativas a los hiperescalares, sino alojar infraestructuras directamente en España, y Germán Sánchez, de Inforges, confirmó una tendencia de retorno parcial tras años de migraciones intensivas al cloud. Primero llegaron los modelos híbridos, y ahora determinadas cargas críticas vuelven a valorarse en entornos locales.

Javier Martí, de Secure&IT, introdujo una precisión importante, que “la localización del dato no es lo mismo que la soberanía del dato”. En su opinión, no basta con conocer dónde reside la información. También importa quién la gestiona, cómo se comparte y bajo qué legislación queda sometida.

Ricardo Martínez, de Excelia, amplió el foco hacia las propias soluciones de seguridad. Para él, la discusión no debería limitarse al datacenter, sino incluir la procedencia tecnológica de las herramientas utilizadas.

Clica en la imagen para ver la galería completa

EL VALOR CRECIENTE DEL MODELO MSP Y MSSP

Con amenazas al alza, presión regulatoria y escasez de profesionales, el avance de los servicios gestionados aparece como consecuencia natural. Las empresas buscan acceso inmediato a conocimiento especializado sin asumir los costes y dificultades de construirlo desde cero.

Corpas, desde ASAC, defendió que para una pyme resulta muy complejo justificar internamente la inversión necesaria para alcanzar un nivel alto de madurez tecnológica y organizativa. “No le va a compensar ni técnica ni económicamente frente a un proveedor que ya tenga esa madurez”.

El argumento se repitió con distintos matices a lo largo del encuentro. No se trata solo de externalizar tareas, sino de incorporar capacidades que de otro modo serían inaccesibles.

Javier Martí, de Secure&IT, incidió en la capacidad operativa del modelo. “Un MSP te da la posibilidad de tener un equipo multidisciplinar formado en un ámbito de 24x7”.

Sin embargo, para el directivo de Secure&IT, el verdadero diferencial no está únicamente en la vigilancia continua, sino en el conocimiento del negocio protegido. Gestionar alertas sin contexto solo genera ruido, e interpretarlas según el impacto real es lo que aporta valor. “Necesito saber si lo que se ha tocado está conectado a la máquina de café o es una base de datos de la empresa”, explicó con ironía.

Germán Sánchez, desde Inforges, añadió otra ventaja decisiva. La economía de escala permite ofrecer servicios avanzados a precios asumibles para compañías medianas y pequeñas. Compartir especialistas, herramientas y experiencia multiplica la eficiencia del modelo.

DEL PRODUCTO A LA RELACIÓN DE SERVICIO

El mercado tecnológico vive además un cambio profundo en la forma de comprar. Durante años, buena parte de la conversación comercial giró alrededor del producto. Hoy el cliente pregunta cada vez más por resultados, acompañamiento y capacidad de respuesta.

Fran Mollá, Channel Account Manager de Ontinet, explicó que muchos partners ya no buscan solo licencias o funcionalidades. “Ya no quieren solo el producto sino a esa persona que hay detrás”. El ejecutivo de Ontinet/ESET España sostuvo que el cliente valora poder llamar, hablar con alguien que conoce su entorno y resolver incidencias con rapidez. Esa proximidad, unida a personal altamen-

RESPONDIENDO A LOS RETOS DEL SECTOR

JOSEP ALBORS, ESET

“Las amenazas actuales afectan a todo tipo de empresas, pero impactan mucho en la pyme”

Tal y como explicaba Josep Albors, head of Awareness and Research en ESET, la situación actual del mundo de la ciberseguridad en España no está viviendo una gran revolución, sino una evolución e incremento de tendencias que han estado presentes en el mercado.

Para este responsable, “lo que estamos viendo es que se están reutilizando muchas técnicas clásicas pero potenciadas, por una parte, por kits que están vendiendo los delincuentes, y, por otra, por la inteligencia artificial, lo que facilita el acceso de los ciberdelincuentes a todo tipo de estafas, fraudes, ciberamenanzas… incluso algunas medianamente avanzadas. La implosión de este tipo de amenazas y el gran número de ellas repercute, sobre todo, en el sector pyme, que es el principal en España”.

te certificado, sería muy difícil de replicar internamente para muchas organizaciones.

Miguel Ángel Romero, desde Minery Report, fue todavía más explícito. “Nosotros no vendemos producto”. Su enfoque pasa por asesorar desde una posición agnóstica y recomendar aquello que realmente necesita el cliente, no lo que más conviene comercialmente al proveedor.

Ricardo Martínez, de Excelia, coincidió en esa evolución del mercado. “En el pasado –señaló–, se implantaban soluciones que luego nadie sabía explotar correctamente. Hoy el cliente quiere entender qué problema resuelve la inversión y cómo se traduce en mejoras tangibles”.

