Panorama Global de Riesgos 2026

Riesgo en todas partes

Extendiendo la responsabilidad más allá de la función de riesgo

PREFACIO

El riesgo surge de todas partes: cambios geopolíticos, disrupciones tecnológicas, volatilidad económica y mucho más.

Koen Claessens
Global Head of Risk Advisory Services,
BDO Belgium
koen.claessens@bdo.be

El ritmo del cambio exige que las empresas ya no puedan permanecer al margen esperando a que las condiciones mejoren: deben estar preparadas para actuar con decisión y asumir riesgos calculados, incluso cuando el futuro sea incierto.

El problema es que muchas organizaciones siguen funcionando con un enfoque de gestión de riesgos demasiado limitado y teórico para actuar con eficacia.

Los líderes empresariales reconocen la preocupante situación de riesgo actual y futura. Ocho de cada diez afirman que el panorama global de riesgos está ahora más marcado por las crisis que nunca. Sin embargo, muchos tienen dificultades para actuar con rapidez porque la gestión de riesgos sigue estando a cargo de equipos especializados que trabajan de forma aislada, lo que limita la perspectiva y ralentiza la toma de decisiones.

El coste estratégico de la lentitud en la actuación, o incluso de la inacción, ya no se limita a las oportunidades de negocio perdidas: la supervivencia de las organizaciones está potencialmente en juego si no son capaces de tomar decisiones proactivas y oportunas en materia de riesgos. En otras palabras, la aversión al riesgo se convierte en un riesgo en sí misma.

Para desenvolverse en este nuevo mundo inestable, las empresas deben abandonar los enfoques tradicionales de gestión de riesgos y adoptar un futuro donde la responsabilidad del riesgo se comparta mediante un enfoque holístico. Esto garantiza que las organizaciones obtengan una visión más integral del panorama de riesgos y de cómo las múltiples amenazas interactúan con las distintas áreas del negocio, lo que permite una toma de decisiones más inteligente y coordinada.

Este informe analiza cómo la responsabilidad interfuncional en la gestión de riesgos puede impulsar mejores resultados y brindar a las empresas la confianza necesaria para asumir riesgos proactivos donde más importa.

8 de cada 10

líderes empresariales afirman que el panorama global de riesgos está ahora más definido por las crisis que nunca

52%

de los líderes empresariales afirma tener dificultades para identificar qué señales de riesgo son realmente importantes y cuáles son el ruido de fondo

Índice

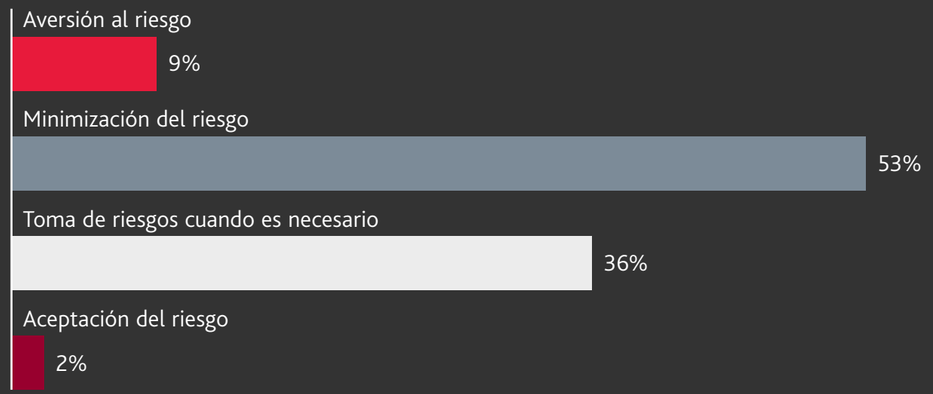
Resumen ejecutivo

Cultivar la confianza en una era de incertidumbre

La incertidumbre es ahora estructural. Las empresas que se mantienen a la defensiva corren el riesgo de ser superadas por aquellas dispuestas a tomar decisiones de riesgo calculado.

Ver página 06

Cómo los líderes empresariales categorizan su tolerancia al riesgo en al año 2026



Geopolítica: el riesgo que condiciona a todos los demás

La geopolítica ya no es un riesgo más entre muchos: es el factor multiplicador que amplifica las vulnerabilidades en la cadena de suministro, la ciberseguridad y la regulación. Los equipos directivos están divididos sobre qué consecuencias son las más importantes, lo cual, en sí mismo, representa un riesgo.

Ver página 12

El riesgo geopolítico es uno de los

tres principales

riesgos para los que los líderes empresariales se sienten poco preparados.

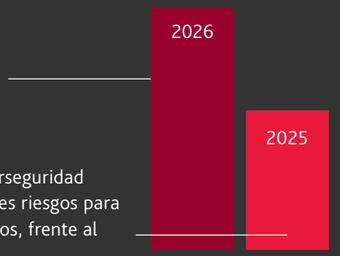
Ciberseguridad: El riesgo número uno sin un plan claro

Según dos de cada cinco líderes empresariales, el ciberriesgo es ahora el principal riesgo para el que las empresas no están preparadas. El gasto en ciberseguridad está aumentando, pero los ataques crecen aún más rápido. Mientras tanto, los equipos de ciberseguridad suelen incorporarse demasiado tarde a las iniciativas de transformación, y solo el 10 % participa en la fase de conceptualización.

Ver página 19

40%

de los líderes citan la ciberseguridad como uno de los principales riesgos para los que no están preparados, frente al 23% en 2025



Fraude: El riesgo mal entendido bajo una ilusión tecnológica

El fraude está perdiendo relevancia: el 93 % de los líderes no lo consideran un riesgo prioritario, y solo el 13 % está actualizando activamente sus medidas de seguridad (frente al 79 % del año pasado). Los líderes empresariales no pueden permitirse el lujo de restar importancia a la mitigación del fraude y esperar a que la tecnología se ponga al día.

Ver página 23

13%

está monitoreando y actualizando activamente sus defensas contra el fraude facilitado por IA, una cifra inferior al

79% del año pasado

IA: del auge a la aplicación práctica, con un control desigual

El optimismo en torno a la IA va en aumento. Sin embargo, a medida que los proyectos piloto pasan a la fase de implementación real, las deficiencias en materia de gobernanza se acentúan. La IA amplifica las deficiencias existentes en los datos, los controles y el cumplimiento normativo, en lugar de corregirlas.

