ENCUENTROS IT RESELLER

DEL MSP REACTIVO AL MSP RESILIENTE:

INTELIGENCIA ARTIFICIAL, IDENTIDAD Y CONTINUIDAD DEL NEGOCIO COMO NUEVOS PILARES DEL SERVICIO GESTIONADO

ORGANIZA

PATROCINADORES

CÓMO LA IA Y EL CUMPLIMIENTO NORMATIVO ESTÁN REDEFINIENDO EL FUTURO DE LOS MSP

Los proveedores de servicios gestionados afrontan una de las mayores transformaciones de su historia. La inteligencia artificial está cambiando la forma en que operan, automatizan tareas y prestan servicios, mientras que el aumento de las exigencias regulatorias abre nuevas oportunidades de negocio en ámbitos como el cumplimiento, la gestión de identidades y la ciberseguridad.

HILDA GÓMEZ

La inteligencia artificial ha irrumpido con fuerza en el ecosistema de los servicios gestionados. Según el informe 2026 State of the MSP Business Report de Nerdio, el 32% de los MSP ya utiliza IA en sus operaciones internas. Sin embargo, la realidad es que solo el 12% afirma haber obtenido mejoras de productividad claramente medibles y únicamente el 14% dispone de una línea de negocio rentable vinculada a servicios de inteligencia artificial. Estas cifras reflejan una situación que se repite en buena parte del mercado: los proveedores están experimentando con IA, pero todavía se encuentran en una fase temprana de monetización.

La tecnología está demostrando su capacidad para automatizar tareas, simplificar operaciones y mejorar la eficiencia, pero convertir esas capacidades en servicios comercializables para los clientes sigue siendo una asignatura pendiente para gran parte del sector.

La transformación tecnológica también está incrementando la presión sobre los equipos técnicos. Según el estudio de Nerdio, seis de cada diez MSP consideran que la complejidad de los entornos de IA crece más deprisa que su propia capacidad para escalar operaciones. Además, el 29% perdió profesionales técnicos durante el último año debido al agotamiento asociado a la carga de trabajo.

> “EL CONCEPTO DE MSP, DENTRO DE CINCO O DIEZ AÑOS, PODRÍA SER PRÁCTICAMENTE IRRECONOCIBLE PARA MUCHOS ACTORES ACTUALES DEL CANAL”
>
> **ROBIN ODY,** director de investigación de **Omdia**

Esta situación pone de manifiesto hasta qué punto la automatización se está convirtiendo en una necesidad más que en una opción. Las organizaciones que continúan dependiendo de procesos manuales y herramientas nativas presentan mayores dificultades para escalar servicios, mantener la consistencia operativa y retener talento especializado.

EL PRIMER CLIENTE DE LA IA DEBE SER EL PROPIO MSP

Uno de los mensajes que más fuerza ha cobrado entre los analistas es que los proveedores deben aplicar primero la inteligencia artificial en sus propias organizaciones antes de intentar venderla al mercado. Durante el Canalys Channel Forum, Robin Ody, director de investigación de Omdia, explicó que “existe una diferencia importante entre utilizar IA para mejorar procesos internos y ser capaz de diseñar servicios basados en IA capaces de generar valor para los clientes”.

Actualmente, la inteligencia artificial ya está ayudando a muchos MSP a automatizar la clasificación de incidencias, agilizar la resolución de tickets, optimizar recursos técnicos y mejorar la gestión operativa. Algunas organizaciones están alcanzando niveles significativos de automatización que les permiten destinar más recursos a actividades consultivas y estratégicas. Pero el verdadero reto consiste en transformar esa experiencia interna en propuestas de valor comercializables.

Paradójicamente, muchas empresas están explorando la inteligencia artificial a una velocidad superior a la de sus propios proveedores tecnológicos. Según los expertos, las organizaciones ya están evaluando herramientas de IA, identificando casos de uso e iniciando proyectos piloto en diferentes áreas de negocio incluso antes de solicitar asesoramiento a sus MSP habituales. Este fenómeno supone un riesgo para aquellos proveedores que continúan

centrados exclusivamente en servicios tradicionales de infraestructura, soporte o administración de sistemas.

