Gestión de Riesgos de Terceros en México

NovaSec GRC

ESTRATEGIAS PARA LA RESILIENCIA EN UN ENTORNO VOLÁTIL

Índice

1. Resumen Ejecutivo.

2. Introducción: ¿Por qué importa la gestión de terceros en México?

3. Contexto mexicano: regulación, sectorial y económico.

4. El Papel Estratégico de GRC en la Gestión de Riesgos de Terceros.

5. Estadísticas y Datos del Mercado (2025).

6. Principales Falencias en la Tercerización.

7. Riesgos Prioritarios con Terceros.

8. Casos de Estudio: Fallas Críticas en la Supervisión de Proveedores Críticos.

9. Buenas Prácticas de TPRM para Organizaciones Mexicanas.

10. Tendencias Futuras y Desafíos Emergentes.

11. Plan de Despliegue TPRM y Herramientas Ejecutivas

12. Conclusiones.

13. Glosario.

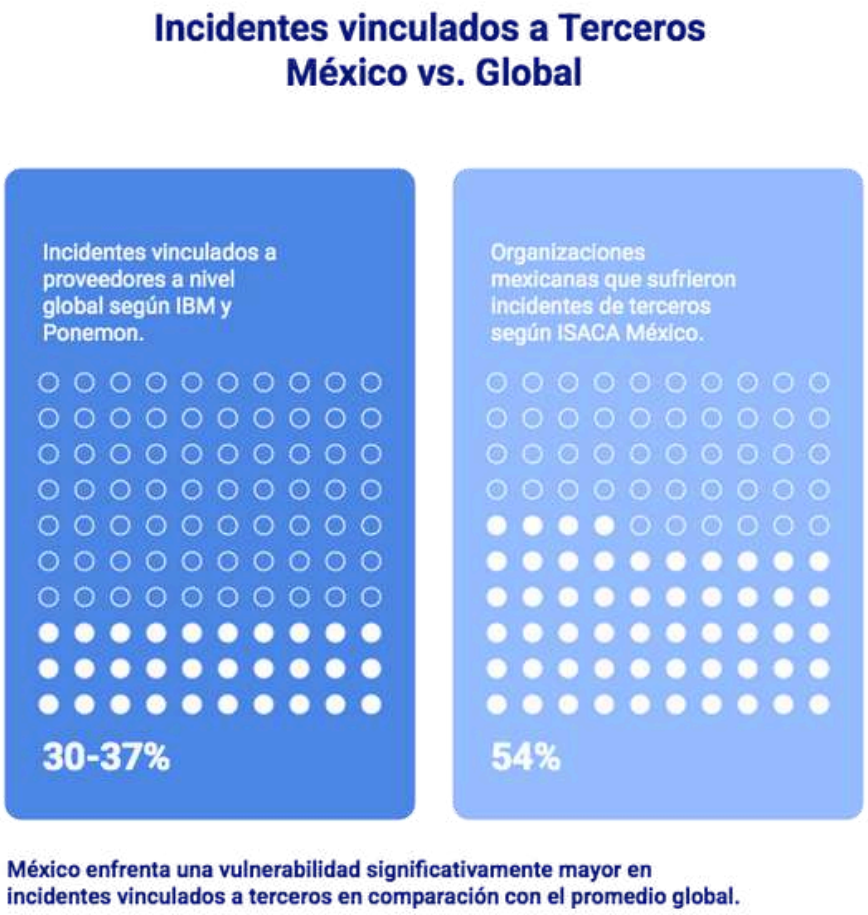
14. Referencias.

Resumen Ejecutivo

En un mundo cada vez más interconectado, donde la digitalización, la externalización y las cadenas de suministro extendidas se han vuelto normas y no la excepción, las organizaciones en México enfrentan un reto crítico: la gestión eficaz de los riesgos derivados de terceros (Third-Party Risk Management, TPRM).
Este whitepaper analiza en profundidad la situación mexicana regulación, sectores clave (financiero, seguros, servicios, tecnología, salud, retail, público) y particularidades locales e identifica por qué implementar un proceso formal de TPRM ya no es una opción, sino una imperativa estratégica.

Key Take-aways para la alta dirección:

Las brechas y los incidentes vinculados a terceros se encuentran en ascenso: Mientras que a nivel global los incidentes vinculados a proveedores oscilan entre el **30% y 37%** (según IBM y Ponemon), **México presenta un escenario crítico: el 54%** de las organizaciones nacionales ya ha sufrido un incidente originado por un tercero (ISACA México). Esta disparidad evidencia que, aunque la amenaza es mundial, la vulnerabilidad en el mercado mexicano es significativamente mayor.



● En México, el mercado de gestión de riesgo de cadena de suministro está creciendo con fuerza, impulsado por la transformación digital, el nearshoring y la necesidad de resiliencia.

● Muchas compañías mexicanas aún presentan debilidades estructurales: falta de visibilidad sobre su universo de terceros, procesos manuales, escasa gobernanza, poco uso de tecnología, lo que las deja vulnerables a sanciones regulatorias, interrupciones operativas y daño reputacional.

● Desde la normativa mexicana —Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP), la Ley Fintech, disposiciones de Comisión Nacional Bancaria y de Valores (CNBV) hasta cumplimiento derivado del Tratado entre México, Estados Unidos y Canadá (T-MEC) existe una presión creciente para que las organizaciones integren la evaluación, monitoreo y mitigación de riesgos de terceros como parte de su sistema de GRC (Gobierno, Riesgo y Cumplimiento).

● Para líderes de negocio, CISO, CRO y compliance officers se presenta una ventana de oportunidad: adoptar un marco integral adaptado al entorno mexicano puede reducir hasta un 40 % de los incidentes relacionados con terceros y reforzar la resiliencia operativa, financiera y reputacional.