Ver página 26

Los cinco principales riesgos de la IA según los líderes empresariales

Encuesta realizada a 500 altos ejecutivos de todo el mundo entre diciembre de 2025 y enero de 2026. Para obtener más información, consulte la página 31.

Cultivar la confianza en una era de incertidumbre

Por qué la propiedad compartida debe ser el nuevo enfoque del riesgo

De un vistazo

Qué está cambiando:

La volatilidad persistente y el colapso de las normas geopolíticas e institucionales están trastocando los modelos tradicionales de gestión de riesgos.

Por qué es importante:

La supervivencia de la empresa está en juego.

Qué hacer:

Tratar la gestión de riesgos como un facilitador estratégico, no como una función defensive.

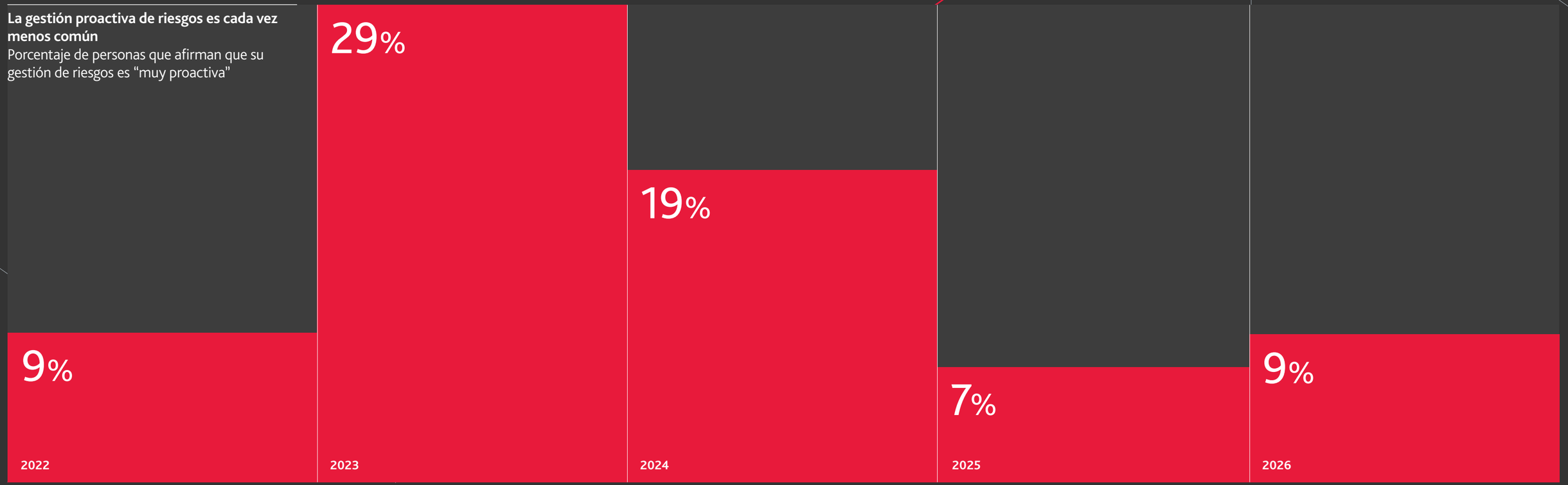
El coste de quedarse de brazos cruzados en tiempos de crisis ya no se limita a perder nuevas oportunidades de negocio. Para muchas empresas, se trata ahora de su supervivencia a largo plazo.

Más de un tercio de los líderes empresariales (68%) coinciden en que la velocidad con la que las crisis impactan en sus organizaciones está aumentando, frente al 54% de hace un año.

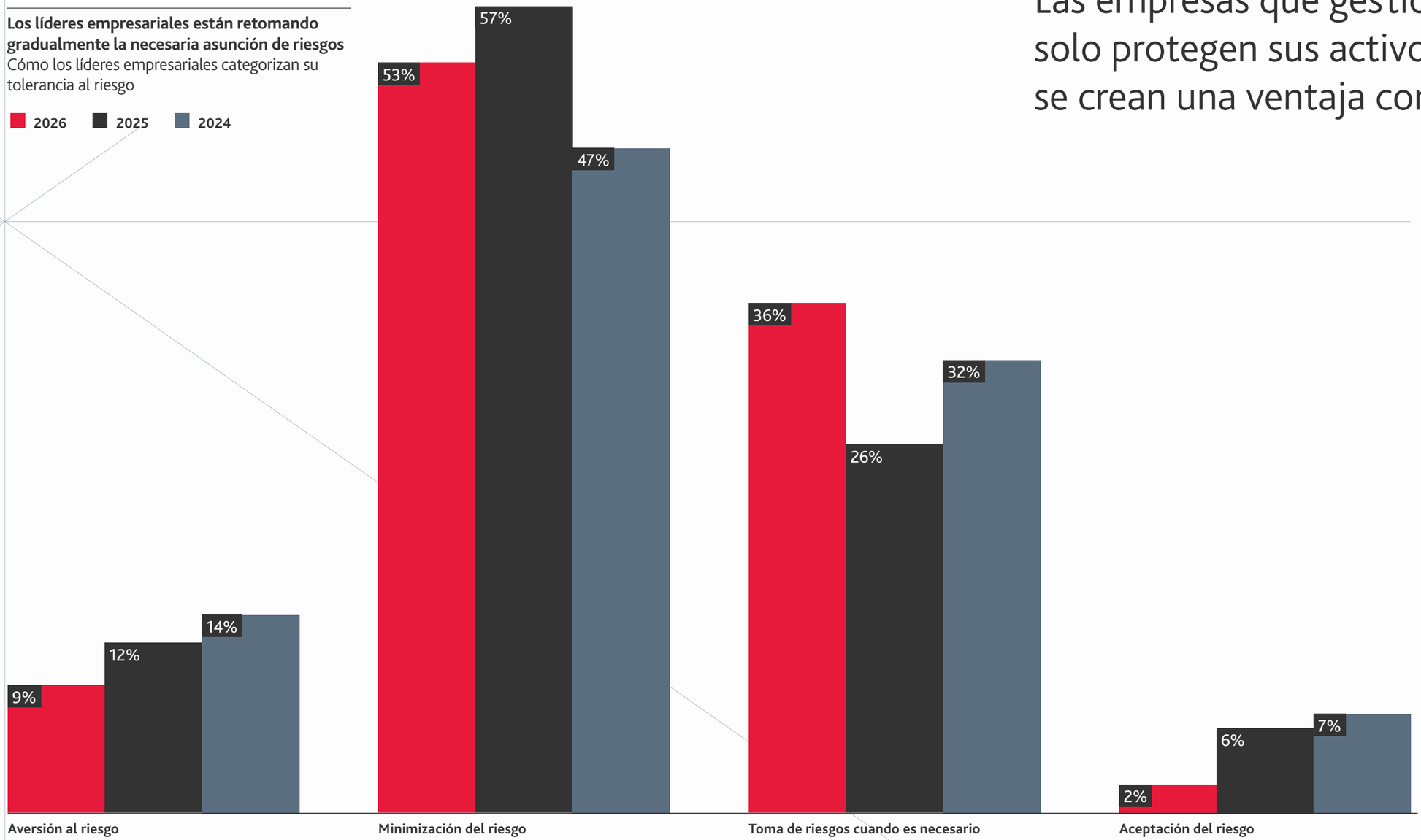
El riesgo de la inacción no se debe únicamente a la frecuencia de las crisis. También está condicionado por el ritmo de cambio global, acelerado por factores como la IA. Ante esta inestabilidad, las organizaciones reconocen cada vez más que los enfoques tradicionales de gestión de riesgos resultan insuficientes: para sobrevivir, necesitan asumir riesgos más calculados.

