Julio de 2025

Informe de mercado

Informe sobre perspectivas de clientes MSP 2025

Qué necesitan las organizaciones de todo el mundo de sus proveedores de servicios gestionados de ciberseguridad

Barracuda®
Your business, secured.

Contenido

Introducción

Este informe analiza lo que las organizaciones de todo el mundo necesitan y esperan de sus proveedores de servicios gestionados (MSP) en materia de servicios de ciberseguridad. Se basa en los resultados de una reciente encuesta internacional realizada a clientes de MSPs encargada a Vanson Bourne.

Los MSPs se han convertido en fundamentales para las empresas. La mayoría de las organizaciones encuestadas ya externalizan parte o la totalidad de sus necesidades de ciberseguridad a MSPs, y otras están explorando oportunidades.

Este informe tiene como objetivo ayudar a los MSPs a comprender qué necesitan de ellos sus clientes ahora y en el futuro, cómo son sus clientes potenciales y dónde encontrarlos, y qué lleva a los clientes a recurrir a la competencia.

En general, los hallazgos muestran que:

- Los clientes necesitan MSPs que los ayuden a gestionar la seguridad a medida que crecen.
- En los próximos años, los clientes necesitarán ayuda especialmente con la implementación de aplicaciones de inteligencia artificial/aprendizaje automático y seguridad de redes, y están dispuestos a pagar más por ello.

Metodología

Barracuda encargó a la empresa independiente de estudios de mercado Vanson Bourne la realización de una encuesta global a 2.000 responsables de la toma de decisiones en materia de seguridad que ocupan puestos de TI y negocio en organizaciones con entre 50 y 2.000 empleados de una amplia gama de sectores en Estados Unidos, Reino Unido, Francia, DACH (Alemania, Austria, Suiza), Benelux (Bélgica, Países Bajos y Luxemburgo), los países nórdicos (Dinamarca, Finlandia, Noruega y Suecia), Australia, India y Japón. La encuesta se llevó a cabo entre abril y mayo de 2025.

Introducción

- La mayoría de los clientes de MSPs se plantearán cambiar de proveedor, entre otras razones por dudas sobre la capacidad de los MSPs para ayudarles a remediar o recuperarse de un ciberataque.

Esperamos que este informe ayude a los MSPs a definir sus estrategias futuras, identificar nuevas oportunidades y abordar posibles carencias. Barracuda está a su disposición para atenderles en cada etapa del camino. Juntos, podemos garantizar que más organizaciones sean ciberresilientes y estén protegidas al enfrentarnos a las adversidades de unas amenazas en constante evolución.

Principales conclusiones

85 %

de las organizaciones de entre 1.000 y 2.000 empleados confían en MSPs para obtener soporte de seguridad, en comparación con el 61 % de las que tienen entre 50 y 100 empleados

48 %

de las organizaciones recurren a los MSPs para obtener soporte de seguridad las 24 horas del día

52 %

de las organizaciones recurren a los MSPs en busca de ayuda cuando el número de herramientas de seguridad se vuelve inmanejable, siendo esta la razón más citada

51 %

de las organizaciones recurren a los MSPs para que les ayuden a evolucionar sus estrategias de seguridad a medida que crecen, siendo esta la segunda razón más citada

39 %

de las organizaciones prevén necesitar el soporte de los MSPs con herramientas y aplicaciones de IA y aprendizaje automático en los próximos años, siendo esta la razón más citada

92 %

de las organizaciones están dispuestas a pagar más por el soporte para la integración de herramientas de seguridad

45 %

cambiarán de MSP si no ven pruebas de sus habilidades, experiencia y capacidad para ofrecerles seguridad 24 horas al día, 7 días a la semana: siendo esta la razón más citada

La base de clientes de los MSPs

Las ciberamenazas siguen evolucionando a medida que los atacantes aprovechan las herramientas de inteligencia artificial y los servicios criminales de alquiler para lanzar ataques cada vez más sofisticados, y para hacerlo más rápido, en mayores volúmenes y con mayor precisión.

Los profesionales de TI y seguridad se enfrentan a un bombardeo constante de este tipo de amenazas. Para mantener protegida la organización y sus activos, necesitan soluciones de seguridad avanzadas, así como capacidades de supervisión, gestión y mitigación las 24 horas del día, y un profundo conocimiento del panorama de amenazas. Pocas organizaciones pueden satisfacer todas esas necesidades con recursos propios.

Conclusión clave: el 73 % de las organizaciones encuestadas subcontratan los servicios de seguridad a un MSP

El 96 % de las organizaciones encuestadas ya trabajan con un MSP o están planteándose hacerlo: el 73 % afirma que ya externaliza los servicios de seguridad a un MSP, mientras que otro 18 % está evaluando proveedores y un 5 % está considerando la posibilidad de utilizar un MSP.

