CISO talk

Gestión de riesgos de terceros

EDICIÓN
JUNIO - JULIO 2026

trustive
Community

Publicado en junio de 2026.

Tabla de contenidos.

Tabla de contenidos.

Gestión de Riesgos de Terceros Third-Party Risk Management (TPRM): de un checklist de cumplimiento a un pilar esencial de la ciberseguridad moderna.

Resumen Ejecutivo

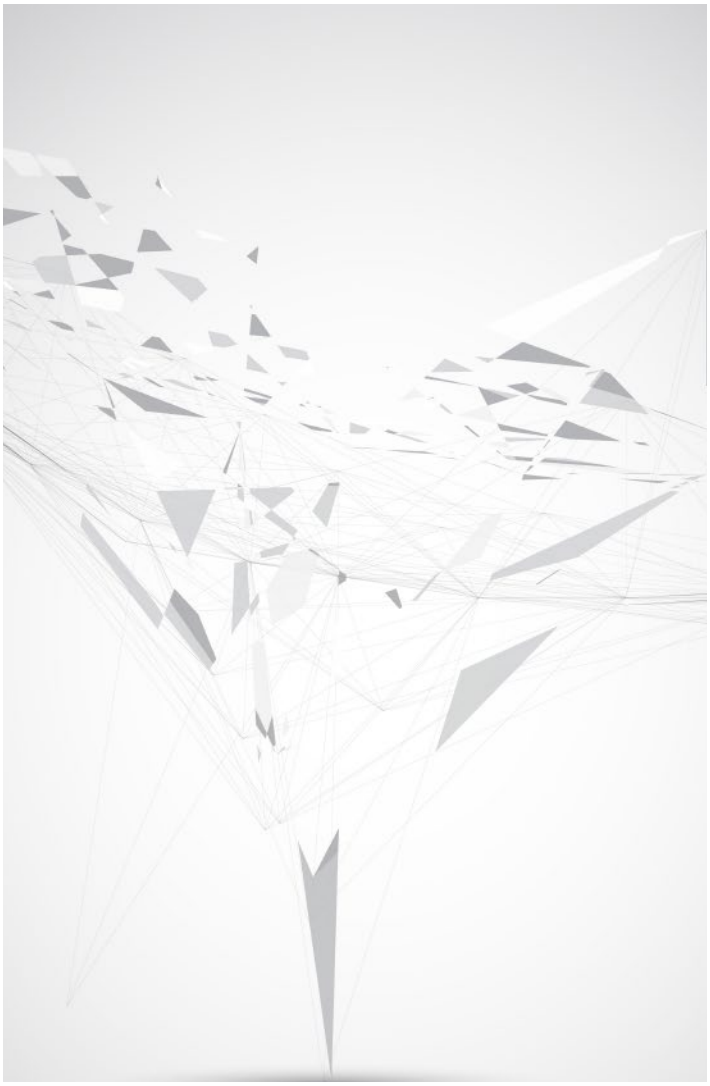
La gestión de riesgos de terceros ha evolucionado drásticamente, de ser un simple ejercicio de cumplimiento ha pasado a convertirse en un **pilar crítico de la ciberseguridad moderna.** En un entorno empresarial donde confías en cientos o miles de proveedores externos para funciones vitales, ¿cómo asegurarte de que ninguno se convierta en el eslabón débil de tu cadena de seguridad? Los ataques recientes han demostrado que las brechas sufridas a través de terceros pueden ser tan devastadoras como las ocurridas directamente. De hecho, el **61% de las organizaciones sufrió en 2023 un incidente de seguridad o brecha de datos originado en terceros, y se estima que casi el 30% de todas las brechas tienen un vector de ataque ligado a un proveedor externo.** Consecuentemente, los directivos y los CISO están poniendo el foco en TPRM de forma inédita, integrándolo en la estrategia de ciber resiliencia corporativa. En este artículo exploraremos por qué la gestión de terceros ya no es un “nice-to-have” sino un imperativo estratégico, analizaremos casos reales que subrayan los peligros de una cadena de suministro digital vulnerable, revisaremos estadísticas recientes de fuentes reconocidas (Gartner, Ponemon, IBM, Deloitte, entre otros) y ofreceremos recomendaciones prácticas para robustecer tu programa de TPRM con miras al futuro (multi-nube, IA generativa, etc.). Al final, plantearemos una pregunta desafiante: ¿estamos **realmente preparados** para gestionar los riesgos ocultos en un ecosistema donde colaboramos con cientos de proveedores digitales y el factor humano sigue siendo el eslabón más débil?

La cadena de suministro digital: el nuevo frente de ataque

Cada organización forma parte de una **cadena de suministro digital compleja,** interconectada por innumerables terceros como: proveedores de software, servicios en la nube, consultores, subcontratistas, SaaS especializados, procesadores de datos,

etc. Esta red amplía la superficie de ataque más allá de tus fronteras. Los datos recientes son reveladores, **la empresa promedio comparte información confidencial con 583 proveedores** externos, y según un estudio de Ponemon Institute, una organización típica puede llegar a tener **en promedio 5.800 terceros en su ecosistema.** Cada uno de esos cientos (o miles) de socios tecnológicos puede convertirse en la puerta de entrada de una amenaza si no gestionamos adecuadamente sus riesgos.

El problema se agrava porque muchas organizaciones todavía carecen de visibilidad plena sobre esta "tercera dimensión" de su seguridad. No es inusual descubrir proveedores "fantasma" (servicios o aplicaciones en la sombra contratados sin pasar por los debidos controles), o **cuartas y quintas partes** (los proveedores de tus proveedores) que escapan a cualquier escrutinio. Los adversarios lo saben, en lugar de atacar directamente a una empresa bien protegida, a veces es más efectivo comprometer a un colaborador externo con defensas más débiles y usarlo como caballo de Troya. Así, tu cadena de suministro se convierte en el nuevo frente de ataque. No sorprende que el volumen de brechas vía terceros esté en auge, pues **el número de brechas vinculadas a terceros se incrementó un 49% interanual, triplicándose desde 2021. Además, el 75% de las brechas de seguridad que**



involucran a terceros se dirigieron a la cadena de suministro de software y tecnología, reflejando cómo los atacantes explotan debilidades en proveedores de IT, bibliotecas de código, outsourcers, etc.

Los efectos de este fenómeno de **"ataque en cascada"** quedaron patente en incidentes globales recientes. Cuando un proveedor clave es golpeado, el impacto se propaga a todos sus clientes. Es por eso que hoy **gestionar la seguridad de tus terceros es tan importante como gestionar la propia,**

el riesgo es compartido. En palabras de Gartner, las as redes de terceros siguen **aumentando en número y alcance,** al punto que el **40% de los líderes de cumplimiento afirman que entre el 11% y el 40% de sus terceros suponen riesgos altos.** Esto ha llevado a que los consejos directivos demanden mayor visibilidad y control sobre la gestión de riesgos de terceros, elevando el tema a prioridad de negocio.

De la diligencia debida al monitoreo continuo: la evolución de TPRM

Tradicionalmente, la gestión de riesgos de terceros se abordaba como un trámite de cumplimiento (compliance), es decir recopilar cuestionarios de seguridad de los proveedores al inicio de la relación, verificar que firmaran ciertas cláusulas contractuales y archivar esa documentación (muchas veces, para no volver a mirarla). Era un enfoque estático, centrado en “tocar base” con cumplimiento normativo más que en una evaluación viva del riesgo. **En resumen, TPRM solía ser sinónimo de una lista de verificación** como requisito de cumplimiento en la inscripción o incorporación (on-boarding) del proveedor. Pero ese paradigma ha quedado obsoleto.

La realidad actual exige un enfoque **dinámico y proactivo.** Los riesgos evolucionan constantemente, y la postura de seguridad de un tercero puede cambiar de un mes a otro (nuevas vulnerabilidades, rotación de personal, cambios en sus subcontratistas, etc.). Como bien apuntan los expertos, “no basta con confiar únicamente en los cuestionarios de due diligence completados durante la incorporación de proveedores”. Aquella foto inicial caduca rápidamente. Por eso, la TPRM moderna se basa en **monitoreo continuo** del riesgo y desempeño de los terceros, supervisar alertas de seguridad, noticias de brechas que afecten a tus proveedores, re-evaluaciones periódicas, indicadores de riesgo clave (KRIs) actualizados, etc. Si hace unos años bastaba con una auditoría anual a un proveedor crítico, hoy necesitamos monitoreo de riesgo en tiempo real.

Esta evolución también se refleja en la estructura organizacional y el cambio cultural. Muchas empresas han pasado de gestionar los riesgos de terceros de forma descentralizada (cada departamento por su cuenta) a **modelos centralizados o federados** con una coordinación clara. Los comités de riesgos y las juntas directivas preguntan por el estado de los principales proveedores igual que preguntan por las amenazas internas. **La gestión de terceros se ha convertido en un componente fundamental de la resiliencia organizacional,** al nivel de la gestión de riesgos internos. Un informe de Deloitte destaca que el **45% de los líderes de TPRM consideran crucial invertir de forma continua en tecnología, automatización y datos** para sus programas, lo que evidencia que las empresas líderes en el tema, están fortaleciendo activamente esta área. Ya no se trata solo de cumplir un requisito de auditoría, sino de **proteger el negocio de forma holística.**

Regulaciones recientes han acompañado (y exigido) este cambio de mentalidad. Por ejemplo, la nueva directiva europea **NIS 2.0** obliga a las entidades esenciales e importantes a **gestionar los riesgos de seguridad no solo en sus propios sistemas, sino también en los de sus proveedores y servicios externalizados.** Del mismo modo, en el sector financiero la normativa DORA (Digital Operational Resilience Act) establece requisitos estrictos de due diligence y supervisión continua sobre los terceros críticos (como proveedores de nube) de los que depende una entidad financiera. Esto implica que si eres un banco, no solo debes preocuparte por tu ciberseguridad interna, sino también por la de aquellos proveedores tecnológicos cuya caída o hackeo podría poner en jaque tu operación. En suma, el mensaje es claro, **la gestión de riesgos de terceros ha pasado de ser un punto secundario de cumplimiento a ser una prioridad estratégica y regulatoria.**

Quien no adapte su programa de TPRM a esta nueva realidad estará navegando un mar de amenazas con los ojos vendados.

