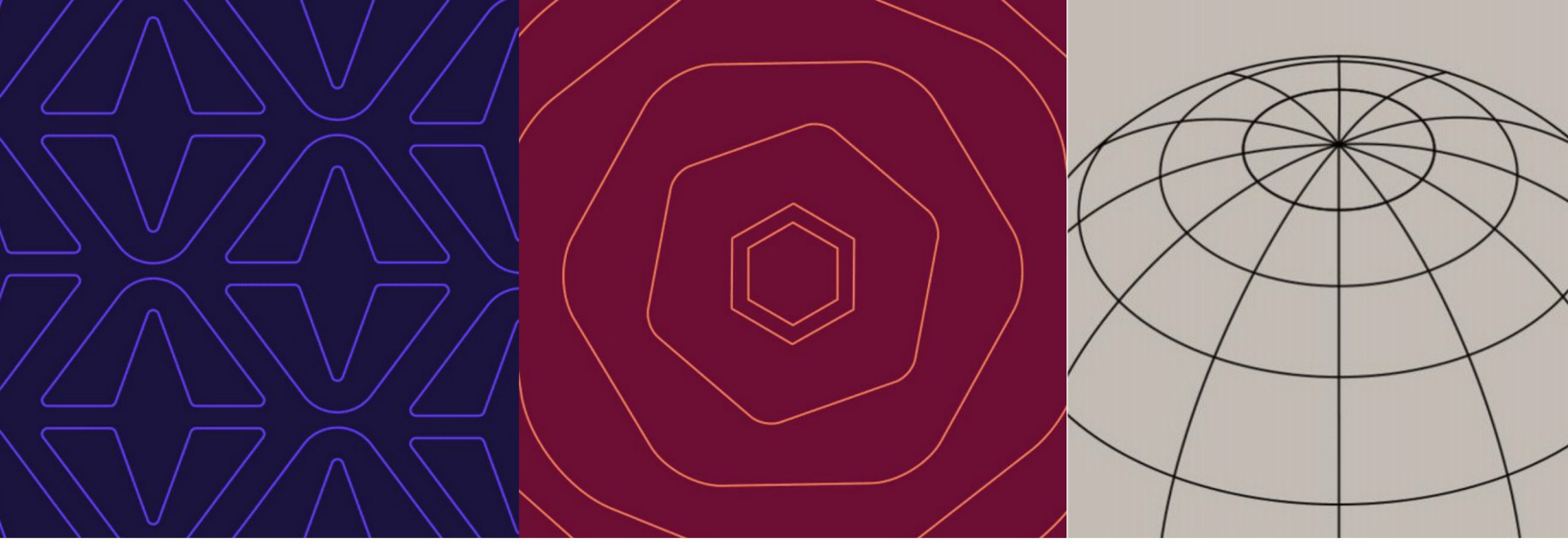


2026 Informe de tendencias de ciberseguridad en la cadena de suministro

La paradoja del riesgo de terceros: la confianza aumenta a medida que crece la exposición

SecurityScorecard

Resumen ejecutivo

Los riesgos de terceros siguen creciendo. Las prácticas de mitigación no evolucionan con la suficiente rapidez.

Por segundo año consecutivo, SecurityScorecard encuestó a líderes que supervisan o gestionan los riesgos de ciberseguridad de terceros dentro de su organización. Los resultados revelan una paradoja en la gestión del riesgo de terceros, definida por una brecha cada vez mayor entre la alta confianza de los líderes y las deficiencias demostrables en sus cadenas de suministro.

Entre los principales hallazgos:

La confianza es alta, pero la preocupación está muy extendida. A pesar de que el 86% de los líderes expresa preocupación por los riesgos de la cadena de suministro, el 90% sigue confiando en que su empresa podría continuar sus operaciones sin problemas si un proveedor sufriera un incidente de ciberseguridad.

Existen enormes brechas en la supervisión de proveedores. La mayoría (78%) de las organizaciones admite que sus programas internos de ciberseguridad cubren menos del 50% de su ecosistema total de proveedores, incluidos terceros, cuartos y quintos, lo que deja puntos ciegos importantes en su creciente panorama de riesgo.

Las prácticas de mitigación son lentas y están desactualizadas. Más de la mitad (55%) de los encuestados aún depende de métodos manuales, como llamadas telefónicas, reuniones o correos electrónicos, para colaborar con los proveedores durante una brecha. Como resultado, el 60% de las organizaciones tarda 8 días o más en remediar un problema de alta gravedad.