"Para algunas empresas, esto es una cuestión existencial", afirma Alisa Voznaya, Partner and Head of Risk Consulting de BDO UK. "Si no asumen riesgos ahora, no habrá negocio. Por lo tanto, aquellas organizaciones que tradicionalmente han sido reacias al riesgo están teniendo que revisar su enfoque; de lo contrario, simplemente no sobrevivirán en el futuro".

La gestión proactiva de riesgos es cada vez menos común
Porcentaje de personas que afirman que su gestión de riesgos es "muy proactiva"



Los líderes empresariales están retomando gradualmente la necesaria asunción de riesgos
Cómo los líderes empresariales categorizan su tolerancia al riesgo



"Las empresas que gestionan bien el riesgo no solo protegen sus activos, sino que también se crean una ventaja competitiva."

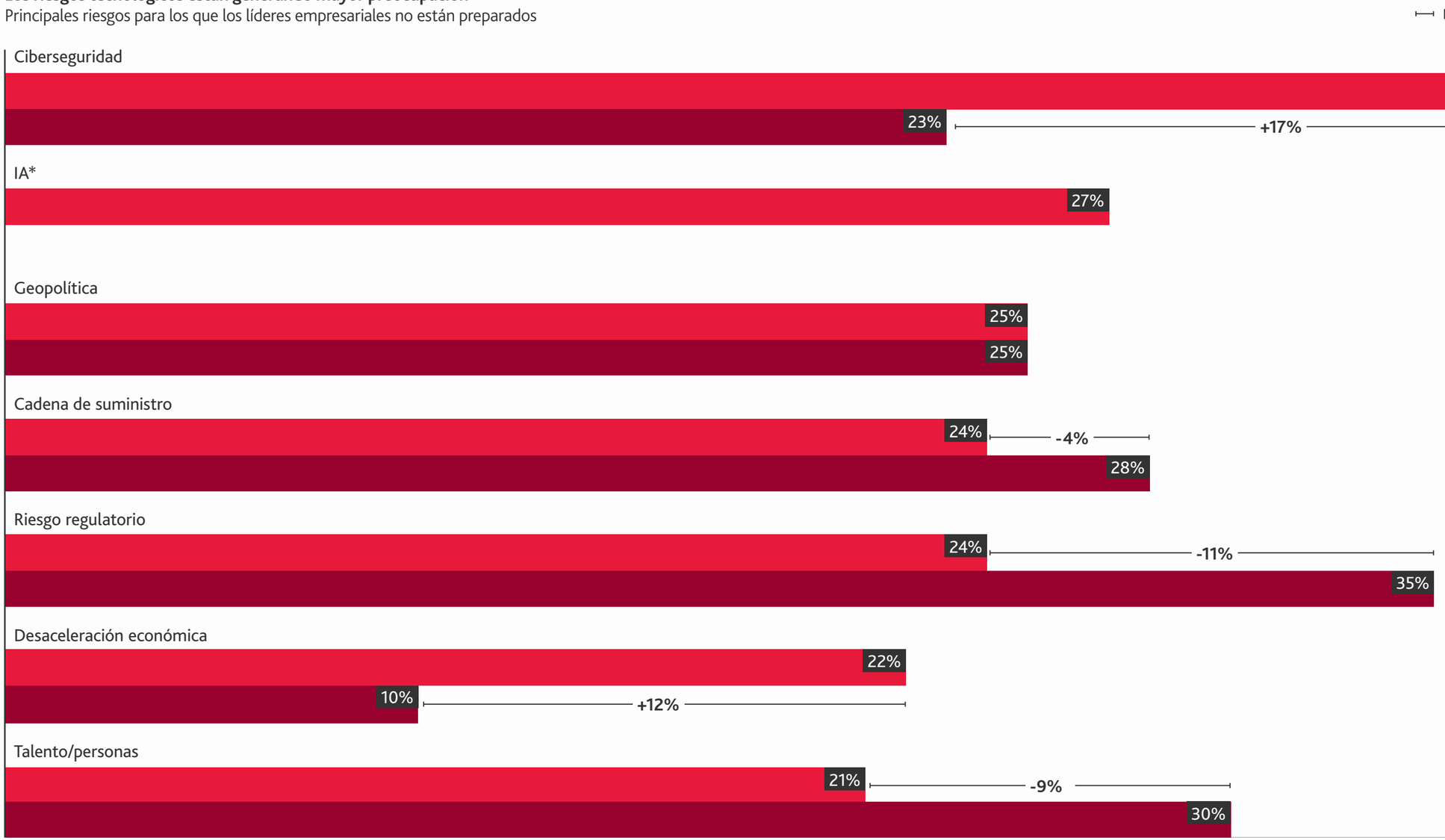
Ese riesgo existencial se ve agravado por una serie de problemas que se presentan simultáneamente: la interrupción de la cadena de suministro, la intensificación de la competencia y el aumento de la carga regulatoria. Individualmente, estos riesgos podrían ser manejables. Pero cuando ocurren todos a la vez, su interacción puede significar que "acaben con tu negocio de inmediato", afirma Voznaya.