Casos reales que despertaron a la industria

Nada ilustra mejor la importancia de TPRM que examinar algunos **ataques emblemáticos** de la cadena de suministro digital ocurridos en los últimos años. Estos incidentes actuaron como verdaderos llamados de atención para muchos CISOs y juntas directivas:

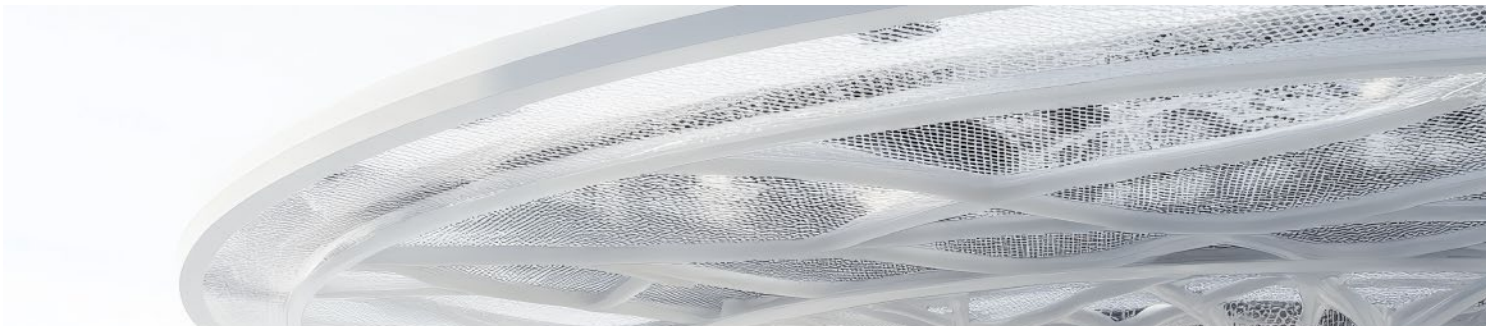
- **Ataque a SolarWinds (2020):** Un caso ya legendario de supply chain attack. Los atacantes (presuntamente respaldados por un Estado) comprometieron la cadena de desarrollo del **software de monitoreo SolarWinds Orion** e introdujeron código malicioso en una actualización legítima. ¿El resultado? Alrededor de **18.000 organizaciones clientes de SolarWinds instalaron sin saberlo una puerta trasera** en sus sistemas. Entre las víctimas hubo agencias gubernamentales de EE. UU. y grandes empresas globales. Los atacantes aprovecharon esta posición para robar datos sensibles y espiar a otras organizaciones, desplegando un acceso prácticamente ilimitado. Este incidente demostró brutalmente cómo un solo proveedor de software comprometido puede dar lugar a una brecha global de enorme alcance. Después de SolarWinds, el mundo entendió que la seguridad de la cadena de suministro de software es tan importante como la seguridad perimetral tradicional. Muchas empresas comenzaron a exigir garantías mucho más fuertes a sus proveedores de software, incluyendo revisiones de código, monitoreo de integridad de actualizaciones y certificados digitales robustos.

- **Ransomware a Kaseya (2021):** El 2 de julio de 2021, la empresa de IT management **Kaseya** sufrió un ataque de ransomware que afectó a su software de administración remota (VSA), muy utilizado por proveedores de servicios gestionados (MSPs). Los ciberdelincuentes (la banda REvil) aprovecharon una vulnerabilidad para distribuir malware de cifrado a través de la herramienta de Kaseya, infectando a cientos de empresas clientes de esos MSP en todo el

mundo. En cuestión de horas, este efecto dominó dejó entre **800 y 1.500 empresas afectadas** en diversos países, incluyendo desde pequeñas clínicas dentales hasta una cadena de supermercados en Suecia que tuvo que cerrar temporalmente cientos de tiendas al quedar inutilizadas sus cajas registradoras. Este ataque evidenció el peligro de confiar ciegamente en herramientas de terceros para la administración de sistemas, si la herramienta central es comprometida, el impacto es masivo. Asimismo, puso sobre la mesa el concepto de **"clientes de segundo nivel":** Kaseya tenía quizá decenas de MSPs como clientes directos, pero a través de ellos tenía un alcance indirecto a miles de negocios. La pregunta obligada que dejó este caso fue: ¿Cómo evalúo no solo el riesgo de mi proveedor, sino el riesgo que mi proveedor puede introducir en sus clientes (mis sistemas)?

- **Brecha de MOVEit Transfer (2023):** En mayo de 2023 se reveló una vulnerabilidad zero-day crítica en **MOVEit Transfer,** un software popular de transferencia segura de archivos, desarrollado por Progress Software y utilizado por miles de organizaciones para intercambiar datos (muchas veces información sensible) con sus socios. El grupo criminal CLOP explotó esta falla para **robar volúmenes masivos de datos de decenas de compañías y agencias gubernamentales a nivel mundial.** Una de las víctimas indirectas más sonadas fue Amazon, aunque sus sistemas centrales no fueron hackeados, un proveedor externo que gestionaba propiedades inmobiliarias para Amazon fue comprometido a través de MOVEit, lo que permitió filtrar datos internos. Amazon confirmó que más de **2,8 millones de registros con datos de empleados** (principalmente correos corporativos, extensiones telefónicas y ubicaciones de oficinas) fueron robados en este incidente ligado a MOVEit.

  La lección aquí es doble: primero, una vulnerabilidad en un software de terceros ampliamente utilizado puede generar un evento de brecha simultáneo en numerosas empresas (un "ataque masivo a la cadena de suministro" en toda regla); segundo,



incluso gigantes tecnológicos con amplios recursos de seguridad son vulnerables a fallos en productos de terceros que utilizan para funciones específicas. Tras este ataque, muchas compañías empezaron a preguntar a sus proveedores de software sobre sus procesos de gestión de vulnerabilidades y parches, y a limitar la información que comparten incluso a través de herramientas "seguras" de terceros.

- **Errores y vulnerabilidades en proveedores cloud:** La confianza en la nube es otro frente de riesgo que ha dado algún que otro susto. Un ejemplo notable fue la vulnerabilidad **"ChaosDB"** descubierta en 2021 en Microsoft Azure Cosmos DB. Investigadores externos hallaron que, mediante una cadena de exploits en una función auxiliar, podían obtener claves que daban **acceso administrativo completo a las bases de datos de miles de clientes de Azure Cosmos DB**. Esta brecha potencial (por suerte descubierta por investigadores éticos y no por atacantes malignos) fue calificada como "la peor vulnerabilidad en la nube que se pueda imaginar". Microsoft tuvo que notificar y corregir urgentemente el fallo para asegurar que no fuese explotado. Imagina por un momento las implicaciones: empresas de todo el mundo confiando sus datos a un servicio administrado de nube, que súbitamente podría exponerlos a terceros no autorizados.

Este incidente dejó claro que incluso los proveedores cloud más grandes pueden introducir riesgos críticos, y que **la responsabilidad compartida no exime a las empresas usuarias de evaluar la seguridad de sus entornos cloud.** Otro ejemplo más común, se da con los errores de configuración (misconfigurations) por parte de proveedores de servicios cloud, que han llevado a brechas de

datos importantes; se calcula que alrededor del **23% de los incidentes de seguridad en la nube se deben a configuraciones incorrectas,** a veces atribuibles al cliente, pero en ocasiones también a implementaciones predeterminadas inseguras del proveedor. Esto subraya la necesidad de validar cómo los proveedores configuran y protegen los entornos que te ofrecen.

Estos casos (SolarWinds, Kaseya, MOVEit, Azure ChaosDB, entre otros) sirvieron para **sacudir la consciencia** de muchas organizaciones. Lo que antes era un riesgo teórico ("¿y si hackean a mi proveedor?") se convirtió en una realidad tangible y costosa. Las conversaciones en los directorios ahora incluyen preguntas directas a los CISOs y responsables de riesgo: "¿Cómo estamos evaluando a nuestros terceros? ¿Qué garantías tenemos de que un 'SolarWinds' no nos ocurra? ¿Tenemos visibilidad de qué datos podrían exponerse si un proveedor crítico es comprometido?". La gestión de terceros adquirió, en pocas palabras, protagonismo central en la agenda de ciberseguridad.

El impacto de las brechas de terceros en cifras

Para dimensionar mejor el problema, veamos algunos **datos y estadísticas recientes** de estudios de la industria que pintan el panorama actual de los riesgos de terceros:

- **Prevalencia de las brechas vía terceros:** Prácticamente ninguna organización está a salvo. Un informe de SecurityScorecard reveló que **el 98%** de las empresas mantiene relaciones con al menos un tercero que ha sufrido una brecha de seguridad. Además, como mencionamos, una mayoría (61%) de empresas reportó al menos una brecha de datos o incidente de ciberseguridad causado por terceros en 2023. No es de extrañar entonces que **la principal preocupación de seguridad relacionada con terceros para el 74% de las organizaciones sea precisamente una brecha de datos.** Cuando 3 de cada 4 empresas temen el mismo escenario, es porque ya lo han visto ocurrir con demasiada frecuencia.

- **Consecuencias multidimensionales:** Los incidentes que involucran terceros no solo causan pérdidas técnicas, sino impactos de negocio amplios. Gartner encontró que **84% de las organizaciones que sufrieron incidentes de riesgo de terceros enfrentaron interrupciones operativas,** 66% sufrieron impacto financiero directo, **59% vieron daños a su reputación,** y en 33% de los casos hubo acciones regulatorias posteriores. Otra encuesta (Venminder) destacó que los mayores impactos percibidos de un incidente de seguridad de terceros fueron daños financieros (29%), daño reputacional (26%) y escrutinio regulatorio (19%). Estos números corroboran que las consecuencias van más allá de "arreglar un servidor" pueden costar clientes, valor de marca y hasta sanciones legales.

- **Costos elevados:** Remediar una brecha causada por terceros suele ser más caro que otras brechas. Gartner estima que el costo de una brecha cibernética originada en terceros es típicamente un 40% más alto que el de una brecha interna equivalente. Esto se debe a varios factores, entre ellos se encuentran: la complejidad de investigar incidentes que involucran a otra entidad, la coordinación legal y de comunicaciones entre ambas partes, y a menudo el doble golpe reputacional (tu empresa y el proveedor bajo escrutinio).