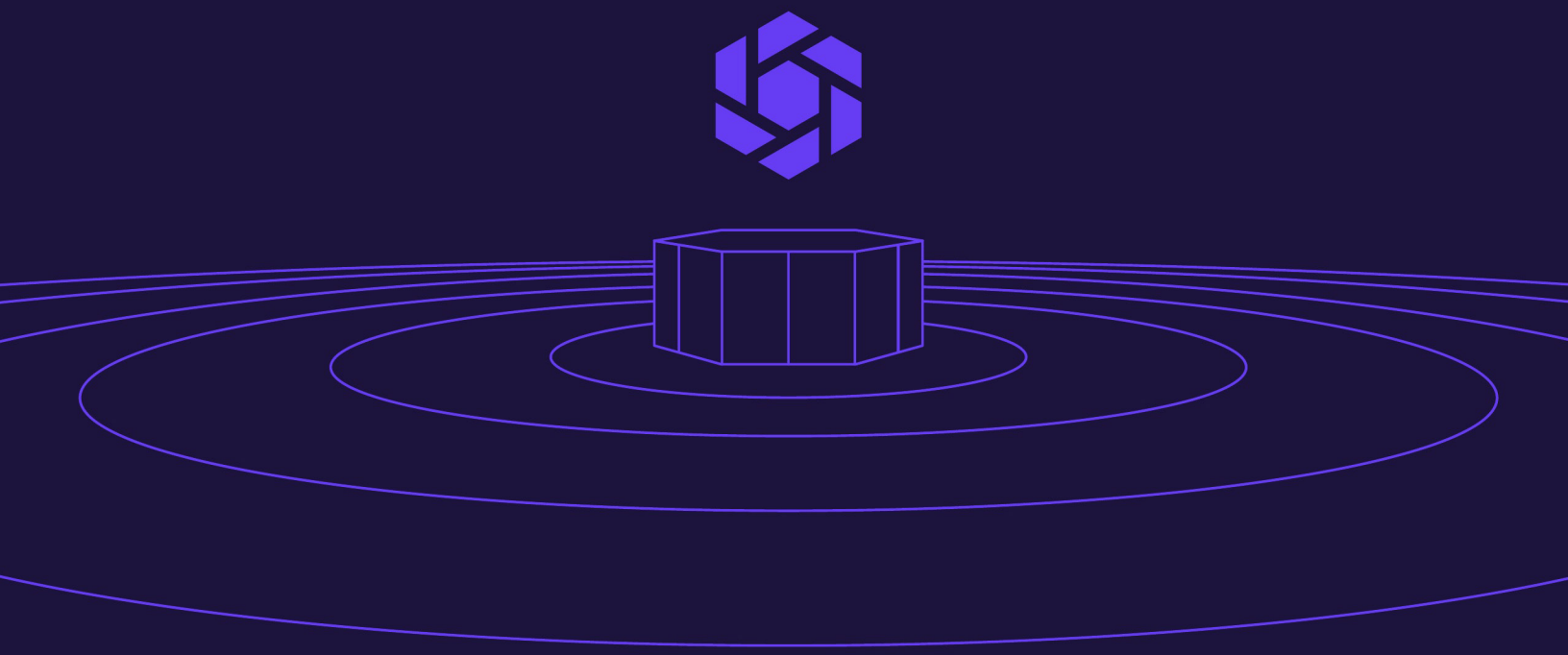
El aumento de las amenazas de IA exige monitoreo continuo. Las organizaciones siguen prefiriendo las evaluaciones estáticas: el 67% utiliza auditorías de seguridad y el 46% depende de un monitoreo periódico (mensual o trimestral), aunque los líderes reconocen el creciente riesgo de las amenazas impulsadas por IA.

La necesidad de estrategias automatizadas de gestión de riesgo de terceros (TPRM) va en aumento. La dependencia de tácticas obsoletas, sumada a que casi la mitad (49%) de los encuestados tiene dificultades para mantenerse al día con los cambios regulatorios, subraya la urgente necesidad de contar con enfoques de TPRM más maduros.

El panorama de proveedores en la cadena de suministro se está multiplicando rápidamente, y la IA está acelerando el ritmo de las amenazas. La pregunta es: ¿las estrategias de gestión de riesgo de terceros (TPRM) de las organizaciones están a la altura de las amenazas de 2026, o siguen dependiendo de prácticas propias de la década de 2010?

Continúe leyendo para conocer el alcance de los ecosistemas de proveedores de sus pares, los desafíos que enfrentan para protegerlos y los planes que están implementando para reducir sus riesgos de terceros, cuartos y quintos.

Índice

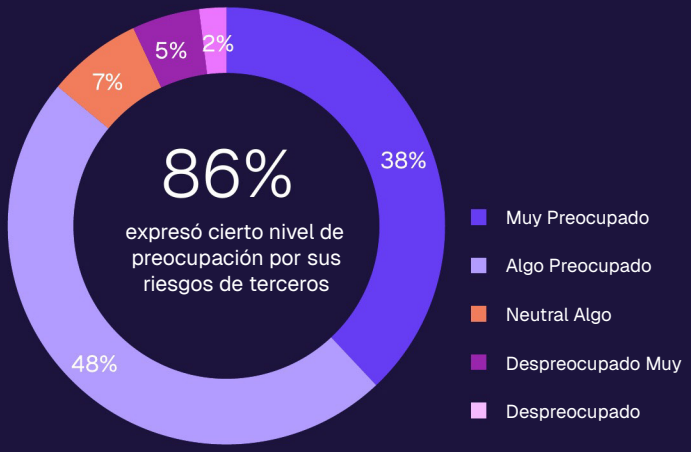


A medida que crecen los ecosistemas de terceros, también lo hacen los riesgos

01

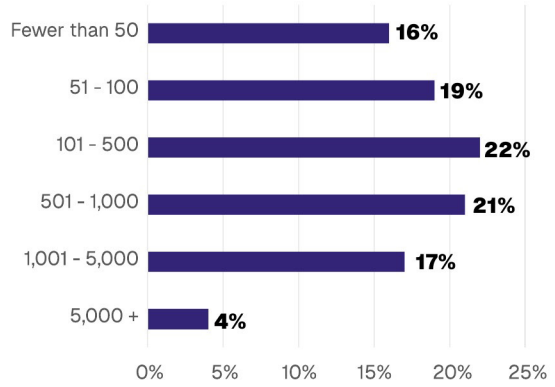
El número de proveedores terceros, cuartos y quintos sigue en expansión, lo que aumenta la preocupación de los líderes por la ciberseguridad de la cadena de suministro. Este año, **el 86% de los encuestados expresó al menos cierto nivel de preocupación por sus riesgos de terceros,** un resultado similar al del año pasado. Sin embargo, las prácticas de TPRM que sigue la mayoría de las organizaciones no han cambiado mucho en los últimos 12 meses.