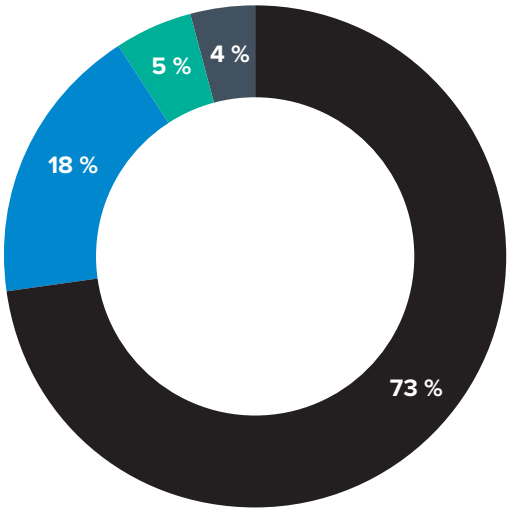

FIGURA 1

¿Externaliza su organización alguna actividad de seguridad informática a un proveedor de servicios gestionados (MSP)?

n=2.000

- Sí
- Actualmente estamos evaluando proveedores
- Estamos considerando la posibilidad
- No

Hay algunas variaciones interesantes en estas cifras.

Por ejemplo, las organizaciones más grandes encuestadas son más propensas a utilizar MSPs que las más pequeñas.

Conclusión clave: el 85 % de las encuestadas de entre 1.000 y 2.000 empleados confía en los MSP para el soporte de seguridad, en comparación con el 61 % de las empresas que tienen entre 50 y 100 empleados

Este mayor nivel de implicación con los MSPs puede reflejar el hecho de que las organizaciones más grandes tienen una mayor complejidad en materia de seguridad y una gama más amplia de herramientas que gestionar.

Por ejemplo, las organizaciones más grandes encuestadas tienden a preocuparse más que las más pequeñas por la creciente complejidad de su entorno de seguridad (42 %) y de los ciberataques (46 %). En el caso de las empresas más pequeñas encuestadas, las cifras correspondientes son del 32 % y el 34 %.

Un 10 % de las organizaciones más pequeñas encuestadas no tiene previsto contratar un MSP para que las ayude con la ciberseguridad, lo cual es preocupante. Las empresas más pequeñas suelen disponer de menos recursos internos para la protección, por lo que este enfoque podría exponerlas a ataques.

Los sectores más propensos a externalizar la ciberseguridad a MSPs son la administración local (84 %) y la educación (78 %). El nivel de implicación es menor en los sectores del ocio y el entretenimiento (60 %), el comercio minorista (65 %) y la fabricación (57 %).

Entre los países encuestados, las organizaciones del Reino Unido y Benelux son las más propensas a trabajar con un MSP (con un 79 % y un 81 %, respectivamente). Los niveles más bajos de colaboración se observan en los países nórdicos (54 %) y Japón (59 %).

Los clientes necesitan que los MSPs les ayuden a gestionar la seguridad a medida que crecen

La investigación muestra que, desde la perspectiva de los clientes, el socio MSP ideal ofrece tanto asistencia práctica, centrada en los productos y la tecnología, como una ayuda más estratégica en términos de planes de seguridad y cumplimiento normativo.

Si nos fijamos en los dos resultados principales, se deduce que los MSPs desempeñan un papel fundamental a la hora de ayudar a las organizaciones a gestionar las implicaciones de la seguridad en el crecimiento empresarial.