IBM, en su reporte anual de Cost of a Data Breach, también ha señalado máximos históricos en los costes promedio aprox 4.45 millones de dólares en 2023, subiendo a 4.88 millones en 2024 y reveló que 1 de cada 3 brechas ahora implica a un tercero en alguna fase. Es claro que los riesgos de terceros pueden traducirse rápidamente en pérdidas económicas significativas.

- **Falta de confianza y visibilidad:** A pesar de que las empresas entienden

el riesgo, muchas admiten tener un talón de Aquiles en cuanto a visibilidad sobre lo que hacen (o dejarían de hacer) sus proveedores en caso de incidente. Según un estudio de RiskRecon y Ponemon Institute, solo 34% de los profesionales confía en que un proveedor crítico les notificaría proactivamente si sufre una violación de datos. En otras palabras, 2 de cada 3 organizaciones temen enterarse demasiado tarde de que un socio ha sido comprometido. Esta falta de confianza no surge de la nada, pues ha habido casos donde proveedores ocultaron o demoraron notificar brechas, exponiendo aún más a sus clientes. Por ello, la tendencia es establecer **obligaciones contractuales estrictas de notificación inmediata** de incidentes, así como implementar fuentes independientes de inteligencia (por ejemplo, monitorear la dark web en busca de datos de tu empresa que pudieran provenir de terceros comprometidos).

En conjunto, estas cifras refuerzan el argumento central: **ignorar los riesgos de terceros ya no es una opción.** Las probabilidades de sufrir un incidente a través de un proveedor son demasiado altas, y las repercusiones demasiado severas, como para dejar este tema en segundo plano. La siguiente pregunta natural es: ¿qué hacer al respecto? A continuación, discutimos cómo la industria está respondiendo, desde la adopción de nuevas tecnologías hasta cambios en la gobernanza y mejores prácticas para mitigar estos riesgos.

Innovación en TPRM: automatización, IA y plataformas GRC

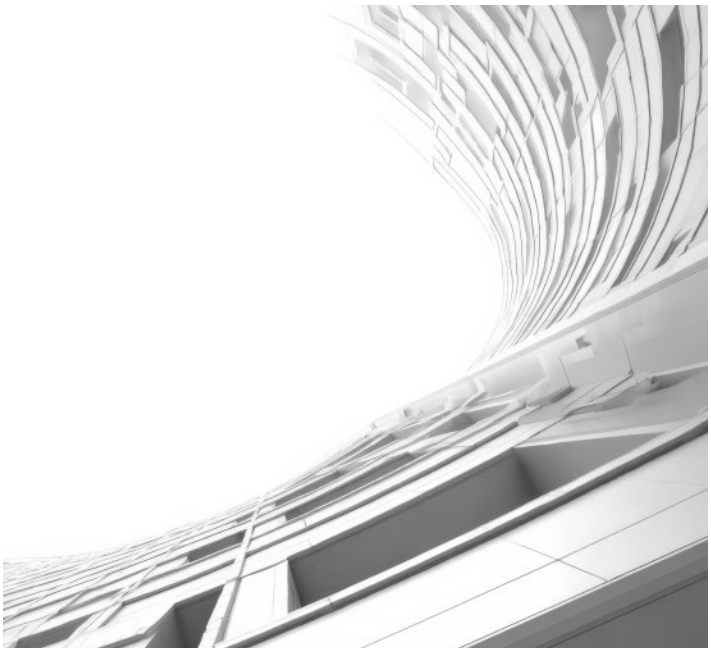
Gestionar el riesgo de cientos de proveedores de forma manual es como tratar de vigilar un enjambre de abejas a simple vista, un desafío casi imposible. Por suerte, así como los atacantes innovan, también lo hacen las herramientas de defensa. En los últimos años hemos visto un **auge de soluciones tecnológicas para TPRM,** incluyendo plataformas de Governance, Risk & Compliance (GRC) especializadas, calificaciones de seguridad de terceros en tiempo real (security ratings), y más recientemente la incorporación de **inteligencia artificial**

(IA) para agilizar tareas. Veamos algunas de las tendencias y cómo pueden ayudar a un CISO o equipo de riesgos a dominar la complejidad:

- **Plataformas TPRM dedicadas:** Son soluciones de software diseñadas para centralizar y automatizar gran parte del ciclo de vida de la gestión de proveedores. Permiten mantener un inventario vivo de todos los terceros, sus riesgos inherentes y residuales, los controles asociados, documentos (contratos, certificados, reportes de auditoría) y actividades de seguimiento. También facilitan la colaboración con los propios proveedores, enviando evaluaciones en línea, recopilando evidencias y haciendo scoring de riesgos. Un beneficio clave es romper los silos, todos los involucrados (seguridad, compras, legal, compliance) trabajan sobre la misma plataforma con información unificada. Sin estas herramientas, muchas organizaciones dependen de hojas de cálculo y correos electrónicos para rastrear riesgos, lo cual no escala. Aún así, **el 60% de las organizaciones encuestadas en 2024 admitió no estar utilizando una plataforma TPRM dedicada.** La buena noticia es que cada vez más empresas están adoptándolas; de hecho, **77% de los encuestados confía ahora en software con funcionalidades de gestión de proveedores para agilizar la gestión de riesgos.** Si tu programa TPRM aún vive en Excel, es hora de considerar modernizarlo
- **Monitoreo continuo y calificaciones** de seguridad: Una innovación muy útil ha sido la aparición de servicios que monitorean de forma continua a tus terceros a través de fuentes abiertas, escaneos externos y feeds de amenazas. Empresas como SecurityScorecard, BitSight, UpGuard, entre otras, ofrecen **ratings de ciberseguridad** de terceros (similares a un puntaje crediticio, pero en seguridad) basados en hallazgos como puertos expuestos, vulnerabilidades conocidas, filtraciones detectadas, etc. Esto permite recibir alertas si un proveedor crítico ve degradar su postura (por ejemplo, si expone por error un servidor o si aparece información suya en una brecha). Complementariamente, algunas

plataformas integran inteligencia de amenazas, donde te avisan si en foros clandestinos se menciona a tu proveedor, o si un nuevo exploit podría afectarlo. Este nivel de vigilancia es imposible de lograr manualmente para decenas de proveedores al mismo tiempo. Sin embargo, todavía está infrautilizado: **solo un 13-14% de los equipos de compras y gestión de proveedores utilizan herramientas de monitoreo continuo** para sus terceros. Esperamos que este porcentaje crezca rápidamente conforme las organizaciones se den cuenta del valor de "no quitar el ojo" a sus aliados críticos.

- **Automatización e IA en los procesos de riesgo:** La inteligencia artificial está empezando a hacer sentir su presencia en TPRM, aunque de forma inicial. Según una encuesta de Prevalent, **solo el 5% de las empresas actualmente aprovechan IA en sus programas de riesgos de terceros, pero un 61% está investigando activamente casos de uso para incorporarla.** ¿En qué puede ayudar exactamente la IA? Un área concreta es en los cuestionarios de seguridad, entrenando modelos en las respuestas históricas de un proveedor, se puede predecir o completar automáticamente respuestas a nuevos acelerando enormemente el proceso de due

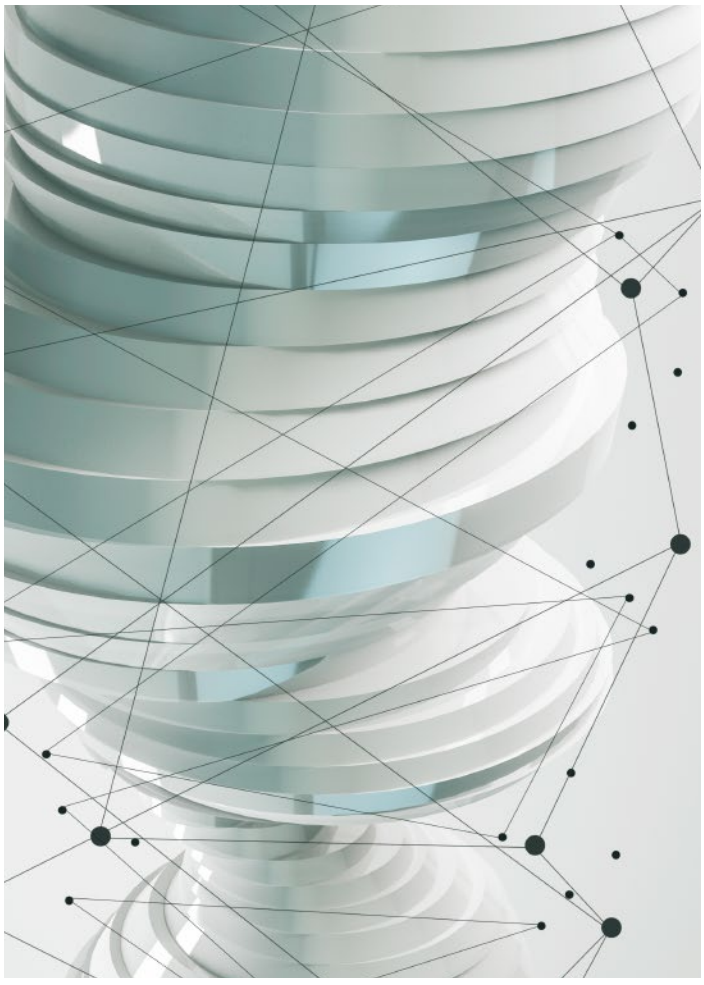


diligence. De hecho, el 54% de las organizaciones señala que su principal motivación para explorar IA en TPRM es acelerar la finalización de cuestionarios mediante autocompletar respuestas con información existente.

