Mantener el impulso de los MSP: Retos y oportunidades en un panorama de seguridad de IT en constante evolución

kaspersky

Índice

Introducción

El mercado de los proveedores de servicios gestionados (MSP) es un gran negocio. Lo que empezó básicamente como el rol del distribuidor de IT para proporcionar, instalar y gestionar una aplicación específica ha evolucionado hasta el punto de que los MSP se han convertido una parte integral de la red de provisión y soporte de IT de una empresa. Para muchas compañías, un MSP es una extensión de su equipo de IT o, en algunos casos, constituye el equipo de IT en sí, lo que suele compensar el déficit interno de conocimientos y recursos, para garantizar que las operaciones de IT se ejecutan sin problemas y con éxito.

Las pymes, en particular, confían en que los MSP sean sus asesores de confianza a medida que evoluciona el panorama de IT, y los conocimientos y presupuestos internos a menudo limitan su capacidad para seguir ese ritmo. El crecimiento previsto y continuado de los servicios en la nube representa solo un ejemplo de contextos en los que los MSP desempeñan un papel importante a la hora de ayudar a las pequeñas empresas a sacar partido de las aplicaciones basadas en la nube.

Gartner prevé que el mercado mundial de servicios de nube pública crecerá un 17,5 % en 2019 hasta alcanzar un total de 214 300 millones de dólares, por lo que existe una gran oportunidad para que los MSP ayuden a las empresas a hacer de estos proyectos un éxito. De hecho, hasta el año 2022, Gartner pronostica que el tamaño del mercado y el crecimiento del sector de los servicios en la nube prácticamente triplicará el crecimiento de los servicios de IT en general.

Por lo tanto, no es de extrañar que, según cifras recientes, se espera que el mercado de servicios gestionados crezca de 180 000 a 282 000 millones de dólares en 2023. Esto se debe en gran medida a que las organizaciones confían en los MSP para "impulsar su productividad empresarial y [satisfacer] la creciente demanda de servicios gestionados basados en la nube". Otro motivo clave de este aumento es el valor asociado a la externalización de la gestión de IT y la seguridad.

No es posible ignorar el hecho de que los ciberataques malintencionados a las empresas van en aumento, lo que hace que las empresas sean mucho más conscientes de los riesgos y consecuencias de un robo de datos o un ataque de ransomware en su negocio. Si bien muchos de los casos conocidos públicamente son de grandes empresas que sufren un robo de datos, las empresas más pequeñas y las de la cadena de suministro resultan igual de vulnerables y sufren unas consecuencias de gravedad similar.

Al ser la tecnología la columna vertebral de todas las empresas, independientemente de su tamaño o sector, mantener el ritmo de las aplicaciones innovadoras y la evolución de las amenazas de seguridad puede suponer todo un reto. Esto es algo particularmente cierto para las empresas sin presupuestos ni recursos a gran escala. De hecho, un reciente estudio de Kaspersky descubría que las empresas con menos de 500 empleados tienen más probabilidades de recurrir a proveedores de servicios externos para garantizar la correcta gestión y seguridad de sus infraestructuras de IT. El 40 % externaliza su gestión de IT y el 33 % externaliza específicamente su seguridad de IT a un tercero.

Estas cifras indican que, con presupuestos y los recursos limitados, las empresas creen que la mejor solución es conseguir que un experto externo le ayude. Aunque la oportunidad que presenta para los MSP sea enorme, como demuestra el crecimiento previsto del mercado mundial, también plantea desafíos y deposita grandes expectativas en los proveedores para cubrir las lagunas de conocimientos, además de para asumir la culpa si una empresa sufre una brecha o un tiempo de inactividad.

Para ayudar a comprender los retos y oportunidades actuales de los MSP en toda Europa, este informe analiza la dinámica del mercado en constante evolución y el impacto de las cambiantes relaciones con los clientes y las expectativas en el sector de los MSP. También realiza recomendaciones a los MSP para que se aseguren de que pueden aprovechar las oportunidades y mantener relaciones a largo plazo con sus clientes, independientemente de los retos que se presenten.

Conclusiones clave

- La externalización de IT y, en particular, la externalización de la seguridad está en alza. Un tercio (33 %) de las empresas europeas con menos de 500 empleados externalizan actualmente su gestión de la seguridad de IT y el 21 % tienen pensado hacerlo en los próximos 12 meses.
- La tendencia a externalizar se debe en gran medida a la falta de conocimientos internos en las empresas y a su deseo de sacar el máximo partido de los presupuestos de IT disponibles. La mitad (51 %) recurre a la externalización para complementar los conocimientos internos y el 52 % cree que trabajar de esta forma les ayudará a reducir los costes relacionados con la seguridad.
- Cuando se reducen los presupuestos de IT, las empresas se inclinan hacia la externalización como método más rentable de garantizar el valor y respaldar las futuras necesidades de gestión de la seguridad de IT.
- Tres cuartas partes (75 %) de los MSP admiten que satisfacer las demandas de los clientes es un reto clave, mientras que dos tercios (68 %) encuentran dificultades para mantener la rentabilidad en las relaciones con los clientes debido a la sobrecarga de recursos para tratar los problemas de seguridad basados en el usuario.
- La reputación en el mercado es clave para atraer y retener clientes: el 83 % de los MSP dependen del boca a boca, las recomendaciones, los vendedores que abordan a los clientes potenciales (50 %) y el patrocinio de eventos (48 %) para impulsar su base de clientes.
- Lo mismo ocurre en lo que respecta a la selección de un partner de seguridad por los MSP: el 92 % elige en función de la reputación y el precio. Al igual que ocurre con sus propios clientes, para añadir valor a su oferta, los MSP deben trabajar con un partner que no solo cuente con las soluciones y la experiencia adecuadas para prestarles asistencia, sino que también puedan ofrecerlas al mejor precio.
- En lo que se refiere a las expectativas de los MSP en la actualidad, ser expertos en infraestructuras de nube y en las instalaciones es la principal cualidad que necesitan los clientes (84 %). Las capacidades de ciberseguridad también aparecen entre los primeros puestos de la lista, pues el 74 % de los clientes las consideran un atributo clave en su partner MSP.
- Hacer frente a situaciones inesperadas puede afectar a las relaciones con los clientes y tener repercusión financiera para los MSP, lo que supondrá un obstáculo para mantener el crecimiento de los ingresos. Tres cuartas partes (78 %) de los clientes esperan que los MSP se encarguen de problemas que no cubre su contrato y el 65 % de los MSP abordan problemas de seguridad creados por errores de los usuarios en lugar de estar relacionados con los servicios que gestionan.
- Esto puede dar lugar a que los MSP a menudo asuman la culpa de incidentes de seguridad que no son fruto de su negligencia. El 43 % de las empresas que han sufrido un robo de datos culpa a su MSP y un 27 % lo achaca a la falta de conocimientos sobre seguridad de IT de su proveedor de servicios.