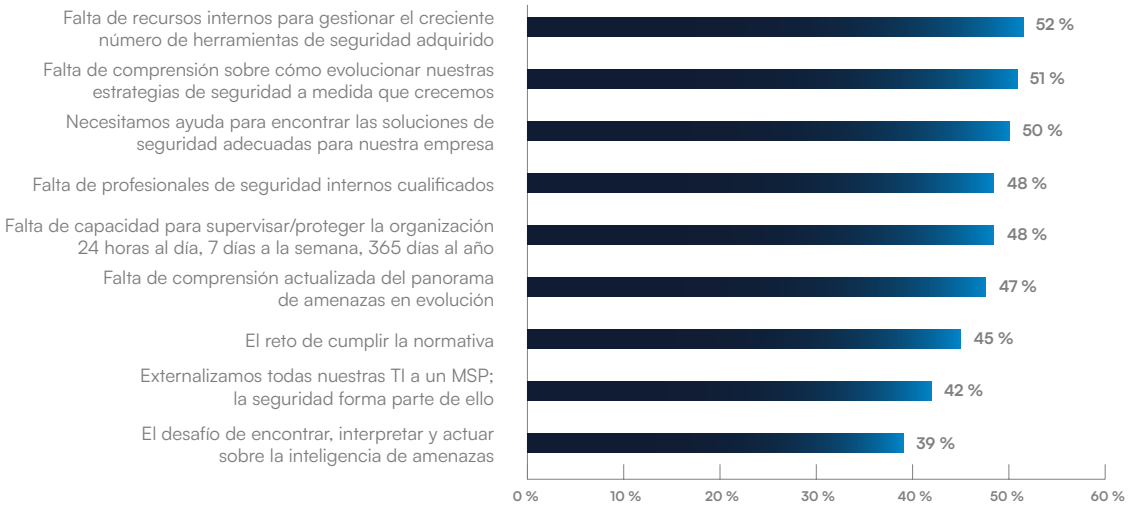

FIGURA 2

Las razones para externalizar la seguridad a un MSP

n=2.000

Conclusión clave: el 52 % de las organizaciones recurren a los MSPs para obtener ayuda cuando el número de herramientas de seguridad se vuelve inmanejable

El soporte para gestionar un número cada vez mayor de productos de seguridad fue la razón más común dada para recurrir a los MSPs. Es probable que muchas de estas herramientas sean de diferentes proveedores y que la mayoría no se integren entre sí.

Esta cifra se eleva al 60 % entre los encuestados del sector manufacturero. Las empresas manufactureras suelen tener un número significativo de sistemas conectados y dispositivos IoT y, por lo tanto, una mayor probabilidad de proliferación de herramientas de seguridad.

Otros resultados del estudio muestran que la falta de integración puede aumentar el riesgo y la exposición a la seguridad, lo que dificulta y encarece la gestión de la seguridad y la detección y mitigación de amenazas.

Conclusión clave: el 51 % de las organizaciones recurren a los MSPs para que les ayuden a evolucionar sus estrategias de seguridad a medida que crecen

La segunda razón más citada para recurrir a un MSP con el fin de obtener soporte sobre seguridad refleja la evolución del papel de los proveedores de servicios como asesores de seguridad: el 51 % recurre a su socio de servicios para que les ayude a evolucionar y actualizar sus estrategias de seguridad a medida que la organización se expande y cambia. Las organizaciones educativas y sanitarias fueron especialmente propensas a citar este motivo para contratar un MSP (ambas con un 55 %).

Las instituciones educativas también se encuentran entre las que más se preocupan por la creciente complejidad de su seguridad informática (48 % frente al 38 % del total), lo que sugiere que tienen dificultades para proteger un número cada vez mayor de activos digitales. Recurrir a un MSP para obtener ayuda es un paso natural para ellas.

Conclusión clave: el 48 % de las organizaciones recurren a los MSPs para obtener soporte de seguridad 24 horas al día

La mayoría de las organizaciones reconocen que la ciberseguridad es una actividad que requiere atención permanente y que ello exige unos niveles de personal y una inversión que muchas de ellas no tienen a su alcance. Confiar en un MSP para que les ayude a supervisar y responder a las amenazas y alertas de seguridad 24 horas al día, 7 días a la semana, es otro de los principales motivos para contratar sus servicios.

Muchos MSPs operan ahora, a menudo junto con proveedores de seguridad, un centro de operaciones de seguridad (SOC) gestionado, que proporciona dicha cobertura especializada. Para obtener la seguridad más completa, puede combinarse con una solución gestionada de detección y respuesta ampliada (XDR) capaz de cubrir toda la superficie de ataque, incluidos los endpoints, el correo electrónico, la nube, las aplicaciones y las redes.

Para muchas de las organizaciones encuestadas, la contratación de MSPs también está estrechamente relacionada con la falta de profesionales de ciberseguridad internos, citada como motivo por el 48 %. La escasez de personal cualificado parece ser un reto universal, ya que la proporción se mantiene constante en empresas de todos los tamaños.

En el caso del 42 % de los encuestados, la seguridad se externaliza a un MSP y se incluye en un paquete con otros servicios de TI. Esto representa tanto una oportunidad como un riesgo para los MSPs, especialmente cuando los clientes deciden trasladar su negocio (véase la sección sobre factores decisivos).

Los clientes necesitarán más apoyo con la IA y la seguridad de la red en el futuro

Durante los próximos dos años, es muy probable que los clientes soliciten ayuda a los MSPs para implementar herramientas y aplicaciones de IA y aprendizaje automático. A ello le sigue la ayuda para implementaciones de seguridad de red, como medidas de zero-trust y soluciones SASE (secure access service edge).