Este documento presenta un análisis profundo, evidencia cuantitativa, buenas prácticas adaptadas, herramientas operativas (check-lists, plantillas simples) y una hoja de ruta para que las organizaciones en México transformen su gestión de terceros de reactiva a proactiva.

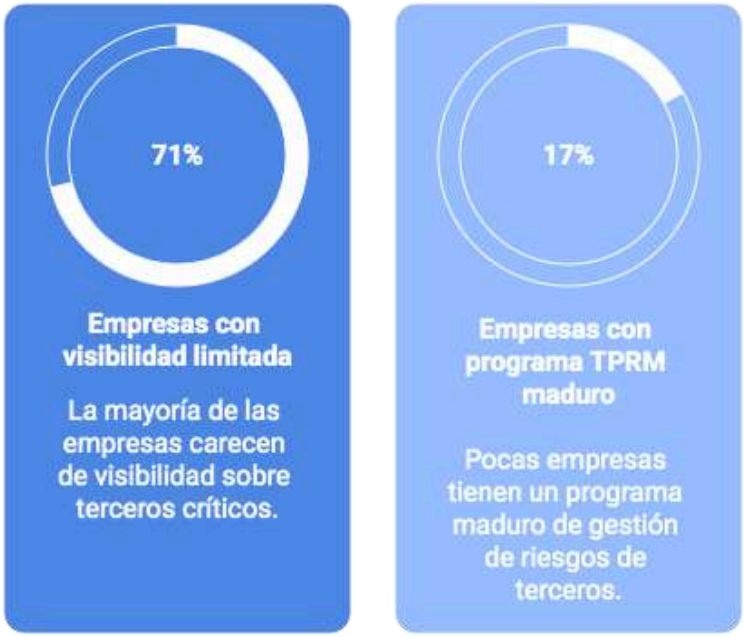
Introducción

Durante los últimos cinco años, México ha acelerado su proceso de transformación digital, impulsado inicialmente por la pandemia y posteriormente por la expansión del nearshoring bajo el T-MEC. Este escenario ha derivado en una rápida adopción de servicios externalizados: **el uso de proveedores cloud, BPO, ciberseguridad gestionada y servicios de data center creció más del 18% anual entre 2021 y 2024**, según estimaciones de IDC e INEGI. Sectores como **financiero, salud, retail, manufactura y tecnología** hoy dependen en gran medida de terceros para operar sus procesos críticos.

No obstante, esta adopción acelerada también incrementa la superficie de ataque y la complejidad operativa. **El 63% de los incidentes de ciberseguridad en 2024 involucró directa o indirectamente a un tercero**, de acuerdo con Deloitte LATAM, y **el 45% de las interrupciones operativas en México fueron atribuibles a fallas en proveedores**, según datos de UNAM e INEGI. Basta con considerar escenarios como una brecha de seguridad en un proveedor cloud que exponga datos regulados o la indisponibilidad de un subcontratista logístico que interrumpa la cadena de suministro: ambos representan impactos reputacionales, regulatorios y financieros significativos.

La volatilidad actual, incremento de las ciberamenazas, tensiones geopolíticas, inflación y cadenas de suministro altamente interdependientes exige que las organizaciones mexicanas abandonen modelos reactivos. **Hoy, el 71% de las empresas reconoce tener visibilidad limitada sobre sus terceros críticos**, y solamente **el 17% cuenta con un programa maduro de TPRM**, muy por debajo de estándares globales. México se posiciona **13° en riesgo de cadena de suministro en LATAM**, evidenciando una brecha estructural en gobierno, monitoreo y respuesta.

Visibilidad y Gestión de Terceros



Frente a este panorama, un **programa de TPRM formal, escalable y plenamente alineado con la regulación mexicana** (CNBV, Banco de México, Ley Fintech, NOM-151, Ley Federal de Protección de Datos Personales y estándares como ISO 27001, ISO 31000 e ISO 22301) deja de ser una buena práctica para convertirse en una condición habilitadora del negocio. Ya no basta con firmar contratos o evaluar proveedores una vez al año. La operación moderna exige:

- **Visibilidad completa del inventario de terceros y cuartos** .
- **Segmentación basada en riesgo operacional, tecnológico y regulatorio** .
- **Evaluaciones continuas, no sólo iniciales.**
- **Monitoreo en tiempo real de amenazas y desempeño** .
- **Métricas claras de cumplimiento, SLA/KPI y resiliencia.**
- **Modelos de respuesta coordinados ante incidentes provenientes de terceros.**

NovaSec GRC

La pregunta es crítica:

¿Está su organización preparada para enfrentar un ataque en la cadena de suministro o una interrupción provocada por un proveedor?

México experimenta ya **un crecimiento del 15% anual en tercerización post pandemia**, impulsado por el nearshoring y la demanda global de infraestructura digital. Sin embargo, el incremento de las dependencias externas no ha sido acompañado del desarrollo equivalente de capacidades de gestión de riesgos. De hecho, **el 58% de las empresas mantiene procesos manuales o poco estandarizados para evaluar a sus proveedores**, lo que genera brechas significativas en los tiempos de respuesta, la calidad de información y el cumplimiento regulatorio.

Este whitepaper, fundamentado en análisis de **INEGI, CNBV, Banco de México, Deloitte, Gartner y estudios académicos de la UNAM**, ofrece una visión integral sobre:

- El estado de madurez del TPRM en México en 2025.
- Riesgos y amenazas emergentes derivados del ecosistema de terceros.
- Datos y estadísticas que evidencian la urgencia de un modelo proactivo.
- Errores comunes en la implementación de programas de TPRM.
- Estrategias accionables para CROs, CISOs, CCOs y responsables de continuidad.
- Prácticas recomendadas para cumplir expectativas regulatorias y del mercado.

