

INFORME

PERSPECTIVAS DE LOS MSP 2026

La opinión de 800 MSP sobre los retos
y las oportunidades que determinan el
futuro de los servicios de ciberseguridad.

SEPTIEMBRE DE 2026



Resumen ejecutivo

La ciberseguridad se enfrenta a una crisis de liderazgo. Solo hay un director de seguridad de la información (CISO) por cada 10 000 organizaciones en todo el mundo¹, lo que deja a la gran mayoría sin la gestión y la estrategia dedicadas que necesitan para garantizar que su seguridad sea demostrable. Mientras tanto, para agravar aún más el problema, los incidentes siguen aumentando, el gasto en seguridad se ha incrementado y la confianza de los consejos de administración sigue siendo baja. Puede que las organizaciones estén invirtiendo más que nunca, pero muchas siguen teniendo dificultades para responder a preguntas fundamentales sobre su riesgo, resiliencia y resultados de inversión.

Esta brecha supone una gran oportunidad para que los proveedores de servicios gestionados (MSP) y otros expertos del canal vayan más allá de la mera prestación de servicios y se conviertan en líderes de confianza en materia de ciberseguridad. La investigación que se recoge en este informe pone de manifiesto que los clientes recurren cada vez más a sus Partners en busca de asesoramiento sobre su programa de ciberseguridad, desde la implementación técnica hasta la gestión integral. Los Partners que sean capaces de aportar claridad ante la complejidad, ayudando a sus clientes a comprender cuál es su situación actual, cómo están mejorando y dónde persisten los riesgos, estarán mejor posicionados para cubrir este vacío de liderazgo.

Sin embargo, ejercer un liderazgo en ciberseguridad a gran escala requiere algo más que conocimientos especializados. Como se muestra en la página 19, **los MSP estiman que podrían ahorrar más de la mitad del tiempo de su equipo** si las actividades de seguridad y cumplimiento se gestionaran a través de una plataforma única y unificada. Esto pone de relieve la importancia crucial de la eficiencia operativa. Para satisfacer la creciente demanda de los clientes, los proveedores necesitan un modelo que haga que sus esfuerzos sean replicables, escalables y cuantificables en toda su base de clientes.



Scott Barlow
VP, Chief Evangelist
Sophos

¹ <https://www.sophos.com/es-es/resources/report/2026-ciso-report>

Introducción

El informe de Sophos «Perspectivas de los MSP 2026» ofrece información detallada sobre tres áreas estratégicas del negocio de los MSP:

- El auge del liderazgo cibernético prestado por los MSP
- El cumplimiento como eje central de la prestación de servicios de los MSP
- La puesta en práctica de la seguridad y el cumplimiento a gran escala

Los resultados se basan en una encuesta independiente y desvinculada del proveedor realizada a 800 MSP ubicados en EE. UU. (200), Reino Unido (100), Alemania (100), Francia (100), Singapur (100), Australia (100) y Brasil (100). Los encuestados son responsables de la toma de decisiones en el ámbito de los MSP, desde altos directivos hasta miembros de consejos de administración.

La encuesta fue encargada por Sophos y realizada por la consultora Vanson Bourne en abril de 2026.

800

MSP

7

áreas de cumplimiento clave

7

países

Conclusiones clave de un vistazo

1. Los MSP se han convertido, en la práctica, en los CISO de sus clientes

- **88 %** de los MSP afirman que al menos el **20 %** de sus clientes recurren a ellos para ejercer de CISO.
- **84 %** de los MSP prevé que la demanda de servicios de CISO aumente en los próximos 12 meses.

2. Los servicios de cumplimiento están muy extendidos, pero aún no han alcanzado la madurez

- **99 %** de los MSP presta servicios de cumplimiento.
- **6 %** ofrece un conjunto completo de servicios de cumplimiento, lo que deja margen para el crecimiento.

3. El cumplimiento promueve la inversión en seguridad

- **50 %** de las decisiones de compra de los clientes se ven influidas por los requisitos de cumplimiento normativo.
- Esta influencia constituye, de media, un factor determinante en el **33 %** de las decisiones de compra.

4. El cambio hacia el cumplimiento continuo es gradual

- **62 %** de los MSP se muestran «muy seguros» de su capacidad para supervisar, gestionar y documentar de forma continua el cumplimiento de múltiples clientes.
- **33 %** afirma sentirse «totalmente seguro», lo que pone de manifiesto que muchos se beneficiarían de las mejoras.

5. La prestación basada en herramientas es el estándar

- **53 %** de los MSP utiliza varias herramientas o plataformas para gestionar de forma centralizada el cumplimiento de las normas de ciberseguridad o las actividades propias de un CISO.
- **36 %** recurre a una sola, lo que implica que los MSP y sus clientes operan dentro de un modelo complejo, fragmentado y potencialmente incompleto.

6. La elaboración de informes de seguridad se está automatizando

- **86 %** de los MSP utiliza un proceso total o parcialmente automatizado para elaborar informes consolidados sobre la postura de seguridad.
- **55 %** sigue requiriendo una intervención manual para consolidar las actividades, lo que sugiere que la mayoría de los procesos de elaboración de informes siguen estando automatizados solo parcialmente.

7. Aún quedan por aprovechar importantes mejoras en la eficiencia

- **53 %** de tiempo ahorrarían los MSP si pudieran utilizar una única plataforma unificada para la gestión y la elaboración de informes sobre la postura de seguridad y el cumplimiento de los clientes.
- **81 %** de los MSP considera que ello reduciría en más de un **30 %** el tiempo que dedican actualmente a estas actividades.

Parte 1: El auge del liderazgo en seguridad prestado por los MSP

1. Los MSP se han convertido, en la práctica, en los CISO de sus clientes

Las organizaciones se enfrentan a una presión creciente debido a un panorama de amenazas en evolución, ataques basados en inteligencia artificial (IA), normativas en expansión y la escasez de competencias en seguridad. Muchas también carecen del liderazgo interno necesario para abordar estos desafíos a través de un programa de ciberseguridad coordinado en lugar de solo la gestión tecnológica. En respuesta a ello, los MSP están ascendiendo en la cadena de valor, pasando de ser proveedores de herramientas tácticas a socios de asesoramiento estratégico.

Los datos del informe muestran que este cambio ya está en marcha. De media, los MSP estiman que **el 46 % de sus clientes** confía ahora en ellos para este tipo de liderazgo cibernético. Esta confianza está muy extendida: **el 88 % de los MSP** ejerce de CISO para más del **20 %** de su cartera de clientes, **el 40 %** para más de la mitad y **el 20 %** para más del **70 %**.