Conclusión clave: el 39 % de las organizaciones prevé necesitar el apoyo de los MSPs con herramientas y aplicaciones de IA y aprendizaje automático en los próximos dos años

La IA y la seguridad de la red son áreas en las que las empresas se centran cada vez más, con vulnerabilidades de seguridad y complejidad técnica. Pueden ser difíciles de entender, especialmente para el 48 % de las organizaciones que carecen de personal suficiente.

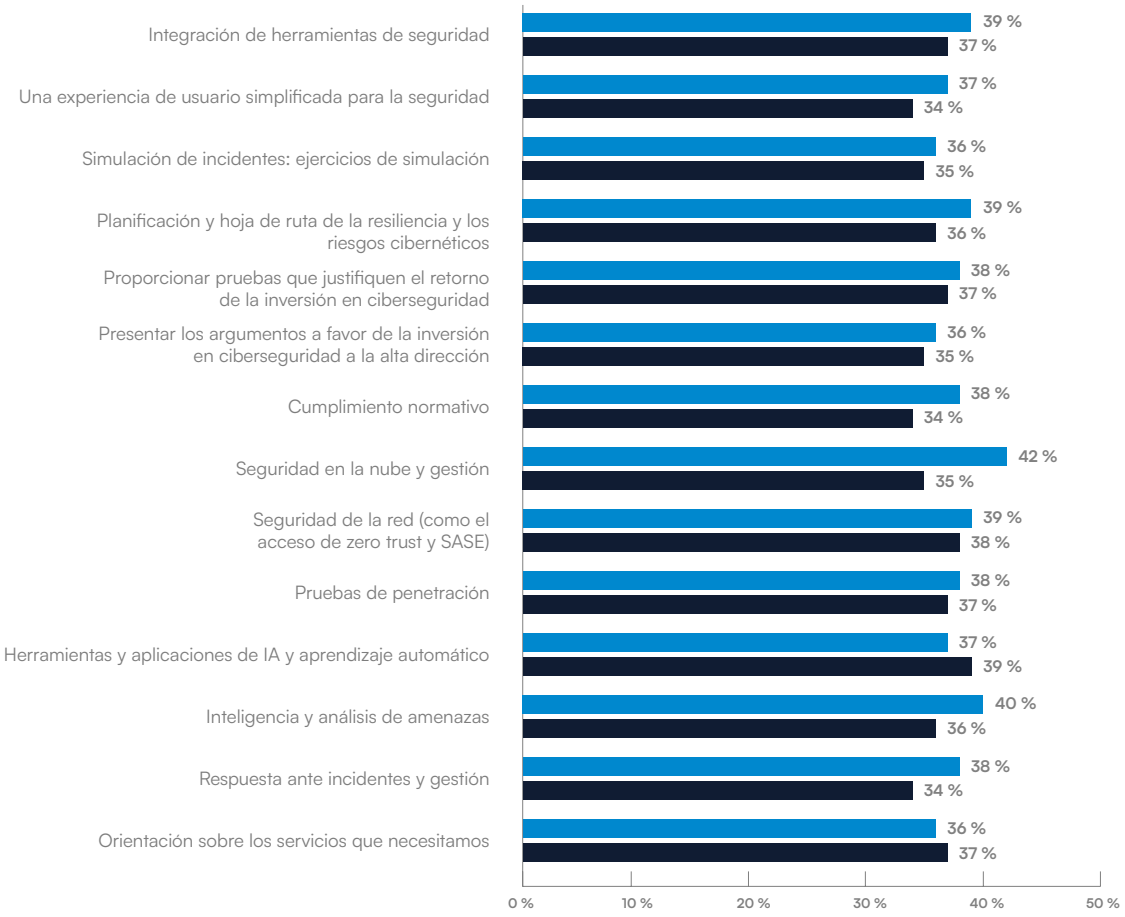

FIGURA 3

Oportunidades de seguridad para los MSPs: donde las organizaciones prevén necesitar apoyo de los proveedores de servicios en los próximos 1 o 2 años

n=2.000

- Ya lo utiliza desde MSP
- Prevé necesitar apoyo

Los resultados ponen de relieve los diferentes recorridos de las organizaciones de distintos tamaños.

Por ejemplo, entre las organizaciones de 50 a 100 empleados, la proporción que busca apoyo futuro con IA aumenta hasta el 44 %, y el 29 % ya lo ha contratado. En el caso de las organizaciones más grandes, el 44 % trabaja con MSPs en materia de IA y el 37 % prevé necesitar apoyo en los próximos dos años.

Esto sugiere que las organizaciones más grandes ya comprenden las limitaciones de gestionar la IA y el aprendizaje automático por sí mismas, y colaboran activamente con los MSPs para optimizar el uso de la IA tanto en TI como en seguridad. Se observa una situación similar, aunque con diferencias menores, en el ámbito de la seguridad de redes.

