INFORME

La realidad de la confianza en materia de ciberseguridad en 2026

Conclusiones de una encuesta independiente realizada a 5000 responsables de TI y seguridad

SOPHOS

Introducción

Cuando las organizaciones seleccionan un proveedor de ciberseguridad, le están confiando su resiliencia operativa crítica, es decir, su personal, sus datos y su facturación.

Sin embargo, a pesar de esta dependencia, según un nuevo estudio de Sophos, la mayoría de organizaciones no confían en los proveedores encargados de garantizar su seguridad.

Para comprender mejor el nivel real de confianza en la ciberseguridad que tienen las organizaciones, Sophos encargó una encuesta global independiente a 5000 responsables de la toma de decisiones en materia de TI y seguridad de 17 países. Llevada a cabo por Vanson Bourne, una consultora especializada, esta encuesta ofrece una visión concreta y estadísticamente significativa de cómo se genera y se pierde la confianza entre los compradores y los proveedores de soluciones de ciberseguridad.

5000

responsables de TI y seguridad de 17 países participaron en una encuesta global desvinculada de cualquier proveedor

Conclusiones clave

Falta de confianza: solo el 5 % de los responsables de TI afirma que tanto ellos como su organización confían plenamente en sus proveedores de ciberseguridad.

Las pruebas verificadas son un factor clave para generar confianza: tanto los equipos de TI como la dirección coinciden en que los elementos demostrables que permiten medir la madurez en materia de ciberseguridad son el principal indicador de fiabilidad.

Evaluar la fiabilidad de los proveedores sigue siendo un reto: al 79 % de las organizaciones les cuesta evaluar la fiabilidad de los nuevos proveedores de ciberseguridad, mientras que al 62 % les cuesta hacerlo con sus proveedores actuales. Los encuestados mencionaron varios factores que mermaban la confianza en los proveedores, entre los que destacaba el hecho de que la información que facilitaban no era lo suficientemente objetiva o detallada.

Esta falta de confianza tiene consecuencias: el 51 % de los encuestados afirma que la falta de confianza genera el temor de que la organización tenga más probabilidades de sufrir un ciberincidente grave.

Los técnicos y los directivos no suelen estar de acuerdo: el 78 % de los encuestados afirma que su equipo de TI y la dirección o el consejo de administración tienen opiniones diferentes sobre la fiabilidad de los proveedores de ciberseguridad de su organización. Casi un tercio de las empresas que respondieron a la encuesta de Sophos afirma que esta diferencia de opiniones se da «a menudo».

La fiabilidad es difícil de evaluar

Solo el 5 % de los responsables de TI afirman que tanto ellos como su organización confían plenamente en sus proveedores de ciberseguridad.

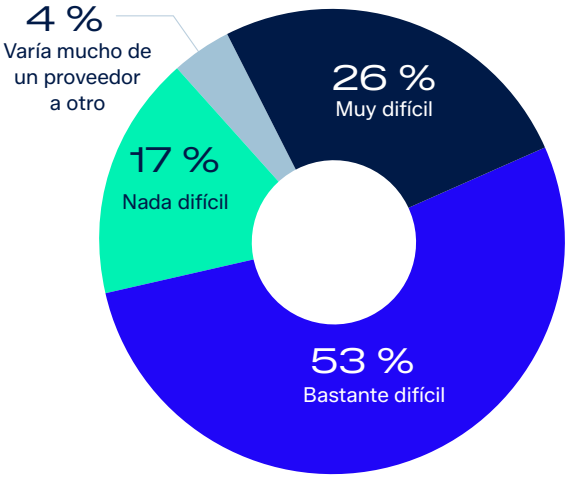
Cuando recurre a su proveedor de ciberseguridad para garantizar la seguridad de su red y el buen funcionamiento de sus operaciones, la confianza es fundamental. Los proveedores de ciberseguridad son quienes protegen su empresa 24/7, incluso por la noche y los fines de semana, así como cuando los miembros del equipo de TI están de vacaciones. En el caso de las pequeñas empresas, que a menudo ni siquiera cuentan con personal de TI dedicado, sus productos o servicios de ciberseguridad pueden desempeñar la función de un empleado más.

Antes de que las organizaciones puedan decidir en quién confiar, se enfrentan a un reto aún más fundamental: evaluar, ante todo, la fiabilidad de un proveedor.