Metodología

Los resultados de este informe se obtienen de dos fuentes de datos:

- Entrevistas telefónicas realizadas entre julio y agosto de 2019 a 101 empleados de MSP en el Reino Unido, Francia, Alemania, España, Italia, Austria, Suecia y Dinamarca.
- Encuesta de riesgos de seguridad de IT corporativa de Kaspersky en 2019: una encuesta anual online a los responsables empresariales de la toma de decisiones de IT realizada en junio de 2019 en 23 países. Este informe se centra en las respuestas de aquellos que trabajan en empresas de toda Europa con menos de 500 empleados.

Externalización de IT: cambio en la dinámica del mercado de MSP

La perspectiva europea

El papel para las empresas de un MSP está pasando de proporcionar simplemente soluciones a convertirse en un asesor de confianza y un eje fundamental para el éxito operativo. Como tal, la externalización de IT se está convirtiendo en la nueva norma, ya que las empresas recurren a los expertos para recibir asesoría y que gestionen su infraestructura de IT en expansión y todo lo que conlleva.

El 40 % de las empresas de toda Europa con menos de 500 empleados externalizan actualmente la gestión de su IT a un tercero. Un tercio (33 %) también externaliza su gestión de la seguridad de IT, lo que sugiere que se trata de un área clave de la asistencia de IT que las empresas confían a su proveedor.

Es un denominador común en toda Europa, con los Países Bajos a la cabeza en lo que respecta a la externalización de la provisión de seguridad de IT (45 %), seguidos de cerca por Suecia (39 %) e Italia (39 %). Sin embargo, otros países también están tomando ritmo: Polonia (35 %), República Checa (24 %), Francia (22 %) y España (22 %) esperan mostrar el máximo crecimiento en la externalización de la gestión de la seguridad de IT en los próximos 12 meses.

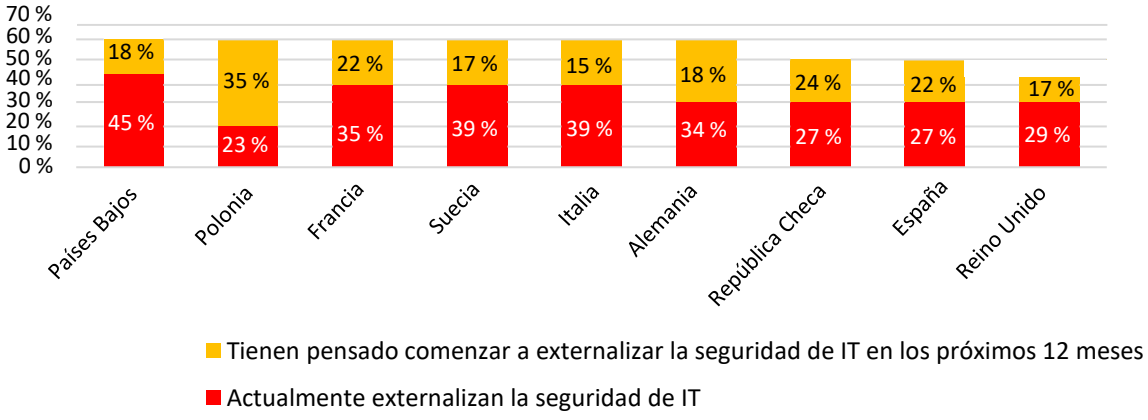

Figura 1. Niveles actuales y crecimiento previsto de la externalización de la seguridad de IT en los próximos 12 meses

Para las empresas que adoptan un enfoque externalizado, el modelo de contratación puede adoptar diferentes formas, dependiendo de los requisitos específicos de la empresa. La mayoría de los MSP observan que sus clientes desean una colaboración o enfoque mixto (51 %), que complemente los conocimientos internos con la experiencia externalizada para obtener el equilibrio perfecto en la gestión de la seguridad de IT. Sin embargo, casi un tercio (29 %) de los MSP consideran que las empresas prefieren externalizar toda el área de IT, incluida la seguridad de IT.

¿Qué motiva la decisión?

