Riesgos en México y Centroamérica 2026

Evolución de la gestión ante la disrupción tecnológica y geopolítica

DELINEANDO ESTRATEGIAS

1 Administración de Riesgos

KPMG México

Contenido

Prólogo

En un entorno marcado por la volatilidad geopolítica, presiones económicas y la irrupción de un gran volumen de tecnologías emergentes con capacidad de transformar las dinámicas sociales y la forma de hacer negocios, las organizaciones en México, Centroamérica y República Dominicana enfrentan una exposición creciente a amenazas operativas en un entorno de riesgos cada vez más complejo, que seguirá poniendo a prueba sus estrategias de evaluación y respuesta a los desafíos presentes y futuros. Por ello, contar con una visión clara de la naturaleza de estos elementos se vuelve esencial para fortalecer la capacidad de prevención y adaptación en escenarios de cambio constante.

Factores como los cambios en el entorno geopolítico, la inseguridad y la falta de Estado de derecho, los ciberataques, los desafíos asociados a la inteligencia artificial (IA) y los temas ambientales, sociales y de gobierno corporativo (ASG) continúan ganando relevancia dentro de la agenda empresarial, en la cual se perfila como una necesidad clave fortalecer los modelos de gestión de riesgos para que sean más integrales, dinámicos y objetivos, al tiempo que generan información útil para robustecer la capacidad de las organizaciones de responder a amenazas emergentes cada vez más complejas y cambiantes, así como para identificar oportunidades en un entorno cada vez más incierto.

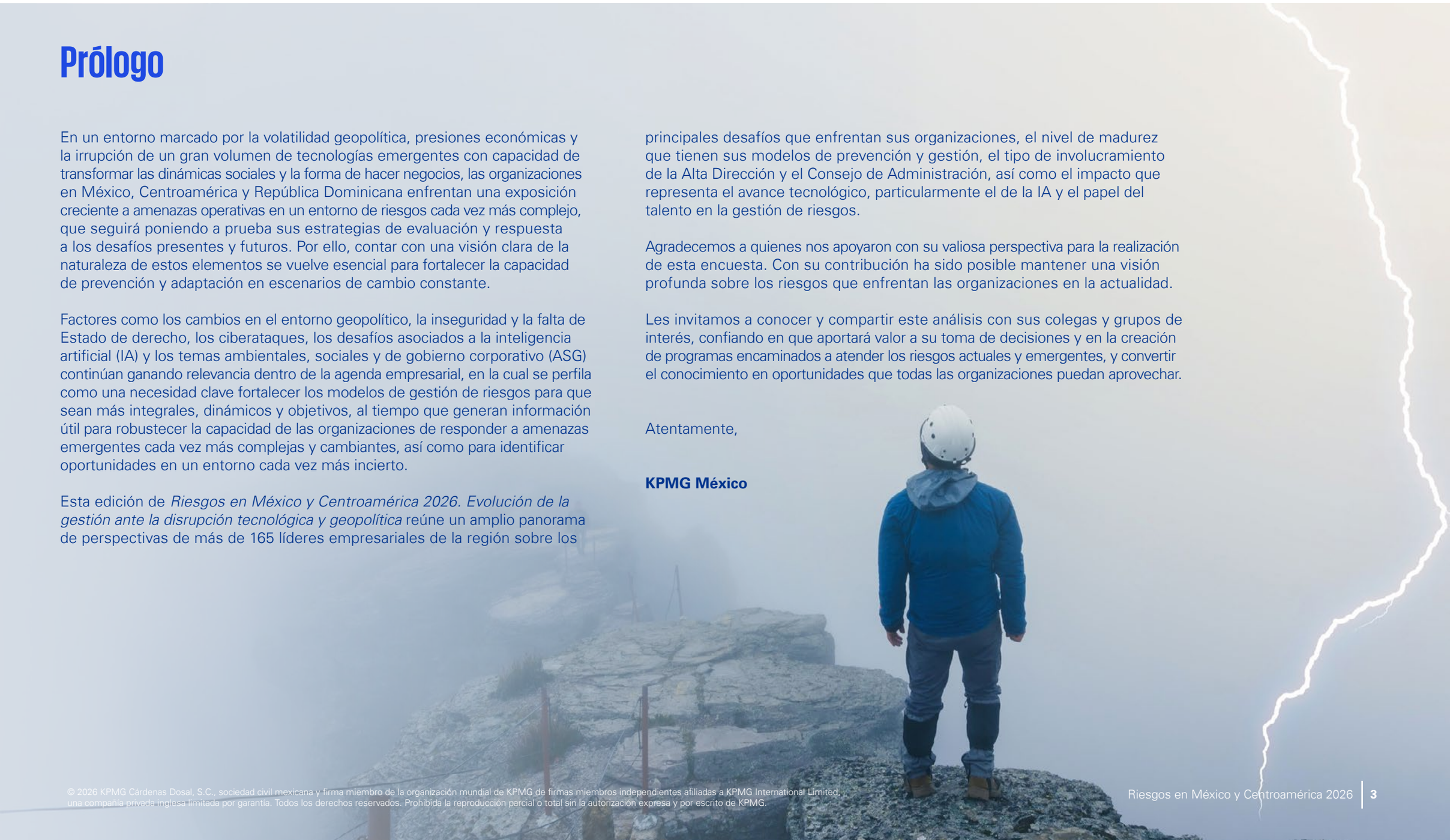
Esta edición de *Riesgos en México y Centroamérica 2026. Evolución de la gestión ante la disrupción tecnológica y geopolítica* reúne un amplio panorama de perspectivas de más de 165 líderes empresariales de la región sobre los principales desafíos que enfrentan sus organizaciones, el nivel de madurez que tienen sus modelos de prevención y gestión, el tipo de involucramiento de la Alta Dirección y el Consejo de Administración, así como el impacto que representa el avance tecnológico, particularmente el de la IA y el papel del talento en la gestión de riesgos.

Agradecemos a quienes nos apoyaron con su valiosa perspectiva para la realización de esta encuesta. Con su contribución ha sido posible mantener una visión profunda sobre los riesgos que enfrentan las organizaciones en la actualidad.

Les invitamos a conocer y compartir este análisis con sus colegas y grupos de interés, confiando en que aportará valor a su toma de decisiones y en la creación de programas encaminados a atender los riesgos actuales y emergentes, y convertir el conocimiento en oportunidades que todas las organizaciones puedan aprovechar.

Atentamente,

KPMG México



Principales riesgos

Impacto de los riesgos en la organización

Las compañías en México y Centroamérica enfrentan una exposición cada vez mayor a factores de riesgo que pueden impactar tanto su fluidez y eficiencia operativa como su capacidad de adaptación a corto y largo plazo.