Otras empresas están empezando a darse cuenta de que no se puede esperar a que se produzca una crisis para reaccionar, añade Voznaya: saben que deben empezar a anticiparse a los posibles riesgos (y oportunidades) que se avecinan.

Los datos muestran que un número creciente de empresas está adoptando un enfoque de riesgo más calculado: el 36% de los líderes empresariales afirma que ahora asume riesgos cuando es necesario, en comparación con el 26% de hace un año.

"Creo que las empresas que gestionan bien el riesgo no solo protegen sus activos, sino que también crean una ventaja competitiva", afirma Matteo De Renzi, CEO de la plataforma de reservas de taxis Gett.

Los riesgos tecnológicos están generando mayor preocupación
Principales riesgos para los que los líderes empresariales no están preparados



Sin embargo, los datos sugieren que las empresas siguen reaccionando a los acontecimientos en lugar de tomar decisiones de riesgo calculadas con antelación, ya que solo el 9% de los encuestados afirma que su gestión de riesgos es "muy proactiva".

De hecho, la mayoría de las empresas aún se encuentran en modo de protección, y el 53 % de los encuestados afirma estar minimizando los riesgos. Una posible razón de esta reticencia al riesgo es que las empresas tienen una visión limitada , teórica y jerárquica de la gestión de riesgos, según Koen Claessens, Global Head of BDO Risk Advisory. La magnitud de la incertidumbre implica que los líderes empresariales también pueden carecer de la confianza necesaria para tomar decisiones proactivas, lo que lleva a muchos a adoptar una postura defensiva en lugar de una visión ofensiva y con visión de futuro del riesgo.

*Esta opción de respuesta se introdujo este año en vista del creciente riesgo de la IA

"Los líderes empresariales deben encontrar el equilibrio adecuado entre la gestión de riesgos y el modo de hibernación, debido al exceso de riesgos a su alrededor; de lo contrario, esto perjudica el crecimiento", afirma Johanna Pudda, CEO de Staci Americas, empresa de gestión de la cadena de suministro y el almacenamiento.

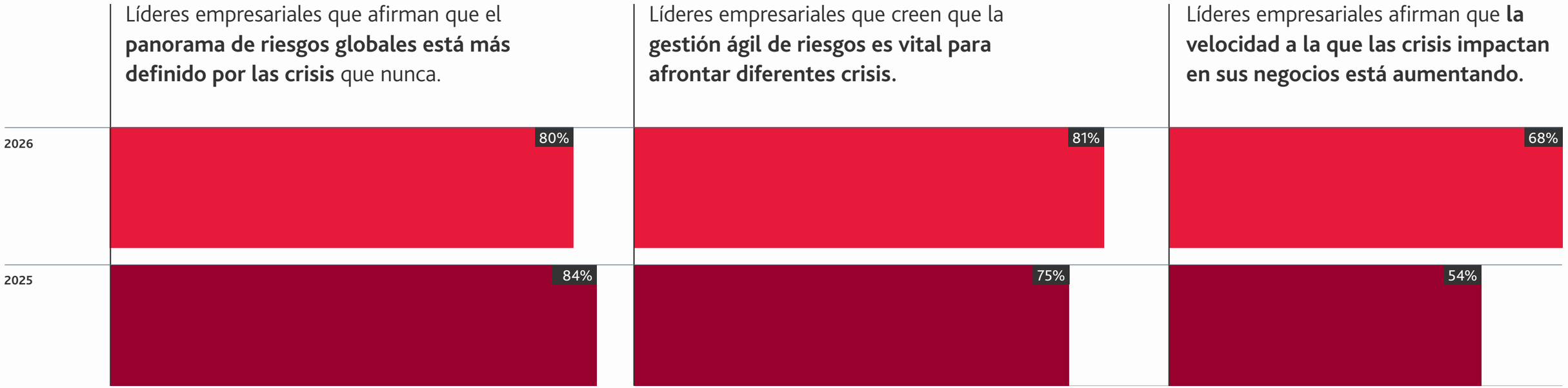
Esto no significa que las organizaciones necesiten una mayor tolerancia al riesgo. Simplemente significa que debe existir una visión más clara y compartida de cómo las decisiones sobre riesgos afectarán al negocio en general.

Un desafío clave es que las empresas a menudo se ven abrumadas por problemas operativos cotidianos. Alrededor del 55% de los líderes empresariales afirman que las presiones operativas a corto plazo frecuentemente prevalecen sobre su planificación de riesgos predictiva o a largo plazo, mientras que el 52% afirma tener dificultades para identificar qué señales de riesgo son realmente importantes y cuáles son el ruido de fondo.

"A las organizaciones les puede resultar muy difícil prever el tipo de riesgo al que se enfrentan, especialmente cuando se trata de algo que no habían considerado anteriormente o si está fuera de su control", afirma Ricky Cheng, Director and Head of Risk Advisory de BDO Hong Kong.

"Las organizaciones no necesitan una mayor tolerancia al riesgo. Debe existir una visión más clara y compartida de cómo las decisiones en materia de riesgo afectarán al conjunto de la empresa."

La crisis es ahora la norma y la agilidad se considera esencial



Las prioridades contrapuestas y abrumadoras son un problema creciente

55%

de los líderes empresariales afirma que las presiones operativas a corto plazo suelen prevalecer sobre su planificación de riesgos a largo plazo o predictiva

52%

afirma tener dificultades para identificar qué señales de riesgo son realmente importantes

Sin embargo, el desafío no reside únicamente en identificar las señales de riesgo, sino en gestionar esos riesgos de forma coordinada. Este es un obstáculo frecuente, ya que la gestión de riesgos suele considerarse una disciplina especializada y no una responsabilidad compartida entre las distintas áreas funcionales. Esto genera una brecha cada vez mayor entre las organizaciones que pueden definir su posición de riesgo con la confianza necesaria para tomar decisiones más ágiles y aquellas que tienen dificultades por carecer de una visión coherente del riesgo en toda la empresa. En este contexto, la capacidad de actuar con cierto grado de incertidumbre se convierte en una ventaja competitiva.