Al igual que ocurre con muchas decisiones empresariales, el coste es el principal factor que impulsa la necesidad de externalizar la gestión de la seguridad de IT. Más de la mitad de las empresas que planean externalizar la gestión de la seguridad de IT (52 %) creen que trabajar de esta forma les ayudará a reducir los costes relacionados con la seguridad y más de un tercio (38 %) pretende subcontratar toda la IT a un tercero, incluida la seguridad, como consecuencia. Curiosamente, un tercio (33 %) de las empresas consideran la externalización de la seguridad de IT como una forma de cubrir la responsabilidad y los SLA. La misma proporción (32 %) de empresas admite que, sencillamente, no disponen de los recursos internos ni de la experiencia necesaria para proporcionar los niveles de seguridad necesarios para su funcionamiento.

Por otra parte, hay motivos por los que las empresas deciden no externalizar su seguridad de IT, algo que deberían tener en cuenta los MSP al tratar de aumentar su oferta y establecer relaciones duraderas con los clientes. Si bien se suelen señalar los conocimientos como el principal motivo para trabajar con un tercero, el 40 % de las empresas que se oponen a la externalización de la gestión de la seguridad de IT con las que hemos hablado consideran que cuentan con la experiencia interna necesaria para gestionar su propia seguridad de IT. Otra fuente de preocupación para un tercio de las empresas (33 %) es el elevado coste, según se percibe, de externalizar la gestión de la seguridad de IT.

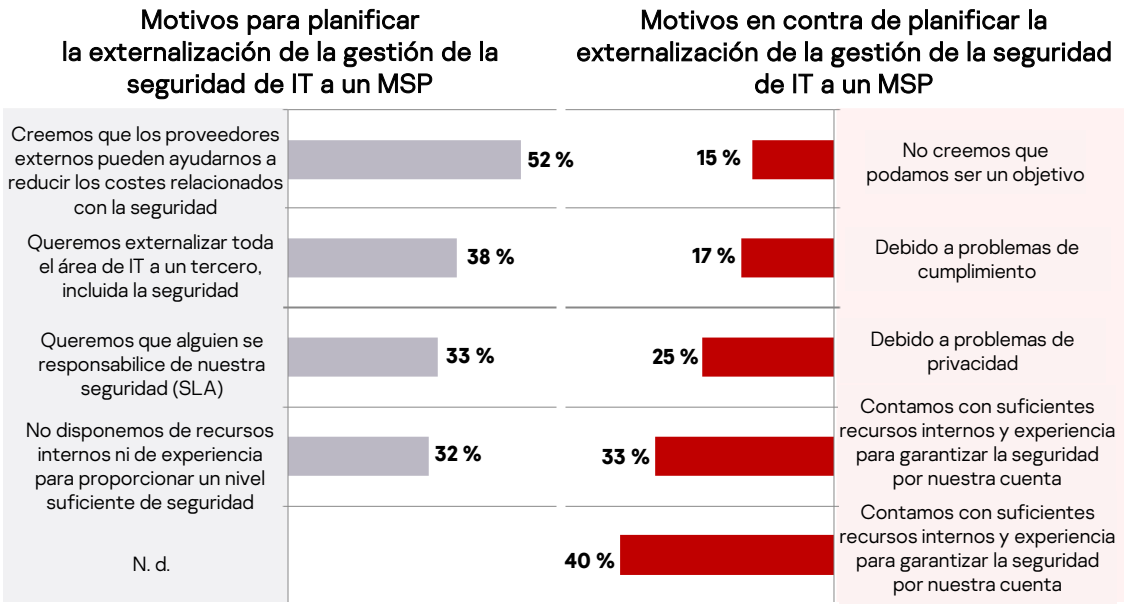

Figura 2. Pros y contras de planificar la externalización de la gestión de la seguridad de IT a un MSP

Si profundizamos en el proceso de toma de decisiones en diferentes sectores, se observa que existen varios factores que motivan la externalización. Aunque el ahorro de costes sea el motor en la mayoría de los sectores, el sector sanitario señala las cuestiones de privacidad como la principal razón para no externalizar y el sector educativo considera que el precio de las soluciones de terceros es demasiado alto.

El dilema del coste frente al presupuesto es sin duda un reto que deben encarar los MSP y empresas. Curiosamente, las empresas que esperan que sus presupuestos de seguridad de IT aumenten invertirán en reforzar el personal de IT interno y especializado. Sin embargo una disminución del presupuesto iría aparejada a una tendencia de las empresas a acudir a los MSP para respaldar la futura gestión de la seguridad de IT, lo que sugiere que consideran más provechoso trabajar de esta forma cuando los presupuestos son ajustados.