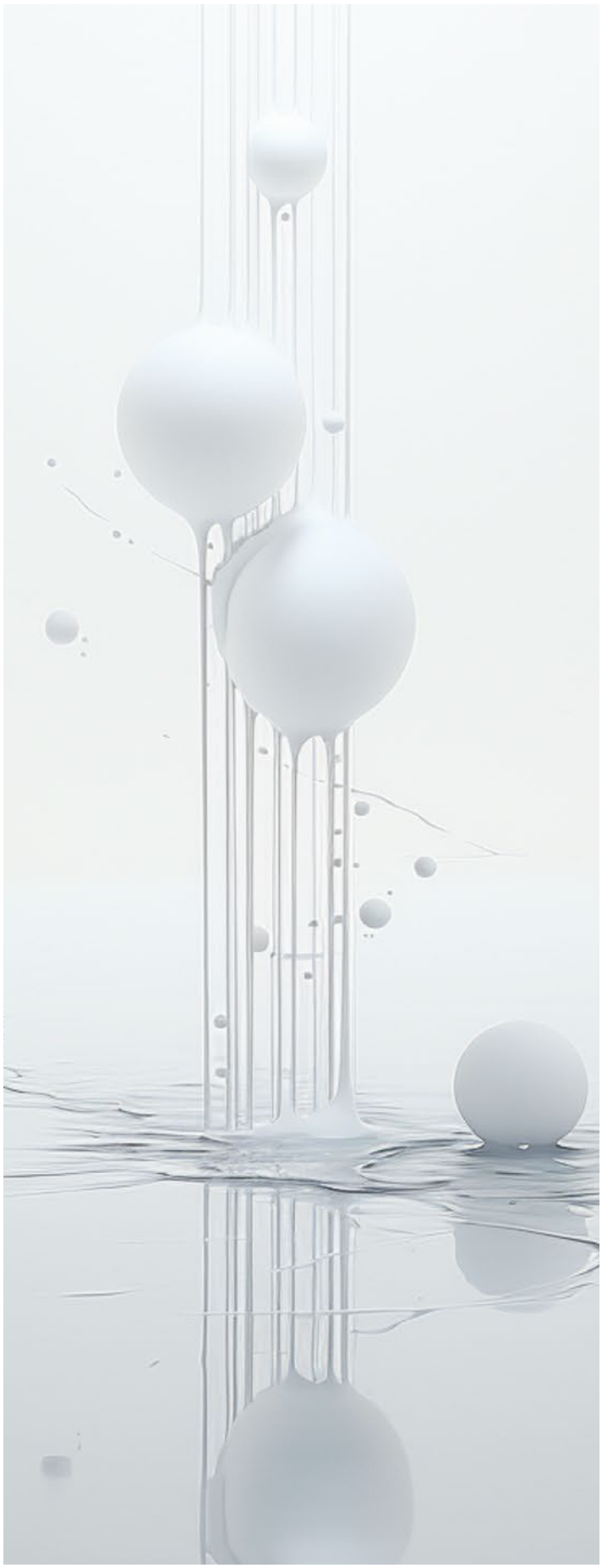
Otra aplicación es el análisis inteligente de riesgos, por ejemplo, usar procesamiento de lenguaje natural (NLP) para leer los informes de auditoría o pen-tests que entrega un proveedor y resumir las principales brechas o recomendaciones. Asimismo, bots de IA podrían escanear continuamente noticias y fuentes de datos para identificar señales tempranas de que un tercero pueda estar comprometido (por ejemplo, cambios inusuales en patrones de tráfico). Aunque estamos en las primeras etapas, compañías grandes ya están haciendo pilotos en este

sentido. **Deloitte** menciona que las organizaciones líderes están enfocándose en “procesos impulsados por tecnología escalable para la gestión dinámica de riesgos”, incluyendo monitoreo en tiempo real potenciado por IA. Eso sí, es importante destacar que la IA no reemplazará el juicio humano; más bien lo potenciará al encargarse de tareas repetitivas y de segmentar grandes volúmenes de datos, dejando a los profesionales de riesgo las decisiones críticas. Un CISO experto seguirá siendo quien interprete las señales y determine acciones, pero contará con “asistentes virtuales” que le darán ventaja frente a la avalancha de información.

- **Integración con GRC y ERM:** Otra tendencia es integrar el módulo de TPRM dentro del marco más amplio de gestión de riesgos empresariales (ERM) y gobierno corporativo. Esto significa que los riesgos de terceros se evalúan con la misma rigurosidad y lenguaje que cualquier otro riesgo de la empresa (financiero, operativo, estratégico). Al vincular TPRM con la matriz de riesgos corporativa, se pueden priorizar las inversiones de mitigación de manera informada, por ejemplo, si un proveedor X soporta un proceso de negocio crítico, su riesgo inherente debe reflejarse en un nivel alto que justifique controles robustos o incluso planes de contingencia (como proveedores alternativos). Varias plataformas GRC integrales (MetricStream, ServiceNow GRC, OneTrust GRC, Archer, etc.) ya incluyen módulos de terceros, o facilitan la incorporación de las evaluaciones de terceros en los dashboards generales de riesgo. El mensaje aquí es que **TPRM no debe verse aislado,** sino como parte de la fotografía total de riesgos de la organización. Esto eleva su perfil y facilita reportar a dirección un panorama consolidado, por ejemplo, en suma, la tecnología y la automatización se han vuelto aliadas indispensables para gestionar TPRM a escala. **La clave es usarlas estratégicamente,** pues una mala

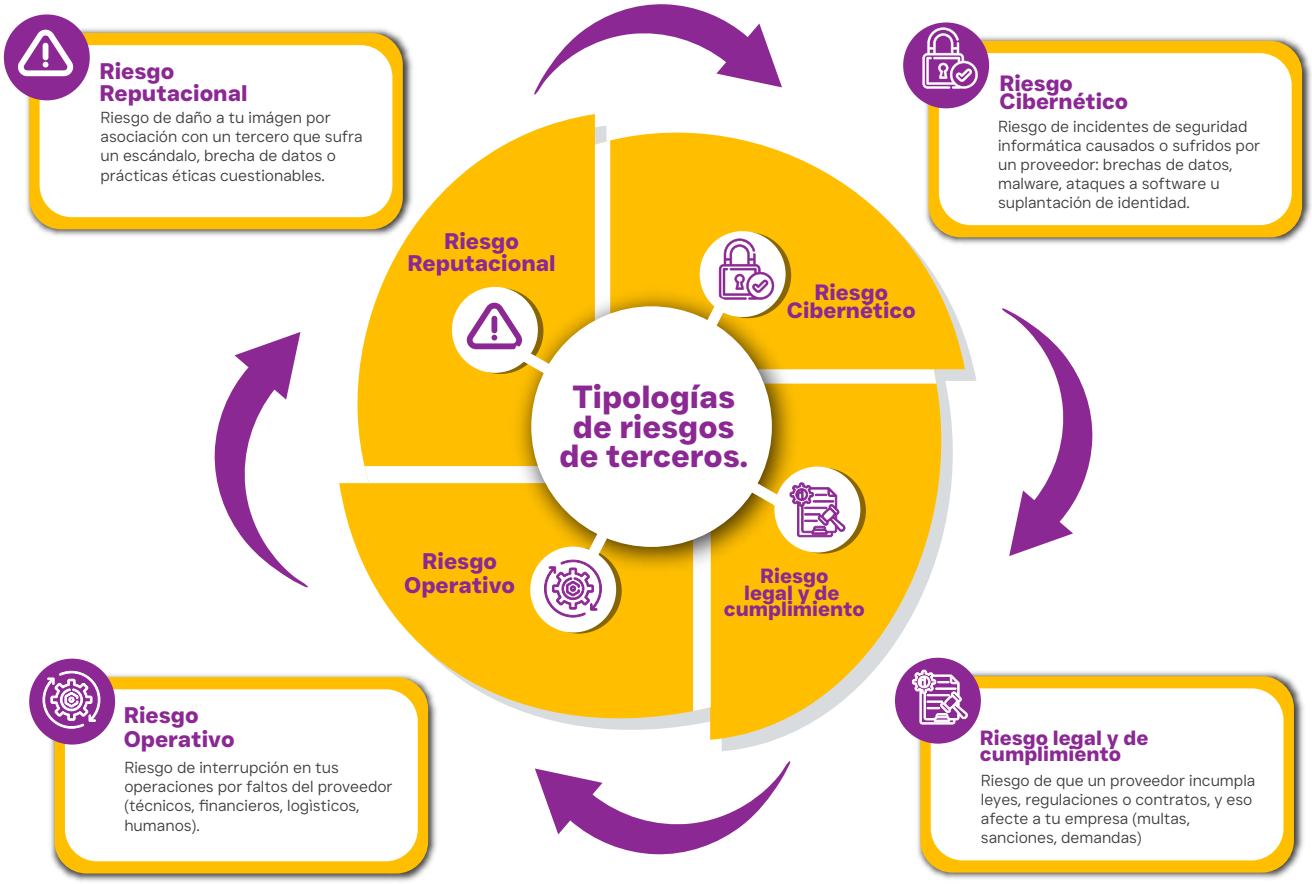


herramienta o mal configurada no solucionará mágicamente el problema. Pero bien empleadas, permiten pasar de un modo reactivo (enterarte de la brecha cuando ya ocurrió) a uno **predictivo y preventivo,** donde puedes anticipar y mitigar riesgos antes de que exploten. Como responsable de seguridad o cumplimiento, vale la pena evaluar qué combinación de estas soluciones encaja con tu programa desde plataformas integrales si buscas una solución end-to-end, hasta servicios puntuales de monitoreo continuo o módulos de IA para reforzar capacidades específicas.