¿Qué tan preocupado está por la ciberseguridad de la cadena de suministro?

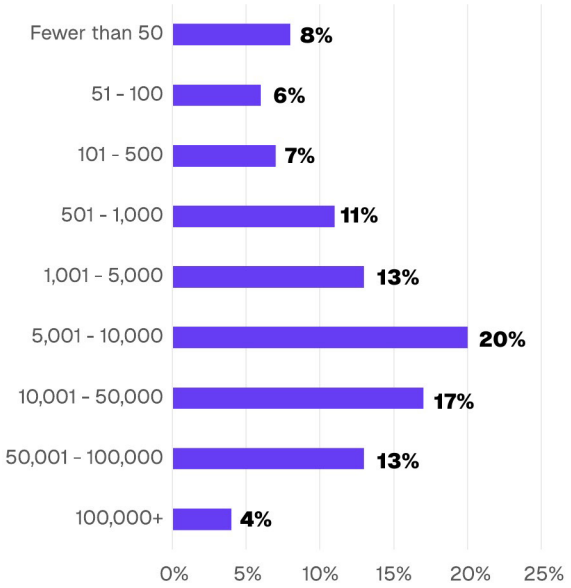


La mayoría de las organizaciones (78%) gestiona 1,000 proveedores externos o menos. Sin embargo, al extrapolar esa cifra a los proveedores cuartos y quintos, la complejidad aumenta. Aproximadamente dos tercios (67%) de los encuestados afirma tener más de 1,001 proveedores en total dentro de su ecosistema, y el 34% cuenta con entre 10,001 y más de 100,000 proveedores.

¿Aproximadamente cuántos proveedores externos tiene su organización?



¿Qué tan grande es el ecosistema total de proveedores de su organización (hasta el quinto nivel)?



"Lo que más escuchamos de nuestros clientes es que, cuando llegan al cuarto y quinto nivel de proveedores, se sienten aún más expuestos", afirma Jeff Barker, vicepresidente de Marketing de Producto en SecurityScorecard. "Basta un solo incidente importante para que la situación se convierta rápidamente en una crisis de gran magnitud".

El desafío, explica Barker, es supervisar y coordinar decenas de miles de proveedores con un equipo interno relativamente pequeño. Los encuestados coinciden. Al preguntárseles cuál es el desafío más importante de su programa actual de ciberseguridad de la cadena de suministro, un encuestado respondió:

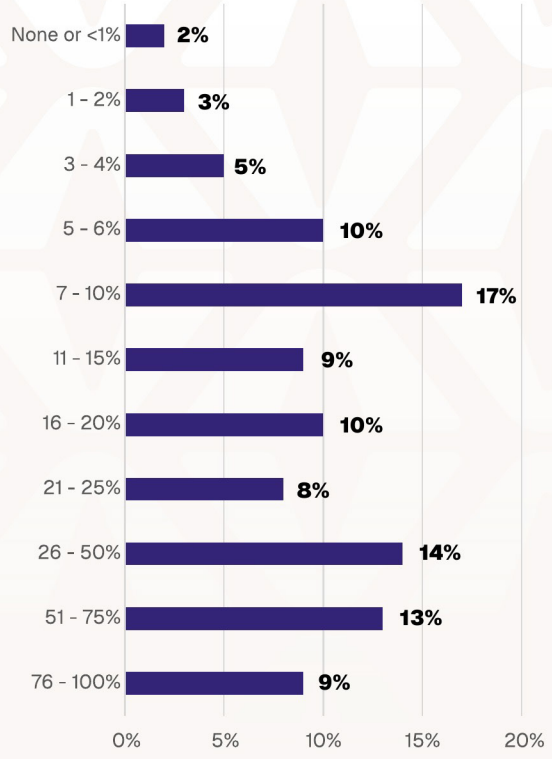
> *"El mayor punto ciego es **la falta de coordinación y comunicación entre nosotros y nuestros distintos proveedores...** A veces me siento abrumado por la gran cantidad de proveedores que tenemos."*

A medida que ha aumentado el número de proveedores de enésimo nivel, también lo han hecho los riesgos. Las brechas de terceros se duplicaron en 2025, según el último informe de investigaciones de brechas de datos de Verizon. Sin embargo, la supervisión interna de los riesgos de la cadena de suministro se mantiene sin cambios respecto al año pasado. **Solo el 9% de los encuestados afirma que más de tres cuartas partes de su ecosistema total de proveedores está supervisado por un programa interno de ciberseguridad de la cadena de suministro,** una cifra similar a la de 2025. Un dato aún más preocupante:

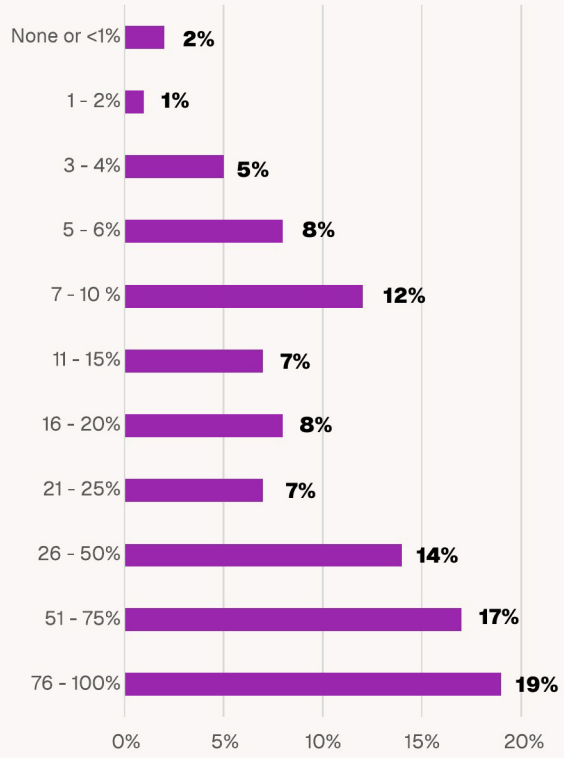
64%

de los encuestados de este año afirma que menos de la mitad de sus proveedores cumple con las normas internas de su organización

¿Qué porcentaje de su ecosistema total de proveedores (hasta el quinto nivel) está supervisado por un programa interno de ciberseguridad de la cadena de suministro?