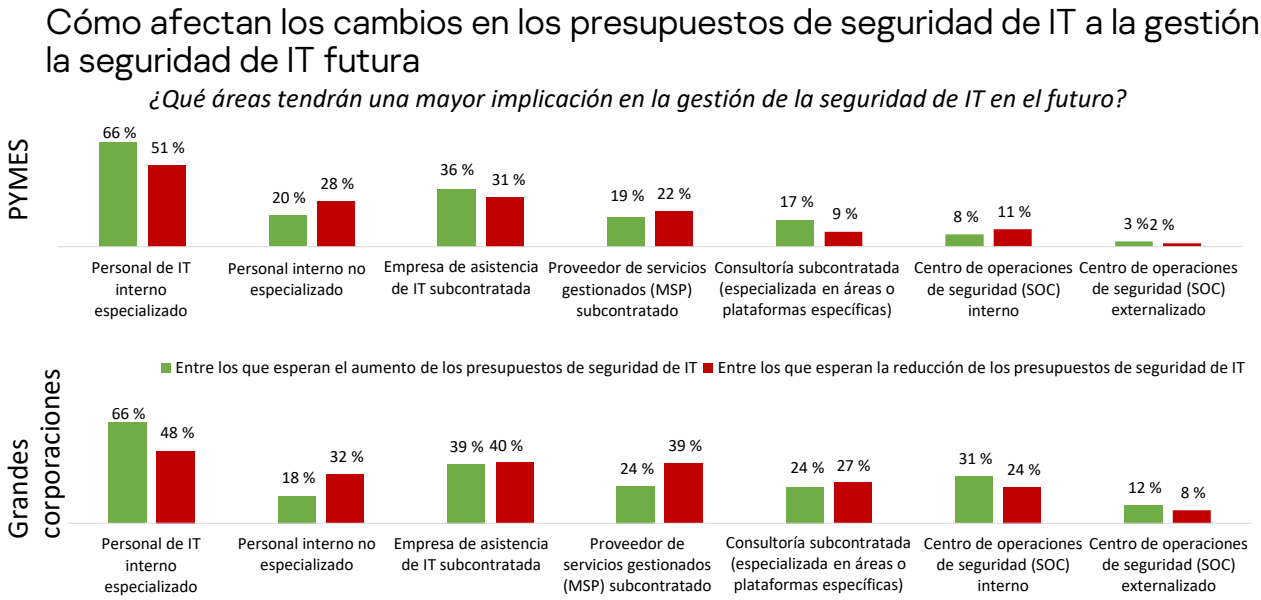

Figura 3. Cómo afectan los cambios en los presupuestos de seguridad de IT a la gestión de la seguridad de IT futura

Es evidente que sacar el máximo partido a los presupuestos disponibles y garantizar que se aplican los recursos y las medidas de seguridad adecuados está impulsando el crecimiento del negocio de los MSP. Sin embargo, los mismos factores de motivación también pueden ser elementos disuasorios para muchas posibles empresas y sectores a la hora de invertir en asistencia externa.

El panorama de MSP en Europa: prioridades y retos

Un MSP "típico"

Ya hemos comprobado que las funciones y las responsabilidades de los MSP están cambiando, por lo que es lógico volver a determinar dónde se encuentran la mayoría de los MSP en el panorama actual con el fin de evaluar las oportunidades y retos específicos a los que se enfrentan.

La mayoría (57 %) de los MSP con los que hemos hablado tienen entre 2 y 20 empleados y, a pesar de ser pequeñas empresas, un tercio (32 %) presta servicio a clientes con más de 300 empleados. El 50 % de los MSP trabajan con una amplia gama de clientes de diversos sectores y un tercio (35 %) se centra principalmente en prestar asistencia a pymes.

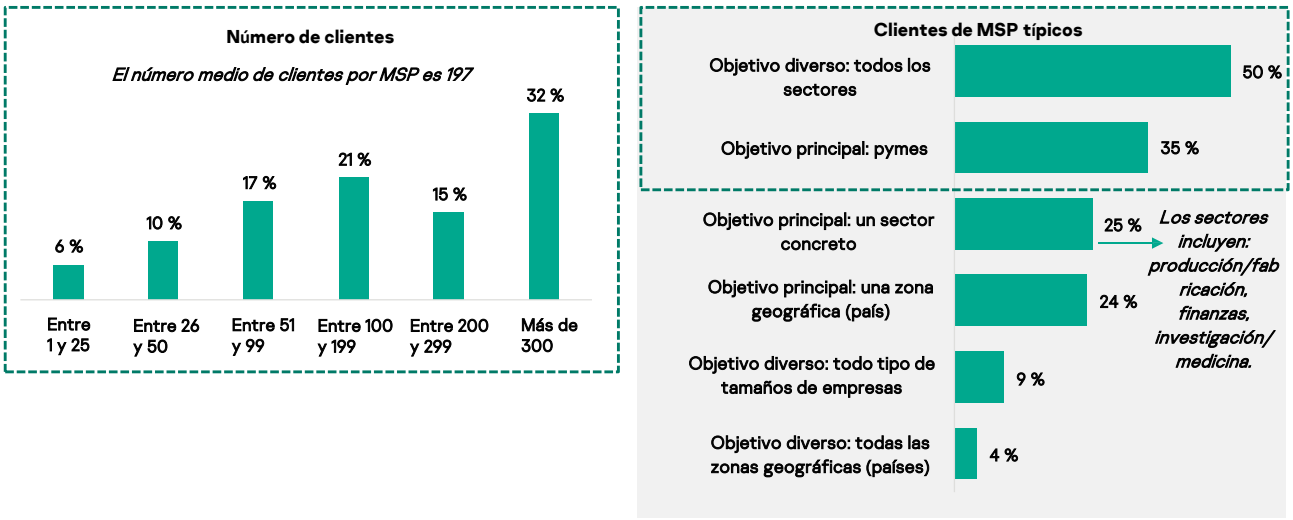

Figura 4. Número de clientes de MSP y clientes de MSP típicos

Tener una clientela tan amplia puede resultar un reto para los MSP, que necesitan demostrar que entienden y pueden respaldar los matices de cada sector y los puntos débiles específicos de las empresas. Por lo tanto, los MSP deben ofrecer una amplia gama de servicios a los clientes para satisfacer sus necesidades, lo que significa que deben contar con conocimientos y experiencia avanzados en diferentes áreas.