Los analistas advierten de que los MSP que no adopten un papel más consultivo pueden quedar fuera de conversaciones estratégicas relacionadas con transformación digital, automatización e inteligencia artificial.

La incorporación de inteligencia artificial también plantea nuevos desafíos relacionados con el control, la gobernanza y la gestión del riesgo. A pesar del creciente interés por estas herramientas, solo el 14% de los MSP aplica de forma consistente un marco documentado de gobernanza de IA en todos los clientes que utilizan soluciones de inteligencia artificial.

Además, un 17% de los proveedores reconoce estar recibiendo consultas sobre IA por parte de sus clientes sin sentirse todavía preparado para responder adecuadamente a esa demanda. La situación refleja un mercado donde la presión comercial avanza más rápido que la capacidad de establecer procesos estructurados de gestión y gobierno tecnológico.

NUEVAS VÍAS DE CRECIMIENTO

Mientras la inteligencia artificial evoluciona hacia un modelo más consultivo, otra tendencia que está generando oportunidades inmediatas para el canal es el cumplimiento normativo. Según datos de Context, las ventas de soluciones relacionadas con compliance, concienciación y formación en ciberseguridad crecieron un 75,9% interanual durante el tercer trimestre de 2026, convirtiéndose en una de las categorías más dinámicas del mercado.

Paralelamente, las herramientas de gestión de identidades y accesos (IAM) aumentaron un 33,7%, muy por encima de otras categorías tradicionales de seguridad.

La explicación radica en que las empresas ya no buscan únicamente protegerse de ataques, sino demostrar que cumplen normativas, gestionan adecuadamente los riesgos y controlan el acceso a información crítica.

Este cambio está teniendo un impacto directo sobre el modelo de negocio del canal. Los clientes demandan cada vez más acompañamiento continuo, auditorías, gestión de identidades, supervisión de accesos, programas de formación y ayuda para cumplir las exigencias regulatorias. Según Joe Turner, vicepresidente de Ventas e Investigación de Context, “esta evolución permite a distribuidores y partners aportar valor más allá de la venta de productos tecnológicos”.

El crecimiento de las áreas de compliance también coincide con una transformación de los modelos de compra. Muchas organizaciones están sustituyendo adquisiciones puntuales por servicios gestionados y contratos recurrentes de largo plazo. Para los MSP, esto implica una oportunidad para ampliar su papel como asesores especializados y consolidar relaciones más estables y rentables con sus clientes.

EL FUTURO DEL MSP SERÁ RADICALMENTE DIFERENTE

La conclusión que emerge de todas estas tendencias es que la figura tradicional del proveedor de servicios gestionados está evolucionando.

La automatización reducirá el peso de muchas tareas operativas rutinarias. La inteligencia artificial permitirá gestionar entornos más complejos con menos intervención manual. El cumplimiento normativo y la ciberseguridad generarán nuevas oportunidades de consultoría especializada. Y la capacidad para integrar, gobernar y explotar tecnologías avanzadas se convertirá en un factor diferencial.

Como advirtió Robin Ody, de Omdia, “el concepto de MSP dentro de cinco o diez años podría ser prácticamente irreconocible para muchos actores actuales del canal”. La combinación de inteligencia artificial, automatización, agentes autónomos y nuevas demandas empresariales obligará a redefinir capacidades, servicios y modelos de generación de valor.