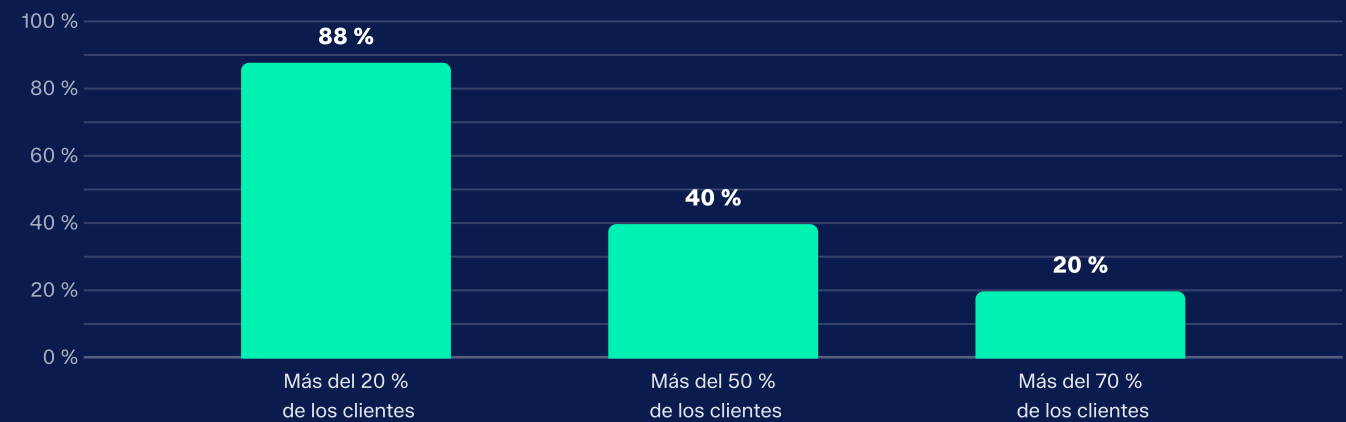
88 %

de los MSP desempeñan la función de CISO para más del 20 % de su cartera de clientes.

46 %

de los clientes de los MSP, de media, esperan que su MSP desempeñe esta función.

Confianza del cliente en los servicios CISO prestados por MSP

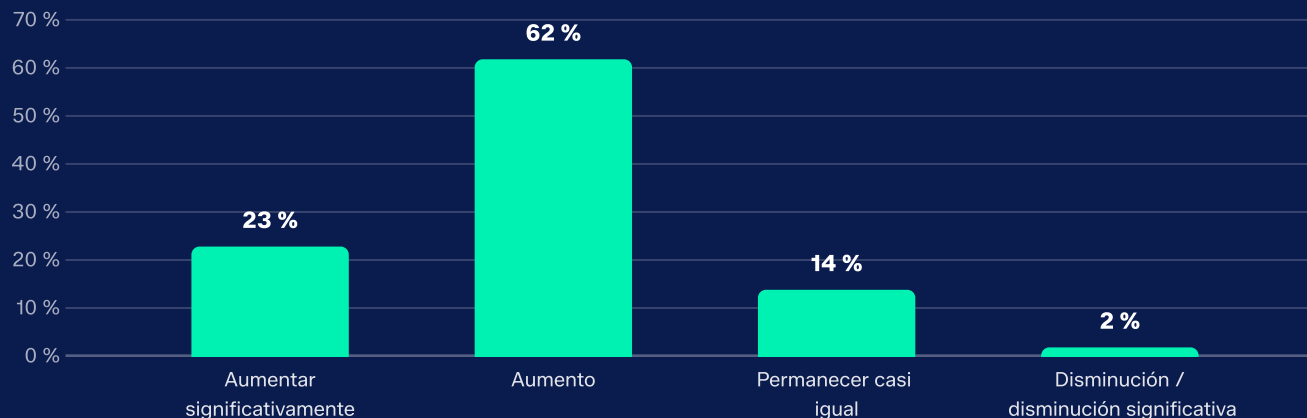


¿Aproximadamente qué porcentaje de sus clientes espera que su organización ejerza de CISO, si es el caso? (n=800)

La demanda de servicios de CISO prestados a través de MSP aumentará

Esta oportunidad para los MSP solo hará más que crecer. El **84 %** prevé que la demanda de servicios de CISO aumente en los próximos 12 meses, incluido un **23 %** que anticipa un crecimiento significativo. Solo el **2 %** prevé un descenso.

Cambio esperado en la demanda de servicios CISO



¿Cómo prevé que esto cambie en los próximos 12 meses, si es que cambia? (n=800)

Los límites tradicionales del papel del MSP están cambiando rápidamente, lo que refleja los desafíos a los que se enfrentan las organizaciones que carecen de la experiencia, los recursos o los fondos para mantener a un responsable de seguridad interno dedicado. Ahora buscan en sus MSP orientación estratégica de ciberseguridad a nivel de CISO, gestión de riesgos y gobernanza que vaya más allá de la gestión tecnológica diaria. Los proveedores que puedan cubrir este vacío y consolidarse como la opción de referencia se encuentran en una posición idónea para hacer frente a la creciente demanda.

84 %

de los MSP prevé que la demanda de servicios de CISO aumente en los próximos 12 meses.

23 %

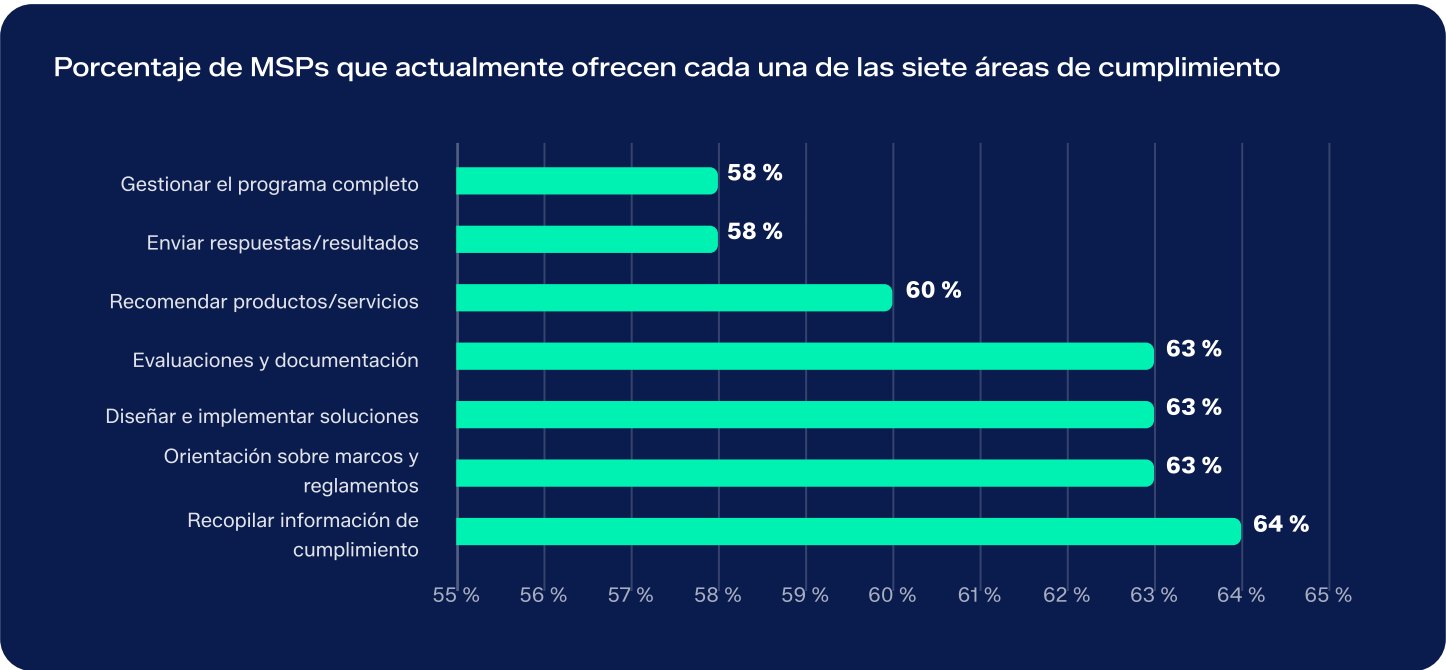
espera que aumente significativamente.