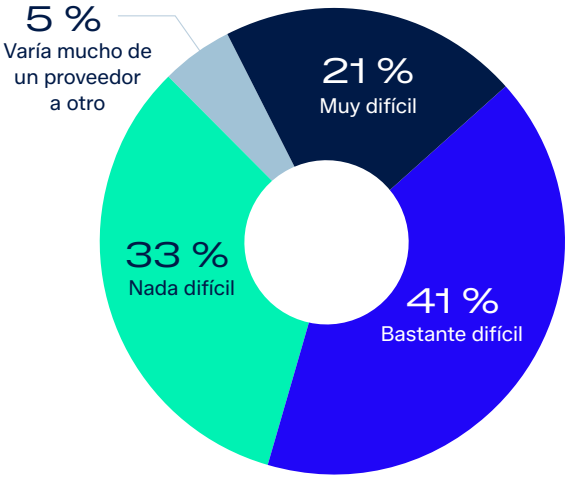
Según la encuesta, el 79 % de los encuestados afirma que resulta difícil evaluar la fiabilidad de los nuevos proveedores o Partners de ciberseguridad. Esto pone de manifiesto la dificultad generalizada a la hora de comparar productos, verificar las afirmaciones y comprender si un proveedor potencial puede proteger realmente a la empresa. Al 62 % también le cuesta evaluar la fiabilidad de los proveedores con los que ya trabaja, lo que indica que la falta de confianza no desaparece una vez firmado el contrato (Figura 1).

79 %

Porcentaje de empresas encuestadas que afirman que les resulta difícil evaluar la fiabilidad de nuevos proveedores o Partners de ciberseguridad



Evaluar la fiabilidad de los **nuevos** proveedores y Partners de ciberseguridad



Evaluar la fiabilidad de los proveedores y Partners de ciberseguridad **existentes**

Figura 1: En general, ¿hasta qué punto resulta complicado, de ser el caso, para su organización evaluar la fiabilidad de los proveedores y Partners de ciberseguridad? n=5000

Dificultades a la hora de evaluar la confianza

Los encuestados mencionaron varias razones que explican la falta de confianza, la mayoría de ellas relacionadas con la transparencia. A muchos les cuesta interpretar los argumentos que esgrimen los proveedores, evaluar los detalles técnicos o encontrar la información que necesitan para tomar decisiones con total confianza.

Casi la mitad (47 %) afirma que la información que proporcionan los proveedores no es lo suficientemente objetiva o detallada, y al 45 % le resulta difícil interpretar o comprender dicha información. Por otra parte, el 43 % admite que carece de las habilidades o los conocimientos necesarios para evaluar a los proveedores de manera eficaz, el 41 % se encuentra con información contradictoria y el 38 % tiene dificultades incluso para encontrar la información que necesita (Figura 2).

Figura 2: ¿Por qué a su organización le cuesta evaluar la fiabilidad de los proveedores de ciberseguridad? n=4483

La principal diferencia entre las pequeñas empresas (menos de 250 empleados) y las grandes empresas (más de 1000 empleados) radica en que las pymes carecen con mucha más frecuencia de las habilidades o los conocimientos necesarios para evaluar de manera eficaz la fiabilidad de los proveedores; las pymes mencionaron este aspecto un 8 % más a menudo que los encuestados de las grandes empresas (Figura 3).