LA CONFIANZA COMO GRAN FACTOR COMPETITIVO

Cuando el encuentro se adentró en la diferenciación entre proveedores, apareció una palabra repetida de forma casi unánime: confianza.

Mario Corpas, de ASAC, lo resumió con claridad. “La ciberseguridad es confianza”. El cliente necesita dedicar tiempo a su negocio y sentirse respaldado por un socio que responda cuando surge un incidente o una necesidad urgente.

Javier Martí, desde Secure&IT, recordó que la reputación en este sector se construye lentamente y puede perderse muy deprisa. “Yo os puedo engañar a todos una vez, pero si engaño una vez ya estoy muerto”, afirmó. La frase resume una realidad conocida en el canal. Y es que las referencias, el boca a boca y la experiencia compartida pesan más que cualquier campaña publicitaria.

Para Germán Sánchez, de Inforges, esa confianza fortalece vínculos duraderos y convierte al proveedor en una extensión operativa del cliente. Ya no se trata de vender una herramienta, sino de estar disponible cuando hace falta, incluso fuera del horario convencional.

Lautaro Fernández, de INSSIDE Ciberseguridad, prefirió definir ese vínculo “no como un proveedor, sino un aliado estratégico”.

EL RETO MENOS VISIBLE SIGUE SIENDO EL TALENTO

Aunque el mercado ofrece crecimiento y oportunidades, los propios proveedores reconocieron un desafío persistente, en la capta-

RESPONDIENDO A LOS RETOS DEL SECTOR

FRAN MOLLÁ, ONTINET

“Debemos proteger al cliente, que deposita su confianza en nosotros”

Desde la perspectiva de Fran Mollá, channel account manager en Ontinet, “una de las principales ventajas que ofrece el modelo MSSP, tanto para los distribuidores como para los usuarios, es la cercanía, el conocimiento y la relación que se extiende en el tiempo y se adapta a las necesidades de las empresas”.

Para ayudar en este terreno a los reseller, “tenemos un gran abanico de productos y podemos adaptarlos a sus necesidades, entendiéndolos y proporcionándoles un trato muy humano con nuestros equipos de soporte e ingeniería técnica”.

De hecho, “como hemos podido ver en el debate, es muy importante cuidar al cliente que deposita su confianza en nosotros, proporcionándole un servicio llave en mano, totalmente gestionado, para que puedan contar con expertos de primer nivel pero sin la necesidad de incrementar su plantilla ni realizar costosas formaciones entre su personal”.

ción y retención de profesionales especializados.

Corpas explicó que muchas compañías invierten meses en formar perfiles junior que, una vez adquieren experiencia, reciben ofertas difíciles de igualar. “El tema de la rotación de personal es complicado”.

Javier Martí, de Secure&IT, añadió que la velocidad del cambio obliga a un aprendizaje continuo. Nuevas tecnologías, amenazas y normativas exigen estudio permanente. “Es un aprendizaje constante”.

Ricardo Martínez, desde Excelia, recordó además que el modelo solo funciona si es rentable. “Hay que dar servicio y encima ganar dinero”. En esta línea, Miguel Ángel Romero, de Minery Report, defendió la combinación entre ingresos recurrentes y proyectos de mayor especialización como vía para sostener crecimiento, talento e inversión futura.

UN MERCADO MÁS MADURO Y EXIGENTE

La jornada dejó una conclusión compartida. El mercado ha madurado. Las empresas ya no compran únicamente tecnología, ni se dejan seducir con facilidad por catálogos interminables de funcionalidades. Buscan criterio, acompañamiento, honestidad comercial y capacidad real de respuesta.

Josep Albors, de ESET España, reivindicó precisamente ese valor relacional al explicar la larga trayectoria de muchos partners con la compañía. Según señaló, el soporte recibido en momentos difíciles pesa tanto como el propio producto. “El boca a boca funciona y la confianza hace muchísimo”.

Fran Mollá, de Ontinet.com, cerró el encuentro con una idea sencilla y muy reveladora. “La mayor ventaja que ofrecemos a los MSSP es la creación de una relación duradera con los clientes”. En un entorno de amenazas crecientes y decisiones cada vez más complejas, esa relación puede ser la diferencia entre un proveedor más y un socio imprescindible. ■

MÁS INFO +

» El rol del proveedor de servicios gestionados ante el estado de la ciberseguridad empresarial

COMPARTIR EN REDES SOCIALES

QUE LA CIBERSEGURIDAD DE TU EMPRESA NO TE QUITE EL SUEÑO

Monitorización, detección y respuesta 24/7 para tu negocio.

SABER MÁS

ESET®

Cybersecurity
Progress. Protected.