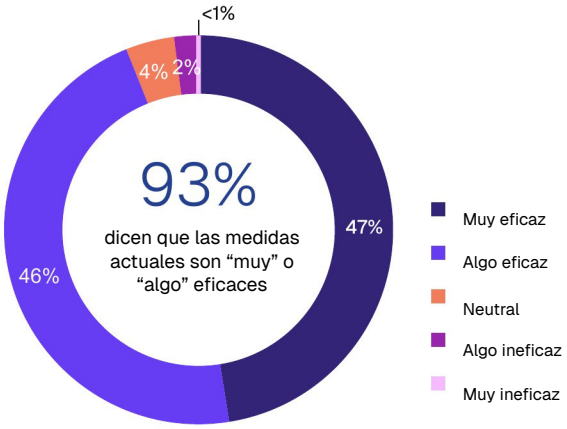
¿Qué porcentaje de su ecosistema de proveedores cumple con sus requisitos de ciberseguridad?



Los líderes expresan confianza, pero surgen nuevas amenazas

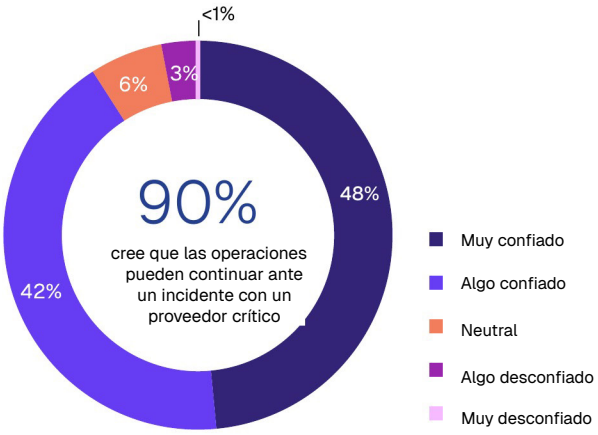
A pesar de que el número de brechas de terceros se ha duplicado a nivel mundial, los equipos de riesgo y seguridad creen tener bajo control los riesgos de su cadena de suministro. **La mayoría (93%) de los encuestados afirma que sus medidas actuales son "muy" o "algo" eficaces.**

¿Qué tan eficaces son las medidas actuales de ciberseguridad de la cadena de suministro de su organización para mitigar riesgos?



Otro 90% cree que puede continuar sus operaciones sin problemas en caso de un incidente con un proveedor crítico. Ese nivel de confianza es 5 puntos porcentuales más alto que lo que los líderes indicaron en la encuesta del año pasado.

¿Qué tan confiado está en que su empresa podría continuar sus operaciones sin interrupciones si ocurriera un incidente de ciberseguridad en un proveedor crítico?



Sin embargo, al preguntárseles qué dependencias influyen más en su confianza para mantener las operaciones durante un incidente relacionado con un proveedor, las respuestas abiertas revelaron puntos de vista contradictorios:

"Muy confiado:

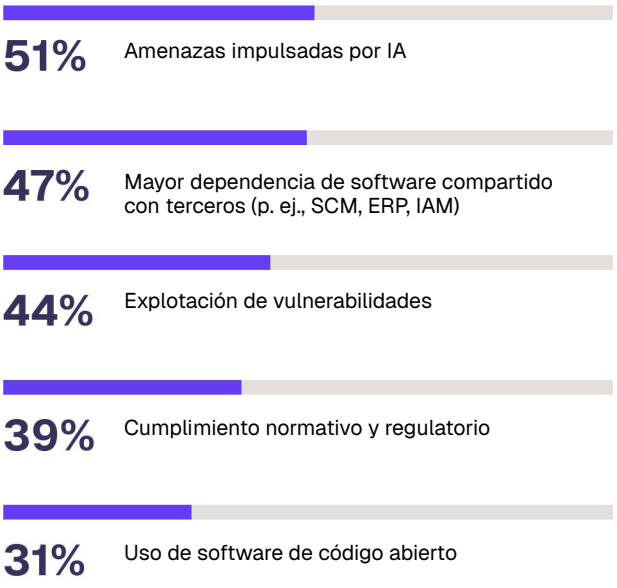
*"Lo que influye en esto es que contamos con uno de los mejores sistemas de gestión de crisis que existen.... Cualquier tipo de problema o crisis suele **resolverse en menos de una hora.**"*

"Algo desconfiado:

"Dependemos en gran medida de unos pocos proveedores críticos para la prestación del servicio.... Si [uno de esos proveedores] sufriera una interrupción global o multirregional, quedaríamos completamente paralizados."

¿Qué podría debilitar aún más la confianza de los líderes? El aumento de las amenazas impulsadas por IA.

¿Qué tipos de riesgos de la cadena de suministro le preocupan más? (Seleccione hasta tres)



03

Mantenerse al día con las regulaciones es un desafío constante

La entrada en vigor en 2025 de la Ley de Resiliencia Operativa Digital (DORA) en la UE es el último ejemplo del mosaico de regulaciones en constante cambio que deben cumplir los equipos de ciberseguridad de la cadena de suministro. Pero, si bien mantener el cumplimiento es necesario, no siempre significa que la seguridad de la cadena de suministro de una empresa sea eficaz.