Tipologías de riesgos de terceros: más allá de lo cibernético

Al hablar de terceros solemos pensar inmediatamente en riesgos **cibernéticos** (brechas de datos, malware, hacking). Sin duda, estos son centrales, pero el **riesgo de terceros es multifacético.** Un proveedor puede causar estragos de varias maneras, y es importante categorizar y entender estos diferentes riesgos para abordarlos con las medidas adecuadas. A grandes rasgos, podemos identificar cuatro tipologías principales de riesgo asociadas a terceros:

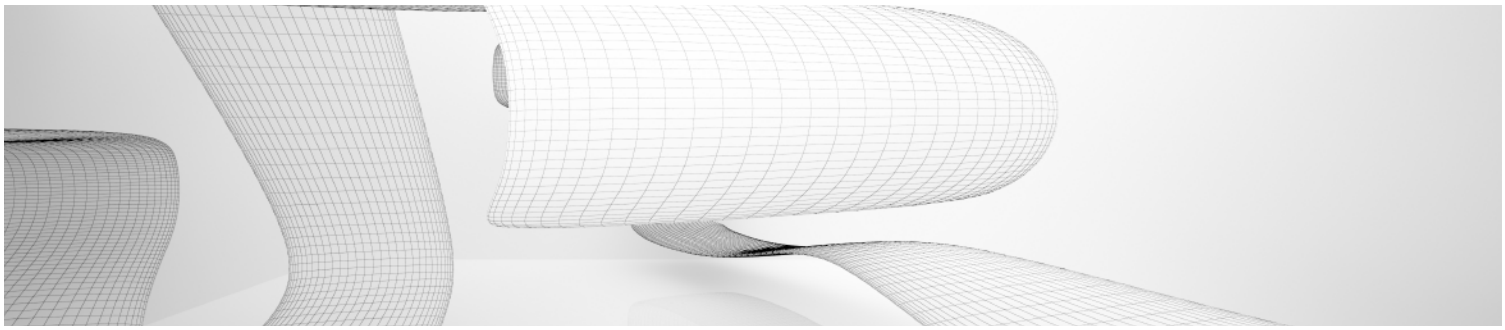


- **Riesgo Cibernético:** Es el más evidente. Se refiere a la posibilidad de que un tercero sufra (o cause) un incidente de seguridad informática que te afecte. Aquí entran **brechas de datos sensibles** almacenados o manejados por el proveedor, ataques que comprometan la confidencialidad, integridad o disponibilidad de sistemas interconectados, introducción de malware, ataques de la cadena de suministro de software, etc. Ejemplos: la filtración de datos de clientes a través del chatbot de Ticketmaster es un riesgo cibernético materializado con impacto en datos personales; el ataque SolarWinds, un riesgo cibernético donde software comprometido del tercero infectó a clientes; o un proveedor de hosting que sufre ransomware y deja inaccesible tu sitio web. Este tipo de riesgo suele mitigarse con exigencias de **controles de ciberseguridad** (firewalls, cifrado, autenticación, monitoreo) en los terceros, evaluaciones técnicas (ej: pentests), y arquitecturas seguras (ej: compartimentalizar las conexiones con terceros, Zero Trust, etc.). También incluye el riesgo de que un tercero malicioso (no autorizado) engañe a la empresa haciéndose pasar por un proveedor

legítimo, logrando acceso (third-party impersonation, ataque de suplantación en la cadena).

- **Riesgo Legal y de Cumplimiento:** Aquí consideramos el potencial de que la relación con un tercero derive en **incumplimientos legales o regulatorios** para tu organización, o en conflictos contractuales. Por ejemplo, si tu proveedor de servicios de pago no cumple con PCI-DSS y ocurre un fraude, tú podrías ser sancionado por las entidades de pago. O si un proveedor maneja datos personales de tus clientes y no sigue las obligaciones de GDPR/CCPA, es tu empresa la que enfrentará multas o demandas. También entra el riesgo contractual: ¿y si el tercero vulnera propiedad intelectual de un tercero y te involucra en una disputa? ¿O si de repente el proveedor incumple un acuerdo de nivel de servicio crítico y causa penalizaciones en tu operación? Un caso real de riesgo legal fue cuando el **proveedor de chat de Ticketmaster** fue hackeado: las autoridades determinaron que Ticketmaster no había hecho la "debida diligencia" en seguridad y eso violó GDPR, resultando en la multa mencionada. La **responsabilidad solidaria** es un concepto clave, muchas leyes asumen que tu empresa es responsable por lo que hagan tus contratistas en el marco del servicio. Para gestionar este riesgo se aplican controles como: rigor en los contratos (cláusulas de indemnidad, cumplimiento normativo, derecho a auditorías), verificación de certificaciones (¿el proveedor tiene ISO 27001, SOC 2, está auditado?), compliance compartido (por ejemplo, exigir que terceros que tratan datos tuyos firmen acuerdos de procesamiento de datos y pasen evaluaciones de privacidad), y monitoreo de cambios regulatorios que puedan afectar la relación (por ejemplo, nuevas leyes que obliguen a evaluar a proveedores en ciertas áreas como ESG, sustainability o sanciones internacionales).

- **Riesgo Operativo:** Aquel que se manifiesta en **disrupciones o fallos en las operaciones** debido a problemas con un tercero. Aquí pensamos en continuidad del negocio, calidad del servicio y dependencia. Si un proveedor crítico **falla en entregar su servicio** (ya sea por un incidente técnico,



desastre natural, huelga, quiebra financiera o incluso incompetencia), tu organización puede quedar tambaleando. Ejemplos: la caída de un proveedor cloud que deja inoperativas tus aplicaciones (downtime prolongado); un proveedor logístico que no entrega materiales claves a tiempo, deteniendo tu producción; o un proveedor de servicios gestionados de TI cuyo error borra datos importantes. Un incidente ilustrativo fue el ataque a Kaseya: aunque fue cibernético en origen, su consecuencia principal para muchas empresas fue **operativa,** cientos de supermercados sin poder operar, escuelas desconectadas, etc. De hecho, en encuestas, **el impacto operativo suele ser el más reportado en incidentes de terceros (afectando al 84% de organizaciones con casos).** La gestión de este riesgo implica asegurarse de que los terceros tengan resiliencia (planes de contingencia, redundancias), diversificar proveedores para evitar puntos únicos de falla, y preparar planes de continuidad internos en caso de caída de un proveedor (por ejemplo, tener inventarios de emergencia, planes manuales de respaldo, backups de datos fuera del entorno del proveedor, etc.). También abarca el riesgo de concentración: si toda una industria depende de un mismo proveedor y éste cae, el impacto es sistémico. (Por ejemplo, una hipotética caída global de un

gran proveedor de certificación de seguridad o de DNS podría afectar a miles a la vez). Las autoridades están muy atentas a esto, especialmente en finanzas – de ahí medidas como las de DORA para supervisar concentración de riesgo en tecnología.

- **Riesgo Reputacional:** En el mundo hiperconectado, **la reputación de tu empresa está vinculada a la de tus socios.** Si un tercero comete un error o sufre un escándalo, las miradas también se posan en ti por asociación. Un clásico son las brechas de datos: los titulares de prensa muchas veces nombran a la empresa principal afectada, no al proveedor detrás de la filtración. Por ejemplo, los clientes de Amazon leyeron que “Amazon sufre filtración de datos de empleados”, aunque técnicamente el incidente ocurrió en sistemas de su proveedor

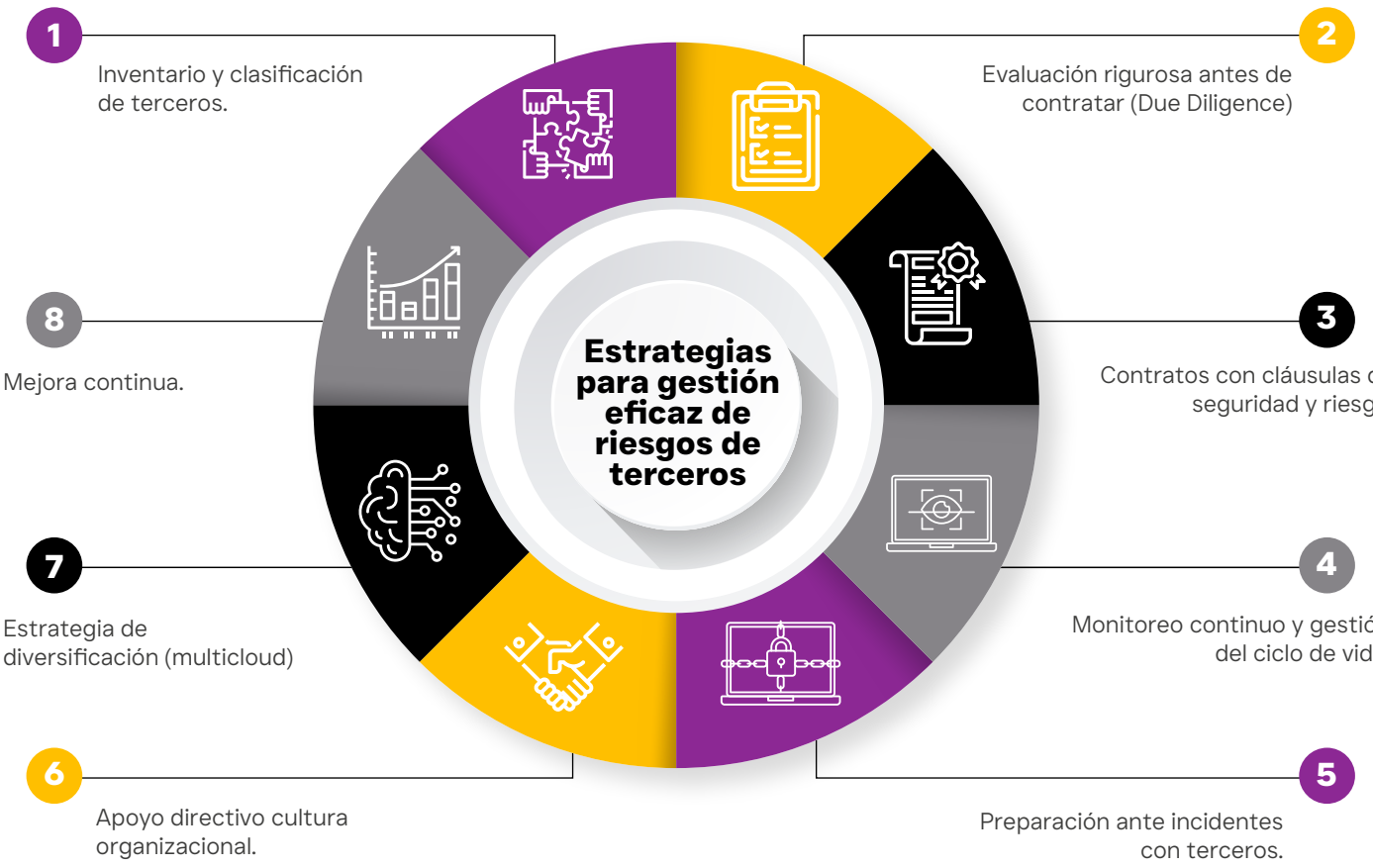
de gestión inmobiliaria a través de MOVEit. A ojos del público, Amazon fue víctima (y quizás descuidada en confiar en ese proveedor). Lo mismo con incidentes como el de Target en 2013 (brecha masiva vía un proveedor de HVAC), la marca principal es la que sufre el golpe reputacional y la pérdida de confianza.