Ante este escenario, en 2026, las empresas en México muestran una mayor preocupación por los cambios en el entorno geopolítico, que incrementan de 75% en 2025 a 81%, y por los ciberataques, que aumentan de 65% a 79%. En contraste, los riesgos económicos que destacaban en 2025, como la recesión (68%) y la imposición de aranceles a importaciones del exterior (75%) pierden protagonismo. Este cambio refleja un desplazamiento hacia riesgos más tecnológicos y estratégicos en el corto plazo.

A largo plazo, las emergencias sanitarias se mantienen como una de las principales preocupaciones en el país (65%), seguido de la falta de controles enfocados en aspectos clave y procesos no conectados e inflexibles (50%), así como los cambios en las tendencias de consumo (48%).

¿En qué momento considera que los siguientes riesgos tendrán un impacto significativo en su negocio?

México

2026 A corto plazo (en los próximos 12 meses)		2025 A corto plazo (en los próximos 12 meses)	
Cambios en el entorno geopolítico actual	81%	Cambios en el entorno geopolítico actual	75%
Ciberataques	79%	Imposición de aranceles a importaciones del exterior	75%
Inseguridad y falta de Estado de derecho	75%	Inseguridad y falta de Estado de derecho	69%
No aprovechar ventajas de utilizar IA	65%	Recesión económica local o global	68%
Perder o no atraer al talento necesario	65%	Ciberataques	65%
Ser víctima de fraudes y robos	61%	Ser víctima de fraudes y robos	63%
Nuevas regulaciones	60%	Imposición de aranceles a nuestras exportaciones	59%

A largo plazo (en los siguientes dos o tres años)	
Emergencias sanitarias	65%
Falta de controles enfocados en aspectos clave y procesos no conectados e inflexibles	50%
Cambios en las tendencias de consumo	48%
Impacto de la IA en el modelo de negocio o en los procesos	44%
Recesión económica local o global	43%
Políticas monetarias restrictivas y reducción extrema de liquidez	41%
Brechas de seguridad creadas por el uso de IA	40%

En Centroamérica, el mapa de riesgos a corto plazo muestra en 2026 una clara intensificación de los factores externos, con los cambios en el entorno geopolítico aumentando de 70% en 2025 a 78%, y los ciberataques consolidándose como una preocupación constante (73%). A diferencia de 2025, cuando los fraudes y robos ocupaban un lugar central (70%), en 2026 cobran mayor peso los retos regulatorios, que suben de 46% a 60%. Esta evolución sugiere un entorno donde la atención empresarial se desplaza hacia riesgos más normativos y de contexto regional, sin dejar de lado la ciberseguridad.

A largo plazo, las emergencias sanitarias, así como las políticas monetarias restrictivas y la reducción extrema de liquidez (50%), adquieren mayor relevancia para las empresas en Centroamérica. Asimismo, destaca el rezago en innovación y transformación digital (48%), lo que refleja un enfoque cada vez más marcado en los desafíos tecnológicos estructurales.

¿En qué momento considera que los siguientes riesgos tendrán un impacto significativo en su negocio?

Centroamérica

2026 A corto plazo (en los próximos 12 meses)		2025 A corto plazo (en los próximos 12 meses)	
Cambios en el entorno geopolítico actual	78%	Ciberataques	73%
Ciberataques	73%	Cambios en el entorno geopolítico actual	70%
Nuevas regulaciones	60%	Ser víctima de fraudes y robos	70%
Perder o no atraer al talento necesario	58%	Perder o no atraer al talento necesario	55%
Desajustes de alto impacto o interrupciones en la cadena de valor	57%	Impacto de la IA en los procesos	48%
Impacto de la IA en el modelo de negocio o en los procesos	57%	Nuevas regulaciones	46%
Ser víctima de fraudes y robos	55%	No detectar recursos de procedencia ilícita en alguna transacción	46%

A largo plazo (en los siguientes dos o tres años)	
Políticas monetarias restrictivas y reducción extrema de liquidez	50%
Emergencias sanitarias	50%
Rezago en innovación y transformación digital	48%
Falta de controles enfocados en aspectos clave y procesos no conectados e inflexibles	47%
No aprovechar ventajas de utilizar IA	43%
Cambios en las tendencias de consumo	42%
Perder o ver afectada la reputación de la marca	40%

Los cambios en el entorno geopolítico han adquirido relevancia por la rapidez con la que se están reconfigurando las relaciones comerciales entre países y regiones, reflejándose en controversias comerciales, la redistribución del liderazgo global en sectores emergentes y dinámicas cambiantes de competencia internacional. Lo que antes podía percibirse como un fenómeno lejano, hoy tiene implicaciones tangibles sobre las cadenas de suministro, la disponibilidad de insumos, la continuidad operativa y la competitividad de las empresas.

Asimismo, la evolución y sofisticación de los ciberataques continúa siendo uno de los riesgos más persistentes por su capacidad de comprometer información sensible, interrumpir operaciones o generar afectaciones reputacionales y regulatorias. Este reto se amplía con el avance de la IA, cuyo impacto no solo se refleja en la capacidad que tiene de transformar modelos de negocio, sino también en nuevos riesgos asociados con temas de privacidad, de propiedad intelectual y del uso inadecuado de herramientas dentro de las organizaciones.

En este contexto, no basta con que las compañías identifiquen los riesgos de manera aislada, o que solo consideren aquellos específicos de sus actividades, ya que muchas de estas amenazas están estrechamente vinculadas y, en diversos casos, deben abordarse desde una perspectiva multidisciplinaria. Un ejemplo de ello es la ciberseguridad, cuyos impactos trascienden el ámbito tecnológico e involucran factores como la cultura organizacional, la capacitación del talento, los tiempos de respuesta y la resiliencia operativa.

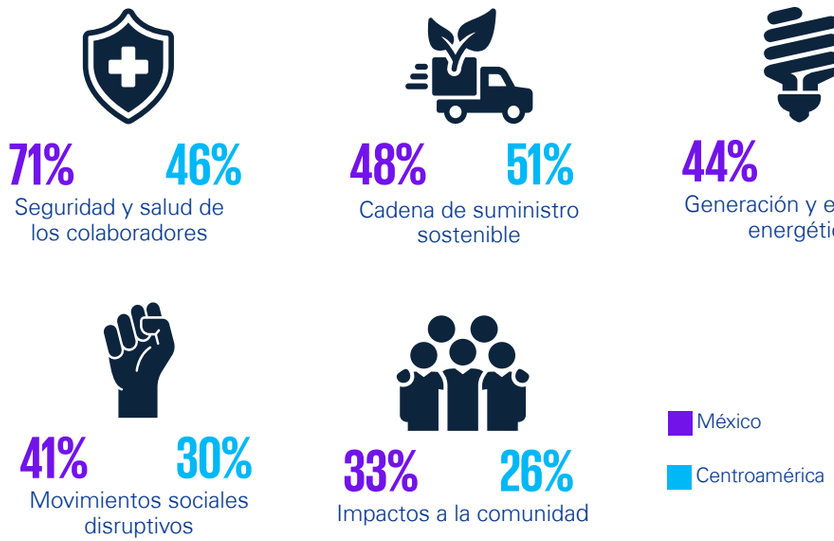
Por ello, resulta fundamental contar con un análisis hecho a la medida que permita identificar cuáles son los riesgos más apremiantes para cada organización, así como priorizarlos con base en su impacto potencial en la empresa, no solo desde un punto de vista financiero, sino también considerando implicaciones operativas, reputacionales, regulatorias y de cumplimiento.