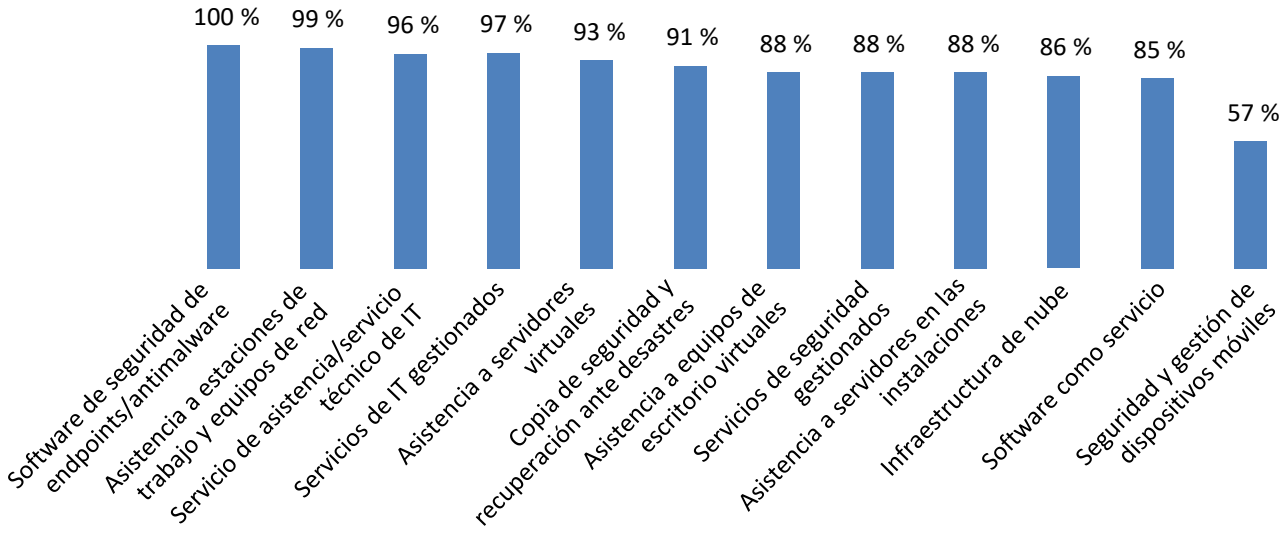

Figura 6. Descripción general de los principales "servicios gestionados" que se ofrecen a los clientes

Sin embargo, a pesar de las elevadas cifras de clientes, en lo que se refiere al número concreto de dispositivos que normalmente gestionan los MSP, un cuarto (23 %) solo gestiona entre 10 y 25 por cliente. Para el 48 % de los MSP, esto se reduce a menos de diez "nodos" por cliente.

Puntos fuertes y débiles

Una base de clientes en crecimiento puede ser una espada de doble filo para los MSP. A pesar de que las empresas claman por sus servicios, los clientes son cada vez más exigentes con sus MSP, fruto del aumento de la competencia que se está produciendo en el mercado. Esto es cierto en tres cuartos (75 %) de los MSP, que admiten que los clientes y usuarios más exigentes presentan importantes desafíos. La misma cifra (78 %) también considera complicado encontrar nuevos clientes y dos tercios (68 %) luchan por mantener la rentabilidad.

El problema de los ingresos se pone de manifiesto en la amplitud de servicios que deben proporcionar los MSP y en los bajos niveles de nodos que gestionan en realidad por cliente. Para ayudar a impulsar su valor para los clientes y proporcionar una mayores oportunidades de ingresos, los MSP podrían ofrecer un descuento en software de seguridad para que el modelo de externalización resulte más rentable para sus clientes y asegurarlos a largo plazo.

Dado que la satisfacción del cliente encabeza las preocupaciones de los MSP, no es de extrañar que las cifras de retención sean la principal medida de éxito para el 43 % de los MSP y que un 41 % se base en las encuestas de satisfacción del cliente para evaluar el rendimiento de su negocio. Por otra parte, las mediciones que se fundamentan en el valor que los MSP proporcionan a los clientes en términos de rentabilidad (33 %) y eficiencia (20 %) son inferiores.

En lo que se refiere a las estrategias para atraer clientes, la mayoría (83 %) de los MSP confían en el boca a boca o en las recomendaciones para impulsar su base de clientes, lo que convierte a la gestión de la reputación en un activo clave en el arsenal de los MSP.

A pesar de estos retos, los MSP europeos prevén un crecimiento empresarial significativo en los próximos dos años y un 63 % espera un fuerte crecimiento de los ingresos (hasta un 20 %). Esto refleja ciertamente la tendencia actual del mercado global y corrobora la previsión de una tasa de crecimiento anual del 9,3 %.