Parte 2: El cumplimiento como eje central de la prestación de servicios de los MSP

1. Los servicios de cumplimiento están muy extendidos, pero aún no han alcanzado la madurez

El cumplimiento de la ciberseguridad es ahora una parte fundamental de la propuesta de valor de los MSP, impulsado por el aumento de las normativas y leyes que exigen una gestión continua y dedicada de los programas de ciberseguridad. Los MSP están perfectamente capacitados para ofrecer este servicio.

En las siete actividades de cumplimiento evaluadas, la prestación de servicios se mantiene en un nivel elevado de forma constante. En cada una de las áreas de servicio enumeradas, **entre el 58 % y el 64 % de los MSP** afirman que ya ofrecen esa capacidad específica a sus clientes.



¿Cuál de las siguientes opciones describe mejor la implicación de su organización en el cumplimiento de las normas de ciberseguridad de sus clientes, tanto en la actualidad como en el futuro? (n=800)

99 %

de los MSP ofrecen algún tipo de servicio relacionado con el cumplimiento.

58 %

ofrece una gestión integral del programa de cumplimiento.

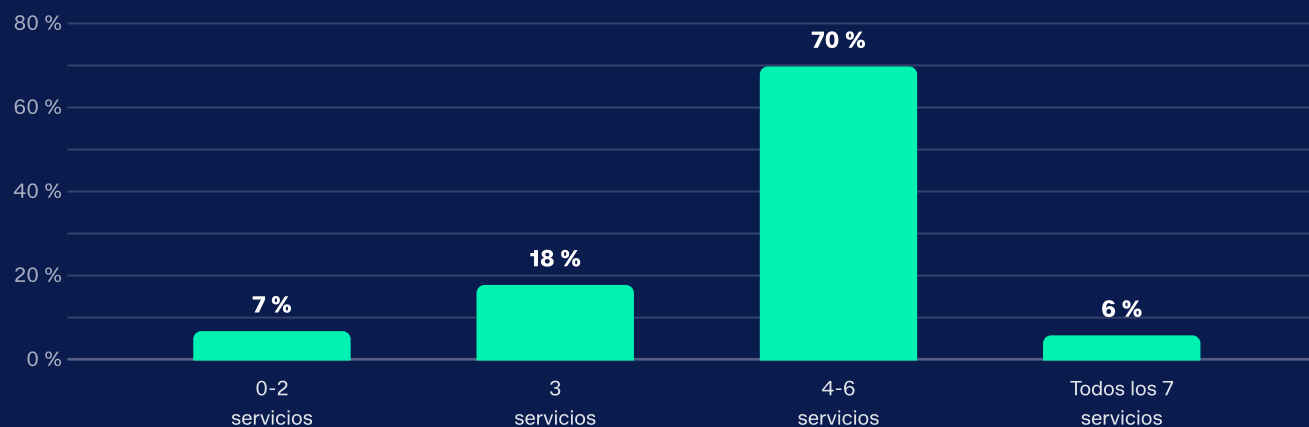
6 %

ofrece un conjunto completo de servicios de cumplimiento.

Son pocos los MSP que ofrecen una gama completa de servicios de cumplimiento

Aunque los servicios de cumplimiento individuales se ofrecen de forma generalizada, la mayoría de los MSP no llegan a cubrir el ciclo de vida completo del cumplimiento; **el 70 %** ofrece entre cuatro y seis de las siete actividades medidas, mientras que solo el **6 %** proporciona las siete. Esto sugiere que muchos MSP todavía necesitan ampliar su oferta y conectar estas capacidades en un programa de cumplimiento integral que proporcione la supervisión exhaustiva que los clientes necesitan.

Profundidad de los servicios de cumplimiento ofrecidos

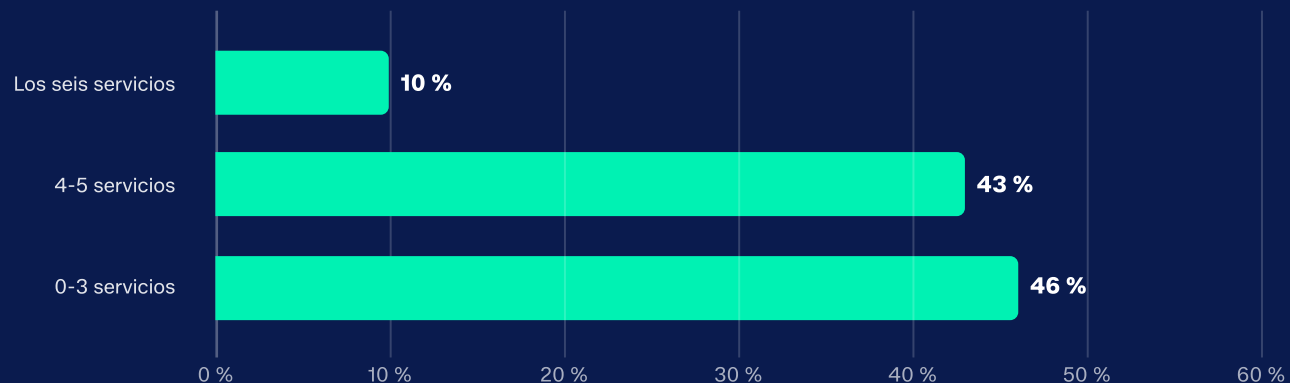


¿Cuál de las siguientes opciones describe mejor la implicación de su organización en el cumplimiento de las normas de ciberseguridad de sus clientes, tanto en la actualidad como en el futuro? (n=800)

Muchos MSP que ofrecen gestión de programas de cumplimiento no ofrecen todos los servicios de apoyo

Si nos centramos específicamente en los MSP que gestionan el programa de cumplimiento completo de sus clientes, se observa una brecha similar. Del **58 % de los MSP** que lo hacen, solo el **10 %** ofrece también los otros seis servicios. Esto sugiere que muchos MSP están asumiendo la responsabilidad a nivel de programa antes de desarrollar una pila integral de servicios de cumplimiento. En la práctica, la gestión de programas de cumplimiento puede implicar la coordinación de actividades realizadas por clientes o especialistas externos, en lugar de prestar cada servicio directamente. En consecuencia, la supervisión del programa y la capacidad de prestación de servicios no siempre van de la mano.