Otro ámbito reputacional es el **ético/social:** si uno de tus proveedores es involucrado en prácticas cuestionables (trabajo infantil, corrupción, daño ambiental), tu empresa puede enfrentar críticas, boicots o requerimientos de esclarecimiento. En la era de la responsabilidad social corporativa, los stakeholders esperan que las empresas **extiendan sus valores y políticas éticas a su cadena de suministro.** Gestionar el riesgo reputacional implica: due diligence no solo en ciber, sino en prácticas de negocio del proveedor; imponer códigos de conducta para terceros; vigilancia de noticias que involucren a tus proveedores; y tener planes de respuesta comunicacional. Cuando algo ocurre, aunque sea totalmente ajeno a tu hacer, necesitas demostrar proactividad ("estamos investigando el incidente de nuestro proveedor X y apoyándolos para proteger a nuestros clientes..."). Vale señalar que un **59% de organizaciones reportó daño reputacional tras un incidente con terceros,** lo que confirma que es una dimensión muy real. La confianza de clientes y socios puede verse mermada si perciben que tu control sobre tu ecosistema es débil.

Estas categorías de riesgo, por supuesto, están interrelacionadas. Un solo evento puede tocar todas a la vez, imaginemos que tu proveedor de hosting sufre un hackeo (riesgo cibernético), exponiendo datos personales de clientes (riesgo legal GDPR, daño reputacional) y dejando tu web caída un par de días (riesgo operativo). Es un combo nada envidiable. Sin embargo, separar los tipos de riesgo ayuda a no **dejar cabos sueltos** al diseñar tu estrategia de TPRM. Debes preguntarte en cada relación, ¿qué puede salir mal en lo técnico? ¿y en lo legal? ¿y si dejan de dar servicio? ¿y si su imagen me salpica? Las respuestas permitirán definir controles específicos para cada frente.

A continuación, pasamos de la teoría a la práctica: ¿qué pasos concretos puedes tomar para robustecer tu gestión de riesgos de terceros y dormir más tranquilo?

Estrategias y mejores prácticas para un programa TPRM eficaz



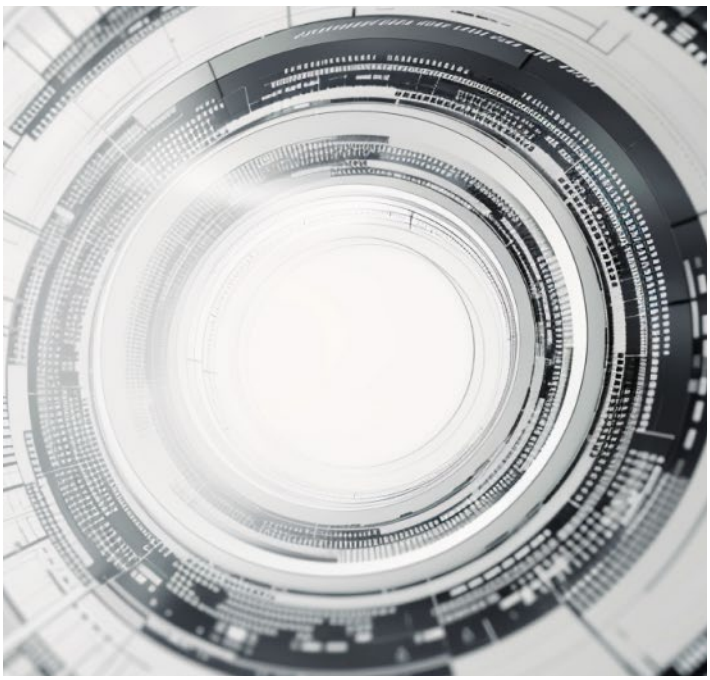
Diseñar e implementar un programa efectivo de **Third-Party Risk Management** puede parecer abrumador dada la amplitud del tema, pero se puede abordar de forma estructurada. A continuación, presentamos recomendaciones prácticas (a modo de pasos o componentes clave) que han demostrado ser exitosas en organizaciones líderes. Estas buenas prácticas te ayudarán a **anticiparte a los riesgos de terceros** y a responder con agilidad cuando surjan problemas:

1. **Inventario completo de terceros y clasificación por criticidad:** No se puede gestionar lo que no se conoce. El primer paso es construir (y mantener) un **inventario centralizado de todos los terceros** con los que tu organización tiene relación. Incluye proveedores de tecnología, servicios profesionales, consultorías, outsourcing, SaaS, proveedores de datos, etc. Para cada uno, identifica qué tipo de servicios provee y qué activos o procesos de tu

empresa impacta. Luego, clasifícalos por **nivel de riesgo o criticidad.** Por ejemplo, un proveedor que maneja información sensible o que soporta una función de negocio crítica será "Alta criticidad", mientras que un proveedor de bajo impacto operativo será "Baja criticidad". Criterios típicos como volumen y sensibilidad de datos accesibles, conectividad a tus sistemas, facilidad de reemplazo, cumplimiento regulatorio asociado, etc. Esta segmentación te permitirá enfocar recursos donde más importa (los terceros críticos requieren evaluaciones y monitoreo más profundos, mientras que a los de bajo riesgo quizá baste con controles estándar). Muchas organizaciones establecen 3 o 4 niveles de riesgo de proveedores (Alto, Medio, Bajo, Insignificante).

2. **Diligencia debida (due diligencie) rigurosa en la incorporación (onboarding):** Antes de contratar o renovar un tercero especialmente si es crítico realiza una **evaluación exhaustiva de sus riesgos.** Esto normalmente implica enviar un **cuestionario de seguridad y cumplimiento** adaptado al servicio (ej.: si manejará datos, incluir secciones de protección de datos; si es cloud, secciones de seguridad cloud; etc.), solicitar evidencias (certificaciones, informes de pruebas de penetración, resultados de auditorías, ISO 27001, PCI, según corresponda), y llevar a cabo evaluaciones adicionales según el caso (por ejemplo, scans de vulnerabilidades externas, revisar sus políticas de continuidad de negocio, o incluso visitas in situ para proveedores muy críticos). Involucra a las áreas relevante TI/Ciberseguridad evaluando controles técnicos, Legal revisando contratos y cumplimiento normativo, Compliance/regulatorio si aplica, Finanzas verificando solvencia (no olvidemos el riesgo financiero, un proveedor al borde de la quiebra es un riesgo operativo). Tras la due diligence, asigna un perfil de riesgo al proveedor (por ejemplo: "Proveedor X – riesgo medio con hallazgos en cifrado mejorable y planes de mejora acordados").

Importante: si la evaluación revela **brechas inaceptables,** debes considerar planes de mitigación antes de firmar (ej.: exigir que subsane ciertos hallazgos, o implementar controles compensatorios). En casos extremos, estar dispuesto a **no**



contratar a un proveedor que no alcance tus estándares mínimos de seguridad, por muy atractivo que sea en precio o funcionalidades recuerda que “lo barato puede salir caro” en términos de riesgo.

3. **Contratos sólidos con cláusulas de riesgo y seguridad:** El contrato es tu red de protección legal y operativa. Asegúrate de incluir cláusulas que obliguen al tercero a **mantener ciertos niveles de seguridad y gestión de riesgos.** Puntos clave a contemplar:

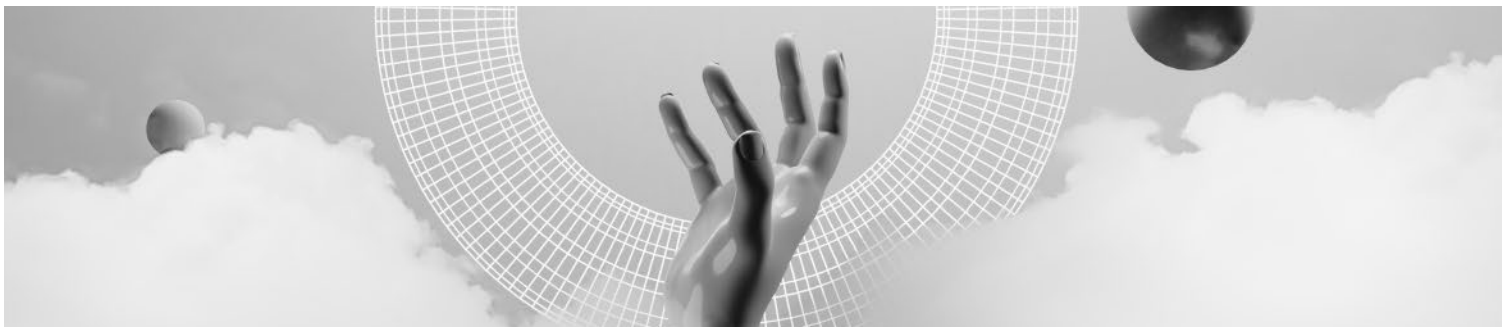
- **Requisitos de seguridad:** por ejemplo, cumplimiento de estándares (ISO 27001, OWASP, etc.), cifrado de datos, controles de acceso, segregación de entornos, etc., según la naturaleza del servicio.

- **Derecho a auditar/monitorizar:** reserva el derecho de realizar auditorías de seguridad o pedir evidencias periódicas de controles. Si el proveedor considera esto invasivo, acuerden al menos entrega anual de reportes de seguridad independientes.

- **Notificación de incidentes:** cláusula de breach notification que obligue al proveedor a informarte de **inmediato (p. ej. en <24 horas)** si sufre cualquier incidente que pueda afectar tu información o servicios. Esto es crítico para que puedas cumplir tus propias obligaciones (ej. notificar a reguladores en 72h bajo GDPR, coordinar respuesta, informar clientes si hace falta).
- **Subcontratación:** exige aprobación o notificación si el proveedor subcontrata parte del servicio a otros (cuartas partes). Debe extender las obligaciones de seguridad a esos subcontratistas.

- **Niveles de servicio (SLA) y continuidad:** define métricas de disponibilidad, tiempos de recuperación ante desastres, backups, etc., y penalizaciones si no se cumplen. Así mismo, pide que tengan un plan de continuidad del negocio y pruebas periódicas.