Los proveedores que consigan anticipar este cambio y evolucionar desde la gestión tecnológica hacia la consultoría estratégica estarán mejor posicionados para capturar las oportunidades de una nueva etapa del canal. Mientras tanto, quienes permanezcan anclados en modelos tradicionales corren el riesgo de perder relevancia en un mercado que ya está cambiando más rápido de lo que muchos esperaban. ■

MÁS INFO +

» Del MSP reactivo al MSP resiliente: inteligencia artificial, identidad y continuidad del negocio como nuevos pilares del servicio gestionado

COMPARTIR EN REDES SOCIALES

DEL MSP REACTIVO AL MSP RESILIENTE:

INTELIGENCIA ARTIFICIAL, IDENTIDAD Y CONTINUIDAD DEL NEGOCIO COMO NUEVOS PILARES DEL SERVICIO GESTIONADO

Durante años, buena parte del mercado identificó a los proveedores de servicios gestionados como compañías encargadas de resolver incidencias, mantener infraestructuras o garantizar que los sistemas funcionaran correctamente. Sin embargo, los participantes en el encuentro coincidieron en que esa etapa empieza a quedar atrás.

La evolución del negocio, el aumento de las amenazas y la creciente digitalización han elevado las expectativas de los clientes. Ya no basta con reparar problemas. Ahora esperan acompañamiento, visión estratégica y garantías de continuidad.

La transformación es especialmente visible en compañías que han conseguido integrarse en procesos críticos de negocio. Sergio Fernández de Tejada, director de ventas y marketing de Aviva Voice Systems &



ENCUENTRO COMUNIDAD IT >> En un encuentro organizado por IT Reseller, representantes de Aviva, BASE10, ADM Cloud & Services, Secture y SEDASER analizaron cómo evolucionan las demandas de los clientes, el impacto de la inteligencia artificial y el papel que jugarán los MSP en un escenario donde la continuidad del negocio se ha convertido en una prioridad estratégica.

Services, explicó que la compañía ha evolucionado desde un proveedor tecnológico convencional hacia una figura con un peso mucho más estratégico dentro de sus clientes.

A través de sus servicios de confianza, firma digital y trazabilidad de procesos, la empresa se ha convertido en una especie de "notario digital" capaz de certificar y acreditar todo el ciclo de relación con el usuario final. En palabras de Fernández de Tejada, “hemos pasado de un proveedor tecnológico a ser un proveedor estratégico para ellos”. Una afirmación que resume bien el cambio que vive el sector.

La misma evolución ha vivido Luis Blanco, director de operaciones y desarrollo de negocio de BASE10 Consultoría y Sistemas 360º. La compañía nació hace casi dos décadas ofreciendo infraestructura y soporte para pymes, pero hoy combina servicios de digitalización, gobierno tecnológico, ciberseguridad, cumplimiento normativo e inteligencia artificial.

Blanco considera que se ha producido una clara maduración del mercado, y que “lo que nos pedían hace 20 años no es lo mismo que nos piden ahora”. Las empresas ya no solicitan únicamente tecnología, sino



que demandan gobierno, dirección y acompañamiento especializado. “La evolución del mercado nos está llevando hacia modelos de CIO as a Service y CISO as a Service cada vez más demandados”, asegura.

Por parte de Secture, Antonio Huerta, cofundador y coCEO de la compañía, describió una trayectoria marcada por el desarrollo tecnológico, la escalabilidad y, más recientemente, la inteligencia artificial. La organización ha ampliado sus capacidades para responder a necesidades cada vez más sofisticadas de las empresas.

Algo similar ocurre en SEDASER. Juan Antonio Clavero, propietario de la compañía, explicó que el foco ya no está en solucionar incidencias puntuales de hardware, conectividad o servidores. El objetivo ahora es proporcionar tranquilidad y capacidad de recuperación.

"La línea en la que vamos ahora es la de dar esa confianza, esa seguridad de que ante un problema no es que yo te arregle un ordenador o te arregle un servidor, es que yo te dé una solución rápida y eficaz", señaló.

Clica en la imagen para ver la galería

Desde la perspectiva de la distribución especializada, Víctor Orive, CEO de ADM Cloud & Services, explicó que la compañía está reorientando gran parte de su estrategia hacia el modelo MSP, apoyando a más de 500 partners mediante preventa, formación y servicios especializados.