Número de servicios de cumplimiento prestados por MSP que ofrecen una gestión completa del programa



⁴Cuál de las siguientes opciones describe mejor la implicación de su organización en el cumplimiento de las normas de ciberseguridad de sus clientes, tanto en la actualidad como en el futuro? MSP que ofrecen una gestión integral del programa de cumplimiento (n=465)

Los MSP tienen previsto ampliar su oferta en materia de cumplimiento

La buena noticia es que es probable que la demanda de estas capacidades impulse una mayor expansión. Muchos MSP que actualmente no ofrecen servicios de cumplimiento tienen previsto introducirlos en el futuro. Se espera que el mayor crecimiento se produzca en la gestión integral de programas de cumplimiento: además del 58 % que ya ofrece esta capacidad, otro 40 % tiene previsto añadirla. Esto sugiere que la gestión de programas se está convirtiendo rápidamente en un componente estándar de las ofertas de cumplimiento de los MSP.

SERVICIO	OFRECE ACTUALMENTE	TIENE PREVISTO INTRODUCIR	TOTAL
Recomendar productos/servicios			
Asesorar sobre herramientas y servicios de seguridad que contribuyan a los objetivos de cumplimiento.	60 %	38 %	99 %
Diseñar e implementar soluciones			
Configurar y desplegar controles de seguridad para satisfacer los requisitos de cumplimiento de forma eficaz.	63 %	37 %	100 %
Marcos normativos y reglamentación			
Identificar los reglamentos, normas y marcos normativos aplicables que afecten al cumplimiento de los clientes.	63 %	36 %	99 %
Recopilar información de cumplimiento			
Proporcionar a los clientes la documentación necesaria para cumplir con sus obligaciones normativas.	64 %	35 %	99 %
Evaluaciones y documentación			
Realizar evaluaciones y elaborar documentación que demuestre el estado de cumplimiento y las deficiencias.	63 %	36 %	98 %
Enviar respuestas/resultados			
Preparar y presentar las respuestas a las auditorías, los cuestionarios y las pruebas de cumplimiento.	58 %	40 %	98 %
Gestionar el programa completo			
Supervisar las actividades de cumplimiento en curso, la recopilación de pruebas, la elaboración de informes y la gobernanza.	58 %	40 %	99 %

Los porcentajes se han redondeado.

¿Cuál de las siguientes opciones describe mejor la implicación de su organización en el cumplimiento de las normas de ciberseguridad de sus clientes, tanto en la actualidad como en el futuro?
Excluye respuestas "No lo sé" (n=800)

Los servicios de cumplimiento son un área en crecimiento para los MSP de todos los tamaños

La madurez de la oferta de servicios de cumplimiento de los MSP no viene determinada por su tamaño. Aunque los MSP con más de 51 empleados son los más propensos a proporcionar los siete servicios de cumplimiento evaluados (**10 %**), los MSP más pequeños siguen siendo competitivos. Aquellos con hasta cinco empleados son más propensos a ofrecer entre cuatro y seis de los siete servicios (**77 %**) que cualquier otro grupo y registran el mayor número medio de servicios prestados.

La adopción de la gestión integral de programas también es relativamente homogénea, oscilando entre **el 54 % y el 62 %**. Esto sugiere que el cumplimiento normativo se está convirtiendo en un área de crecimiento para los MSP de todos los tamaños, lo que desplaza la competencia de la disponibilidad de los servicios hacia la rapidez de prestación, la profundidad y la madurez de los mismos.

TAMAÑO DEL MSP	0-2 SERVICIOS	3 SERVICIOS	4-6 SERVICIOS	LOS SIETE SERVICIOS	N.º MEDIO DE SERVICIOS	GESTIÓN INTEGRAL DEL PROGRAMA
1-5 empleados	5 %	11 %	77 %	7 %	5	62 %
6-25 empleados	8 %	25 %	65 %	2 %	4	54 %
26-50 empleados	8 %	17 %	70 %	6 %	4	59 %
>51 empleados	5 %	17 %	69 %	10 %	4	59 %

Los porcentajes se han redondeado.

¿Cuál de las siguientes opciones describe mejor la implicación de su organización en el cumplimiento de las normas de ciberseguridad de sus clientes, tanto en la actualidad como en el futuro? Excluye respuestas "No lo sé" (n=800)

Los MSP han logrado un progreso significativo en la creación de prácticas de cumplimiento normativo, y casi todos los proveedores ofrecen ahora al menos un servicio de cumplimiento y la mayoría ofrece múltiples capacidades a lo largo del ciclo de vida del cumplimiento. La gestión integral de programas se está generalizando y va camino de convertirse en una oferta casi universal, lo que refleja la creciente demanda de los clientes de un apoyo continuo en materia de cumplimiento.

Sin embargo, no debe confundirse la amplitud de la oferta de servicios con la madurez. Aunque muchos MSP han ampliado su oferta más allá de los servicios básicos de asesoramiento, son relativamente pocos los que han desarrollado una oferta de cumplimiento verdaderamente completa. La mayoría sigue operando con una pila parcial de servicios. Incluso entre aquellos que ofrecen una gestión integral del programa, solo una pequeña minoría proporciona el conjunto completo de servicios de apoyo al cumplimiento.

A medida que los servicios de cumplimiento se vayan generalizando, la ventaja competitiva dependerá cada vez más de la rapidez, la exhaustividad, la calidad y la fluidez de la prestación de dichos servicios, más que de la mera oferta de los mismos. **Los MSP que sean capaces de integrar el asesoramiento, la implementación, la documentación, la elaboración de informes y la gestión de programas en una práctica de cumplimiento normativo coherente estarán mejor posicionados para diferenciarse como líderes del mercado.**

El cumplimiento normativo se ha convertido en un factor determinante de la inversión en ciberseguridad. Los MSP afirman que el cumplimiento normativo influye, de media, en el **50 %** de las compras de ciberseguridad de sus clientes, y que en el **33 %** de los casos dicha influencia es «considerable» o «decisiva». Esa influencia está muy extendida:

el **81 % de los MSP** afirma que el cumplimiento normativo afecta al menos al **25 %** de las compras de sus clientes, y el **51 %** afirma que influye al menos en la mitad de ellas. En otras palabras, el cumplimiento ya no es solo un requisito de generación de informes, sino que está determinando de forma activa la forma en que los clientes establecen sus prioridades en materia de gasto en seguridad.