La regulación es el principal impulsor de los programas de TPRM, según el 47% de los encuestados. Sin embargo, **el 49% afirma que el trabajo administrativo necesario para mantener el cumplimiento entorpece a sus equipos.**

¿Qué factores impulsan con más fuerza su programa de ciberseguridad de la cadena de suministro o de TPRM? (Seleccione hasta tres)

- **46%** Requisitos regulatorios
- **42%** Requisitos de seguro cibernético
- **41%** Objetivos de reducción de riesgo
- **35%** Mejores prácticas del sector
- **28%** Requisitos de los clientes
- **27%** Incidentes de seguridad recientes

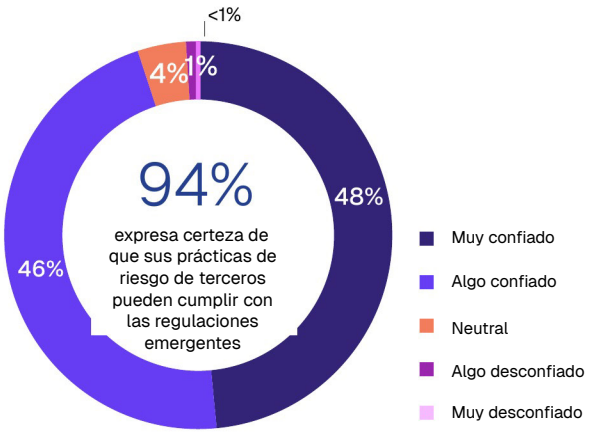
¿Qué áreas del cumplimiento de terceros o de la cadena de suministro presentan los mayores desafíos? (Seleccione hasta tres)

- **49%** Mantenerse al día con los cambios regulatorios
- **40%** Alinearse con múltiples marcos regulatorios
- **38%** Remediación desigual entre proveedores
- **34%** Requisitos de documentación de evidencia
- **34%** Requisitos de notificación de incidentes
- **32%** Demostrar monitoreo continuo

La mayoría (94%) de los encuestados expresa certeza de que sus prácticas de riesgo de terceros pueden cumplir con las regulaciones emergentes.

Sin embargo, a pesar de esa confianza declarada, **el 38% de los líderes considera que las presiones regulatorias son una preocupación mayor que la escasez de talento o la falta de visibilidad de la cadena de suministro.** Estos hallazgos muestran que el cumplimiento normativo sigue siendo un punto crítico que muchas organizaciones aún no han resuelto.

¿Qué tan confiado está en que las prácticas de riesgo de terceros de su organización cumplen con las regulaciones emergentes de ciberseguridad en la cadena de suministro?



¿Qué eventos, desafíos o brechas específicas influyen más en su nivel de preocupación? (Seleccione uno)

38% Aumento de la presión regulatoria

22% Brechas recientes de alto perfil

16% Falta de recursos/herramientas internas

13% Falta de visibilidad de mis propios proveedores

11% Fusión, adquisición u otro cambio de propiedad

Más allá del cumplimiento normativo, los desafíos en la mitigación de riesgos revelan tendencias interanuales notables. En 2025, la sobrecarga de datos y la incapacidad de priorizar problemas y amenazas se ubicaron como las principales barreras. Este año, la sobrecarga de datos cayó al puesto No. 3. **El nuevo No. 1: las dificultades para evaluar la postura de seguridad de los proveedores.** Este comentario de un encuestado explica el motivo de esta preocupación:

*"Los proveedores no nos rinden cuentas, y **no tenemos control sobre la falta de respuesta o las respuestas lentas de su parte.** No tenemos visibilidad de las investigaciones ni de las remediaciones que realiza el proveedor."*

¿Cuáles son sus mayores desafíos al gestionar el riesgo de ciberseguridad de la cadena de suministro? (Seleccione hasta tres)

35% Dificultad para evaluar la postura de seguridad de los proveedores

32% Recursos limitados para dedicar a la ciberseguridad de la cadena de suministro

30% Sobrecarga de datos; incapacidad de priorizar problemas y amenazas

28% Resistencia o falta de compromiso para resolver los problemas

27% Falta de visibilidad de la cadena de suministro

23% Demasiados procesos manuales

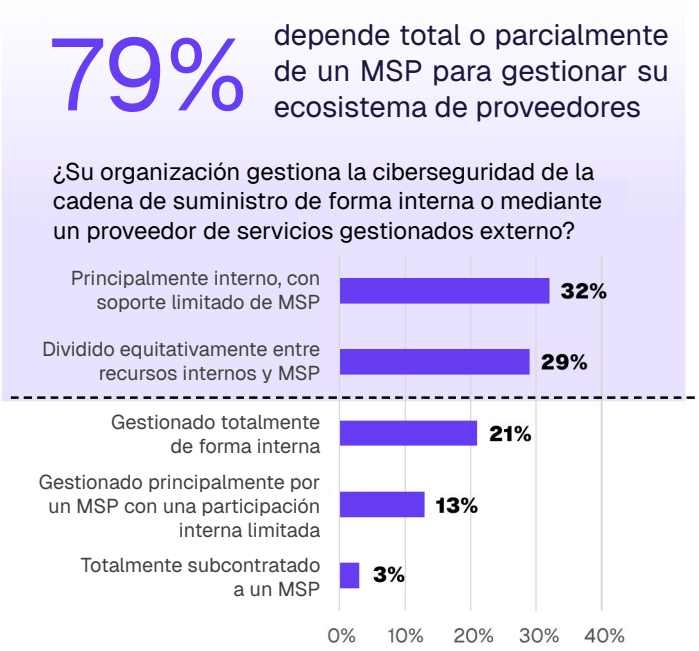
Las prácticas de seguridad de la cadena de suministro del pasado ya no son suficientes

04

En un entorno donde los actores maliciosos pueden usar herramientas de IA para lanzar ataques contra proveedores externos a la velocidad de una máquina, depender de prácticas obsoletas como las evaluaciones puntuales genera vulnerabilidades graves. Sin embargo, aunque los líderes afirman confiar en la seguridad de su cadena de suministro, sus prácticas reales no están a la altura de esa confianza, lo que subraya aún más la paradoja de la gestión del riesgo de terceros.