También cabe destacar el uso generalizado y la demanda de servicios estratégicos como la planificación de la resiliencia y los riesgos cibernéticos, la simulación de respuesta a incidentes y la presentación de argumentos a favor del retorno de la inversión en ciberseguridad.

Los clientes están dispuestos a pagar más por los servicios que desean

La encuesta reveló que casi todos los clientes de MSPs están dispuestos a pagar más por los servicios adicionales que necesitarán en los próximos dos años, y alrededor del 70 % aceptaría pagar hasta un 10 % o un 25 % más.

Conclusión clave: el 92 % de las organizaciones están dispuestas a pagar más por soporte para integrar herramientas de seguridad

Los servicios por los que están más dispuestos a pagar más incluyen herramientas y aplicaciones de inteligencia artificial y aprendizaje automático, seguridad en la nube y seguridad de redes. Los resultados son similares en empresas de todos los tamaños.

En general, las herramientas y actividades operativas obtienen mejores resultados en lo que respecta al gasto adicional. Existe cierta reticencia a gastar más en servicios «más intangibles», como la simulación de incidentes, la presentación de argumentos a favor de la inversión en ciberseguridad o el asesoramiento sobre los servicios necesarios.

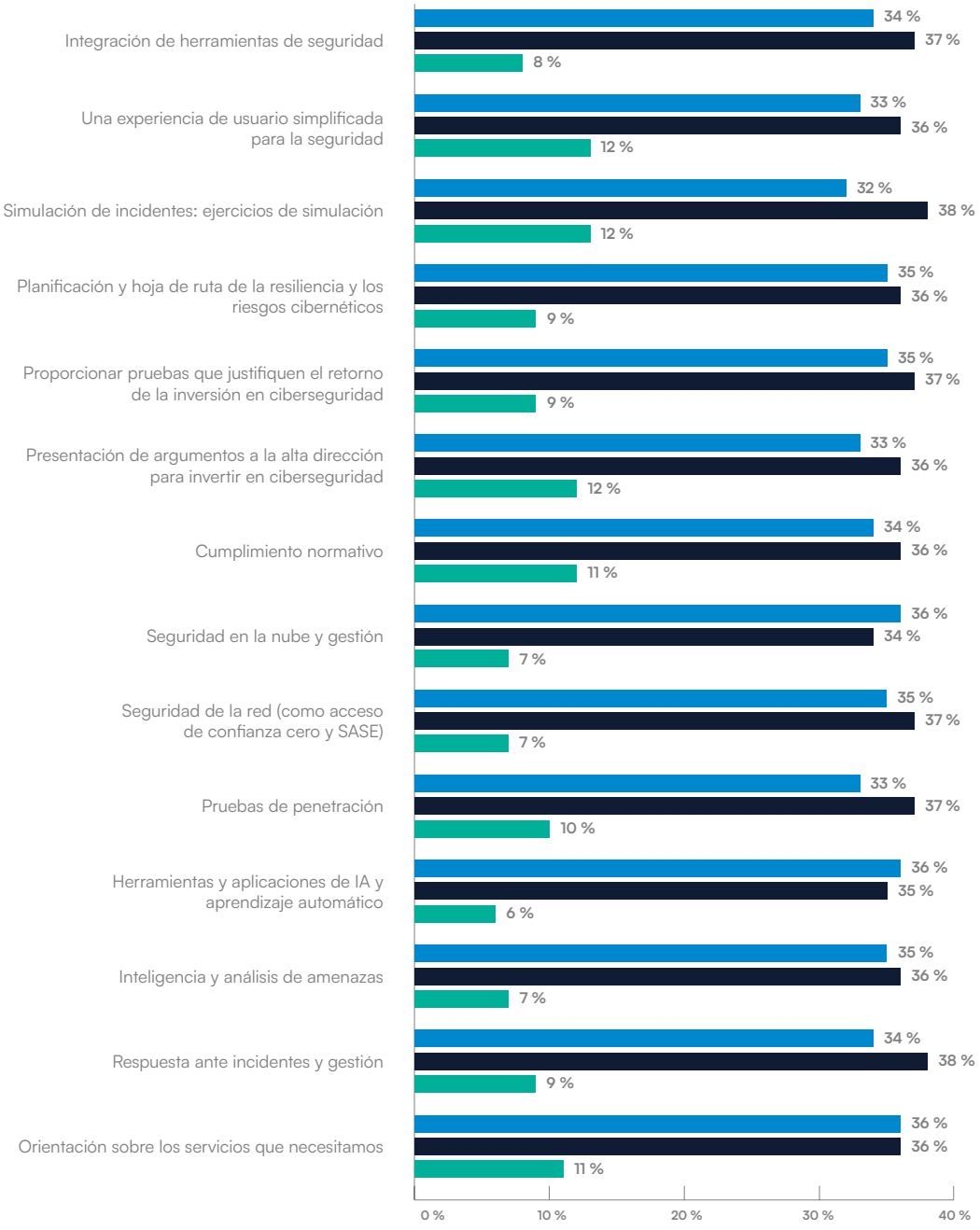

FIGURA 4

Costes adicionales que las organizaciones están dispuestas a pagar por estos servicios a los MSPs en los próximos 1 o 2 años

n=2.000

- Dispuestas a pagar hasta un 25 % más
- Dispuestas a pagar hasta un 10 % más
- No está dispuesta a pagar más por esto