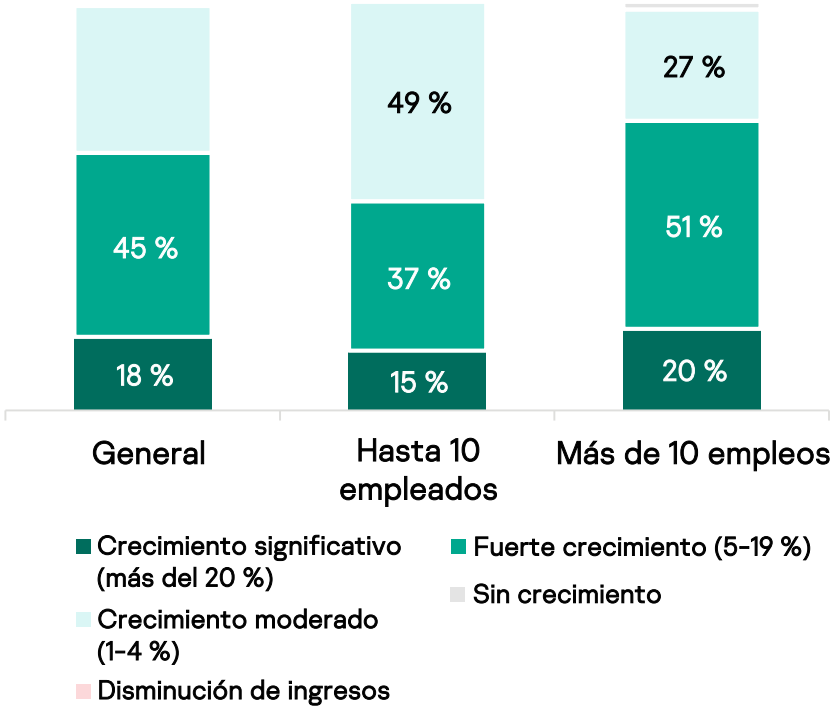

Figura 6. Crecimiento del negocio de los MSP previsto

El partner de seguridad perfecto

Queda claro que la externalización de la gestión de la seguridad de IT es una prioridad empresarial, por lo que ¿cómo pueden los MSP pueden seguir satisfaciendo esa necesidad y garantizar que las soluciones y servicios que proporcionan están a la altura? A la hora de asociarse con un proveedor de seguridad de IT, el 92 % de los proveedores de servicios gestionados elige en función de la reputación y el precio. Le siguen de cerca factores como la facilidad de gestión, integración y adquisición de licencias (88 %).

La forma en que los MSP adquieren las licencias también tiene efectos tanto en los riesgos como en las recompensas obtenidas, pues ayuda a acelerar y simplificar la prestación de servicios a los clientes. Los MSP prefieren flexibilidad en sus licencias: casi la mitad (47 %) afirma que prefieren adquirir licencias individuales para cada cliente. Mientras tanto, otros (44 %) deciden pagar por el software y los servicios de seguridad de IT de los proveedores a través de un modelo de suscripción mensual. Ambas opciones permiten que los MSP se protejan en caso de perder un cliente, pero también gestionar sus licencias de forma más eficaz.

Los MSP también prefieren usar un sistema de pedidos y de gestión de licencias sencillos, algo con bastante peso en su decisión al elegir un proveedor y una solución de seguridad. De hecho, más de la mitad (56 %) afirma que utilizan un portal de gestión de licencias de proveedores para obtener las licencias. Los MSP también se benefician de las herramientas de supervisión y gestión remotas (RMM), así como de automatización de servicios profesionales (PSA) integradas con software de seguridad para la supervisión y gestión centralizadas además de la automatización de las tareas rutinarias cotidianas.

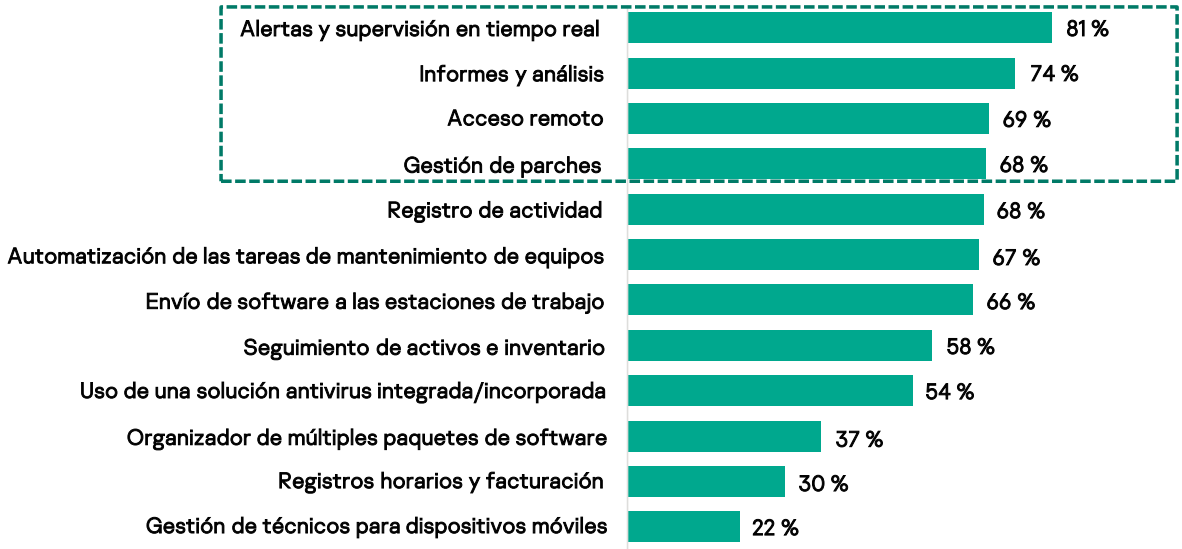

Figura 8. Usos principales de las plataformas de RMM entre los MSP

Altibajos en las relaciones

Cualidades frente a retos

Como en cualquier tipo de relación, ambas partes esperan mucho, pero inevitablemente habrá desafíos y obstáculos que superar a lo largo del camino. En lo que se refiere a las expectativas de los MSP actuales, ser expertos es la cualidad que los clientes buscan por encima de todas los demás (84 %), ya sea para soluciones de infraestructuras en nube o en las propias instalaciones. Los MSP también deben poder ayudar con el cumplimiento y las normativas (82 %), y responder rápidamente, así como adherirse a los SLA de alto nivel (80 %).