Una posible razón de esta confianza es la fe en sus proveedores de servicios gestionados (MSP), ya que **el 79% depende total o parcialmente de un MSP para gestionar su ecosistema de proveedores.**

79% depende total o parcialmente de un MSP para gestionar su ecosistema de proveedores



Las auditorías anuales y las pruebas de penetración son los métodos más utilizados por los encuestados para garantizar el cumplimiento de los proveedores. **Otro 46% de los líderes depende de evaluaciones periódicas, realizadas mensual o trimestralmente.** La buena noticia: las plataformas compartidas de remediación o seguridad, que pueden ayudar a gestionar el riesgo de terceros en tiempo real, ganan popularidad, con un 37% de los encuestados que ya utiliza una.

¿Qué métodos utiliza su organización para garantizar el cumplimiento de los proveedores con los requisitos de ciberseguridad?
(Seleccione hasta tres)

53% Auditorías anuales o pruebas de penetración

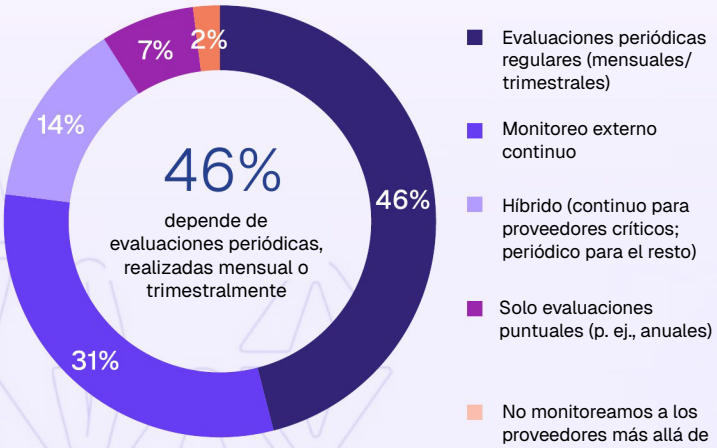
49% Asesoría directa de nuestro equipo

43% Aceptación de certificaciones de proveedores (SOC 2, ISO)

38% Cláusulas contractuales (penalizaciones/rescisión)

37% Plataformas compartidas de remediación o seguridad

¿Qué opción describe mejor su enfoque para monitorear el riesgo cibernético de terceros?



Los encuestados parecen coincidir en que el monitoreo continuo es una prioridad, y el 52% afirma que es parte integral de sus programas. **Sin embargo, el 67% todavía considera las auditorías de seguridad estáticas como su principal método de evaluación de riesgos**, seguidas de las herramientas y el monitoreo. Esta desconexión podría deberse a la falta de capacidad o habilidades para realizar un monitoreo más frecuente, o a que el monitoreo continuo está distribuido entre varios equipos. También podría indicar que las posturas de seguridad de la cadena de suministro de las organizaciones se encuentran en etapas tempranas de madurez.

¿Qué componentes forman parte de su programa de ciberseguridad de la cadena de suministro?
(Seleccione todos los que correspondan)

52% Monitoreo continuo

50% Capacitación de empleados en concientización de seguridad

45% Cobertura de seguro cibernético para incidentes en la cadena de suministro

44% Evaluaciones de riesgo de proveedores

41% Informes periódicos a la dirección/junta directiva

36% Proceso formal de incorporación y desvinculación de proveedores

¿Qué métodos utiliza para evaluar el riesgo de terceros? (Seleccione todos los que correspondan)

67% Auditorías de seguridad

63% Herramientas de evaluación de riesgo de terceros

55% Monitoreo externo continuo

46% Pruebas de penetración

41% Cuestionarios de autoevaluación

1% No evaluamos actualmente el riesgo de terceros

Los conflictos en los métodos de mitigación de riesgos dependen de en qué punto de la curva de madurez de TPRM se encuentre cada organización.

Nivel 1 **(el menos maduro): diligencia debida básica.** Solo se realizan revisiones de ciberseguridad durante la contratación.

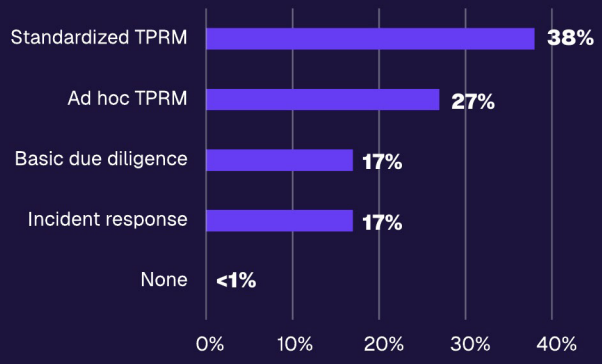
Nivel 2: **TPRM ad hoc (o periódico).** Se siguen políticas y flujos de trabajo informales de gestión de riesgos.

Nivel 3: **TPRM estandarizado (o continuo).** Se implementan controles proactivos de prevención de brechas, incluido el monitoreo automatizado.