Sin embargo, lo que los clientes priorizan y en lo que están dispuestos a invertir es muy diferente cuando se ve a través del prisma de un incidente de seguridad, como un ataque basado en el correo electrónico o de ransomware. Consulte la sección sobre el impacto de una brecha de seguridad más abajo.

Los MSPs corren el riesgo de perder clientes si no pueden demostrar su experiencia

Los resultados muestran que, cuando se trata de mantener la fidelidad a un socio MSP, esta es limitada y depende de la confianza del cliente en la experiencia, la calidad y la estabilidad empresarial del proveedor de servicios. Solo el 2 % de los encuestados afirmó que no se imaginaba cambiar a otro MSP. Para todos los demás, hay algunos factores que son claramente decisivos.

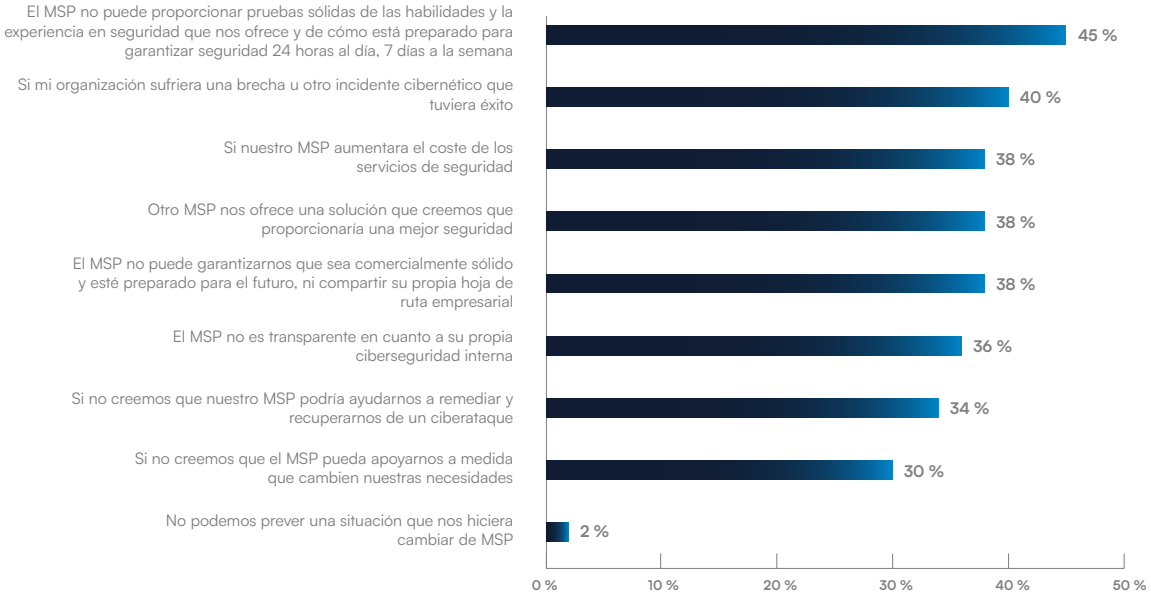

FIGURA 5

¿Qué le haría plantearse cambiar a otro MSP para obtener apoyo en ciberseguridad?

n=2.000

Una brecha de seguridad es un claro motivo para romper una relación y, para más de un tercio (38 %) de los clientes de MSPs, un aumento de precio o una oferta mejor de otro MSP les llevaría a cambiar de proveedor.

Conclusión clave: el 45 % cambiaría de MSP si no viese pruebas de sus habilidades, experiencia y capacidad para ofrecerles seguridad 24 horas al día, 7 días a la semana

Para los MSPs afectados, no se trata solo de perder el contrato relativo a la ciberseguridad: el 89 % de los clientes que se dan de baja y habían contratado servicios de TI junto con seguridad también eliminarán esas actividades, ya sea en ese mismo momento (46 %) o más adelante (42 %).