DE LA RESOLUCIÓN DE INCIDENCIAS A LA CONTINUIDAD DEL NEGOCIO

Uno de los mensajes más repetidos durante el encuentro fue que los clientes han dejado de medir el valor de un MSP por el número de incidencias que resuelve. Hoy la pregunta es, ¿qué ocurre cuando se produce una caída crítica? ¿Cuánto tiempo tardará la organización en volver a operar?

Para Juan Antonio Clavero, las empresas buscan seguridad, pero sobre todo continuidad. “Más que comprar tecnología, lo que los clientes están buscando es seguridad”, afirmó. El



> LA IDENTIDAD DIGITAL VA A SER UNO DE LOS ELEMENTOS FUNDAMENTALES SOBRE LOS QUE SE CONSTRUYA LA CONFIANZA EN LOS PRÓXIMOS AÑOS

SERGIO FERNÁNDEZ DE TEJADA, director de ventas y marketing de **Aviva Voice Systems & Services**



> LA EVOLUCIÓN DEL MERCADO NOS ESTÁ LLEVANDO HACIA MODELOS DE CIO AS A SERVICE Y CISO AS A SERVICE CADA VEZ MÁS DEMANDADOS

LUIS BLANCO, director de operaciones y desarrollo de negocio de **BASE10 Consultoría y Sistemas 360º**

Clica en la imagen para ver la galería completa

responsable de SEDASER considera que el cliente quiere tener garantías de recuperación ante cualquier escenario: desde una caída de servidor hasta un ransomware o una filtración de información sensible. La conversación ya no gira alrededor de herramientas concretas, sino alrededor del tiempo necesario para volver a operar con normalidad.

Fernández de Tejada, de Aviva, compartió esa visión, aunque introduciendo un elemento adicional: la confianza demostrable. Según explicó, ya no basta con afirmar que un proceso funciona correctamente, sino que hay que ser capaz de demostrarlo documentalmente. "La confianza no es que lo hagas bien, porque para eso te contrato. La confianza está en poder demostrar cómo se han hecho las cosas, en tiempo y forma", afirmó durante el encuentro.

Desde BASE10, Luis Blanco observó una tendencia parecida desde otro ángulo. A su juicio, muchas

Clica en la imagen para ver la galería completa

organizaciones comenzaron preocupándose por el cumplimiento normativo y por reducir riesgos legales. Sin embargo, progresivamente están adoptando una actitud más preventiva y estratégica.

Por su parte, Antonio Huerta cree que ese cambio se debe a que “no hay empresa que no haya tenido algún tipo de incidente o ataque”.

RECUPERAR ES TAN IMPORTANTE COMO PREVENIR

Si hay una idea que atravesó toda la conversación fue la necesidad de dejar atrás una visión excesivamente centrada en la prevención. Los participantes coincidieron en que ninguna protección es infalible y que la verdadera diferencia la marca la capacidad de recuperación.

Juan Antonio Clavero fue especialmente contundente en este punto. Según explicó, muchas organizaciones siguen confundiendo una copia de datos con un verdadero sistema de recuperación. "Hay

> NO HAY EMPRESA QUE NO HAYA TENIDO ALGÚN TIPO DE INCIDENTE O ATAQUE

ANTONIO HUERTA,
cofundador y coCEO de **Secture**



muchas empresas que dicen: yo tengo backup. Pero si se te cae el servidor, ¿cómo recuperas el servidor?", planteó.

Para el responsable de SEDASER, cualquier MSP debería disponer de entornos de prueba y procedimientos testados capaces de garantizar una recuperación rápida cuando aparece una situación crítica. De lo contrario, el retorno a la normalidad puede prolongarse durante días o incluso semanas.