Para lograrlo, la gestión de riesgos debe pasar de ser una función defensiva a una capacidad estratégica. Por lo tanto, las organizaciones deben definir su tolerancia al riesgo y dónde enfocar sus esfuerzos para mitigarlo. Esto implica identificar oportunidades de gestión de riesgos y no solo adoptar una postura defensiva automática ante las interrupciones.

"Si no comprendes tu nivel de riesgo, terminas sin moverte, y no moverse también es una decisión", afirma Richard Liao, CEO de Hwa-Hsia Glass, empresa taiwanesa de embotellado de vidrio. "Significa que tus competidores serán quienes aprovechen las oportunidades que tú no".

INSIGHT

El riesgo no es una barrera. Quedarse quieto sí lo es

Por qué ya no se sostiene el argumento a favor de una gestión cautelosa del riesgo

Alisa Voznaya

Partner and Head of Risk Consulting at BDO UK

En los últimos años, las empresas han adoptado un enfoque que minimiza los riesgos, o incluso los evita, en la gestión de sus operaciones, con la esperanza de "abordar los problemas cuando las cosas mejoren". Esta mentalidad ya no sirve : las empresas se han dado cuenta de que ya no es posible quedarse de brazos cruzados y esperar resultados positivos.

Muchas empresas reconocen ahora que es fundamental asumir riesgos calculados. Existen dos enfoques paralelos. Uno es el de la supervivencia del modelo de negocio: la idea de que las empresas deben cambiar no para prosperar, sino simplemente para sobrevivir . El otro es una visión del riesgo más centrada en la previsión, donde se busca identificar vulnerabilidades y oportunidades.

El mundo ha cambiado. Desde una perspectiva estratégica, las reglas y normas tradicionales ya no son aplicables. Y si se han roto todas las reglas, los procesos antiguos no funcionarán. Es necesario pensar de forma innovadora para estar a la altura del desafío.

Geopolítica: El riesgo que moldea a todos los demás

Por qué ninguna función por sí sola puede gestionar el riesgo geopolítico

De un vistazo

Qué esta cambiando:

La geopolítica se está volviendo aún más impredecible y volátil.

Por qué es importante:

La geopolítica atraviesa todos los riesgos, amplificando otras exposiciones y actuando más como un factor causal.

Qué hacer:

Reunir puntos de vista interfuncionales para comprender el impacto colectivo en el negocio.

"El riesgo geopolítico solía ser una preocupación aislada. Ahora se está convirtiendo en el principal multiplicador de riesgos que nos preocupa a todos", Head of Risk Advisory Services de BDO Sudáfrica.

El riesgo geopolítico se reconoce cada vez más como un riesgo singular, ya que trasciende todos los demás riesgos y amplifica las vulnerabilidades en la cadena de suministro, la regulación y la ciberseguridad. Ante un contexto cada vez más volátil y unos impactos más pronunciados, las empresas están empezando a replantearse cómo gestionan las consecuencias geopolíticas.

Sin embargo, si bien los líderes coinciden en la magnitud de la amenaza, tienen opiniones divergentes sobre sus posibles impactos. Los Directores Ejecutivos, por ejemplo, creen que el principal impacto serán las cadenas de suministro fragmentadas, mientras que los líderes tecnológicos opinan que la mayor amenaza reside en la divergencia regulatoria. Por su parte, los directores financieros consideran que las amenazas geopolíticas relacionadas con la ciberseguridad serán la consecuencia más grave.

Esto subraya la necesidad de que las empresas adopten un enfoque compartido, coherente y ágil para la gestión de riesgos, que tenga en cuenta las perspectivas de todos los departamentos. Como explica Gonzalo García-Liñán, Risk Advisory Services Partner de BDO España: "El riesgo no afecta a todas las áreas de una empresa de la misma manera: su impacto es diferente en el departamento de finanzas que en el de operaciones o tecnología, por ejemplo. La mejor forma de gestionar los riesgos es dar voz a todos los implicados. Si se excluye a alguien, se perderá una perspectiva crucial".

"Nos enfrentamos a lo incontrolable", afirma Johanna Pudda, de Staci Americas. "Ahí es donde la agilidad de la organización cobra importancia, la estructura subyacente y la resistencia y resiliencia de la empresa ante este tipo de riesgos incontrolables en la actualidad".

El verdadero desafío reside en comprender cómo interactúan los riesgos y gestionar las demandas contrapuestas en materia de resiliencia, coste, velocidad y acceso al mercado. Ziad Akkaoui, Partner and National Risk Advisory Practice Leader de BDO Canadá, lo explica con claridad: "Las organizaciones toman mejores decisiones cuando dejan de tratar esto como un problema de coordinación y empiezan a abordarlo como un problema de modelo de decisión. Riesgo, operaciones, tecnología y finanzas deben colaborar desde el principio, con derechos de decisión claros, escenarios comunes y una visión consensuada de las ventajas y desventajas".

Las prioridades regionales difieren, pero la presión subyacente de los riesgos geopolíticos es la misma.
Amenazas geopolíticas para las organizaciones por región (próximos 12-18 meses)

	Europa	Oriente Medio	África	Asia-Pacífico	América
#1	Fragmentación de las cadenas de suministro	Restricciones tecnológicas/de datos transfronterizas	Divergencia regulatoria	Fragmentación de las cadenas de suministro	Amenazas geopolíticas habilitadas por la ciberseguridad
#2	Divergencia regulatoria	Divergencia regulatoria	Amenazas geopolíticas habilitadas por la ciberseguridad	Divergencia regulatoria	Divergencia regulatoria
#3	Amenazas geopolíticas habilitadas por la ciberseguridad	Fragmentación de las cadenas de suministro	Cambios arancelarios impredecibles	Amenazas geopolíticas habilitadas por la ciberseguridad	Restricciones tecnológicas/de datos transfronterizas

El riesgo geopolítico es uno de los tres principales riesgos para los que los líderes empresariales se sienten menos preparados este año.