Cabe mencionar que el 38 % de los clientes de MSPs afirman que cambiarían de MSP si este aumentara los costes. Si se tiene en cuenta la disposición a invertir, esto sugiere que los clientes de

MSPs estarán dispuestos a pagar más por los servicios que desean y necesitan, pero se sienten menos cómodos con las subidas de precios impuestas arbitrariamente por el MSP.

La buena noticia es que los posibles motivos de ruptura del contrato son casi todos ámbitos que los MSPs pueden abordar invirtiendo en su propio negocio y en la resiliencia de la seguridad, tanto la suya como la de sus clientes, y reforzando la confianza y la transparencia.

Las organizaciones afectadas por una brecha de seguridad invierten más en seguridad y externalización

Una brecha de seguridad en el correo electrónico o un ataque de ransomware que tenga éxito cambia las prioridades en materia de seguridad.

Las diferencias entre los que se han visto afectados y los que no son evidentes cuando se analizan los servicios por los que están dispuestos a pagar más y las actividades de las que se han dado cuenta que no pueden gestionar eficazmente de forma interna. Estos resultados ponen de relieve las áreas en las que las víctimas pueden sentirse especialmente expuestas.

Conclusión clave: el 91 % de las víctimas de ataques están dispuestas a pagar más por una experiencia de usuario simplificada en materia de seguridad, frente al 77 % de las que no han sido víctimas

Por ejemplo, el 91 % de las víctimas están dispuestas a pagar más por una experiencia de usuario simplificada en materia de seguridad, frente al 77 % de las que no han sido afectadas. La cifra global es del 88 %. Esto sugiere que, para muchas víctimas, los errores humanos o la configuración incorrecta, ambos fácilmente provocados por interfaces de usuario complejas, pueden haber influido en el ataque.

Las víctimas también están más dispuestas a pagar más por servicios de ciberresiliencia, como la planificación de la respuesta a incidentes, la comprensión y el cumplimiento de la normativa, y la orientación estratégica sobre servicios de seguridad. Esto sugiere que las víctimas están dispuestas a invertir en áreas que les permitan estar mejor preparadas para responder y recuperarse de futuros ataques.

En cuanto a las actividades realizadas internamente o externalizadas, se observa la misma disparidad: quienes no se han visto directamente afectados por un incidente son más propensos a creer que pueden manejar las cosas por sí mismos.

Conclusión clave: el 81 % de las víctimas de ataques planean externalizar la seguridad en la nube y la gestión, en comparación con el 73 % que no han sido víctimas

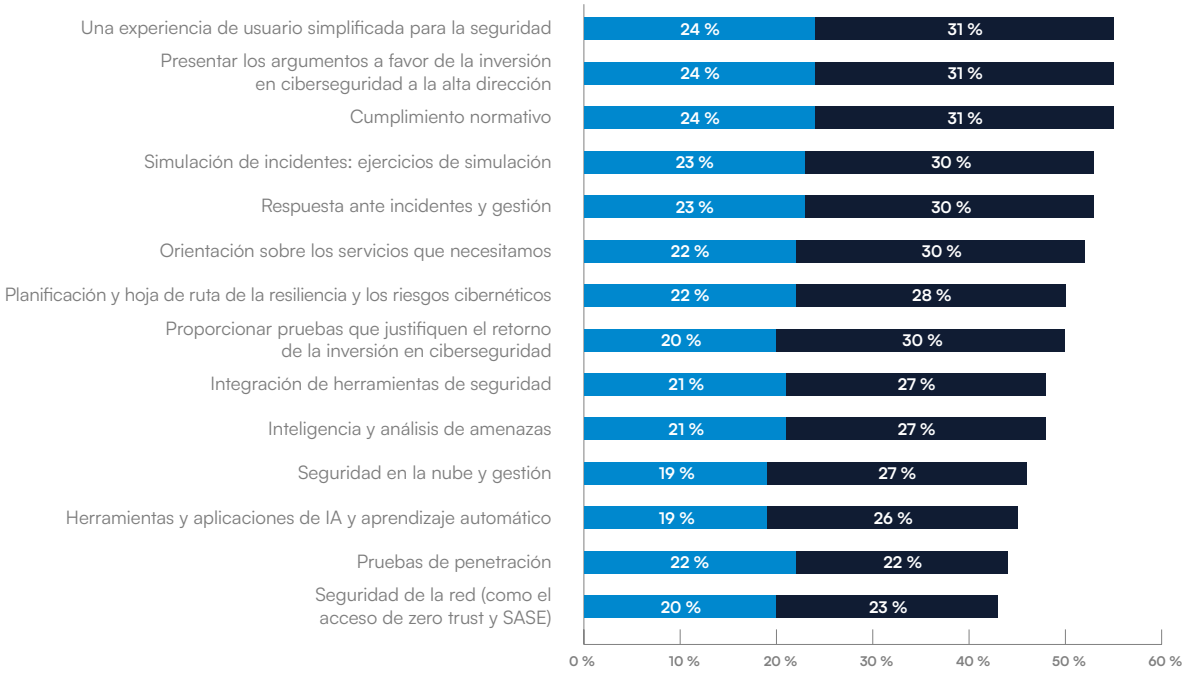

FIGURA 6

Organizaciones que planean gestionar cada uno de los siguientes aspectos internamente en los próximos 1 o 2 años

n=2.000

- Ha sufrido una violación de la seguridad del correo electrónico o un ataque de ransomware con éxito en el último año
- No ha sufrido una violación de la seguridad del correo electrónico ni un ataque de ransomware con éxito en el último año