Aviva también ha llevado esta filosofía al extremo. Fernández de Tejada explicó que la compañía está sometida a auditorías continuas y pruebas constantes derivadas de su pertenencia al grupo Constellation Software. Además, mantiene infraestructuras duplicadas y entornos de

Clica en la imagen para ver la galería completa

pruebas permanentes para validar la resiliencia de sus sistemas. "Todos los días nos hacen incluso ataques ellos mismos a nosotros para comprobar nuestra resiliencia", explicó.

LA IDENTIDAD COMO NUEVO CAMPO DE BATALLA

Otro de los grandes temas del encuentro fue el crecimiento de los

> MÁS QUE COMPRAR TECNOLOGÍA, LO QUE LOS CLIENTES ESTÁN BUSCANDO ES SEGURIDAD

JUAN ANTONIO CLAVERO,
propietario de **SEDASER**



ataques relacionados con la identidad digital. La proliferación de la inteligencia artificial, los procesos automatizados y la digitalización de servicios han convertido la identidad en uno de los activos más sensibles para las organizaciones.

Fernández de Tejada considera que “la identidad siempre ha sido un tema clave, pero ahora mucho más, con el tema de la IA”. Según explicó, el fraude asociado a la suplantación de identidad está creciendo de forma constante, especialmente en procesos de contratación, financiación y onboarding digital. Por ese motivo, considera que tecnologías como la identidad

Clica en la imagen para ver la galería completa

verificable y la futura wallet europea pueden jugar un papel decisivo. “La identidad digital va a ser uno de los elementos fundamentales sobre los que se construya la confianza en los próximos años”, apunta el directivo.

Clavero también alertó sobre el aumento de las suplantaciones y sobre la dificultad que muchas em-

presas tienen para reaccionar ante incidentes relacionados con identidades comprometidas.

La cuestión preocupa además porque se cruza directamente con el avance de la inteligencia artificial, capaz de generar contenidos, comunicaciones o identidades aparentemente legítimas con una facilidad cada vez mayor.

ENTRE LA PRODUCTIVIDAD Y LOS RIESGOS DE LA IA

Y hablando de la inteligencia artificial, todos los participantes coincidieron en que la IA está acelerando la productividad de las organizaciones, pero también está multiplicando las superficies de riesgo. Clavero advirtió que los empleados ya utilizan estas herramientas de forma masiva, independientemente de que las compañías tengan o no políticas corporativas definidas. “Queramos o no, dentro de la empresa están utilizándola”, afirmó.

Antonio Huerta fue aún más lejos al señalar que muchas organizaciones están impulsando la productividad mediante IA mientras mantienen enormes dudas sobre el uso de datos corporativos en estas plataformas. “Hay una contradicción que se tiene que resolver”, aseguró.



Clica en la imagen para ver la galería completa

Desde BASE10, Luis Blanco recordó que incluso la normativa europea ya exige formación en IA para quienes la utilizan profesionalmente, aunque lamentó la falta de mecanismos efectivos de supervisión. Blanco también subrayó que el verdadero reto está en gobernar los agentes, asistentes y automatismos que empiezan a proliferar dentro de las organizaciones.

> “LA VISIBILIDAD ES FUNDAMENTAL PARA PODER ESTABLECER CUALQUIER ESTRATEGIA DE GOBIERNO TECNOLÓGICO”
>
> **VÍCTOR ORIVE,**
> CEO de **ADM Cloud & Services**

Mientras tanto, Orive puso el foco en la necesidad de visibilidad. Según el responsable de ADM Cloud & Services, resulta imposible controlar aquello que ni siquiera se conoce. Antes de implantar políticas o restricciones, las empresas deben conocer qué herramientas emplean sus usuarios y qué uso hacen realmente de ellas. “La visibilidad es fundamental para poder establecer cualquier estrategia de gobierno tecnológico”, recalcó.