Ahora es el momento de dotar a esa influencia de un carácter más estratégico. Solo el **9 %** de los MSP afirma que el cumplimiento normativo influye «en gran medida» o «de manera decisiva» en una mayoría significativa (**75 %**) de las adquisiciones de ciberseguridad de los clientes. Esto deja margen para que los MSP utilicen el cumplimiento normativo como punto de partida para entablar conversaciones de asesoramiento más amplias, ofrecer servicios más exhaustivos y desarrollar programas de seguridad más estructurados.

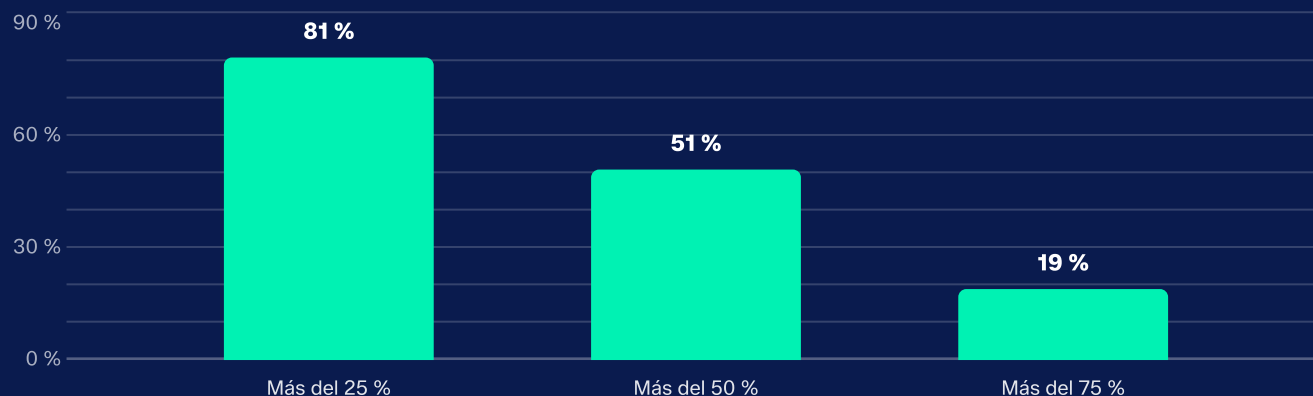
50 %

de las decisiones de compra de los clientes se ven influidas por los requisitos de cumplimiento.

33 %

de esas decisiones se ven muy influidas por los requisitos de cumplimiento.

Porcentaje de compras de clientes influenciadas por el cumplimiento



¿Qué porcentaje de las decisiones de compra de ciberseguridad de sus clientes están influidas, al menos en parte, por los requisitos de cumplimiento normativo, si los hay? (n=800)

Los MSP pueden aprovechar el cumplimiento normativo de sus clientes para entablar conversaciones estratégicas

En conjunto, los resultados muestran que el cumplimiento está pasando de ser una obligación reglamentaria a convertirse en un factor clave para el negocio. Ya ejerce una clara influencia en el gasto de los clientes en materia de seguridad. Sin embargo, son pocos los MSP que lo han convertido en una vía rentable para abordar temas más amplios relacionados con la ciberseguridad. Esto les brinda la oportunidad de cubrir ese vacío y transformar la demanda derivada del cumplimiento en relaciones de asesoramiento más profundas y en servicios estratégicos de mayor valor.

Porcentaje de compras de clientes "fuertemente" o "decisivamente" influenciadas por el cumplimiento

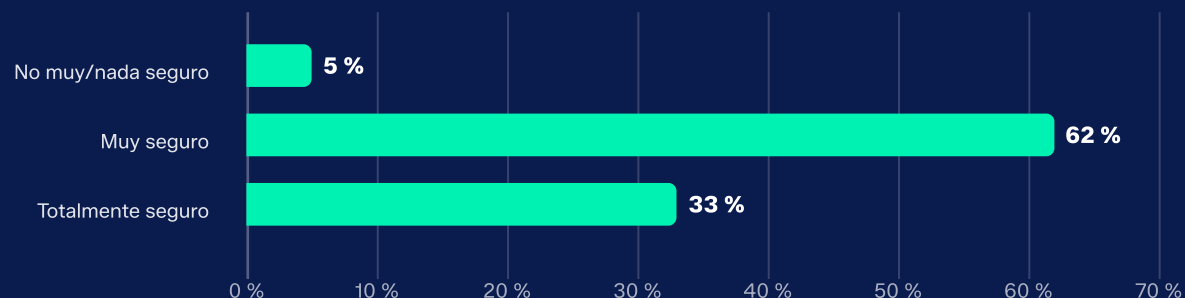


¿Qué porcentaje de las decisiones de compra de ciberseguridad de sus clientes están influidas de forma importante o decisiva por los requisitos de cumplimiento normativo? (n=800)

3. El cambio hacia el cumplimiento continuo es gradual

Los MSP están adoptando cada vez más un enfoque continuo en la gestión del cumplimiento. Los niveles de confianza indican que la mayoría de los proveedores consideran que están bien preparados para prestar apoyo a sus clientes a medida que el cumplimiento pasa de las auditorías periódicas a la supervisión y la gobernanza continuas. En general, el **95 % de los MSP** se muestran «muy» o «totalmente» seguros de su capacidad para supervisar, gestionar y documentar continuamente el cumplimiento de múltiples clientes.

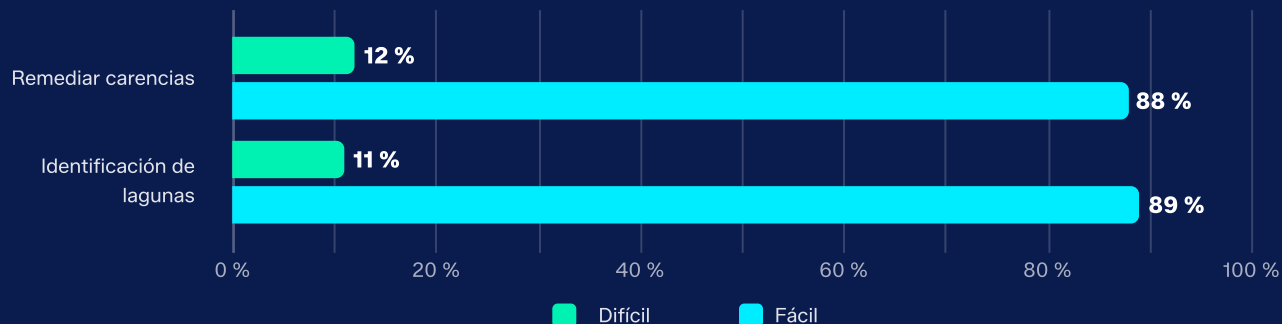
Confianza de los MSP en la gestión continua del cumplimiento



¿En qué medida confía en la capacidad actual de su organización para supervisar, gestionar y documentar de forma continua los requisitos de cumplimiento de múltiples clientes, si es el caso? (n=800)

Esta confianza también se refleja en lo preparados que están los MSP para identificar y subsanar las brechas de cumplimiento y control de sus clientes, y solo una pequeña minoría informa de dificultades en ambos aspectos.