Es interesante señalar que casi tres cuartos (74 %) de los clientes que buscan asistencia en la gestión de IT destacaron como atributo obligatorio para los MSP las capacidades de ciberseguridad. El hecho de que este requisito figure tan arriba en su lista de prioridades evidencia que la capacidad de mantenerse al día con un panorama de ciberseguridad en constante evolución es algocon lo que las empresas también necesitan asistencia.

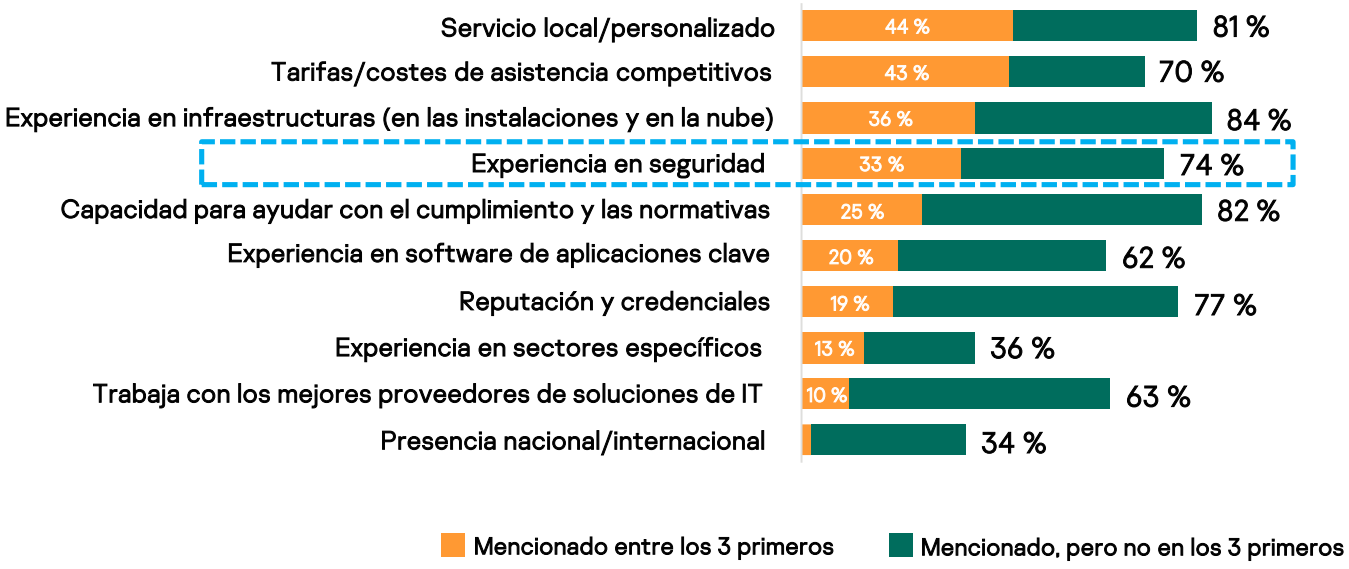

Figura 8. Cualidades más buscadas por los clientes en los MSP

Además de los requisitos indicados, también se espera que los MSP se ocupen de lo inesperado. Lamentablemente, ser un proveedor de confianza y experto plantea retos adicionales. Tres cuartas partes (78 %) de los clientes esperan que los MSP se encarguen de problemas que no cubre su contrato. Para otros, son los problemas que crean los usuarios los que les dan más trabajo (65 %) o la incapacidad de seguir los procesos del servicio de asistencia técnica (59 %) lo que añade trabajo innecesario a la lista de tareas pendientes.