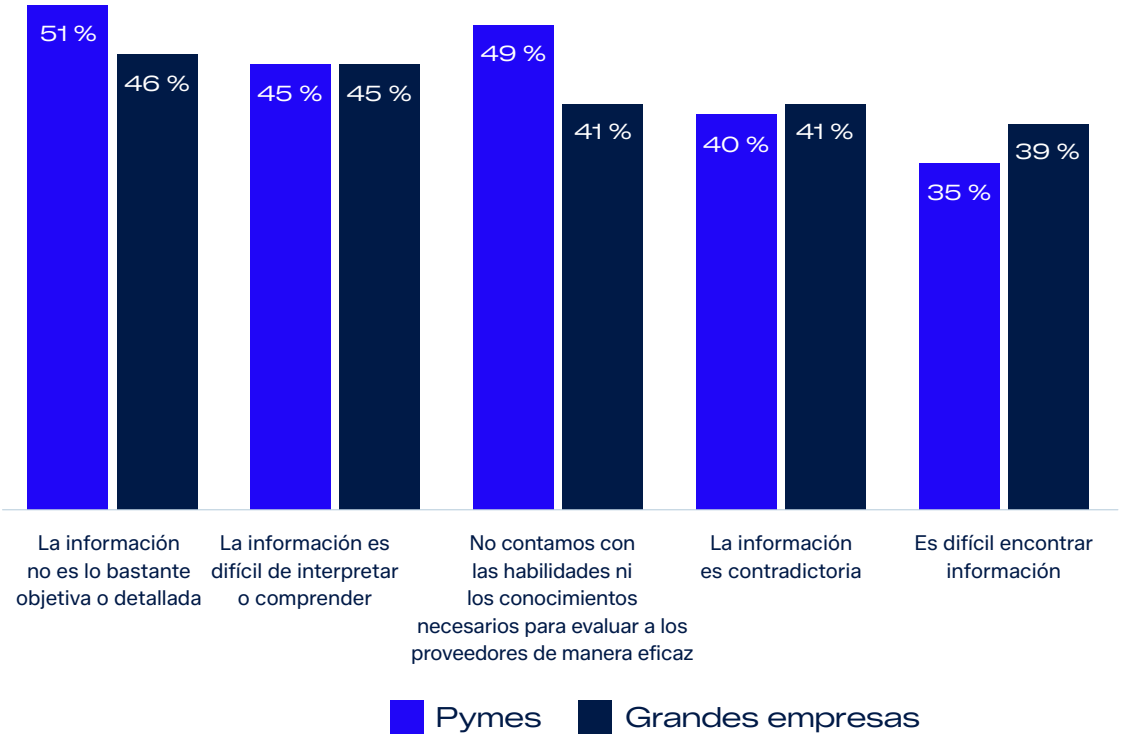


Figura 3: ¿Por qué a su organización le cuesta evaluar la fiabilidad de los proveedores de ciberseguridad? n=504 (pymes), 2260 (grandes empresas).

La falta de confianza tiene consecuencias

Este estudio cuantifica el impacto que tiene la falta de confianza entre un proveedor de seguridad y sus clientes, lo cual constituye un problema significativo en múltiples aspectos. Cuando se les preguntó por las repercusiones de la falta de confianza en sus proveedores de ciberseguridad, los encuestados mencionaron una combinación de consecuencias emocionales y operativas:

- El **51 %** manifiesta una mayor preocupación por la posibilidad de que su organización sufra un ciberincidente grave.
- El **45 %** afirma que esto aumenta la probabilidad de cambiar de proveedor, lo que para la mayoría de las empresas supone un proceso costoso y laborioso.
- El **42 %** prevé un endurecimiento de los requisitos de supervisión.
- El **41 %** afirma sentirse menos seguro en lo que respecta a su postura de ciberseguridad.
- El **38 %** expresa su preocupación por la posibilidad de que ellos o su empresa hayan elegido al proveedor equivocado.

Estas repercusiones se suman a las dificultades operativas a las que ya se enfrentan los equipos de TI y ciberseguridad.

Opiniones divergentes entre el departamento de TI y la dirección

Otro reto fundamental es la falta de consenso entre las personas que utilizan las herramientas de ciberseguridad a diario y las que aprueban los contratos. El 78 % de los encuestados afirma que su equipo de TI y la dirección o el consejo de administración tienen opiniones distintas sobre la fiabilidad de sus proveedores de ciberseguridad, y casi un tercio señala que esos desacuerdos se producen «a menudo» (Figura 4).

Los encuestados indicaron que el equipo directivo sigue estando muy involucrado en las decisiones de compra. Solo el 1 % de las organizaciones señaló que el consejo de administración o la dirección no interviene en las decisiones de compra relacionadas con la ciberseguridad.

1 %

Porcentaje de organizaciones encuestadas que afirman que la alta dirección no desempeña ningún papel en las decisiones de compra de ciberseguridad.

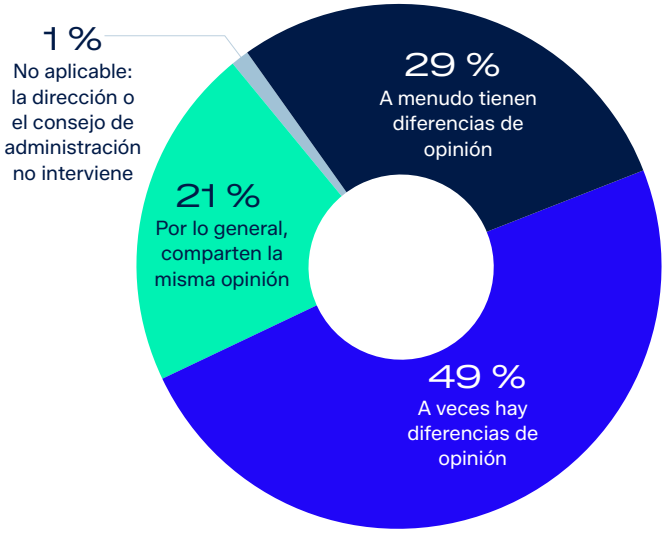


Figura 4: ¿Existen diferencias de opinión entre el equipo de TI y la dirección/el consejo de administración en cuanto a la fiabilidad de los proveedores de ciberseguridad de su organización? n=5000.