Riesgos ASG

Los temas ASG se han convertido en un componente central de la gestión de riesgos, con efectos cada vez más importantes en la reputación de las compañías, en su capacidad de adaptación y, en consecuencia, en la continuidad del negocio. Su relevancia no solo responde a las exigencias del mercado y de los grupos de interés, sino a la creciente necesidad de anticipar riesgos vinculados con la sociedad, el clima y la naturaleza, así como con la sostenibilidad a corto y largo plazo.

En este sentido, se observan diferencias notables en la priorización de riesgos ASG entre regiones. Mientras que en México sobresalen aspectos relacionados con la seguridad y salud de los colaboradores (71%), la cadena de suministro sostenible (46%), la generación y eficiencia energética (44%) y los movimientos sociales disruptivos (41%), en Centroamérica adquieren mayor peso factores como la generación y eficiencia energética (54%), los eventos climáticos extremos y la cadena de suministro sostenible (51% en ambos casos), seguidos por la seguridad y salud de los colaboradores (46%).

¿Qué riesgos ASG son prioritarios para su organización?



La suma de las variables no es igual a 100% debido a que era posible seleccionar más de una opción.

Actualmente, las organizaciones comprenden, desde una perspectiva más amplia, la seguridad y salud de los colaboradores. Este factor ya no se limita al entorno físico de trabajo, sino que ahora también incorpora elementos como la seguridad en los trayectos, el bienestar emocional y la capacidad de adaptación frente a entornos de transformación acelerada. En este contexto, la incertidumbre asociada a la adopción de nuevas tecnologías y a la evolución de ciertas funciones también puede generar preocupación y resistencia al cambio, con implicaciones directas sobre la productividad, la capacitación y la resiliencia organizacional.

Ahora bien, el contraste de los riesgos entre regiones puede estar asociado a factores regulatorios, así como a las prioridades internas de cada organización y a la exposición particular de cada geografía.

En México, por ejemplo, tienen mayor visibilidad aspectos como los movimientos sociales disruptivos, cuyo impacto puede traducirse en afectaciones a la movilidad, la operación, la seguridad y la continuidad de los negocios. Por su parte, en Centroamérica, se le da mayor peso a algunos riesgos ambientales, lo que podría estar relacionado con una mayor exposición a fenómenos climáticos, presiones sobre recursos naturales y exigencias crecientes en materia de sostenibilidad.

En este sentido, temas como la gestión de desechos, los eventos climáticos extremos y la descarbonización deben entenderse no solo desde una óptica ambiental, sino también por su impacto sobre la cadena de suministro, la capacidad de exportación o la estabilidad y viabilidad del negocio a largo plazo.

Materialización del riesgo

Posibles escenarios

En México, las compañías identifican las implicaciones ante la posible materialización de los principales riesgos, entre los cuales destacan: la pérdida de clientes (53%), la reconfiguración del modelo de negocio (52%) y la necesidad de realizar ajustes relevantes en la estructura organizacional de la empresa (44%).

Por su parte, en Centroamérica también se señala la pérdida de clientes en primer lugar (64%), seguido de la reconfiguración del modelo de negocio (52%), así como la interrupción o reducción de la capacidad operativa y el desplazamiento por modelos basados en digitalización o automatización (45% respectivamente).

¿La posible materialización de riesgos empresariales tendrá alguno de los siguientes efectos en su organización?

La suma de las variables no es igual a 100% debido a que era posible seleccionar más de una opción.

Para las empresas, comprender cómo se materializan los riesgos tiene una relación directa con la capacidad de identificar las amenazas críticas para su operación y anticipar escenarios que fortalezcan la sostenibilidad de su propuesta de valor, su competitividad y la retención de sus clientes.

Riesgos como los cambios geopolíticos, la inseguridad o las disrupciones en la cadena de suministro pueden traducirse en aumentos de costos, incluyendo insumos clave y su disponibilidad, así como en retrasos operativos y una menor capacidad de respuesta en el mercado.

En este contexto, la reconfiguración del modelo de negocio deja de ser una decisión estratégica a largo plazo para convertirse en una alternativa que permite reaccionar con mayor agilidad ante cualquier incidente. La volatilidad del entorno puede obligar a las organizaciones a replantear su operación, su capacidad de adaptación y, en algunos casos, incluso la viabilidad de ciertas líneas de negocio. Esta presión se intensifica por la aceleración tecnológica, la digitalización y el uso de la IA, las cuales están redefiniendo la forma de competir y, al mismo tiempo, elevando el riesgo de rezago para aquellas empresas que no se adapten con suficiente rapidez.

A lo anterior se suman factores externos que pueden modificar abruptamente las condiciones del mercado, como cambios regulatorios, decisiones políticas o ajustes arancelarios, con efectos directos sobre la demanda, las exportaciones y la continuidad operativa.

En este entorno, la diferencia entre las compañías que solo reaccionan a los cambios y aquellas que puedan anticiparse resulta crítica. Es decir, la capacidad de identificar estos riesgos de manera oportuna, preparar escenarios alternos y tomar decisiones con agilidad será determinante, no solo para preservar su base de clientes, sino también para sostener la operación y la viabilidad del negocio a largo plazo.

Acciones de mitigación

Dentro de las acciones contempladas para atender los riesgos, en México destaca la definición de un programa de gestión de riesgos con escenarios alternos para amenazas con alta probabilidad de materialización (18%), mientras que, en Centroamérica se enfocan en el desarrollo o fortalecimiento de un plan de continuidad de negocio (19%).

Derivado de los riesgos que podrían amenazar la estrategia de su organización, ¿ha realizado alguna de las siguientes acciones?