Entorno Regulatorio

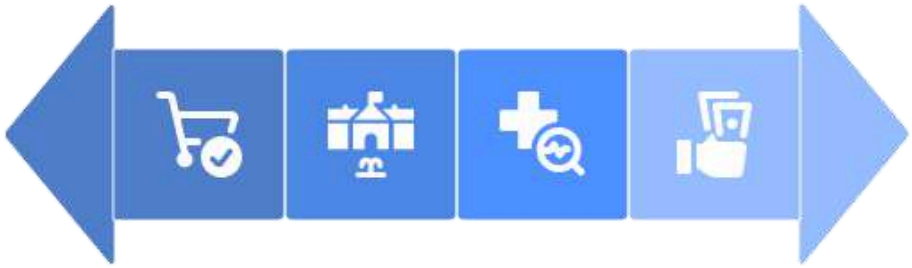
Regulación	Enfoque en TPRM	Ejemplos de controles
LFPDPPP	Protección de datos personales en relaciones con terceros; responsabilidades del responsable y del encargado	Medidas administrativas y técnicas; cláusulas contractuales de tratamiento; procedimientos ARCO; registros de transferencia
Ley Fintech	Requisitos de operación para plataformas y gestión de riesgos por proveedores externos	Controles operativos y de seguridad; auditorías periódicas; cláusulas de continuidad y restitución de servicios
Disposiciones CNBV	Supervisión prudencial y gobernanza para entidades financieras respecto a terceros	Due diligence, monitoreo continuo, pruebas de penetración y evaluación de proveedores críticos
INAI	Supervisión del derecho al acceso y protección de datos personales; transparencia y rendición de cuentas	Protocolos de atención a solicitudes ARCO; registro y evidencia de consentimientos; evaluaciones de impacto

Entorno económico y sectorial

- México ocupa una posición geográfica clave en los sectores de manufactura, logística, tecnología y servicios compartidos (nearshoring), lo que incrementa su exposición a riesgos de la cadena de suministro.
- El mercado mexicano de gestión de riesgos de la cadena de suministro muestra crecimiento, impulsado por la adopción de IA, la analítica y la diversificación de proveedores.

En sectores clave

- Financiero y seguros: elevada regulación y expectativas de resiliencia.
- Salud: protección de datos sensibles, cumplimiento de estándares internacionales.
- Retail y manufactura: cadenas globales, dependencia de terceros logísticos y tecnológicos.
- Sector público: aumento de la externalización de servicios digitales y necesidad de transparencia en los contratos.



Madurez del mercado mexicano

Aunque cada vez más organizaciones mexicanas están conscientes de la importancia del TPRM, existe un rezago estructural comparado con mercados maduros (EE.UU, Europa):

- Procesos manuales, falta de visibilidad de proveedores de 2.ª o 3.ª capa ("fourth party risk").
- Poca adopción de tecnologías de monitoreo continuo.
- Enfoque fragmentado entre compliance, TI y compras.
- Este rezago representa una brecha de competitividad y resiliencia para las organizaciones mexicanas.
- Roles GRC poco formalizados.
- Falta de gobierno corporativo sobre terceros.
- Segmentación limitada.
- Auditorías dispersas.

Conclusión de esta sección

El contexto mexicano **exige** que TPRM pase de ser una herramienta de compras a un pilar del GRC empresarial.

El Papel Estratégico de GRC en la Gestión de Riesgos de Terceros

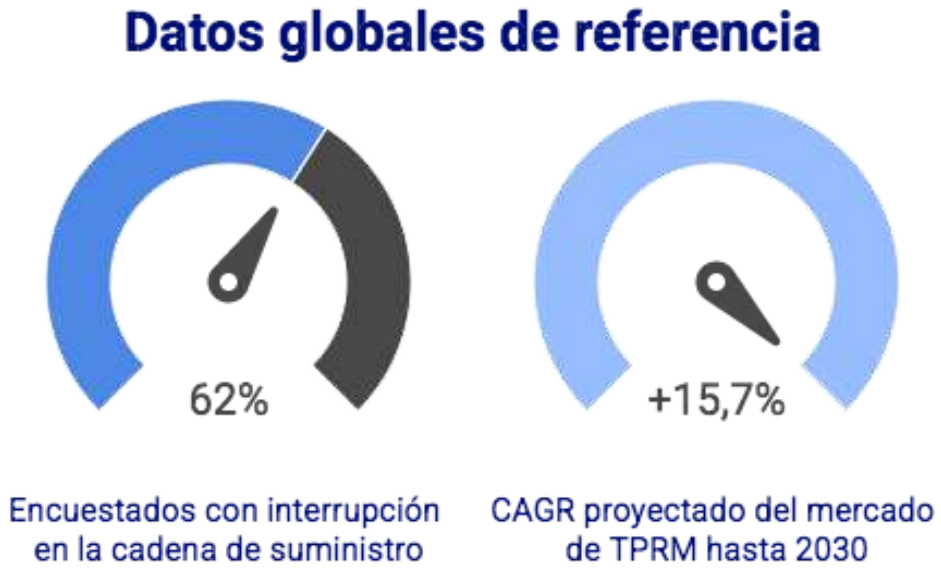
GRC (Gobierno, Riesgo y Cumplimiento) integra tres pilares fundamentales:

- **Gobierno** (Governance): Establece políticas, roles y responsabilidades claras para la toma de decisiones en las relaciones con terceros.
- **Riesgo (Risk)**: Identifica, evalúa y mitigar riesgos operativos, cibernéticos y reputacionales de manera proactiva.
- **Cumplimiento (Compliance):** Asegura la conformidad con las regulaciones mexicanas (LFPDPPP, CNBV, Ley Fintech) y los estándares internacionales (T-MEC, GDPR).

En TPRM, GRC actúa como marco unificador que evita silos, automatiza el monitoreo y genera reportes integrados. Las organizaciones con GRC maduro reducen brechas en un 40 % y multas en un 30 %. NovaSec GRC ejemplifica este enfoque al ofrecer módulos para autoevaluación de terceros, determinación de criticidad y planes de mitigación, transformando procesos manuales en sistemas automatizados y auditables.