Nivel 4 (el más maduro): respuesta a incidentes (TPRM basado en amenazas). Se realiza una remediación rápida de los problemas de seguridad de los proveedores.

Si bien el 43% de los encuestados se encuentra en una etapa temprana de madurez (diligencia debida básica y TPRM ad hoc), otro **55% es más maduro (TPRM estandarizado y respuesta a incidentes).** Lo interesante, sin embargo, es que el porcentaje de encuestados que utiliza los niveles más altos de madurez cayó 5 puntos porcentuales de 2025 a 2026, lo que demuestra que aún queda mucho trabajo por hacer.

¿Qué nivel de gestión de riesgo de la cadena de suministro implementa su organización?



Otras medidas de respuesta utilizadas por los encuestados subrayan la importancia de avanzar en la curva de madurez de TPRM. Según un líder:

*"Pasar de cuestionarios anuales a un monitoreo continuo basado en datos permite a los equipos **identificar los riesgos de terceros, en lugar de depender de informes obsoletos y puntuales.**"*

¿Qué capacidades de respuesta a incidentes de la cadena de suministro tiene su organización? (Seleccione todas las que correspondan)

58% Fuentes de inteligencia de amenazas en tiempo real

56% Detección automatizada de actividad de alto riesgo de proveedores

48% Seguimiento de remediación con evidencia

43% Flujos automatizados de triaje o escalamiento

40% Correlación entre múltiples problemas de proveedores

38% Plataforma compartida de remediación de proveedores

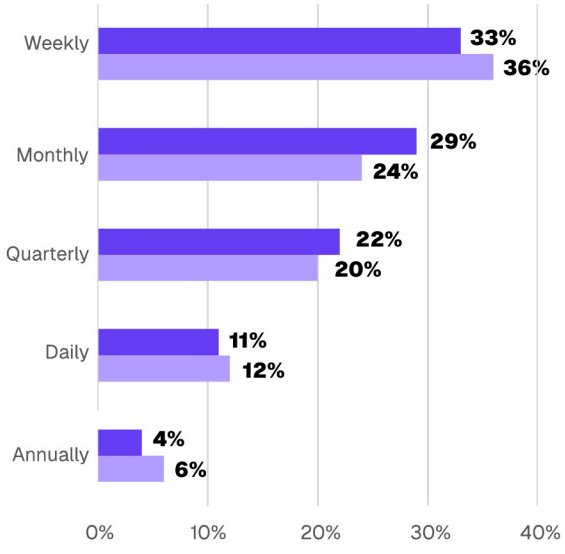
05

En la respuesta a incidentes, el tiempo no está de su lado

Los incidentes en la cadena de suministro varían en tamaño y alcance. Si bien las organizaciones pueden tener tiempo para resolver una vulnerabilidad recién descubierta o adaptarse a un cambio en el perfil de riesgo de un proveedor, los incidentes críticos requieren una remediación rápida. Pero encontrar y responder a los riesgos no siempre ocurre con rapidez, según los encuestados.

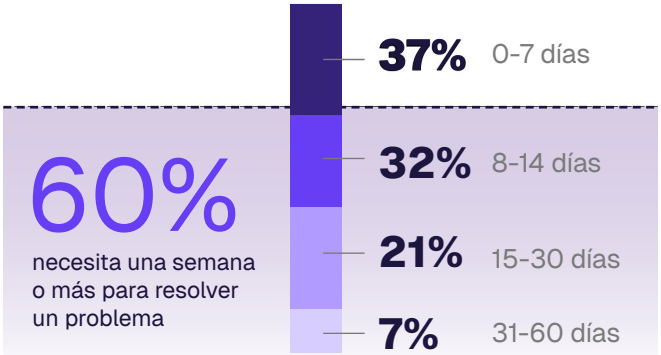
Mientras el 44% de los líderes afirma realizar evaluaciones de riesgo de terceros a diario o semanalmente, otro 51% solo las realiza mensual o trimestralmente. Además, el 44% afirma que solo actualiza o reevalúa las evaluaciones de riesgo de sus proveedores críticos de Nivel 1 mensual o trimestralmente.

- ¿Con qué frecuencia realiza su organización evaluaciones de riesgo de terceros?
- ¿Con qué frecuencia se actualiza o reevalúa la evaluación de riesgo de los proveedores críticos de Nivel 1 de su organización?



¿Con qué rapidez pueden los encuestados remediar un problema de alta gravedad? Mientras el 37% de los encuestados puede hacerlo en 0 a 7 días, el 60% necesita de 8 a 60 días. La razón No. 1 de la respuesta lenta es el uso de métodos de comunicación manuales y deficientes, mencionado por 4 de cada 10 encuestados.

¿Cuál es el tiempo promedio que tarda un proveedor crítico en remediar un problema de seguridad de alta gravedad?



¿Cuáles son las mayores barreras para una remediación oportuna de los proveedores?
(Seleccione todas las que correspondan)

Un análisis más detallado de los métodos de colaboración con proveedores revela la desconexión. Entre los encuestados, el 24% utiliza una plataforma compartida de seguridad y remediación para una comunicación de incidentes fluida y en tiempo real. **Pero el 55% aún depende de llamadas, reuniones, correos electrónicos o contactos comerciales clave para remediar incidentes, todo lo cual toma demasiado tiempo.** "Si esperas a escribir un correo electrónico, un actor malicioso ya habrá cifrado, infiltrado y secuestrado el sistema del proveedor antes de que presiones enviar", afirma Barker, de SecurityScorecard.