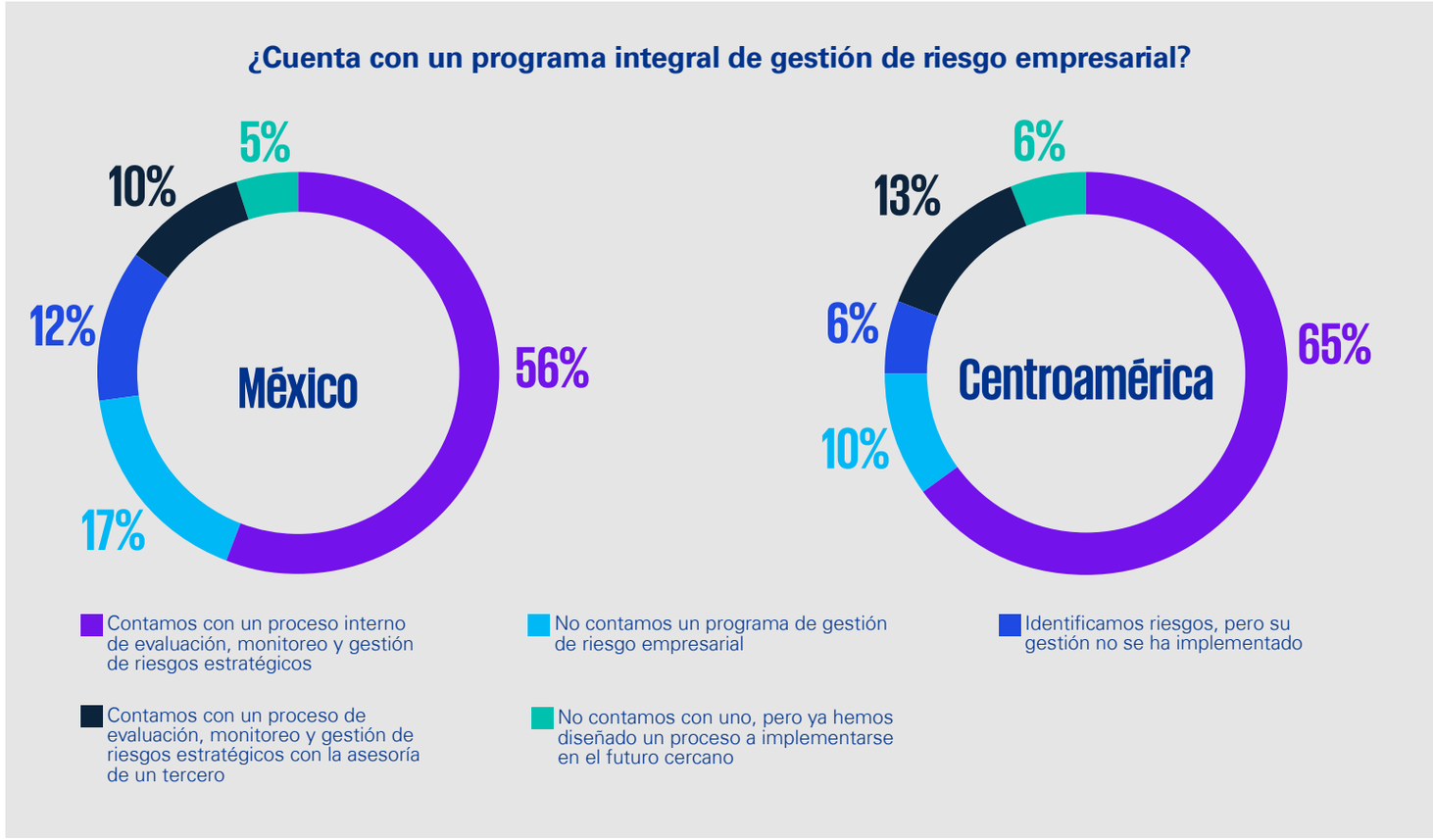
- 18% / 11% — Definición de un plan de gestión de riesgos con escenarios alternos para amenazas con alta probabilidad de materialización
- 14% / 19% — Desarrollo o fortalecimiento del plan de continuidad de negocio
- 11% / 9% — Contratación de terceros para recibir asesoría especializada en gestión de riesgos
- 11% / 13% — Desarrollo de políticas y procedimientos internos más robustos
- 11% / 11% — Integración de riesgos y oportunidades ASG a la gestión integral de riesgos de negocio
- 10% / 5% — Contratación de terceros para responder ante un evento específico (por ejemplo: investigaciones sobre ciberseguridad, fraude, prevención de lavado de dinero, entre otros)
- 10% / 11% — Desarrollo de un plan de gestión integral de IA
- 7% / 11% — Inversiones tecnológicas
- 7% / 4% — Implementar programas de capacitación
- 0% / 4% — Identificación de riesgos relacionados con el cambio climático y desarrollo de un plan para su gestión
- 1% / 2% — No se planea llevar a cabo ninguna acción

México | Centroamérica

Programas de gestión de riesgo

Ante este escenario, 56% de las empresas en México y 65% en Centroamérica afirman contar con un proceso interno de evaluación, monitoreo y gestión de riesgos estratégicos, mientras que 10% y 13% respectivamente cuentan con un proceso llevado a cabo con la asesoría de un tercero.

A pesar de la creciente importancia de los procesos de monitoreo y gestión, los resultados de las organizaciones en la región muestran áreas de oportunidad relevantes: 17% y 10% respectivamente no cuentan con un programa de gestión de riesgo empresarial; 12% y 6% sí los identifican, pero aún no han implementado su gestión y, 5% y 6% señalan que, si bien aún no cuentan con un programa formal, ya han diseñado un proceso para implementarlo a corto plazo.



A pesar de que existe una adopción similar, y en el caso de México, mayor, de programas de gestión de riesgos respecto al año anterior, particularmente a través de procesos internos (46% y 67% respectivamente en 2025), el hecho de que 34% de las empresas en México y 22% en Centroamérica no cuenten con un programa integral puede responder a distintos factores, entre ellos la percepción de complejidad de implementación, la necesidad de priorizar recursos, la volatilidad del entorno, la propia dinámica o evolución de los riesgos emergentes o la búsqueda de modelos que resulten verdaderamente prácticos, útiles y alineados con la toma de decisiones del negocio.