Facilidad para los MSP a la hora de encontrar y remediar brechas de cumplimiento y control



¿En qué medida resulta fácil o difícil para su organización identificar y remediar las deficiencias en materia de cumplimiento o de control que afectan a sus clientes en la actualidad? (n=800)

62 %

de los MSP se muestran «muy seguros» de su capacidad para supervisar, gestionar y documentar de forma continua el cumplimiento de múltiples clientes.

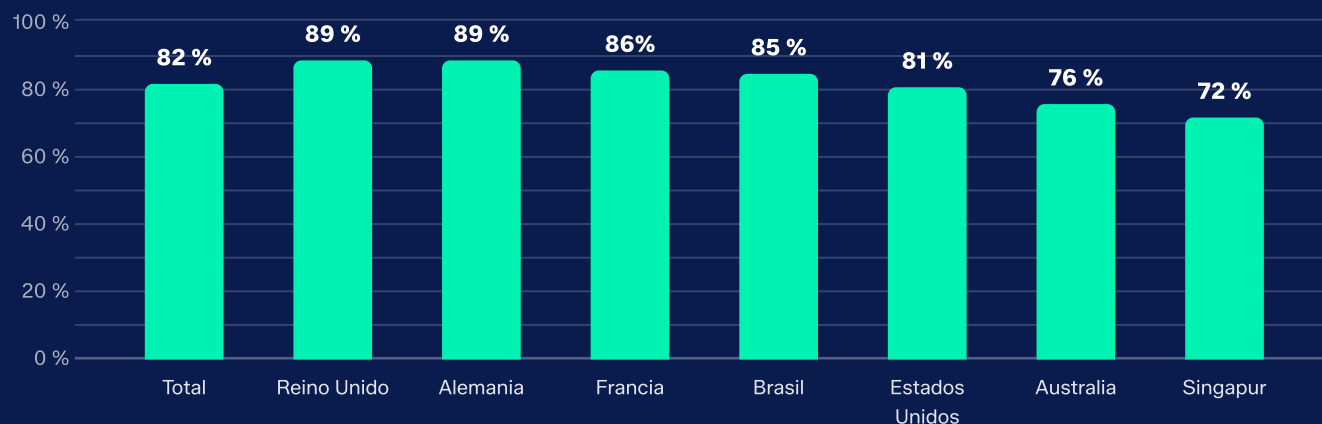
33 %

se muestra «totalmente seguro» de su capacidad.

La confianza en la gestión de las deficiencias en materia de cumplimiento y control varía según el país

Si bien la gestión de las deficiencias en materia de cumplimiento y control es una capacidad bien consolidada para la mayoría de los MSP, el grado de confianza varía según el país. Los MSP del Reino Unido y Alemania afirman que son los que tienen más probabilidades de identificar y remediar fácilmente estas deficiencias (**89 %**), en comparación con el **81 %** en EE. UU., el **76 %** en Australia y el **72 %** en Singapur. Estas diferencias sugieren que, si bien muchos proveedores cuentan con procesos operativos establecidos, el reto práctico de mantener el cumplimiento normativo y reducir el riesgo es mayor en algunos mercados que en otros.

La facilidad para identificar y remediar las deficiencias de cumplimiento varía según el país



¿En qué medida resulta fácil o difícil para su organización identificar y remediar las deficiencias en materia de cumplimiento o de control que afectan a sus clientes en la actualidad? (n=800)

Los MSP de todos los tamaños confían en su capacidad para gestionar de forma continua el cumplimiento de los clientes

Los niveles de confianza se mantienen notablemente homogéneos entre los MSP de todos los tamaños. Los proveedores más pequeños son los que registran la mayor confianza general: el **98 % de los MSP** con entre 1 y 5 empleados afirman tener «total» o «much» confianza en su capacidad para gestionar el cumplimiento continuo, en comparación con el **92 %** de los MSP con 51 o más empleados. La confianza total sigue siendo mucho menor en todos los tramos de tamaño, oscilando entre el **30 % y el 36 %**. La diferencia entre la alta confianza y la certeza total sugiere que, si bien las capacidades de cumplimiento normativo continuo se están consolidando en toda la comunidad de MSP, a muchos proveedores les convendría mejorar su modelo actual.

CONFIANZA EN LA GESTIÓN CONTINUA DEL CUMPLIMIENTO	TOTAL	1-5 EMPLEADOS	6-25 EMPLEADOS	26-50 EMPLEADOS	51+ EMPLEADOS
Totalmente seguro	33 %	36 %	34 %	30 %	31 %
Muy seguro	62 %	62 %	62 %	65 %	60 %
No muy seguro	4 %	2 %	4 %	5 %	7 %
Para nada seguro	0 %	0 %	0 %	1%	1%
Totalmente o muy seguro	95 %	98 %	96 %	95 %	92%

¿En qué medida confía en la capacidad actual de su organización para supervisar, gestionar y documentar de forma continua los requisitos de cumplimiento de múltiples clientes, si es el caso? (n=800)

La ciberresiliencia depende de la demostración continua del cumplimiento, más que de garantías periódicas. Para los clientes, esto supone una evidencia clara de que los controles funcionan, de que se detectan las deficiencias y de que se van introduciendo mejoras con el tiempo. El nivel de confianza de los MSP demuestra que esta capacidad está surgiendo claramente, pero la falta de una certeza absoluta pone de relieve tanto las oportunidades como los riesgos. Los proveedores que sean capaces de cubrir este vacío para ofrecer servicios de cumplimiento coherentes, escalables y replicables se encontrarán en una posición privilegiada para expandirse hacia servicios de gobernanza de mayor valor. Aquellos que no puedan hacerlo podrían tener dificultades para proporcionar el nivel de garantía que necesitan los clientes, a medida que las amenazas, las normativas y los riesgos empresariales continúan intensificándose.