- **Responsabilidad e indemnización:** establece claramente la responsabilidad del proveedor en caso de incidentes causados por él, incluyendo coberturas de seguro ciber



si aplica, e indemnizaciones por daños (aunque la responsabilidad nunca puede tercerizarse del todo, al menos hay respaldo financiero y compromiso).

- **Terminación y restitución:** condiciones para terminar la relación si hay incumplimientos graves de seguridad, y procedimientos para retorno o destrucción segura de la información al finalizar el contrato. Estas cláusulas, negociadas con apoyo del equipo legal, alinean incentivos y dejan claro al proveedor que l**a seguridad** no es opcional. También educan al proveedor sobre tus expectativas. En sectores regulados, muchas de estas cláusulas ya son estándar.

4. **Monitoreo continuo y gestión del ciclo de vida:** No “guardes en un cajón” la evaluación inicial; la relación con un tercero es dinámica y evoluciona. Implementa un proceso de seguimiento periódico acorde al riesgo del proveedor:

- **Para proveedores críticos o de alto riesgo:** evalúa su seguridad **al menos una vez al año** (o incluso de forma continua con herramientas automáticas). Esto puede incluir reenviar cuestionarios actualizados, revisar nuevos informes de auditoría, o usar servicios de vigilancia que te alerten de brechas o cambios (como las calificaciones de seguridad mencionadas antes).

- **Para proveedores medios:** quizá un ciclo bianual o cada 2-3 años, complementado con monitoreo pasivo (p. ej., estar suscrito a boletines de seguridad de esos proveedores).

- **Para proveedores bajos:** mantener registro de ellos, pero con re-evaluaciones más ligeras, a menos que cambie algo (por ejemplo, si de pronto empiezan a manejar datos más sensibles).

- **Gestión de cambios:** muy importante, establece un mecanismo interno para ser notificado si un área de negocio planea ampliar el alcance de un proveedor (ej.: darle acceso a nuevos sistemas) o contratar uno nuevo. Esto debe disparar, según corresponda, una re-evaluación. Integrarse con procesos de compras o TI (por ejemplo, que no se pueda dar de alta un usuario de un

proveedor en tus sistemas sin aprobación de riesgo) ayuda a no perder visibilidad.

- **Indicadores clave de riesgo (KRI):** define algunos KRI para terceros y revísalos trimestralmente. Por ejemplo, % de proveedores críticos con evaluaciones vencidas, número de incidentes de seguridad relacionados con terceros ocurridos, número de hallazgos críticos abiertos en proveedores, etc. Si alguno se vuelve rojo, tomas acción (más recursos, escalamiento, etc.).

- **Relación y colaboración:** cultivar una comunicación fluida con el proveedor. Tener contactos designados de seguridad en ambos lados. Reuniones periódicas (ej. comités de seguimiento trimestrales con proveedores estratégicos) para discutir no solo desempeño, sino también temas de riesgo, mejoras, novedades (p. ej., “estimado proveedor, ¿han tenido incidentes recientes?, ¿han implementado esa autenticación multifactor que discutimos?”). Un proveedor bien gestionado debe casi verse como una extensión de tu equipo en mentalidad de seguridad.

5. **Preparación para incidentes con terceros:** Asume que, tarde o temprano, algo ocurrirá. Prepara planes de respuesta a incidentes que incluyan a terceros. Algunos consejos:

- **Mapa de decisiones:** documenta cómo evaluar rápidamente si un incidente en un tercero te afecta y en qué medida (¿qué datos o sistemas tuyos están con ese proveedor?). Ten identificados los contactos de emergencia del proveedor.

- **Simulacros:** realiza ejercicios de table-top donde simules, por ejemplo, que tu proveedor de RRHH fue hackeado. ¿Cómo te enteras? ¿Qué haces? Practica la coordinación de comunicación: ¿quién notifica a quién (proveedor a ti, tú a ellos, ambos a clientes)? Esto expone brechas en la preparación.

- **Plan de comunicación:** si un incidente de un tercero impacta a tus clientes o stakeholders, ten preparada una estrategia de comunicación transparente y proactiva. Que no te pase como a organizaciones que tardaron días en reconocer “sí,

nuestro proveedor X tuvo un incidente y comprometió datos de nuestros usuarios". Mejor liderar con el ejemplo: informar rápido, con hechos y con empatía hacia quienes pudieran verse afectados.

- **Soporte mutuo:** coordina de antemano con cada proveedor crítico cómo se asistirán mutuamente en caso de incidente. Ej.: si el proveedor sufre ransomware, ¿cómo te entregará data de backup para que puedas operar por tu cuenta? O al revés, si tú tienes un incidente, ¿cómo el proveedor lo manejará para proteger tu información en sus sistemas?

5. **Apoyo de la alta** dirección y cultura de riesgos: Un programa TPRM solo prosperará si cuenta con respaldo desde dirección y con una cultura corporativa que lo entienda. Educa a la alta dirección con reportes claros del estado de riesgos de terceros (como mencionamos, incluyendo esto en comités de riesgo). Asegura presupuesto para las herramientas y personal necesarios haciéndoles ver el ROI en prevención de incidentes multimillonarios. Por otro lado, sensibiliza a las áreas de negocio, muchos usuarios internos pueden sentirse frustrados por "trámites" adicionales al querer contratar un nuevo servicio. Explícales por qué es crucial (por ejemplo, comparte historias de incidentes reales en la industria). Incorpora la gestión de terceros en las políticas de la empresa (política de seguridad de la información, código de conducta de proveedores, etc.), de modo que quede institucionalizado.

7. **Considera la multicloud y estrategia de diversificación:** Si tu empresa depende fuertemente de proveedores cloud o SaaS, evalúa una estrategia multicloud o de contingencia. Esto no significa duplicar todo por duplicar, sino analizar si vale la pena tener proveedores alternativos en espera para ciertas funciones. Por ejemplo, si usas un solo CDN global, tal vez planear cómo migrar a otro rápidamente si el primero falla. O si tienes todo en un único hiper-escalador de nube, identificar aplicaciones críticas que podrían moverse a otra nube si ocurre una caída severa prolongada en la principal. Esto es parte de TPRM porque esencialmente es gestionar

riesgo de concentración. La resiliencia a veces viene de no poner todos los huevos en la misma canasta de proveedor. Sin embargo, la multicloud también añade complejidad (más proveedores que gestionar), así que encuentra el equilibrio según tu apetito de riesgo.

8. **Mejora continua:** El panorama de riesgo de terceros no es estático, y tu programa tampoco debe serlo. Realiza **evaluaciones periódicas de la madurez de tu TPRM** (hay marcos de evaluación de madurez que puedes usar, o contrata una revisión independiente). Incorpora las lecciones aprendidas de cualquier incidente o casi-incidente ¿falló algo en el proceso? ¿se escapó evaluar algo? Actualiza tus cuestionarios, tus criterios, tus contratos modelo, etc., con base en lo que vas aprendiendo. Mantente al tanto de las mejores prácticas de la industria, foros de CISOs, publicaciones especializadas, incluso benchmarks que indican qué están haciendo los líderes (por ejemplo, si ves que muchas empresas comienzan a evaluar a los cuartos y quintos proveedores, quizá debas sumarlo a tu alcance). La gestión de riesgos de terceros es un proceso de ciclo de vida, no un proyecto con fin definido.

Aplicando estas medidas, irás construyendo una postura robusta frente al riesgo de proveedores. No significa riesgo cero nada puede garantizarlo, pero sí significa que podrás

dormir más tranquilo sabiendo que tienes identificados los puntos débiles, que estás encima de ellos, y que cuando ocurra algo inesperado (porque ocurrirá), tendrás planes listos para reaccionar rápida y eficazmente.

El futuro de TPRM: entornos multicloud e IA generativa

Mirando hacia adelante, el entorno de terceros seguirá **evolucionando e incrementando su complejidad.** Dos tendencias despuntan en el horizonte inmediato de los CISOs y líderes de riesgo, la adopción de arquitecturas multicloud/distribuidas y la irrupción de proveedores de inteligencia artificial generativa en las operaciones empresariales. ¿Qué desafíos y consideraciones trae esto para TPRM?

- **Entornos multicloud e infraestructura distribuida:** Muchas organizaciones están migrando hacia estrategias multicloud, ya sea para evitar dependencia de un solo proveedor, por costos, capacidades específicas o para estar más cerca de sus clientes geográficamente. También proliferan las arquitecturas compuestas de múltiples servicios as-a-service, microservicios de distintos proveedores y cadenas de API interconectadas. Desde la perspectiva de riesgos, esto significa que el número de terceros claves podría **aumentar aún más,** y la interdependencia entre ellos vuelve más difusa la frontera de quién es responsable de qué. Un posible riesgo es la **complejidad en la gestión,** manejar seguridad consistente en diversos entorno (AWS, Azure, GCP, proveedores locales) puede dificultar
- la supervisión. Además, crece el riesgo de **errores de configuración en la integración** entre nubes o servicios distintos. Un caso hipotético es el de una compañía que usa la nube A para sus datos y la nube B para sus aplicaciones; un fallo en la conexión segura entre ambas podría exponer datos, y ¿de quién es la culpa, del cliente o de alguno de los proveedores? Asimismo, el riesgo de **fallos globales o sectoriales** existe, hemos visto grandes outages de nubes que tumban servicios populares. Si bien distribuir en multicloud puede mitigar ese riesgo, también puede introducir concentration risk de otra forma algunas soluciones de seguridad (por ejemplo, un SIEM central, o un CASB) se vuelven “terceros críticos” transversales; si esas soluciones fallan, podrían impactar todas tus nubes a la vez. ¿Qué hacer? El futuro de TPRM en multicloud exigirá **orquestación:** herramientas que den visibilidad unificada de la postura de seguridad en todos los proveedores, políticas de seguridad unificadas (por ejemplo mediante infraestructura como código), y acuerdos claros con cada cloud sobre soporte en incidentes. También cobra fuerza el concepto de “**Chaos engineering”** aplicado a proveedores probar periódicamente qué pasa si cierto proveedor cae (simular cortes) para robustecer la tolerancia a fallos. En resumen, multicloud no elimina la importancia de TPRM, al contrario, la multiplica, habrá que realizar risk management a nivel de cada proveedor cloud y también del entramado completo.