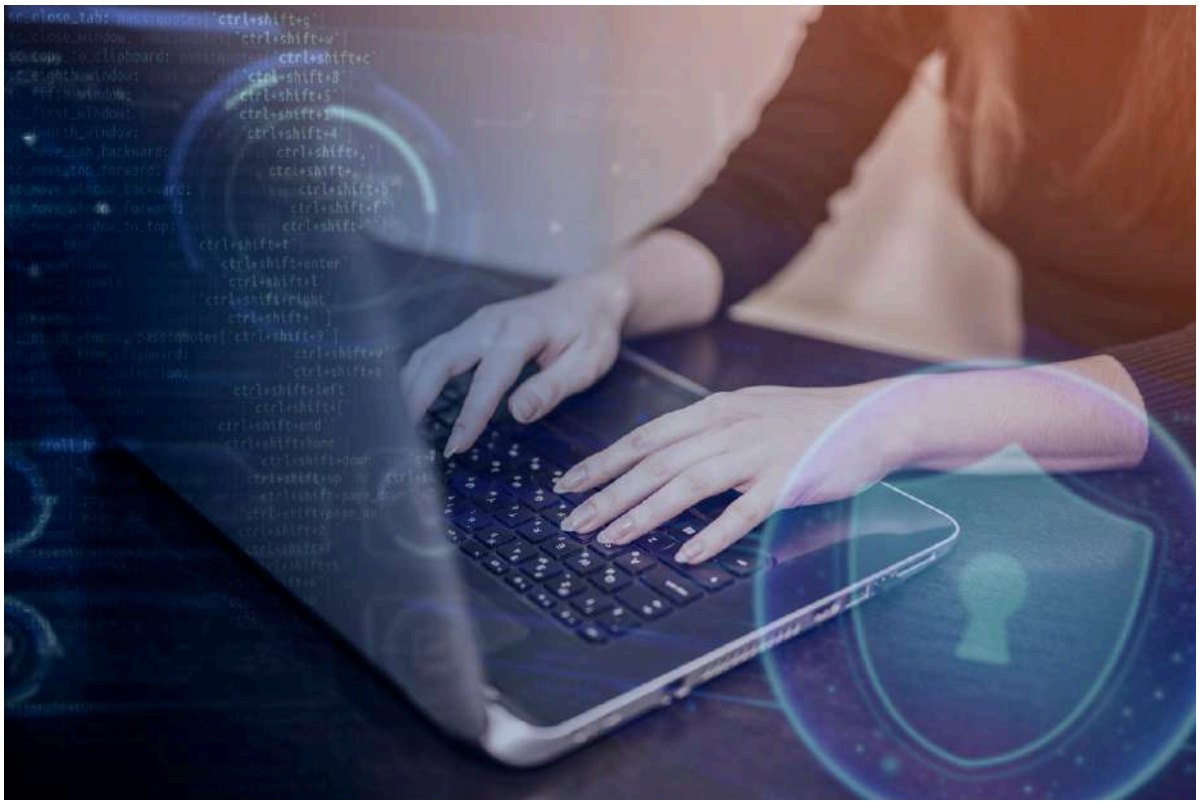
Estadísticas y Datos del Mercado
Datos globales de referencia

- En el reporte 2024 de Hyperproof, el 62 % de los encuestados sufrió una disrupción en la cadena de suministro por parte de terceros durante el último año cercano.
- Según la encuesta 2024 de RiskRecon, el riesgo de terceros ya no es solo cibernético: incluye reputación, cumplimiento, operatividad.
- A nivel global, el mercado de TPRM alcanzó aproximadamente USD 7,42 mil millones en 2023 y se proyecta que llegará a USD 20,59 mil millones para 2030 (CAGR ~15,7 %).



Datos específicos para México

- El informe de 6Wresearch señala que el mercado mexicano de gestión de riesgo de cadena de suministro está en expansión, con foco en la adopción de soluciones tecnológicas y la diversificación de proveedores.
- Sólo como referencia: el reporte indica crecimiento sostenido de 2024 a 2031 y un énfasis creciente en riesgos cibernéticos y de cumplimiento.
- Aunque no hay un dato público masivo que reporte el porcentaje exacto de brechas en México por terceros, según Reuters, México concentró más de la mitad de los ciberataques en Latinoamérica en la primera mitad de 2024 (31 mil millones de intentos).
- Según fuentes de monitoreo global, las organizaciones que experimentan una brecha por terceros enfrentan costos promedio superiores por ~40 % respecto a las que experimentan una brecha interna.



Análisis cuantitativo y proyección

Brechas de Terceros

Aproximadamente el 30% de las brechas de seguridad involucran a terceros. ¡Mantenlo en mente!

Costo Promedio

El costo promedio de una brecha de un tercero supera los USD 5 millones a nivel global. ¡Ojo con los regulados!

Mercado TPRM Global

El mercado global de TPRM crece a un ritmo de ~15.7% (2024-2030). ¡México debe seguir el ritmo!

Crecimiento en México

El crecimiento del mercado en México es pronunciado, especialmente en servicios, manufactura y tecnología.

Implementación TPRM

Hay baja visibilidad de métricas mexicanas. ¡Tenemos una oportunidad de liderar en TPRM!

Principales Falencias en la Tercerización

A continuación, se detallan las principales debilidades que afectan a las organizaciones mexicanas al trabajar con terceros:

Visibilidad limitada

- Muchas empresas mexicanas no tienen un inventario actualizado de sus proveedores críticos, y menos aún visibilidad de los sub proveedores (terceros de segunda o tercera capa).
- La segmentación de terceros por criticidad aún es incipiente: los proveedores que manejan datos sensibles o infraestructura clave no siempre se identifican adecuadamente.