Parte 3: La puesta en práctica de la seguridad y el cumplimiento a gran escala

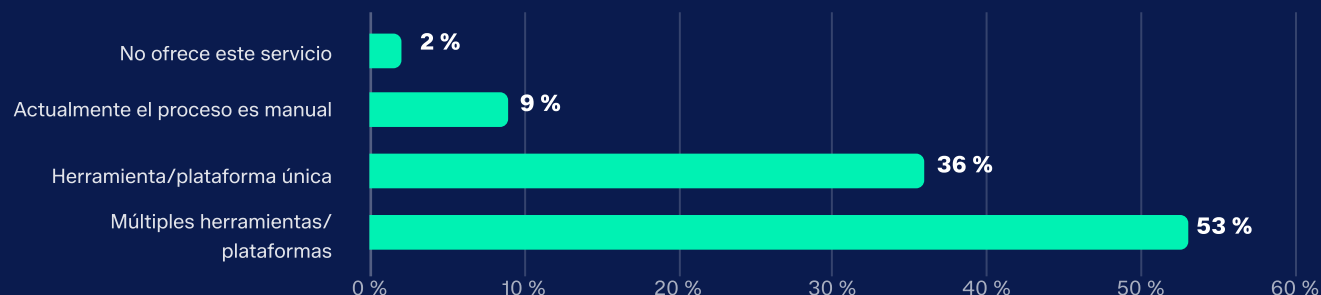
1. La prestación basada en herramientas es el estándar

A medida que los MSP amplían su papel en el cumplimiento de las normas de ciberseguridad y en los servicios de asesoramiento estratégico, la prestación de servicios basada en herramientas se ha convertido en una práctica habitual. El **89 % de los MSP** utiliza actualmente una o varias herramientas o plataformas para gestionar de forma centralizada el cumplimiento o las actividades propias de un CISO en toda su cartera de clientes. Solo el **9 %** sigue dependiendo de procesos totalmente manuales, mientras que el **2 %** no ofrece estos servicios en absoluto.

La adopción de estas tecnologías operativas no ha dado lugar a una consolidación generalizada. Son más los MSP que utilizan varias herramientas o plataformas (**53 %**) que aquellos que emplean una única solución (**36 %**), lo que sugiere que muchos prestan estos servicios a través de un conjunto de plataformas especializadas, en lugar de un único sistema unificado.

Esto podría reflejar la creciente complejidad que supone gestionar a gran escala los requisitos de cumplimiento normativo, las evaluaciones de riesgos, la elaboración de informes, las actividades de gobernanza y las comunicaciones con los clientes. Asimismo, pone de relieve un reto común: muchas herramientas no pueden transferir datos a una plataforma central de elaboración de informes, lo que obliga a consolidar manualmente las actividades en un único informe dirigido al cliente. Los resultados sugieren una creciente demanda de enfoques más unificados para la gestión y la generación de informes sobre los programas de cumplimiento.

Enfoque de plataforma para la prestación de cumplimiento/actividad CISO



¿Qué enfoque utiliza actualmente su organización para ofrecer cumplimiento de ciberseguridad o actividades de tipo CISO en toda su base de clientes? (n=800)

53 %

de los MSP utiliza varias herramientas o plataformas para gestionar de forma centralizada el cumplimiento de las normas de ciberseguridad o las actividades propias de un CISO.

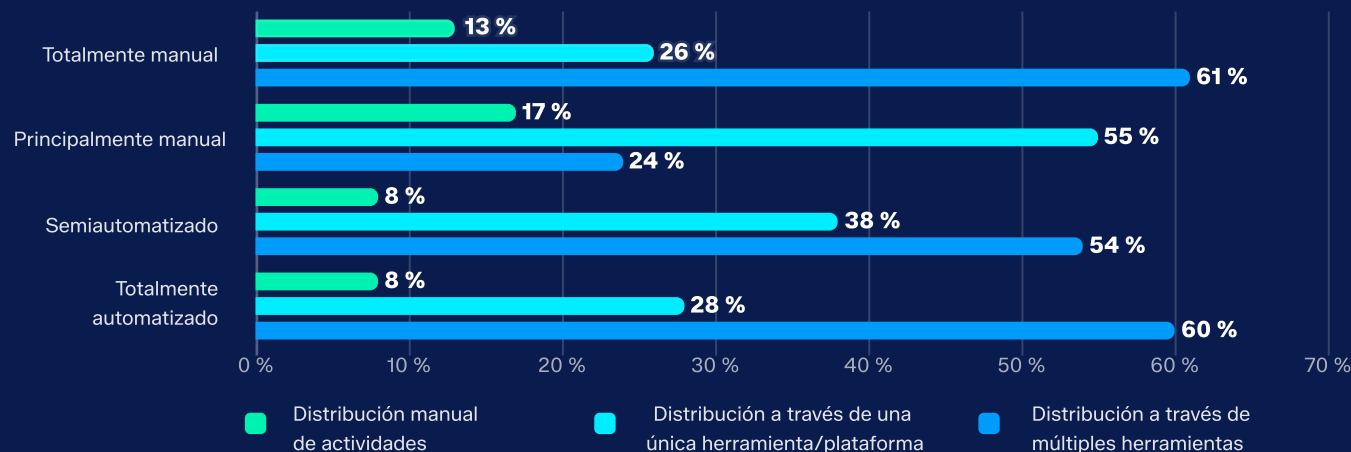
36 %

de los MSP recurre a una única herramienta o plataforma

2. La elaboración de informes de seguridad se está automatizando

La mayoría de los MSP han dejado atrás los procesos de generación de informes totalmente manuales, y el **86 %** utiliza métodos totalmente automatizados o semiautomatizados para elaborar informes consolidados sobre la postura de seguridad. Sin embargo, la automatización completa aún no se ha normalizado. Solo el **31 % de los MSP** puede generar informes rápidamente mediante un proceso totalmente automatizado, mientras que el **55 %** sigue dependiendo de cierto esfuerzo manual para combinar datos, añadir contexto y ultimar los informes.

Nivel de automatización de informes por enfoque de entrega



¿Qué enfoque utiliza actualmente su organización para garantizar el cumplimiento de la ciberseguridad o llevar a cabo actividades propias del CISO entre su base de clientes, en comparación con el grado de automatización del proceso de su organización para elaborar informes consolidados sobre la postura de seguridad de los clientes, en los que se muestren la situación de la ciberseguridad, los riesgos y las recomendaciones (n=800)?

Esto demuestra que la estrategia de plataforma por sí sola no equivale a la madurez en materia de automatización; los MSP, independientemente de su nivel de automatización, utilizan múltiples herramientas, lo que puede deberse a la fragmentación de los procesos o a la existencia de flujos de trabajo más automatizados en un conjunto de herramientas más amplio. En cualquier caso, la necesidad de automatización y el valor que esta puede aportar a los MSP es generalizada.

86%

de los MSP utiliza un proceso total o parcialmente automatizado para elaborar informes consolidados sobre la postura de seguridad.

31 %

pueden generar informes rápidamente gracias a la automatización.