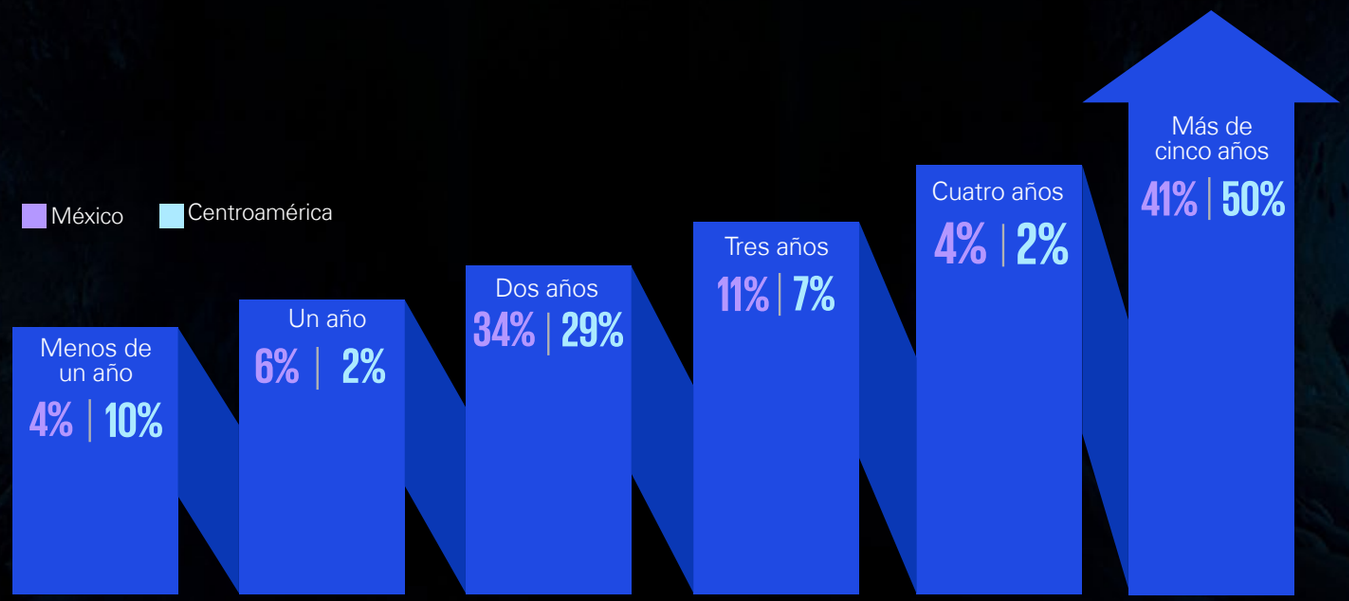
Si bien en muchas organizaciones los riesgos se gestionan de manera natural a partir de la experiencia que brinda la operación diaria, y el conocimiento del mercado, esto no necesariamente se traduce en un esquema formal, estructurado y sostenido. Por ello, implementar un programa de gestión de riesgo empresarial resulta imprescindible, ya que permite identificar, evaluar y monitorear los principales riesgos de forma sistemática, así como aprovechar el conocimiento que la organización tiene sobre su operación, procesos y dinámicas de negocio para impulsar acciones de respuesta a los mismos; no obstante, el acompañamiento de un tercero puede aportar una visión complementaria e independiente, capaz de identificar puntos ciegos, conectar riesgos que no siempre se analizan de forma integrada y abordar temas sensibles con mayor objetividad.

Por ello, los modelos de gestión más sólidos suelen ser aquellos que combinan el conocimiento interno del negocio con una perspectiva externa especializada, particularmente en riesgos que, por su complejidad o naturaleza cambiante, requieren capacidades técnicas específicas, como ciberseguridad, sostenibilidad o análisis geopolítico.

Tiempo y calidad de la evaluación

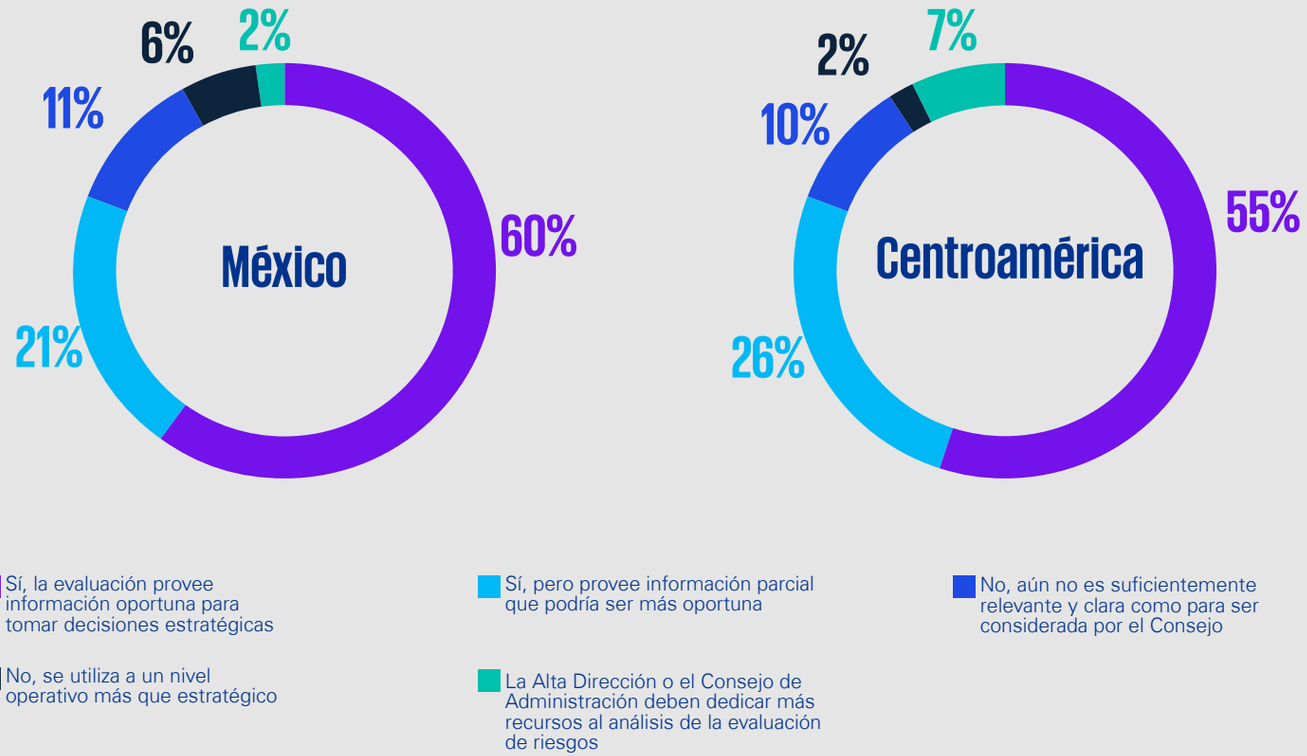
Respecto a la antigüedad de los programas de gestión de riesgos, 41% de las organizaciones en México y 50% en Centroamérica afirman haber llevado a cabo procesos de evaluación, monitoreo y gestión de riesgos durante más de cinco años, mientras que 34% y 29% respectivamente, durante al menos dos años.

¿Cuánto tiempo lleva realizando evaluaciones, monitoreo y gestión de riesgos empresariales?



Derivado de estas medidas, 60% de las compañías en México y 55% en Centroamérica consideran que la evaluación de riesgos provee información oportuna para la toma de decisiones en el Consejo de Administración o en reuniones de la Alta Dirección; no obstante, un porcentaje relevante también señala que la información generada sigue siendo parcial y podría ser más oportuna (21% y 26% respectivamente).

¿Su evaluación de riesgo empresarial provee información oportuna para la toma de decisiones estratégicas en el Consejo de Administración o en las reuniones de la Alta Dirección?