Procesos manuales y fragmentados

- Las evaluaciones se apoyan en cuestionarios, hojas de cálculo (spreadsheets) y auditorías periódicas, sin integración tecnológica ni seguimiento continuo. A nivel global, se reporta que el 26 % de las organizaciones aún utiliza hojas de cálculo para TPRM.
- Falta de integración entre compras, TI, cumplimiento y auditoría interna, lo que ocasiona vacíos de gobernanza.

Falta de gobernanza y sponsor ejecutivo

- En encuestas globales, el 48 % de los líderes indicaron que necesitan mayor patrocinio del nivel ejecutivo para TPRM. En México, muchas organizaciones aún tratan la gestión de terceros como un proceso de compras más que como un riesgo estratégico.

Evaluación de riesgos insuficiente

- No siempre se consideran factores complejos, como los riesgos de cuarta parte, los geopolíticos, los de concentración o los de resiliencia de proveedores.
- La debida diligencia (due diligence) de integridad, cumplimiento y continuidad a veces es superficial o relega la revisión a los nuevos proveedores, sin monitorear a los existentes.

Monitoreo insuficiente y falta de métricas de desempeño

- Una vez que se firma un contrato, la supervisión continua suele ser débil o inexistente. Esto expone a la organización a cambios adversos en la condición del proveedor: problemas financieros, exposición de datos, incidentes de ciberseguridad, etc.
- Pocos programas tienen métricas cuantificadas de riesgo (por ejemplo % impacto, probabilidad, tiempos de detección) o vinculadas a la estrategia de negocio.

Escasa tecnología y automatización

- Aunque la conciencia está aumentando, muchas empresas mexicanas aún no han adoptado herramientas de TPRM que integren inteligencia, analítica, automatización o monitoreo continuo.
- En un entorno donde la IA y la automatización están emergiendo, quedarse atrás implica una mayor vulnerabilidad.

Dependencia de proveedores extranjeros y falta de resiliencia local

- Debido al modelo de nearshoring y a la tercerización de servicios globales, muchas organizaciones mexicanas dependen de proveedores extranjeros o de infraestructuras ubicadas fuera del país, lo que incrementa los riesgos de jurisdicción, interrupciones logísticas, diferencias regulatorias y de continuidad.
- Esta dependencia combina con la inestabilidad geopolítica, flujos de datos transfronterizos y cadenas logísticas complejas, lo que exige una capa extra de control.

Inadecuada alineación regulatoria y de cumplimiento

- Muchas entidades mexicanas aún no adaptan de manera sistemática sus procesos de gestión de terceros al nuevo entorno regulatorio digital (privacidad de datos, ciberseguridad, transparencia contractual).

Abordando las principales falencias en la tercerización

Dependencia de roveedores extranjeros

ea vulnerabilidades en a cadena de suministro

Monitoreo insuficiente

oide la mejora continua

Falta de gobernanza

Conduce a la toma de isiones descoordinada

Visibilidad limitada

ficulta la supervisión y el control

Alineación regulatoria inadecuada

Genera problemas de cumplimiento

Escasa tecnología

Limita la eficiencia y la innovación

Evaluación de riesgos insuficiente

Expone a vulnerabilidades imprevistas

Procesos manuales

Aumenta los errores y los retrasos

Riesgos Prioritarios con Terceros

(clasificados por tipo y sector)

En el contexto mexicano, los riesgos derivados de terceros pueden agruparse en las siguientes categorías, adaptadas a los sectores clave:

1

Riesgo Cibernético

Brechas de seguridad en proveedores pueden causar interrupciones y fugas de datos. ¡Ojo con el ransomware!

5

Riesgo Concentración

Depender de un solo proveedor es peligroso. ¡Diversifica tus opciones!

2

Riesgo Operativo

Si un proveedor falla, tus operaciones se detienen. ¡Ten un plan B listo!

6

Riesgo Geopolítico

Políticas y logística internacional impactan tus insumos. ¡Mantente informado!

3

Riesgo Regulatorio

Incumplir las leyes mexicanas te puede costar caro. ¡Cumple con LFPDPPP y Fintech!

7

Riesgo de Datos

Protege los datos de tus clientes y empleados. ¡Evita problemas regulatorios!

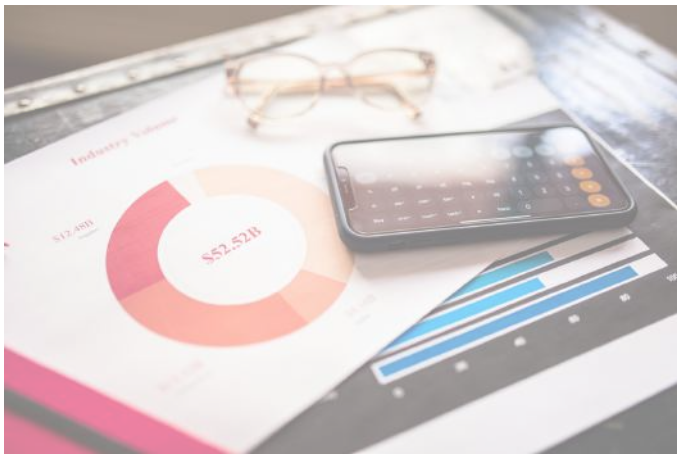
4

Riesgo Reputacional

La mala fama de un proveedor mancha tu marca. ¡Elige con cuidado!

Sectorial – Ejemplos de exposición

- **Financiero y seguros**: alta regulación de la CNBV, fuerte presión por ciberseguridad, outsourcing de TI/bpo.
- **Salud**: manejo de datos sensibles (historial clínico, diagnóstico), cumplimiento de estándares subcontratación de procesamiento,internacionales.
- **Retail & manufactura**: cadenas globales, logística, múltiples proveedores de servicios (TI, almacén, transporte).
- **Tecnología / servicios**: proveedores cloud, SaaS, globales, riesgo de datos y continuidad.
- **Sector público**: externalización de servicios digitales, dependencia de proveedores, obligación de transparencia y de buen gobierno.