Los líderes coinciden en la magnitud de la amenaza, no en el peligro específico
Amenazas geopolíticas para las organizaciones según el puesto de trabajo (próximos 12-18 meses)

	CEOs	Líderes tecnológicos	Directores financieros
#1	Fragmentación de las cadenas de suministro	Divergencia regulatoria	Amenazas geopolíticas habilitadas por la ciberseguridad
#2	Divergencia regulatoria	Restricciones tecnológicas/de datos transfronterizas	Restricciones tecnológicas/de datos transfronterizas
#3	Inestabilidad política regional	Amenazas geopolíticas habilitadas por la ciberseguridad	Amenazas geopolíticas habilitadas por la ciberseguridad

"El objetivo no es esperar a tener la información perfecta, sino crear la alineación necesaria, con la suficiente antelación, para actuar con decisión. Así es como se traduce realmente la democratización del riesgo en la práctica: mayor responsabilidad, juicios más rápidos y mejores decisiones a nivel empresarial".

Estas decisiones son demasiado trascendentales como para limitarse a una única función de gestión de riesgos, razón por la cual la toma de decisiones coordinada entre equipos se ha vuelto tan importante.

Fundamentalmente, las organizaciones deben definir su tolerancia al riesgo. Esto implica comprender claramente las amenazas existentes. Más aún, implica determinar qué riesgos son aceptables, cuáles requieren mitigación y cuáles exigen una acción inmediata.

En este entorno, el riesgo ya no es un evento esporádico y aislado. Es el nuevo modelo operativo el que determinará si las empresas pueden sobrevivir y prosperar en un mundo cada vez más inestable.

"El objetivo no es esperar a disponer de toda la información, sino crear el consenso suficiente, con la debida antelación, para actuar con decisión."

La geopolítica está obligando a las empresas a pensar de manera diferente sobre el riesgo

Erin Sells
Principal, Risk Advisory Services
at BDO USA

Para lograr respuestas más contundentes se necesitan voces diversas

Para combatir el riesgo, es necesario considerar la diversidad de perspectivas en todas las áreas funcionales, reconociendo que existen diferentes estilos de liderazgo en cada país.

Hoy más que nunca, es preciso incorporar diversas perspectivas a la planificación de riesgos de una manera innovadora. Se trata de garantizar que todas las áreas funcionales tengan voz y voto en la forma en que las empresas abordan el riesgo.

Richard Walker
Head of Risk Advisory Services
at BDO South Africa

Por qué esperar no es una opción cuando se trata del riesgo geopolítico

Cuanto más rápido se intensifican los riesgos geopolíticos, antes deben los líderes empresariales empezar a evaluar su exposición, lo que a veces implica tomar decisiones basadas en datos incompletos.

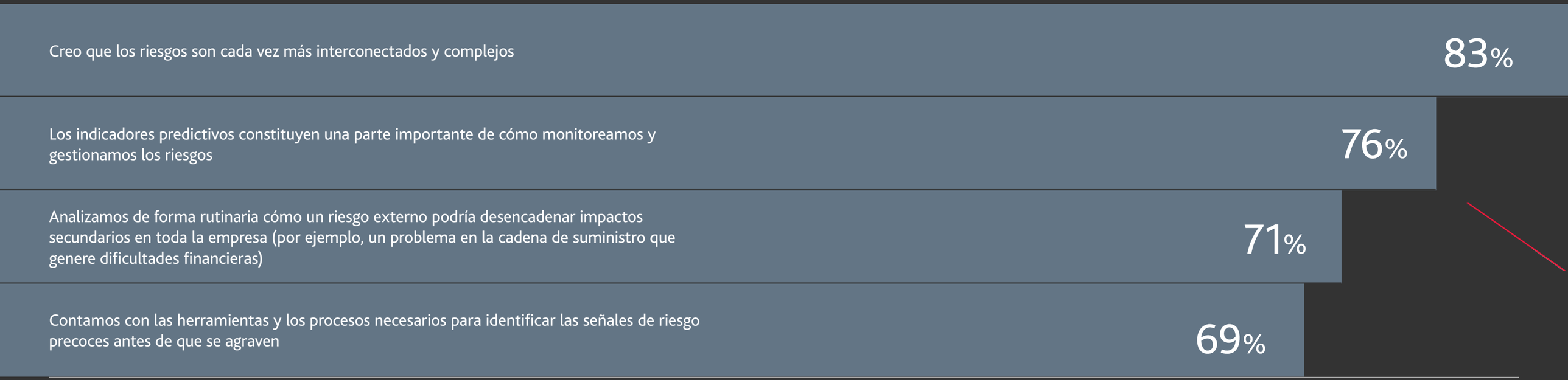
Si la información o la inteligencia recibida es apresurada e incompleta, la planificación de escenarios se vuelve esencial para mitigar el riesgo y determinar si el balance general puede afrontar la decision.

Cómo responden los líderes empresariales a la disrupción

Las organizaciones saben que los riesgos se multiplican y están cada vez más interconectados. Pero la mera concienciación no basta. Nuestros hallazgos revelan dónde residen las verdaderas deficiencias y qué están haciendo los líderes empresariales para subsanarlas.

89% considera las interdependencias entre los riesgos (por ejemplo, geopolíticos, de la cadena de suministro, cibernéticos, económicos) al evaluar las amenazas

Los líderes empresariales reconocen cómo los riesgos se influyen mutuamente y lo reflejan en su gestión de riesgos