En este contexto, es importante destacar que la madurez del modelo de gestión de riesgos no depende únicamente del tiempo que lleva implementado, sino de su capacidad para generar información clara, relevante y oportuna para la toma de decisiones, además de su capacidad para impulsar acciones de respuesta y monitoreo ante las amenazas emergentes. Por ello, el hecho de que una proporción relevante aún perciba la información como parcial o poco oportuna sugiere que, en algunos casos, los programas todavía no generan el nivel de utilidad que se espera de ellos.

El riesgo y su gestión en la organización

El papel del Consejo de Administración

En cuanto al involucramiento del Consejo en la gestión de riesgos, 37% de las empresas en México y 48% en Centroamérica señalan que el programa es aprobado directamente por este órgano de gobierno, lo que refleja un papel activo en la supervisión del tema. Por otro lado, solo 13% y 8% respectivamente reportan la falta de involucramiento por parte del Consejo.

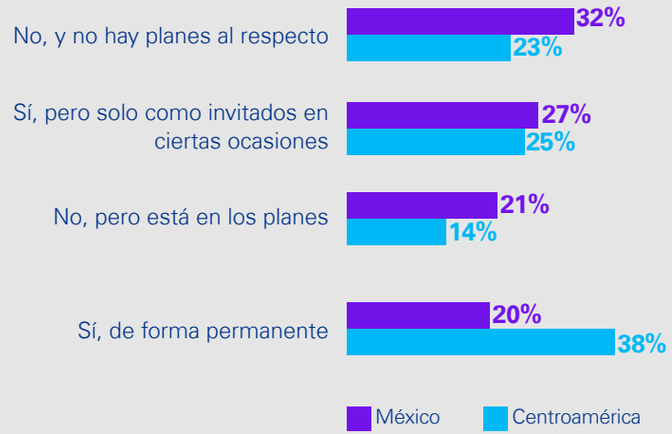
¿Qué enunciado refleja mejor el involucramiento del Consejo de Administración en la gestión de riesgos?

Apoyo de especialistas en la gestión de riesgos

Respecto al apoyo de especialistas en la gestión de riesgos, 27% de las organizaciones en México y 25% en Centroamérica indican que incorporan a estos perfiles como invitados en ciertas ocasiones, mientras que 20% y 38% respectivamente señalan que su participación es de forma permanente.

Sin embargo, una proporción importante aún no cuenta con este tipo de apoyo: 53% en México y 37% en Centroamérica no integran especialistas en sus esquemas de gestión o supervisión de riesgos.

¿El Consejo de Administración incorpora especialistas en la gestión de riesgos?



En este contexto, el involucramiento del Consejo juega un papel determinante, ya que su participación directa en la aprobación de los programas de gestión de riesgos implica un enfoque proactivo, así como una comprensión más clara de las distintas amenazas; no obstante, en un entorno donde los riesgos relacionados con la IA, la ciberseguridad, la sostenibilidad o la geopolítica se vuelven cada vez más complejos, la participación del Consejo puede fortalecerse aún más cuando se complementa con una visión técnica especializada.

En este sentido, la incorporación de especialistas puede aportar mayor profundidad de análisis, ayudar a traducir riesgos emergentes en implicaciones concretas para el negocio y fortalecer la calidad de las decisiones.

Herramientas tecnológicas y uso de la IA

Inteligencia artificial

Respecto a la integración de los riesgos y oportunidades relacionados con la IA en los programas de gestión de riesgos, 50% de las organizaciones en México afirman realizar un seguimiento activo de la evolución tecnológica y las tendencias de la IA en su industria, mientras que, en Centroamérica, 48% señala integrar factores relacionados con la vulnerabilidad de la información.

¿Están integrados los factores de riesgo y oportunidades de la IA en su programa de gestión de riesgo empresarial?

50% 25%
Hacemos seguimiento de la evolución tecnológica y tendencias relacionadas con la IA en nuestra industria

39% 48%
Hemos integrado factores relacionados con la vulnerabilidad de la información (por ejemplo, exposición a ciberataques o filtración de datos)

26% 38%
No incluimos la IA en nuestros procesos

15% 29%
Hemos integrado riesgos de dependencia tecnológica de sistemas de IA o su posible falla

14% 8%
Evaluamos periódicamente el impacto de la IA en la relación con clientes y proveedores para garantizar transparencia y confianza

12% 25%
Hemos integrado riesgos éticos del uso de IA (por ejemplo, posibles sesgos en algoritmos o impactos en la equidad)

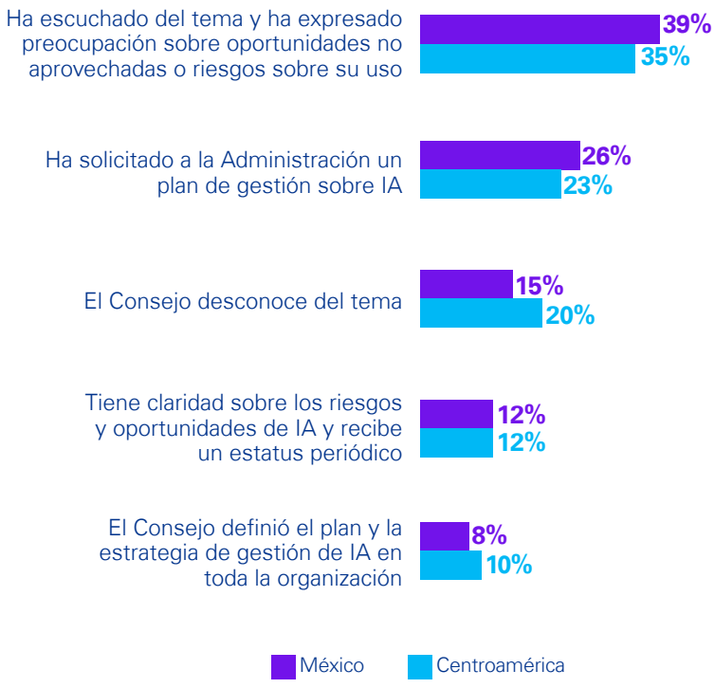
8% 0%
Incorporamos medidas para mitigar problemas reputacionales asociados al uso de tecnologías de la IA (por ejemplo, decisiones automatizadas mal interpretadas por clientes o proveedores)

México
Centroamérica

La suma de las variables no es igual a 100% debido a que era posible seleccionar más de una opción.

Asimismo, 39% en México y 35% en Centroamérica han expresado que su Consejo de Administración tiene inquietud sobre los riesgos y oportunidades no aprovechadas de la IA, mientras que 26% y 23% respectivamente señalan que el Consejo ha solicitado a la Administración la integración de un plan de gestión específico en la materia.