Potenciales impactos de mala gestión

- Multas regulatorias: por ejemplo, la infracción a la LFPDPPP puede acarrear sanciones económicas de hasta 4 % de los ingresos (según el caso).
- Pérdida de clientes: un incidente de tercero puede dañar la confianza de los usuarios y provocar una fuga masiva de clientes.
- Interrupción de servicios críticos: en banca o en salud, la falta de continuidad puede acarrear pérdidas económicas cuantificadas, multas regulatorias y daño reputacional. Costos de remediación: globalmente, las brechas de terceros cuestan ~40 % más que las brechas internas.
- En México, dada la creciente exposición (ver sección de datos) y los sectores regulados, el efecto multiplicador del riesgo de terceros es tangible y urgente.

Casos de Estudio: Fallas Críticas en la Supervisión de Proveedores Críticos

A continuación se presentan dos ejemplos ilustrativos (anonimizados) adaptados al entorno mexicano que muestran cómo una deficiente gestión de terceros puede impactar gravemente a una organización.

NovaSec GRC

Buenas Prácticas TPRM Integradas al GRC en Organizaciones Mexicanas

Marco de TPRM adaptado

Ciclo de vida del TPRM

- Identificación de terceros y subterceros.
- Valoración y segmentación de riesgos
- Due diligence (integridad, ciberseguridad, continuidad, cumplimiento).
- Contratación inteligente (cláusulas de servicio, SLA, KPIs, auditoría, derecho de auditoría)
- Monitoreo continuo y gestión del desempeño.
- Remediación y salida (terminación o sustitución de terceros).

Referencias de marco internacional adaptadas:

ISO 31000 (gestión de riesgos),
NIST SP 800-161 para supply-chain

Tendencias Futuras y Desafíos Emergentes

Impacto de IA y Automatización

La IA transforma el TPRM con detección de anomalías, análisis de riesgo en tiempo real y predicción de incidentes, posicionándose como un diferenciador clave en México.

23%

de CISOs anticipa su uso

Integración con Criterios ESG

La gestión de terceros debe incorporar activamente criterios ambientales, sociales y de gobernanza (ESG), impulsada por la conciencia global y la presión de inversionistas.

Nuevas Regulaciones y Ciberresiliencia

La próxima Ley Nacional de Ciberseguridad en México creará nuevas obligaciones, exigiendo a las organizaciones reforzar la ciberresiliencia de sus proveedores.

Resiliencia en Cadenas de Suministro

El rol de México como hub de nearshoring amplía la superficie de riesgo, haciendo esencial la gestión geopolítica y la visibilidad de riesgos de "cuarta y quinta parte". p>

Plan de Despliegue TPRM y Herramientas Ejecutivas

Check-list resumido para México

01 **Inventario completo de terceros**
Registro centralizado y actualizado regularmente

02 **Clasificación por criticidad**
Segmentación según impacto operativo y data

03 **Evaluación de riesgos integral**
ciber, continuidad, cumplimiento, reputación, concentración, geopolítico

04 **Política de terceros aprobada**
Política formal validada por dirección y cumplimiento

05 **Cláusulas contractuales estándar**
Cláusulas de SLA, seguridad y cumplimiento en contratos

06 **Monitoreo continuo con KPIs y KRIs**

07 **Tecnología de soporte**
Herramientas para onboarding, evaluación y monitoreo

08 **Formación y concienciación**
Capacitación a equipos operativos y compras

09 **Pruebas y simulacros periódicos**
Pruebas de continuidad y ejercicios de ciberrespuesta

10 **Reporte al consejo y altos mandos**
Informes regulares con métricas y riesgos críticos

11 **Revisión cualitativa mínima periódica**
Frecuencia sugerida: revisión cualitativa al menos anual

Adaptaciones sectoriales en México

- **Sector financiero/seguros**: incluir criterios de la CNBV de continuidad, pruebas de auditoría y reporte al supervisor.
- **Salud**: enfatizar la protección de datos personales sensibles, el cumplimiento de normas nacionales e internacionales.
- **Retail/manufactura**: enfoque en continuidad logística, localización de proveedores, diversificación frente al nearshoring.
- **Sector público**: mayor transparencia, control de subcontrataciones, alineamiento con buen gobierno y auditoría interna.

Indicadores de madurez sugeridos

- Nivel 0: sin programa formal de TPRM
- Nivel 1: inventario y cláusulas contractuales básicas
- Nivel 2: evaluación anual de terceros críticos, algunos KPIs
- Nivel 3: monitoreo continuo, dashboard ejecutivo, integración con GRC
- Nivel 4: inteligencia-driven, uso de IA/analítica, cuarta y quinta parte visibles, reporte de cuantificación monetaria del riesgo.

Puntos clave GRC:

- **Gobierno:** políticas, roles, estructuras.
- **Riesgos:** matrices, KRIs, metodologías.
- **Controles:** ciberseguridad, contractual, operativo.
- **Cumplimiento:** regulaciones aplicables.
- **Auditoría:** pruebas, evidencias, informes.
- **Continuidad:** resiliencia, capacidad operativa, aseguramiento.
- **Terceros:** evaluación continua y due diligence dinámico.

Tendencias Futuras y Desafíos Emergentes

Impacto de la IA y automatización

- La inteligencia artificial está entrando en el TPRM: detección de anomalías en datos del proveedor, análisis de riesgo en tiempo real, predicción de incidentes. Según la encuesta de 2024, el 23 % de los CISO esperan usar IA para el descubrimiento de activos de terceros.
- En México, la adopción de IA en GRC y TPRM será un diferenciador. Las organizaciones que no la adopten podrían quedar rezagadas.

Integración con ESG

- La gestión de terceros debe integrar criterios ESG: prácticas laborales del proveedor, impacto ambiental, transparencia de la cadena. A nivel global, ya se observa una mayor concienciación.
- En México, con mayor enfoque regulatorio y presión de inversionistas, esto gana relevancia.