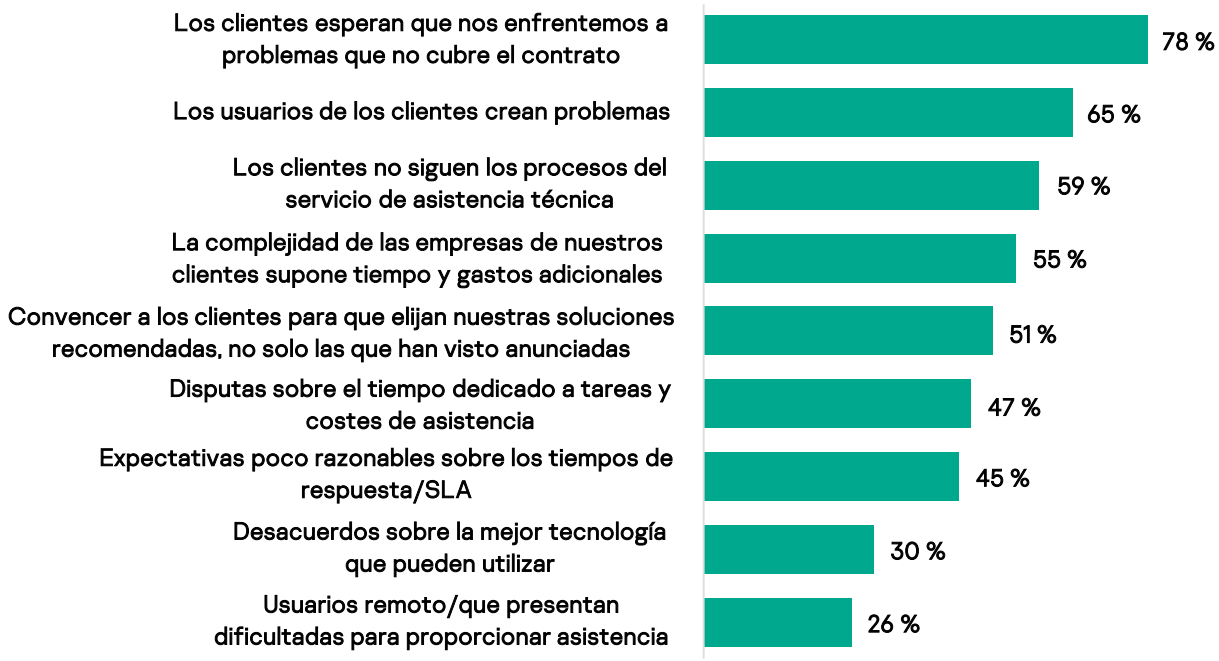

Figura 10. Puntos débiles que los MSP se encuentran con sus clientes

Sin embargo, el mayor reto al que se enfrentan los MSP es, sin duda, el volumen de ciberataques e infecciones de malware que provocan tiempos de inactividad para sus clientes (72 %), seguido de cerca por los ataques de ransomware (65 %). Pero no son solo las amenazas externas las que causan quebraderos de cabeza para los MSP: el factor humano sigue generando problemas, ya que el 69 % de los MSP consideran que los errores cometidos por los usuarios y no seguir las política de seguridad son importantes amenazas para la seguridad del cliente.

Qué significa esto para los MSP

El impacto de cualquier incidente de seguridad puede tener consecuencias graves no solo para el cliente, sino también para el MSP implicado. El reciente robo de datos de Capital One, que afectó a más de 100 millones de personas, se debió a una configuración errónea del firewall para aplicaciones web en Amazon Web Services. Pero aunque AWS quedó en el punto de mira, no se debió a un hackeo y problema se atribuyó a un cliente que no había configurado correctamente el firewall de la nube.

Este es solo un ejemplo de un tercero en la línea de fuego por un robo de datos de un cliente y, sin duda, no será el último. De hecho, de los clientes de MSP encuestados que han sufrido un robo de datos, el 43 % responsabilizaron a su MSP, comparado con solo un 41 % que aceptó que el fallo lo había producido su personal. Lo que es más sorprendente es que un cuarto (27 %) de aquellos que han experimentado una brecha lo achacaron a la falta de conocimientos sobre seguridad de IT por parte de su proveedor de servicios.

Sin embargo, los errores de seguridad del cliente también pueden afectar al MSP en términos de tiempo dedicado a resolver el problema (el 67 % está de acuerdo) y un tercio (38 %) incluso ha perdido dinero para arreglar un problema que no se debía a una negligencia suya ni a falta de experiencia.

Conclusión y recomendaciones

Queda claro que reducir los costes y sacar el máximo partido a los presupuestos de IT disponibles es el principal impulsor para que las empresas externalicen su gestión de IT. Esto, aparejado a la falta de recursos y conocimientos internos en seguridad de IT, brinda a los MSP una clara oportunidad de convertirse en expertos en ciberseguridad y cubrir la carencia en gestión de seguridad para las empresas europeas.

Por lo tanto, es vital que los MSP estén completamente equipados para ofrecer este nivel de servicio y satisfacer la creciente demanda de externalización de servicios de seguridad. Para ayudar a atraer nuevos clientes y aumentar los ingresos, necesitan ampliar la lista de servicios que ofrecen y centrarse en el posicionamiento en el mercado y en la gestión de la reputación para superar a sus competidores.

Los clientes esperan de su MSP la protección de la seguridad, pero también la experiencia en seguridad de la información. La falta de competencia en este terreno puede dar lugar a la pérdida de clientes y a la incapacidad de ser asesor y partner de confianza que estos necesitan. Es imprescindible que los MSP fomenten la confianza y la fidelidad de los clientes, lo que solo puede lograrse con las herramientas y conocimientos adecuados para apoyar a los clientes en cada paso del proceso.

La reputación es clave y un simple desliz producir consecuencias duraderos para atraer y retener a los clientes. Contar con toda la variedad de servicios de seguridad respaldados por un partner de ciberseguridad fuerte y fiable, hará que los MSP se sitúen en buena posición para hacer realidad el crecimiento previsto del mercado, lo que genera beneficios y estabilidad empresarial a largo plazo.

Los proveedores desempeñan un importante papel y pueden ofrecer asistencia vital a los MSP. No es ningún secreto que los MSP desean ampliar sus servicios de seguridad en los próximos años, de modo que los proveedores que pueden ofrecer evaluaciones de seguridad, respuesta ante incidentes y pasarelas de correo electrónico o de Internet se beneficiarán de la creciente demanda.

Los proveedores de seguridad pueden transmitir importantes conocimientos sobre ciberseguridad e impulsar las habilidades relacionadas, así como asistencia con el marketing y las ventas. La asociación para proveedores de servicios gestionados de Kaspersky ofrece productos de ciberseguridad exclusivos para el uso de los MSP, junto con formación específica, materiales educativos y eventos sobre ciberseguridad. Kaspersky cuenta con un amplio portfolio diseñado para MSP, que les permite implementar soluciones en las instalaciones o basadas en la nube, desde la protección de endpoints hasta la seguridad en la nube híbrida, protección de acceso web y correo electrónico. Estas soluciones pueden integrarse con plataformas de supervisión y gestión remotas (RMM) y automatización de servicios profesionales (PSA) para ayudar a los proveedores de servicios a automatizar las tareas rutinarias. El programa de partners también incluye ventajas financieras y de marketing para todos los partners de Kaspersky.

En el sitio web de Kaspersky encontrará más información sobre el programa de partners para proveedores de servicios gestionados de Kaspersky.

© 2019 Kaspersky Lab Iberia, España. Todos los derechos reservados. Las marcas registradas y logos son propiedad de sus respectivos dueños.