¿Cómo colabora principalmente su organización con los proveedores durante la remediación? (Seleccione uno)

24% Plataforma compartida de seguridad/remediación

21% Llamada telefónica o reunión directa

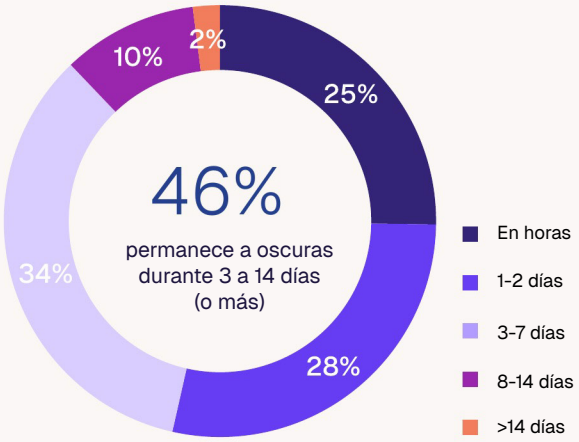
19% Sistema de tickets (ServiceNow, Jira)

19% Correo electrónico directo

15% Colaboración con el responsable de la relación comercial

A muchas organizaciones también les toma demasiado tiempo determinar si una vulnerabilidad crítica afecta a alguno de sus proveedores externos. **Mientras el 25% de los encuestados lo sabe en cuestión de horas, el 46% permanece a oscuras durante 3 a 14 días (o más).**

¿Cuánto tiempo le toma habitualmente a su organización determinar si una vulnerabilidad crítica recién anunciada (p. ej., de día cero) afecta a alguno de sus proveedores externos?



Una respuesta más rápida requiere una mejor comunicación, como explica un encuestado:

"Garantizar la retroalimentación y los informes continuos entre ambas partes, incluso durante una brecha, y que el SOC y el equipo de TPRM sigan un mismo plan. ***Si la comunicación general es deficiente, esto provoca horas de retraso."***

Conclusión

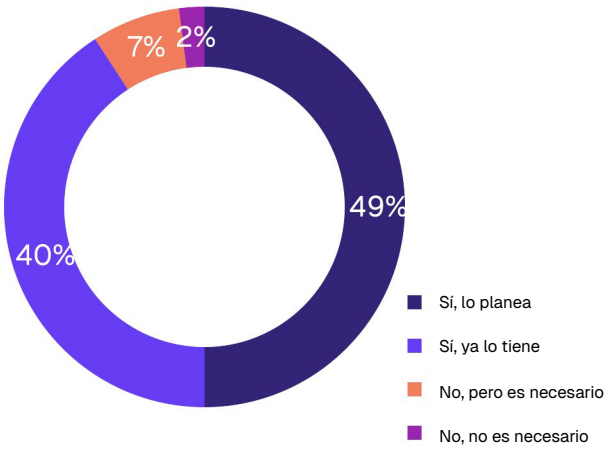
Cierre la brecha entre confianza y protección con inteligencia de amenazas más sólida.

Las auditorías anuales, las evaluaciones periódicas y la comunicación manual ya no protegerán a las organizaciones frente a los riesgos modernos y de rápida evolución en la cadena de suministro. Para mantenerse al día, las empresas deben adoptar estrategias de TPRM habilitadas por IA que puedan automatizar los conocimientos y optimizar los flujos de trabajo de detección y seguimiento de remediación en minutos, no en días o semanas.

El mensaje ya está llegando al **40% de los encuestados que ha implementado una función dedicada de respuesta a incidentes en la cadena de suministro.** Otro 49% afirma que "planea desarrollar una". Pero las buenas intenciones por sí solas no remediarán los riesgos de la cadena de suministro. Las organizaciones deben actuar ahora para avanzar en la curva de madurez y cerrar la brecha entre la confianza mal ubicada y la detección de amenazas basada en inteligencia.

SecurityScorecard puede ayudar. Descubra el poder de los conocimientos accionables, la IA y la automatización para la ciberseguridad de su cadena de suministro. Obtenga más información sobre nuestra plataforma TITAN AI y regístrese para una prueba gratuita de 14 días.

¿Planea desarrollar una función dedicada de respuesta a incidentes en la cadena de suministro?



Datos firmográficos

Países representados

U.S.	58%
Canadá	11%
Reino Unido	11%
Sudáfrica	9%
Singapur/ Filipinas/ Australia/Nueva Zelanda	7%
India	4%

Industrias representadas

Tecnología	27%
Manufactura	24%
Servicios financieros/ seguros	18%
Comercio minorista/ electrónico	16%
Salud	7%

SecurityScorecard es el líder global en gestión de riesgo de terceros basada en amenazas (TPRM), protegiendo las cadenas de suministro del mundo. La empresa ofrece un enfoque moderno de TPRM basado en amenazas que permite a las organizaciones eliminar el riesgo desde su origen. A través de visibilidad continua, inteligencia acelerada por IA y conocimientos predictivos, la plataforma transforma el riesgo de terceros en una ventaja competitiva, permitiendo a las organizaciones reducir el riesgo de forma proactiva antes de que ocurran incidentes y responder con confianza cuando ocurren, ofreciendo una resiliencia medible en la cadena de suministro. Cuenta con la confianza de más de 3,300 organizaciones, incluido el 70% de las empresas Fortune 100, y está reconocida como un recurso confiable por la Agencia de Ciberseguridad e Infraestructura de EE. UU. (CISA). Respaldada por Evolution Equity Partners, Silver Lake Partners, Sequoia Capital, Google Ventures, NGP Capital, Intel Capital y Riverwood Capital, SecurityScorecard ofrece ciberseguridad integral para la cadena de suministro que protege la continuidad del negocio. Proteja la cadena de suministro detrás de su negocio. Obtenga más información en securityscorecard.com.