Resiliencia de la cadena de suministro y nearshoring

- México se posiciona como un hub estratégico de nearshoring. Esto implica un mayor volumen de relaciones con terceros logísticos, de manufactura y de tecnología, lo que amplía la superficie de riesgo. La diversificación regional y la gestión de riesgos geopolíticos serán vitales.

Cuarta-parte y quinta-parte (nth-party risk)

Como advierten estudios globales, el riesgo ya no lo representa solo el proveedor directo, sino también su red de subcontratistas. Las organizaciones en México deben ampliar su visibilidad más allá del primer nivel.

Ciberresiliencia y nuevas regulaciones

- Con más de la mitad de los ciberataques de Latinoamérica ocurriendo en México (2024), las organizaciones mexicanas deben asumir que sus proveedores también son blanco.
  Se espera que se apruebe una ley de ciberseguridad nacional en México, lo que generará nuevas obligaciones para terceros.

Enfoque GRC agregado:

- IA debe integrarse a KRIs dentro del GRC.
- ESG y TPRM se alinean con el gobierno de la empresa.
- Nearshoring aumenta el volumen de proveedores → GRC permite
- controlarlos.
  Nuevas regulaciones deben mapearse dentro del programa de cumplimiento.

Plan de Despliegue TPRM y Herramientas Ejecutivas

Justificación Financiera y ROI

30-40%
Reducción en probabilidad de incidentes graves de terceros.

12-24 m
Justificación de inversión vs costos de brechas (>5M USD).

Autoevaluación para Consejos

- ¿Visibilidad completa de terceros y subterceros?
- ¿Segmentación por criticidad y monitoreo continuo de riesgos?
- ¿Contratos con cláusulas clave y uso de tecnología/IA?
- ¿Alineación regulatoria (LFPDPPP, Fintech, CNBV) y estratégica?
- ¿Reporte regular al órgano de gobierno con métricas?

Conclusiones

TPRM: Pilar Estratégico Indispensable

La gestión de riesgos de terceros ha evolucionado de un proceso operativo a una imperativa estratégica, extendiendo el riesgo corporativo y exigiendo un enfoque transversal en toda la organización.

Integración GRC para la Resiliencia

El valor real del TPRM emerge al integrarse en un marco unificado de Gobierno, Riesgo y Cumplimiento (GRC), elevando los riesgos a nivel ejecutivo y garantizando la protección operativa y el cumplimiento regulatorio.

Tecnología como Habilitador Fundamental

La madurez del TPRM depende de la automatización y la analítica. La adopción de plataformas GRC es crucial para consolidar la gestión de riesgos, controles y cumplimiento, superando procesos manuales y ofreciendo visibilidad en tiempo real.

Conclusiones

La gestión de riesgos de terceros en México ya no es un ejercicio operativo ni un proceso aislado en áreas como compras o TI. Las tendencias globales, la creciente presión regulatoria y la complejidad del entorno digital han demostrado que **los proveedores se han convertido en una extensión directa del riesgo corporativo**. En consecuencia, las organizaciones requieren un enfoque más amplio, transversal y estratégico.

El papel del GRC es fundamental

El verdadero valor del TPRM se alcanza sólo cuando está integrado en un marco de **Gobierno, Riesgo y Cumplimiento (GRC)** que articule políticas, responsabilidades, controles, auditoría y continuidad bajo una visión unificada. Esto permite:

- Elevar los riesgos de terceros a niveles ejecutivos.
- Conectar las decisiones de negocio con el apetito de riesgo.
- Asegurar el cumplimiento regulatorio ante la CNBV, el INAI, el IFT y el T-MEC.
- Trazar relaciones entre proveedores, procesos, áreas y riesgos.
- Proteger la operación frente a incidentes, interrupciones y brechas.

Un TPRM desconectado del GRC carece de profundidad, trazabilidad y capacidad de respuesta. Por ello, las empresas mexicanas necesitan evolucionar de evaluaciones estáticas a un modelo dinámico y basado en el gobierno.

La madurez futura dependerá de la integración tecnológica.

El volumen de proveedores, la velocidad de negocio y el riesgo creciente exigen automatización y analítica. Las organizaciones que continúen gestionando proveedores con hojas de cálculo, correos y procesos manuales enfrentarán:

- Brechas no detectadas.
- Falta de evidencia ante auditorías.
- Criterios inconsistentes.
- Aumentos en el riesgo residual.
- Incapacidad para monitorear n-th parties.

Glosario

GRC (Governance, Risk & Compliance)

Marco que unifica **gobernanza**, **gestión de riesgos** y **cumplimiento** para asegurar que una organización tome decisiones seguras, responsables y alineadas a regulaciones. Es la base estructural del TPRM.

TPRM (Third-Party Risk Management)

Proceso sistemático para **identificar, evaluar, monitorear y gestionar** riesgos y subproveedores.

Incluye riesgos tecnológicos, operativos, regulatorios, financieros y de conyinuidad.

Proveedor Crítico

Tercero cuya falla podría provocar **interrupciones severas**, multas, pérdida de datos o afectación reputacional. Sujetos a monitoreo y auditoría reforzada.

Due Diligence

Evaluación formal previa a la contratación de un proveedor. Analiza controles, cumplimiento, ciberseguridad, continuidad, privacidad y capacidad operativa.

Riesgo Inherente / Riesgo Residual

- **Inherente:** riesgo natural antes de aplicar controles.
- **Residual:** riesgo que queda después de implementar controles del proveedor y la organización.

KRIs (Key Risk Indicators)

Indicadores que alertan sobre cambios en el nivel de riesgo de un tercero. Fundamentales en monitoreo continuo y GRC.

SLA / OLA (Acuerdos de Nivel de Servicio / Operación)

Compromisos de desempeño, disponibilidad y seguridad que el proveedor debe cumplir. Base contractual en TPRM.