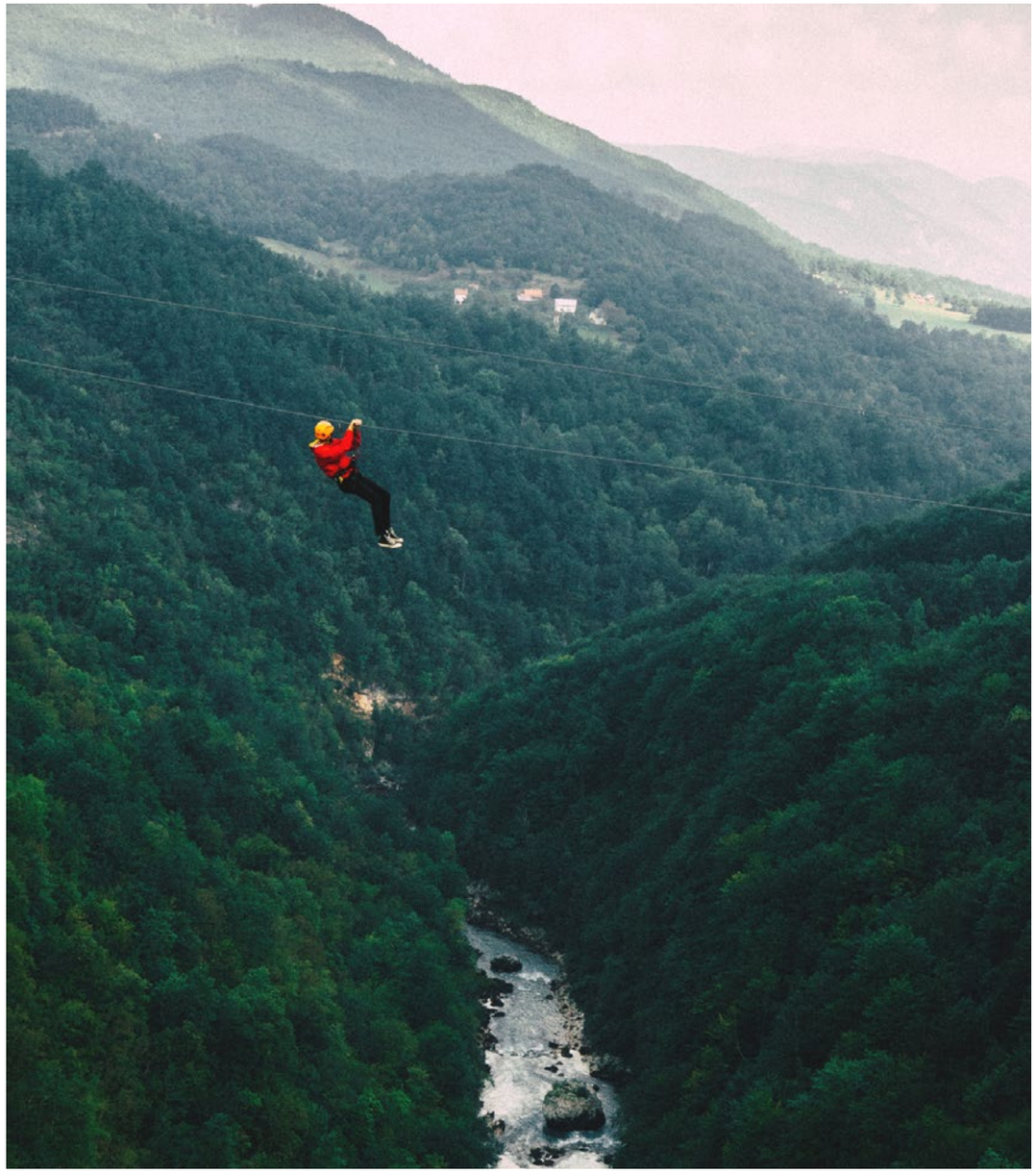
¿Cuál es el enfoque actual del Consejo de Administración sobre la IA?



En 2026, las compañías son conscientes de que la IA representa una oportunidad clave para fortalecer procesos, generar eficiencias y mejorar la capacidad de análisis, pero al mismo tiempo, puede convertirse en un riesgo relevante, principalmente cuando su adopción ocurre de manera apresurada, sin lineamientos claros, controles adecuados o visibilidad suficiente sobre su uso dentro de la organización.

En este contexto, uno de los principales retos no es solo evaluar los riesgos asociados con la implementación de la IA, sino también reconocer que no adoptarla o hacerlo de forma desordenada puede generar desventajas en términos de competitividad, eficiencia y capacidad de respuesta. A ello se suma el hecho de que, en muchos casos, estas herramientas ya están siendo utilizadas de manera informal por colaboradores, lo que puede derivar en amenazas adicionales, como fuga de información, exposición de datos sensibles y nuevas vulnerabilidades operativas y cibernéticas.

Por lo tanto, integrar la IA dentro del modelo de gestión de riesgos no solo implica identificar sus amenazas, sino también establecer un esquema de gobernanza que permita comprender dónde se utiliza, con qué propósito, bajo qué controles y de qué forma puede generar valor para la organización, controlando, al mismo tiempo, los riesgos que presenta.



En esta misma línea, prevalece un rezago tecnológico significativo en la región, pues 65% en México y 54% en Centroamérica aún no utilizan herramientas especializadas para la gestión de riesgos.

¿Utiliza alguna herramienta tecnológica para la gestión de riesgos?

Si bien una organización puede llevar a cabo ejercicios de identificación, evaluación y respuesta de amenazas de manera manual, gestionar este tipo de procesos sin apoyo tecnológico resulta cada vez más complejo. La velocidad con la que evolucionan los riesgos, la necesidad de revisar continuamente su nivel de impacto y la operación en entornos cada vez más regulados provocan que los enfoques manuales tiendan a limitar su capacidad para identificar relaciones, tendencias o señales tempranas que puedan ser relevantes para el negocio y, en ciertos casos, incluso pueden volverse obsoletos.

En este contexto, la incorporación de herramientas tecnológicas resulta primordial, ya que impulsa la eficiencia operativa, además de que fortalece la capacidad de monitorear y dar seguimiento a la evolución de los riesgos desde distintas funciones dentro de la organización, al consolidar información que antes se encontraba dispersa, permitiendo enriquecer las perspectivas de análisis. Adicionalmente, puede contribuir a generar información más oportuna, conectada y accionable para la toma de decisiones, fortaleciendo así el valor estratégico de la gestión de riesgos dentro de la organización.

Sin duda, el impacto de la IA y las tecnologías emergentes no se limita únicamente a la gestión y mayor procesamiento de la información, sino que también está transformando la forma en que las organizaciones operan y estructuran su fuerza laboral. Al respecto, 42% de las empresas en México y 43% en Centroamérica identifican como principal riesgo los desafíos éticos asociados con el uso de la IA, seguido de los retrasos operativos derivados de la falta de competencias adecuadas para su implementación (38% y 33% respectivamente).

¿Qué riesgos identifica su organización en relación con la implementación de una fuerza laboral habilitada por IA?

La suma de las variables no es igual a 100% debido a que era posible seleccionar más de una opción.