Pero aún existen deficiencias en la eficiencia

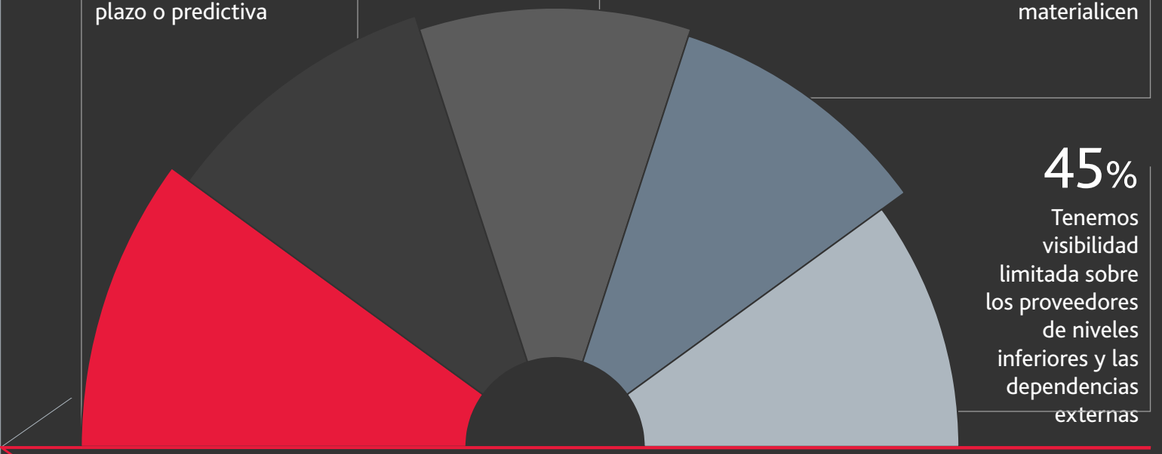
Los principales retos en materia de gestión de riesgos señalados por los líderes empresariales

55%
Las presiones operativas a corto plazo suelen prevalecer sobre la planificación de riesgos a largo plazo o predictiva

52%
Nos cuesta identificar qué señales de riesgo son realmente importantes y cuáles son el ruido

50%
La información sobre riesgos permanece aislada en distintos departamentos o funciones

49%
Carecemos de indicadores de alerta temprana consistentes para actuar antes de que los riesgos se materialicen



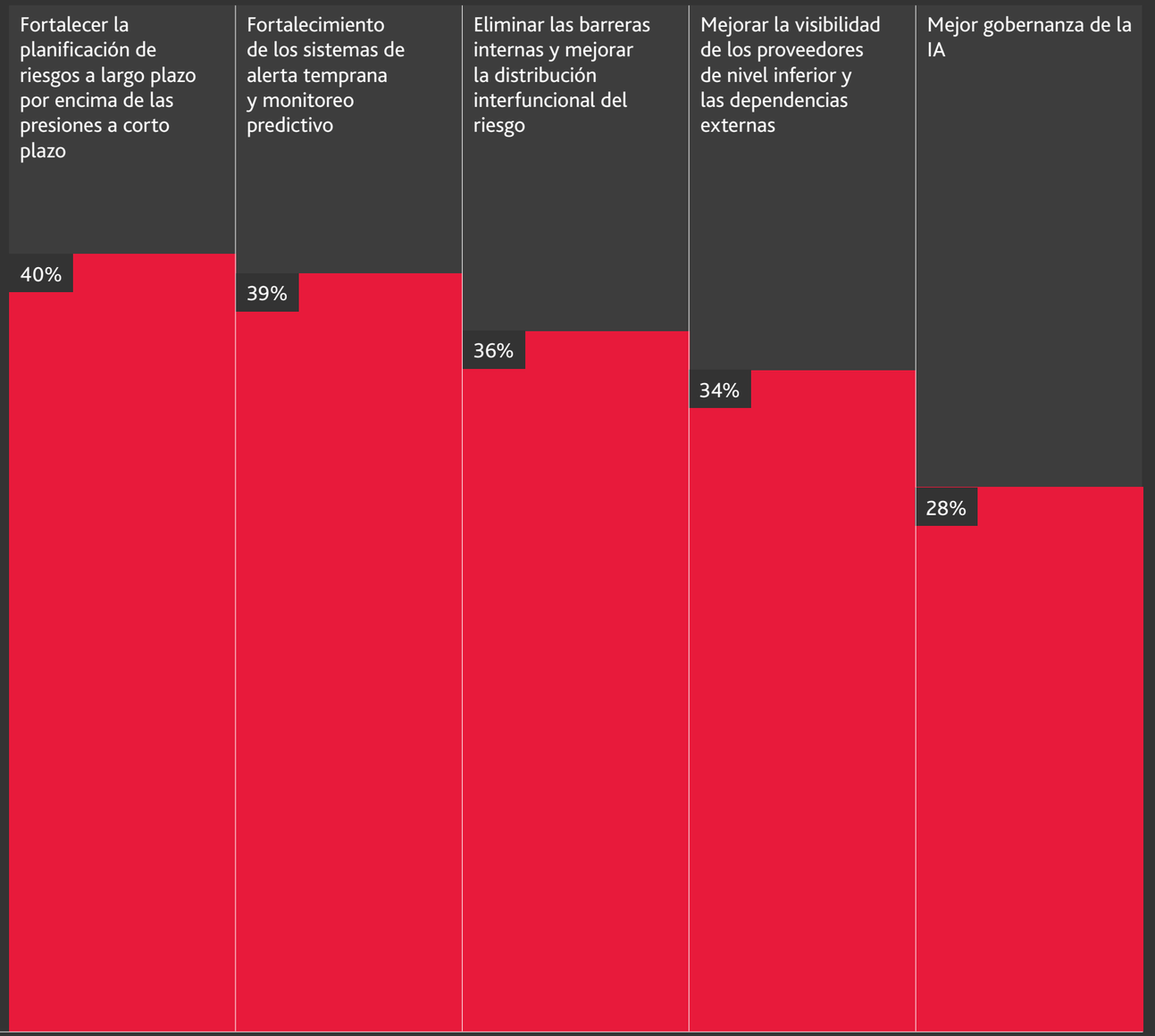
45%
Tenemos visibilidad limitada sobre los proveedores de niveles inferiores y las dependencias externas