Continuidad del Negocio / DRP

Conjunto de planes y capacidades para mantener operaciones ante una interrupción, incluyendo fallas de proveedores. Deriva de **ISO 22301**.

Controles Internos

Medidas para asegurar seguridad, cumplimiento y operación confiable. En proveedores incluyen: cifrado, accesos, backups, segregación de funciones, etc.

Cadena de Subcontratación (N-th Party)

Red extendida de proveedores de un proveedor. Fuente crítica de riesgo (supply chain risk).

Apetito de Riesgo

Nivel de riesgo aceptable que el Consejo o Comité de Riesgos define. Base estratégica del programa GRC y TPRM.

Brecha de Seguridad (Data Breach)

Acceso, exposición o pérdida de datos. Regulado en México por **LFPDPPP** y supervisado por el **INAI**.

Normativas Clave (México)

LFPDPPP

Ley de Protección de Datos Personales. Exige medidas de seguridad, contratos con terceros y notificación de incidentes.

Disposiciones de la CNBV

Normativa para banca y financieras sobre:

- Continuidad.
- Ciberseguridad.
- Tercerización.
- Auditoría.
- Riesgos operativos.

Ley Fintech (ITFs)

Regula proveedores tecnológicos, ciberseguridad y servicios tercerizados.

Normativas Internacionales Relevantes

ISO 27001 – Seguridad de la información

Base para evaluar proveedores tecnológicos.

ISO 31000 – Gestión del riesgo

Marco general aplicado a GRC.

ISO 22301 – Continuidad del negocio

Relevante para proveedores de servicios críticos.

NIST CSF

Framework de ciberseguridad usado para evaluar riesgos tecnológicos y de supply chain.

T-MEC

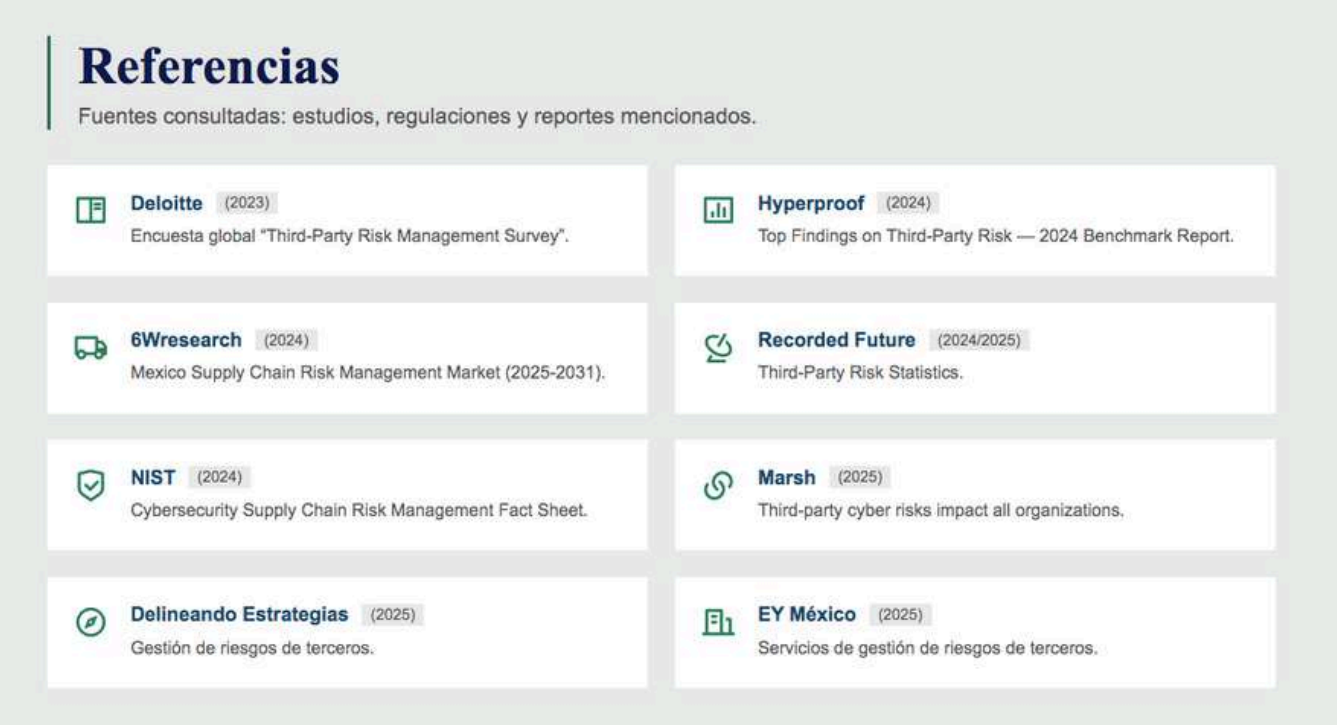
Exige trazabilidad y responsabilidad compartida en cadenas de suministro entre México, EE.UU. y Canadá.

Regtech

Tecnologías, como plataformas GRC, que automatizan procesos de cumplimiento y gestión de riesgos.

Gobierno Corporativo

Estructura de comités, roles, políticas y responsabilidades que dirige a la organización. Enmarca y dirige todo el ecosistema GRC y el TPRM.



Referencias

Fuentes consultadas: estudios, regulaciones y reportes mencionados.

Deloitte (2023)
Encuesta global "Third-Party Risk Management Survey".

Hyperproof (2024)
Top Findings on Third-Party Risk — 2024 Benchmark Report.

6Wresearch (2024)
Mexico Supply Chain Risk Management Market (2025-2031).

Recorded Future (2024/2025)
Third-Party Risk Statistics.

NIST (2024)
Cybersecurity Supply Chain Risk Management Fact Sheet.

Marsh (2025)
Third-party cyber risks impact all organizations.

Delineando Estrategias (2025)
Gestión de riesgos de terceros.

EY México (2025)
Servicios de gestión de riesgos de terceros.