Conclusión

Los resultados muestran que, en 2025, los MSPs se encontrarán con muchas oportunidades prometedoras, pero también con algunos retos.

Por ejemplo, muchos clientes necesitan ayuda para gestionar la proliferación de la seguridad. Sin embargo, ayudar a varios clientes a manejar múltiples productos puede convertirse rápidamente en una tarea abrumadora para los proveedores. Los fabricantes de seguridad tienen un papel importante que desempeñar a la hora de ayudar a los MSPs a integrar las actividades de gestión, respuesta y generación de informes, a través de paneles centralizados y de la consolidación de productos. Del mismo modo, los fabricantes pueden ayudar a los MSPs a atender la evidente demanda de supervisión de la seguridad 24 horas al día, 7 días a la semana, con SOC gestionados.

Luego está la necesidad de apoyar a los clientes en el cumplimiento de las normas y reglamentos, así como en la implementación de herramientas y aplicaciones de inteligencia artificial y aprendizaje automático.

Además, los MSPs deben prepararse para los clientes que desean servicios más proactivos y predictivos, como inteligencia sobre amenazas, planificación de la respuesta a incidentes, gestión de riesgos y consultoría estratégica.

Por si fuera poco, los MSPs también deben velar por su propia viabilidad comercial y demostrar su experiencia y un modelo de negocio sólido; de lo contrario, se arriesgan a perder clientes frente a la competencia. Esto requiere una cartera de productos avanzada e innovadora, pero también fácil de comprar, implementar y utilizar para los clientes. También exige proveedores de seguridad comprometidos a colaborar.

Conclusión

Cómo puede ayudar Barracuda

En Barracuda, estamos 100 % comprometidos con el canal y ayudamos a nuestros socios a alcanzar el éxito y crecer.

BarracudaONE™

BarracudaONE es una plataforma de ciberseguridad basada en inteligencia artificial, que ofrece productos integrados accesibles desde un panel de control centralizado para maximizar la protección y la ciberresiliencia, siendo además fácil de comprar, implementar y utilizar.

La plataforma simplifica la administración de las herramientas de seguridad para un MSP en todos sus clientes, garantizando que las herramientas estén correctamente configuradas, que las alertas estén centralizadas y que se proporcionen informes que muestren el valor que un MSP aporta a sus clientes en materia de seguridad.

BarracudaONE está disponible sin coste adicional para los MSPs, otros socios de canal y los clientes que ya utilizan Barracuda Email Protection, Barracuda Cloud-to-Cloud Backup y Barracuda Data Inspector. La plataforma proporciona una interfaz centralizada para que los MSPs y los socios puedan gestionar fácilmente las soluciones y las licencias.

Barracuda Managed XDR™

Los MSPs, los socios y los usuarios finales pueden reforzar aún más su postura de seguridad con Barracuda Managed XDR, servicio disponible 24 horas al día, 7 días a la semana, que ofrece detección y respuesta expertas ante amenazas, respaldadas por el galardonado SOC de Barracuda.

Sobre Barracuda

Barracuda es una empresa líder mundial en ciberseguridad que ofrece protección completa contra amenazas complejas para empresas de todos los tamaños. Nuestra plataforma impulsada por IA asegura el correo electrónico, los datos, las aplicaciones y las redes con soluciones innovadoras, XDR gestionado y un panel de control centralizado para maximizar la protección y fortalecer la ciberresiliencia. Con la confianza de cientos de miles de profesionales de TI y proveedores de servicios gestionados de todo el mundo, Barracuda ofrece defensas potentes que son fáciles de comprar, implementar y usar.

Acerca de Vanson Bourne

Vanson Bourne es un especialista independiente en investigación de mercados para el sector tecnológico. Su reputación en lo referente a análisis sólidos y creíbles basados en la investigación reside en rigurosos principios de investigación y en su capacidad para recabar las opiniones de los principales responsables de la toma de decisiones en todas las funciones técnicas y empresariales, en todos los sectores empresariales y en los principales mercados. Para obtener más información, visite vansonbourne.com.