- **Proveedores de IA generativa y nuevos riesgos digitales:** La explosión de la IA generativa (ChatGPT, GPT-4, Bard, servicios de coding AI, etc.) ha dado lugar a una nueva clase de proveedores tecnológicos. Muchas empresas están integrando estos servicios en sus productos o flujos de trabajo, usando una API de GPT para generar respuestas automatizadas, o alimentando modelos con datos internos para obtener análisis. Esto abre oportunidades enormes, pero también riesgos relativamente nuevos que el TPRM debe contemplar. Por un lado, está el **riesgo de datos,** es decir cuando usas un servicio de IA externa, es probable que estés enviando datos hacia ese modelo. ¿Cómo se almacenan? ¿Formarán parte del entrenamiento general de la IA (potencial fuga)? Un error famoso ocurrió en Samsung, donde ingenieros introdujeron código propietario en ChatGPT y esa información acabó almacenada en servidores de OpenAI, generando preocupación por posible exposición. Samsung tuvo que restringir el uso de la herramienta para evitar un incidente mayor. Este ejemplo subraya que debemos **evaluar las políticas de manejo de datos de los proveedores de IA:** ¿retienen tus prompts? ¿los comparten? Muchos están implementando opciones de opt-out para no guardar datos de clientes, pero no es universal.

  Otro aspecto es el **riesgo de desinformación o decisiones incorrectas,** si dependes de una IA para análisis, ¿qué pasa si genera un resultado erróneo o sesgado? Podría llevar a errores operativos o incluso implicaciones legales (imaginemos asesoría médica o financiera dada por IA equivocada). Podríamos pensar “eso no es un riesgo de **terceros,** es riesgo tecnológico general”, sin embargo, el hecho de que el **modelo es un tercero** fuera de tu control lo convierte en parte de TPRM. **La opacidad de los algoritmos** es un tema a diferencia de un software tradicional, con la IA es más difícil obtener certificaciones de qué hace o cómo protege información. Por otro lado, está el **riesgo ciber directo:** ¿qué tal si alguien compromete la IA en sí? Un ataque a la cadena de suministro de IA (por ejemplo, “envenenar” el modelo con datos malignos, o hackear el servicio

de un proveedor de IA para manipular respuestas) podría afectar simultáneamente a muchas empresas usuarias. Pensemos en phishing mejorado, un proveedor de correo que integra IA para filtro antispam fue comprometido, y su modelo manipulado para dejar pasar ciertos mails maliciosos. Los escenarios son nuevos y aún teóricos, pero posibles. Entonces, ¿cómo prepararse?

1. **Incluir a los servicios de IA en tu inventario de terceros** (no olvidarse de evaluarlos solo porque “es algo experimental” si procesa información de tu empresa, cuenta como tercero).
2. **Actualizar tus evaluaciones de riesgo** para cubrir aspectos de IA: preguntar por política de datos, seguridad del modelo, donde se alojan, cumplimiento de marcos emergentes.
3. **Educar a los usuarios internos:** si desarrolladores o analistas van a usar herramientas de IA, pautar qué se puede y qué no se puede subir a estas plataformas (para evitar filtraciones accidentales).

4. Seguir de cerca las **mejores prácticas de “AI Risk Management”.** Firmas como PwC, McKinsey y otras ya publican guías sobre gobernanza de IA. Ver cómo encajan con tu modelo de TPRM será crucial.

5. Reconocer que la **IA también puede ser aliada en TPRM** (como ya discutimos), en el futuro, es muy posible que tu programa de riesgos tenga asistentes de IA que automaticen buena parte del monitoreo y análisis. Será un poco una carrera armamentista usando IA para gestionar riesgos de proveedores que usan IA.

En esencia, el futuro traerá **más interconexión y más velocidad,** pero también herramientas más avanzadas para enfrentarlo. Las organizaciones deben estar preparadas para un **TPRM 2.0,** donde manejarán un ecosistema diverso, desde su proveedor de nube, pasando por la startup de IA que provee un algoritmo crucial, hasta quizás alianzas de intercambio de datos con

terceros. La ciberseguridad en este contexto será tan fuerte como el eslabón más débil (que puede ser una persona, un procedimiento o un tercero descuidado).

Al final del día, gestionar riesgos de terceros se trata de **conocer con quién te estás "jugando los cuartos",** exigirles el nivel de seguridad y resiliencia que esperas de ti mismo, y mantener una vigilancia constante sin caer en la complacencia. La pregunta final que debes hacerte como CISO o responsable de riesgos es: "¿Estamos realmente preparados para evaluar y gestionar los riesgos ocultos que suponen miles de conexiones con proveedores digitales en un entorno donde el eslabón más débil sigue siendo humano?".

Bibliografía

Bonnie, E. (12 de 09 de 2024). secureframe. Obtenido de Más de 99 estadísticas y tendencias esenciales sobre riesgos de terceros para 2024: https://secureframe.com/es-es/blog/third-party-risk-statistics

Dembosky, L., Feigelson, J., Gesser, A., & Garrett, R. M. (24 de 11 de 2020). Debevoise & Plimpton. Obtenido de Para las empresas sujetas al RGPD: cinco conclusiones sobre ciberseguridad derivadas de la multa de la ICO a Ticketmaster: https://www.debevoisedatablog.com/2020/11/24/ico-ticketmaster-fine/#:~:text=1,%E2%80%9D

Diaroti. (30 de 08 de 2021). Obtenido de Investigadores de seguridad describen el fallo de Azure Cosmos como “la peor vulnerabilidad en la nube que se pueda imaginar”.: https://diarioti.com/fallo-en-microsoft-azure-expuso-miles-de-bases-de-datos-de-clientes/117346#:~:text=Investigadores%20de%20seguridad%20describen%20el,nube%20que%20se%20pueda%20imaginar%E2%80%9D

Fortinet. (s.f.). Fortinet . Obtenido de Ciberataque SolarWinds: Una descripción general: https://www.fortinet.com/lat/resources/cyberglossary/solarwinds-cyber-attack#:~:text=resultado%20del%20ataque%2C%20m%C3%A1s%20de,luego%20espiar%20a%20otras%20organizaciones

Garther. (s.f.). Garther. Obtenido de Gestión de riesgos de terceros (TPRM): una guía esencial: https://www.gartner.com/en/legal-compliance/topics/third-party-risk-management-tprm#:~:text=Third,to%20federated%20or%20centralized%20models

IBM. (s.f.). IBM. Obtenido de Informe sobre el coste de una filtración de datos (2024): https://www.ibm.com/reports/data-breach#:~:text=USD%204,of%20breaches%20that%20involved

Infobae, N. (26 de 12 de 2024). Infobae. Obtenido de Amazon confirma el robo de más de 2,8 millones de líneas de datos de sus empleados tras el hackeo de MOVEit Transfer: https://www.infobae.com/america/agencias/2024/11/12/amazon-confirma-el-robo-de-mas-de-28-millones-de-lineas-de-datos-de-sus-empleados-tras-el-hackeo-de-moveit-transfer/#:~:text=Amazon%20ha%20confirmado%20el%20robo,sus%20proveedores%20externos%2C%20MOVEit%

McCowan, S., Watson, C., & Lehanka, K. (02 de 08 de 2024). EY. Obtenido de Cómo reinventar su programa TPRM con GenAI y operaciones escalables: https://www.ey.com/en_us/cro-risk/reimagine-your-tprm-program#:~:text=Reimagine%20your%20TPRM%20program%20,time

ORCA, E. d. (19 de 06 de 2024). ORCA. Obtenido de Gestión de riesgos de terceros en la banca: un panorama en evolución: https://blog.orcagrc.com/gesti%C3%B3n-riesgos-terceros-banca-panorama-evoluci%C3%B3n#:~:text=En%20un%20informe%20reciente%20del,una%20organizaci%C3%B3n%20tiene%205800%20proveedores

Orizábal, D. (s.f.). pwc. Obtenido de Gestión de los riesgos de la IA generativa : https://www.pwc.com/ia/es/Issues/agenda-de-liderazgo/Efecto-Tecnologico/IA-Analitica/Gestion-de-los-riesgos-de-la-IA-generativa.html#:~:text=Gesti%C3%B3n%20de%20los%20riesgos%20de,Si%20no%20se%20utiliza

Reuters. (06 de 07 de 2021). El Economista. Obtenido de Ciberataque contra Kaseya afectó hasta 1,500 empresas: https://www.eleconomista.com.mx/empresas/Ciberataque-contra-Kaseya-afecto-hasta-1500-empresas--20210705-0076.html#:~:text=Entre%20800%20y%201%2C500%20empresas,el%20lunes%20su%20presidente%20ejecutivo

Sivsa. (02 de 08 de 2024). Obtenido de Incidentes de seguridad en la nube: cómo prevenirlos: https://www.sivsa.com/site/incidentes-de-seguridad-en-la-nube-como-prevenirlos/#:~:text=Incidentes%20de%20seguridad%20en%20la,errores%20de%20configuraci%C3%B3n%2C%20como

Srecker, R. (19 de 08 de 2024). ludwigadvisors. Obtenido de Centrarse en el riesgo de terceros y la IA generativa para mejorar la gestión del riesgo operativo: https://www.ludwigadvisors.com/content/focus-on-third-party-risk-and-generative-ai-to-improve-operational-risk-management#:~:text=,by%20its%20use%20within

Team, C. 4. (25 de 03 de 2024). Tarlogic. Obtenido de Los riesgos de usar IA generativa en las empresas: Protege tus secretos: https://www.tarlogic.com/es/blog/riesgos-usar-ia-generativa-empresas/#:~:text=%C2%BFQu%C3%A9%20suceder%C3%ADa%20si%20un%20actor,forma%20de%20incidente%20de%20seguridad

Torres, I. (23 de 02 de 2025). IVE Consultores . Obtenido de NIS2 y proveedores: ¿Cómo afecta la normativa a tu cadena de suministro?: https://iveconsultores.com/cadena-de-suministro-en-la-nis2/#:~:text=La%20NIS2%20obliga%20a%20las,proveedores%20y%20prestadores%20de%20servicios

CISO talk

Publicado en junio de 2026.