Cómo generar confianza en la ciberseguridad

Los encuestados señalaron que las prácticas de seguridad transparentes y basadas en pruebas son fundamentales para generar confianza. Las organizaciones buscan proveedores que inspiren confianza mediante la transparencia, la claridad y unas prácticas de seguridad respaldadas por pruebas.

Tanto entre la dirección como entre los equipos de TI, los «elementos demostrables que permiten medir la madurez en materia de ciberseguridad» se situaron como el principal factor que genera confianza en los proveedores de ciberseguridad. Entre estas pruebas se incluyen programas de recompensas por la detección de errores, un Trust Center público, avisos que contienen detalles sobre las vulnerabilidades de sus productos (y las correcciones que se han aplicado), evaluaciones de terceros y certificaciones.

La «transparencia y la comunicación rápida durante incidentes y divulgaciones» fue considerada el segundo factor más importante por los miembros de la dirección y el tercero por los equipos de TI.

Factores que determinan la confianza en los proveedores de ciberseguridad

Factores	Dirección/ Consejo	Equipo de TI/ ciberseguridad	Factores determinantes
Factores principales	N.º 1	N.º 1	Elementos demostrables que indican la madurez en materia de ciberseguridad, p. ej.: programas de recompensa por la detección de errores, Trust Center, avisos de seguridad, evaluaciones de terceros y certificaciones
	N.º 2	N.º 3	Transparencia y comunicación rápida durante incidentes y divulgaciones
	N.º 3	N.º 4	Comentarios de expertos tras ciberincidentes importantes, p. ej., declaraciones en prensa o en televisión
	N.º 4	N.º 2	Prestación constante de servicios y productos de ciberseguridad de alta calidad
	N.º 5	N.º 5	Resultados obtenidos en informes elaborados por analistas, p. ej., el Magic Quadrant de Gartner
Factores secundarios	N.º 6	N.º 9	Transparencia en los procedimientos de seguridad interna
	N.º 7	N.º 7	Resultados obtenidos en pruebas independientes, p. ej., MITRE, SE Labs
	N.º 8	N.º 6	Servicio de soporte ágil y fiable
	N.º 9	N.º 8	Recomendación de su Partner en ciberseguridad
Factores terciarios	N.º 10	N.º 13	Calidad de las publicaciones sobre investigación en materia de amenazas
	N.º 11	N.º 12	Cobertura en la prensa financiera y empresarial
	N.º 12	N.º 11	Experiencia de otros (compañeros/clientes)
	N.º 13	N.º 10	Experiencia personal

¿Qué factores influyen o influirían más en el nivel de confianza de la dirección o del consejo de administración en un proveedor de ciberseguridad? Respuestas clasificadas como n.º 1
¿Qué factores influyen o influirían más en el nivel de confianza del equipo de ciberseguridad o de TI en un proveedor de ciberseguridad? Respuestas clasificadas como n.º 1

El compromiso de Sophos por ganarse la confianza de clientes y Partners

En Sophos, sabemos que la confianza no se exige, se construye, y trabajamos para ganárnosla cada día a través de la transparencia, la integridad y el firme compromiso de proteger la seguridad y la privacidad.

En el centro de nuestra labor está el Sophos Trust Center, donde publicamos avisos de seguridad, documentamos las vulnerabilidades de los productos y las soluciones correspondientes, exponemos nuestra postura de cumplimiento normativo y compartimos cómo protegemos los datos de nuestros clientes.

Esta transparencia también se refleja en la investigación Pacific Rim llevada a cabo por Sophos X-Ops, que documentó públicamente una campaña de cinco años llevada a cabo por ciberdelincuentes con base en China y compartió información detallada sobre las tácticas, técnicas y procedimientos (TTP), los indicadores de peligro (IOC) y recomendaciones de defensa para ayudar a las organizaciones a reforzar la resiliencia en todo el sector.

Al sacar a la luz las sofisticadas actividades de los Estados nación, colaborar con los gobiernos y otros proveedores, y ser transparentes sobre nuestros puntos fuertes y débiles, Sophos reitera que la confianza hay que ganársela día a día, a través de la honestidad, la responsabilidad y el compromiso de proteger todo el ecosistema digital.

Más información

Para obtener más información sobre nuestro compromiso de fomentar la confianza, así como sobre los recursos que ofrecemos para ayudarle a evaluar el nivel de confianza en Sophos, visite el Trust Center o póngase en contacto con su Partner o representante de Sophos.

SOPHOS

Para obtener más información , visite el Trust Center o póngase en contacto con su Partner o representante de Sophos.

Ventas en España
Teléfono: (+34) 913 756 756
Correo electrónico: comercialES@sophos.com

Ventas en América Latina
Correo electrónico: Latamsales@sophos.com