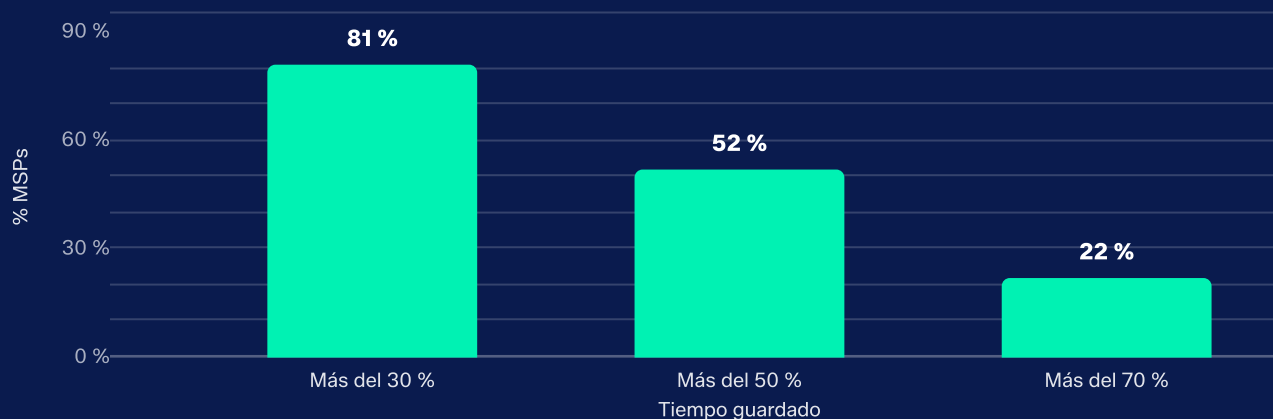
55 %

sigue necesitando cierto esfuerzo manual para consolidar las actividades.

3. Aún quedan por aprovechar importantes mejoras en la eficiencia

La consolidación de plataformas podría suponer un aumento sustancial de la eficiencia para los MSP. De media, los MSP estiman que una única plataforma totalmente unificada podría reducir en un **53 %** el tiempo que dedican sus equipos a gestionar y elaborar informes sobre la postura de seguridad y el cumplimiento normativo de los clientes. En general, el **81 % de los MSP** prevé un ahorro de tiempo superior al **30 %**, el 52 % superior al 50 % y el 22 % superior al 70 %.

Ahorro estimado de tiempo de una plataforma unificada



¿Qué proporción del tiempo de su equipo se podría ahorrar si toda la gestión y los informes de la postura de seguridad y el cumplimiento de los clientes se gestionaran a través de una única plataforma totalmente unificada? (n=800)

El ahorro percibido es especialmente elevado entre los MSP que ya ofrecen una gestión integral de programas de cumplimiento; el **84 % de los MSP** que ofrecen este servicio afirman que podrían ahorrar más del **30 %** de tiempo, frente al **64 %** de los MSP que ni ofrecen ni tienen previsto ofrecer dicho servicio. Esto sugiere que quienes gestionan actividades de cumplimiento más integrales o integradas pueden ser los que más se benefician de la consolidación de plataformas.

Estos resultados ponen de manifiesto la carga operativa a la que aún se enfrentan muchos MSP a la hora de gestionar los servicios de generación de informes, cumplimiento normativo y asesoramiento en múltiples plataformas y flujos de trabajo. A medida que crece la demanda de servicios de mayor valor, como la gestión del cumplimiento y el asesoramiento propio de un CISO, resulta cada vez más imprescindible encontrar formas de rediseñar la gestión de los programas de ciberseguridad a gran escala.

Los resultados sugieren que los MSP aprecian un valor significativo en el uso de un modelo unificado que integre el programa de cumplimiento normativo en su totalidad, lo que ayuda a sus equipos a dedicar menos tiempo a consolidar información y más tiempo a generar resultados estratégicos para sus clientes.

53 %

de tiempo ahorrarían los MSP si pudieran utilizar una única plataforma unificada para la gestión y la elaboración de informes sobre la postura de seguridad y el cumplimiento de los clientes.

81 %

de los MSP afirma que un enfoque unificado permitiría ahorrar más del 30 % del tiempo de su equipo.

22 %

afirma que ahorraría más del 70 % de ese tiempo.

Conclusión

El panorama de los MSP está experimentando un cambio significativo. Cada vez más, los clientes esperan que sus proveedores ofrezcan liderazgo estratégico en ciberseguridad, además de la gestión tecnológica. Los MSP responden ampliando su oferta a la gestión del cumplimiento, los servicios de asesoramiento cibernético y otras funciones propias de un CISO. Dado que **el 84 % de los MSP encuestados prevé que la demanda de servicios de CISO aumente durante el próximo año**, estos servicios de mayor valor representan una oportunidad creciente para el crecimiento y la diferenciación empresarial.

Al mismo tiempo, la gestión a gran escala de la postura de seguridad, el cumplimiento normativo y la elaboración de informes para los clientes sigue planteando dificultades operativas. Aunque la mayoría de los MSP han adoptado plataformas y procesos automatizados, muchos siguen dependiendo de múltiples herramientas y del trabajo manual para prestar estos servicios. En muchos sentidos, esto refleja la complejidad a la que se enfrentan los CISO y los equipos de seguridad, lo que hace que los MSP se vean obligados a lidiar con los mismos retos que intentan ayudar a sus clientes a superar.

Los MSP que sean capaces de ofrecer, de forma fiable y eficiente, un liderazgo escalable en materia de ciberseguridad, una gestión continua de los programas y resultados de seguridad cuantificables estarán mejor posicionados para consolidar las relaciones con los clientes, aumentar las ventas y sacar partido de la próxima ola de oportunidades.

Sophos CISO Advantage

[Sophos CISO Advantage](#) ofrece a los MSP la oportunidad de liderar un tipo diferente de diálogo sobre ciberseguridad: uno centrado en los resultados, el riesgo empresarial, el cumplimiento normativo progresivo y la mejora cuantificable.

Prestado a través de [Sophos Fusion](#), el Sophos AI-Native Cybersecurity Defense System, transforma la función de CISO que la mayoría de los MSP ya desempeñan en un servicio estructurado, escalable y facturable de gestión de programas de ciberseguridad.

Los flujos de trabajo de evaluación, generación de informes y elaboración de hojas de ruta, acelerados por la IA agéntica, proporcionan a estos Partners esenciales una forma sistemática de ofrecer información lista para presentar al consejo de administración, pruebas que se ajustan al marco normativo y planes de acción priorizados para toda su base de clientes.

Además, abre una vía clara hacia nuevos ingresos recurrentes, oportunidades de crecimiento y relaciones más sólidas con los clientes a partir de los proyectos existentes. Cada evaluación pone de manifiesto las brechas de seguridad y cada una de ellas traza una hoja de ruta para la mejora, lo que permite a los MSP ofrecer esas soluciones de seguimiento.

Sophos CISO Advantage responde a una demanda que la comunidad de seguridad lleva años dejando patente. Al adoptar esta solución desde el principio, los MSP pueden asumir plenamente el papel de líderes que sus clientes esperan de ellos.

Para obtener más información sobre Sophos CISO Advantage, los MSP pueden visitar el [Portal para Partners](#).

¿Quiere convertirse en Partner de Sophos? **Regístrese aquí.**

Ventas en España

Teléfono: (+34) 913 756 756

Correo electrónico: comercialES@sophos.com

Ventas en América Latina

Correo electrónico: Latamsales@sophos.com