En el caso de los desafíos éticos relacionados y la carencia de competencias, la capacitación del personal, la definición de lineamentos de uso y la formación en prácticas responsables en materia de IA adquieren mayor relevancia, pues la incorporación de estas tecnologías no solo modifica los procesos y la forma de trabajo, sino también la manera en que el talento interactúa con ellas dentro de la organización.

En este sentido, uno de los principales retos no radica únicamente en incorporar nuevas herramientas, sino en asegurar que la organización cuente con las capacidades, la preparación y los criterios necesarios para utilizar estas tecnologías de forma responsable, en sincronía con la visión ética de la organización y atendiendo las exigencias de los distintos grupos de interés y regulaciones. De lo contrario, su implementación puede traducirse en ineficiencias, comportamientos no éticos y una adopción poco articulada que limite el valor que la IA puede generar.

Metodología

México Centroamérica

Género

Femenino		Masculino	
23%	45%	77%	55%

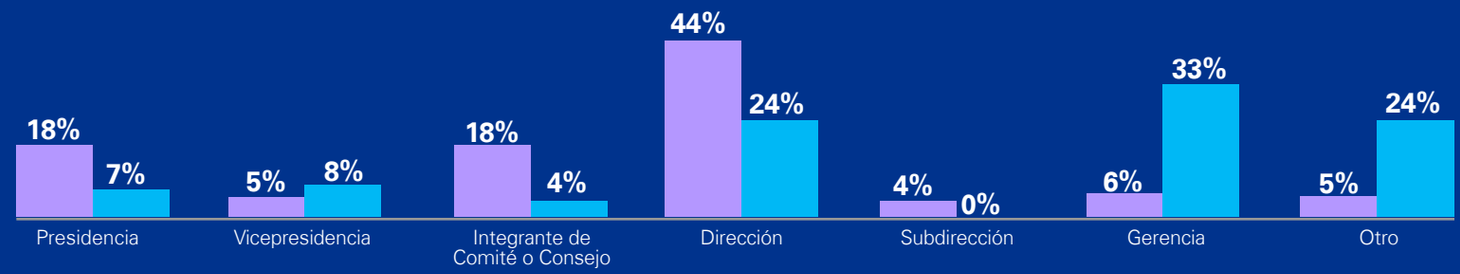
Ubicación de la empresa

Costa Rica
México
El Salvador
Nicaragua
Guatemala
Panamá
Honduras
República Dominicana

Sector al que pertenece la organización

	México	Centroamérica
Servicios financieros	22%	35%
Servicios especializados	16%	9%
Manufactura / Industrial	10%	8%
Automotriz	8%	3%
Servicios	7%	4%
Consumo / *Retail*	6%	5%
Alimentos y bebidas	4%	7%
Salud	7%	3%
Soluciones tecnológicas	6%	3%
Gobierno	0%	9%
Inmobiliaria / *Real estate*	4%	1%
Transporte	4%	1%
Construcción / Infraestructura	2%	4%
Medios de comunicación	3%	0%
Telecomunicaciones	0%	4%
Energía y recursos naturales	0%	3%
Entidades no lucrativas	1%	0%
Química / Farmacéutica	0%	1%

Nivel del participante



Importe de ventas anuales en millones de dólares

Conclusiones

En un entorno empresarial cada vez más volátil, interconectado y en constante cambio, la gestión de riesgos se ha convertido en un elemento central de la toma de decisiones. Los principales desafíos que hoy enfrentan las organizaciones en México y Centroamérica, desde los cambios geopolíticos, la inseguridad y la falta de Estado de derecho hasta los ciberataques, la IA y sus retos asociados, la transformación tecnológica o los temas ASG, evidencian que las compañías operan en un contexto cada vez más expuesto a factores internos y externos que pueden modificar con rapidez su contexto operativo, regulatorio y competitivo.

Frente a este panorama, la gestión de riesgos debe evolucionar de la misma forma en que lo hacen las amenazas emergentes, es decir, debe reevaluarse y fortalecerse continuamente para ser resiliente y actuar de forma proactiva y no solo reactiva. Por ello, resulta cada vez más relevante contar con un programa integral de gestión de riesgos que vaya más allá de la identificación de amenazas y determine verdaderamente cuáles son prioritarias para cada organización, mediante la evaluación de su posible impacto desde una perspectiva financiera, operativa, reputacional y regulatoria, así como la revisión de los mecanismos de respuesta existentes.

En un contexto en el que los riesgos evolucionan con rapidez, la capacidad de una organización para anticipar escenarios, ajustar su evaluación y traducir ese análisis en acciones concretas marcará una diferencia significativa en su resiliencia y capacidad de adaptación.

En este sentido, la efectividad de estos modelos depende, en gran medida, de su capacidad para generar información clara, útil y oportuna para la Alta Dirección y el Consejo de Administración. Aquí, el involucramiento del Consejo, así como la posibilidad de complementar la visión interna con la perspectiva de especialistas externos en temas cada vez más complejos, como ciberseguridad, geopolítica, sostenibilidad o IA, puede aportar mayor claridad, objetividad y perspectiva de análisis.

Asimismo, la tecnología y el talento se han convertido en factores cada vez más determinantes para garantizar una gestión de riesgos eficiente, los cuales deben estar acompañados de capacitación, prevención y cumplimiento de los marcos que la compañía establezca. La incorporación de herramientas especializadas, el fortalecimiento de competencias internas y la adopción estratégica de tecnologías como la IA pueden contribuir a hacer más eficiente la gestión, fortalecer el monitoreo y facilitar una respuesta más ágil frente a riesgos emergentes.

Más allá de responder a los desafíos del presente, el reto para las organizaciones de México y Centroamérica consiste en construir capacidades de gestión que les permitan adaptarse a los riesgos del futuro. En un entorno donde los cambios se producen con gran rapidez, la diferencia no estará únicamente en reducir la exposición, sino en contar con la visión, la flexibilidad y la disciplina necesarias para anticiparse, responder oportunamente y convertir la gestión de riesgos en un componente cada vez más relevante para la toma de decisiones y la resiliencia organizacional.

kpmg.com.mx
800 292 KPMG (5764)
asesoria@kpmg.com.mx

KPMG MÉXICO
@KPMGMEXICO
KPMG MÉXICO
KPMGMX

Contactos

Juan Carlos Reséndiz

Socio Líder de Asesoría en Gobierno Corporativo, Riesgo y Sostenibilidad de KPMG México

Líder de Asesoría en temas ASG del Clúster de México y Centroamérica*

Alberto Dosal

Socio de Asesoría en Gobierno Corporativo, Riesgo y Cumplimiento de KPMG México

Federico García

Socio de Asesoría en Gestión de Riesgos de KPMG Costa Rica

SÚPER EMPRESAS EXPANSIÓN 2025 TOP companies

ESR Empresa Socialmente Responsable Inclusión Social

Norma Mexicana en Igualdad Laboral y No Discriminación