En relación con la IA, para Orive el debate gira alrededor de una tensión permanente entre productividad y riesgo. Las empresas quieren aprovechar las ventajas de la inteligencia artificial, pero al mismo tiempo desean minimizar cualquier exposición de datos o procesos críticos. "Si controlas no eres productivo. Y si eres productivo, tienes que dejar de controlar", resumió.

Pese a todo, los participantes coincidieron en que frenar la adopción no parece una alternativa viable. La clave estará en combinar formación, gobierno y tecnología de protección.

AUDITORÍA, FORMACIÓN Y ESPECIALIZACIÓN SON LAS NUEVAS PRIORIDADES

A medida que aumenta la complejidad del mercado, también crecen las expectativas sobre fabricantes y mayoristas.

Juan Antonio Clavero fue claro al explicar que espera de ellos información útil, capacidad de filtrado y ayuda para identificar qué soluciones aportan verdadero valor. "Quiero que, si hay un problema, me den una solución, y ya está", resumió.

Blanco destacó especialmente el papel de la preventa, la postventa y el conocimiento especializado que aportan los distribuidores de valor añadido. Según explicó, la comple-

jidad de algunos productos hace imposible que los partners puedan dominar todos los detalles técnicos y comerciales sin apoyo externo.

Al respecto, Orive describió un proceso de selección extremadamente exigente antes de incorporar nuevas tecnologías al catálogo de ADM Cloud & Services. La compañía analiza funcionalidad, soporte, rentabilidad y encaje comercial antes de recomendar cualquier herramienta a sus partners.

Para Antonio Huerta, además, resulta clave contar con referencias y comparativas que permitan calibrar correctamente el nivel de riesgo de cada cliente y seleccionar la solución más apropiada para cada escenario. ■

MÁS INFO +

» Del MSP reactivo al MSP resiliente: inteligencia artificial, identidad y continuidad del negocio como nuevos pilares del servicio gestionado

COMPARTIR EN REDES SOCIALES

RESPONDIENDO A LOS RETOS DEL SECTOR

VÍCTOR ORIVE, CEO DE ADM CLOUD & SERVICES

"El MSP debe ser el partner tecnológico de las empresas, su socio de confianza"



Tal y como nos explica Víctor Orive, CEO de ADM Cloud & Services, "el debate ha sido muy interesante. Hemos contado con empresas de diferentes tamaños y con diferentes mercados objetivos, y esto ha aportado un gran valor a la conversación, porque hemos podido ver distintos puntos de vista de esta evolución de los MSP reactivos a una figura de MSP resiliente". Esto supone que "el MSP tiende a convertirse realmente en el partner tecnológico de las empresas. Ya es realmente un socio de confianza, es una extensión más de la compañía, pero ahora da un paso más allá porque el cumplimiento normativo, por ejemplo, implica una mayor responsabilidad en los niveles directivos y esto hace esencial contar con un partner tecnológico que ofrezca la confianza necesaria ante cualquier incidente o problema, y que pueda dar respuesta, que sepa informar de qué es lo que ha pasado y que tenga la capacidad para recuperar rápidamente los sistemas para asegurar la continuidad de negocio".

En este sentido, la oferta de soluciones de N-able "es muy completa. Ahora se añade una de las novedades que ya ha lanzado este año y que se potenciará en los próximos meses, N-able DRaaS (Disaster Recovery as a Service), es decir, la posibilidad de poder recuperar una infraestructura en la nube de N-able de tal manera que los tiempos de recuperación van a ser siempre mucho menores y, por lo tanto, la continuidad de negocio está garantizada. Además, gracias a la IA, N-able quiere ayudar a los a los MSP a conocer mejor cuáles son los problemas de sus clientes, los riesgos a los que están expuestos para poder anticiparse, siendo más efectivos y generando la confianza que los clientes necesitan".

N-ABLE™ ADM Cloud & Services

¿Con qué rapidez y hasta qué punto puedes restaurar tus datos cuando más importa?

Descarga nuestra guía gratuita y comprueba si tu protección de Google Workspace está a la altura.

Descarga la guía gratuita