99%

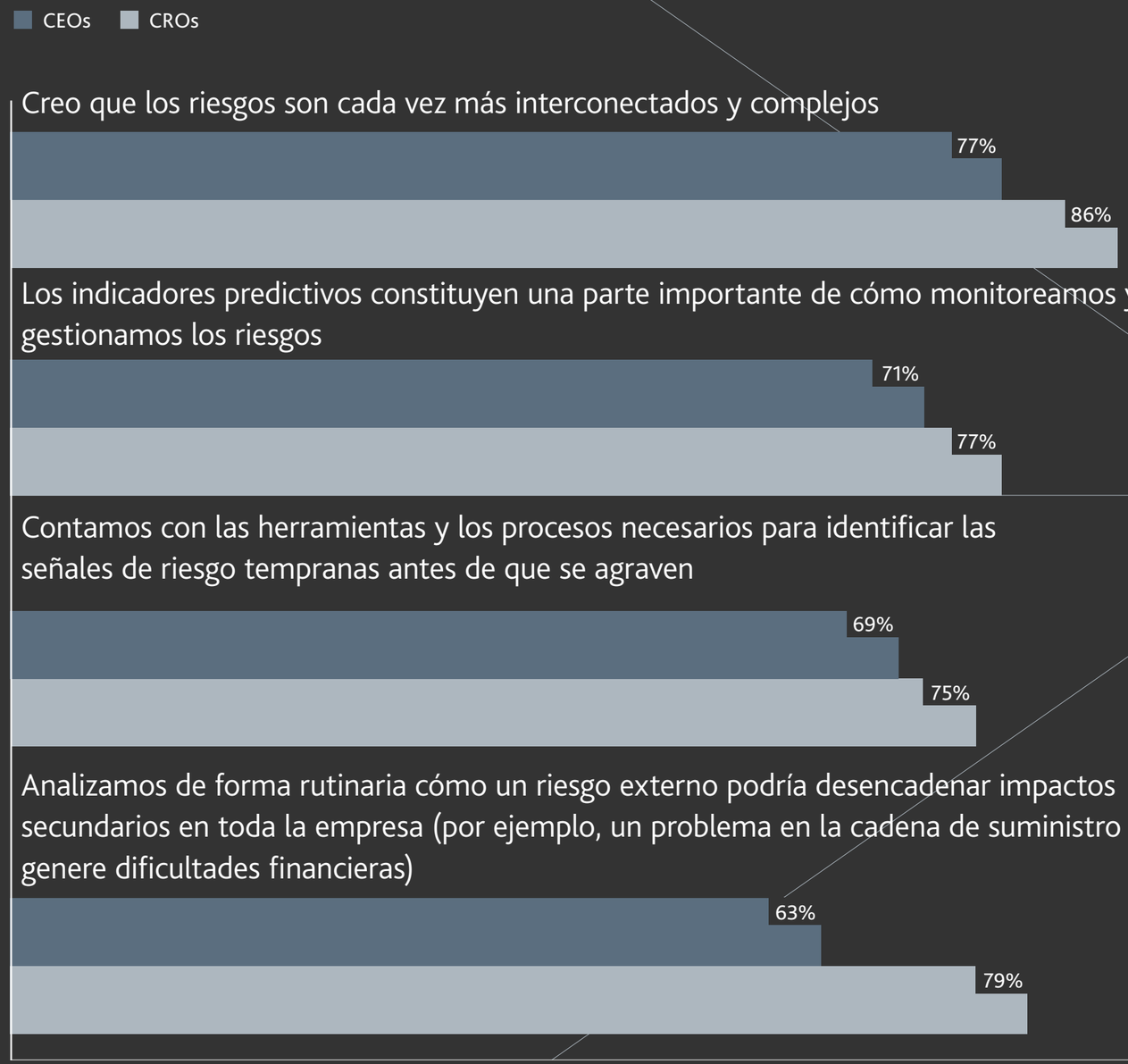
priorizará algún tipo de mejora en la gestión de riesgos para los próximos tres años

Si bien existe un claro deseo y acciones concretas para cerrar estas brechas…

Las mejoras en la gestión de riesgos que las organizaciones se han marcado como prioridad para los próximos tres años



...los equipos directivos aún no están completamente de acuerdo sobre la magnitud del problema



81%

de los líderes empresariales no priorizan la toma de decisiones equilibrada y compartida sobre el riesgo para el futuro

Ciberseguridad: El riesgo número uno sin un plan claro

Las crecientes amenazas están poniendo de manifiesto los límites de las estrategias tradicionales de ciberdefensa

De un vistazo

Lo que está cambiando:

Los ciberataques siguen aumentando a pesar del gasto cada vez mayor en ciberdefensa.

Por qué es importante:

La transformación tecnológica se está acelerando. La ciberseguridad debe mantenerse al día.

Qué hacer:

Preocúpese menos por una protección generalizada. En su lugar, busque una resiliencia más amplia.

Las organizaciones están invirtiendo sumas cada vez mayores en ciberseguridad. Sin embargo, esto no está frenando el ritmo de los ataques.

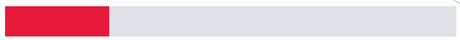
Según el Foro Económico Mundial, el número medio de ataques semanales aumentó un 58% a nivel mundial entre 2023 y 2025, o que ha elevado el riesgo cibernético al primer puesto entre los riesgos para los que, según afirman los líderes empresariales, no están preparados.

Parte del desafío radica en que los métodos tradicionales de gestión de riesgos cibernéticos ya no pueden seguir el ritmo de la rápida evolución de la tecnología y las capacidades que esta ofrece . Esto se debe a la resistencia organizacional o a que los equipos de ciberseguridad no se incorporan lo suficientemente pronto en el ciclo de transformación, afirma Rocco Galletto, Partner and Global Cybersecurity Leader de BDO Canadá.

Si bien muchos equipos de ciberseguridad se incorporan durante la fase de planificación de las iniciativas de transformación (57%), solo el 10% participa durante la fase de ideación y el 26% tiene que esperar hasta la fase de ejecución.

El panorama de amenazas evoluciona más rápido de lo que la gestión de riesgos cibernéticos puede seguirle el ritmo, y los ciberdelincuentes se aprovechan de las nuevas tecnologías. A diferencia de las empresas, que deben pasar por procesos de adquisición y aprobación complejos, los hackers pueden empezar a utilizar la tecnología de inmediato.

Los líderes empresariales no confían plenamente en sus inversiones en ciberseguridad.



23%

de los CEOs afirma que su empresa está invirtiendo menos de lo necesario en ciberseguridad.

1. Cybersecurity awareness: AI threats and cybercrime in 2025 | World Economic Forum

Las organizaciones deben aceptar que lo que funcionó en el pasado no funcionará en el futuro.

"Existen muchos problemas con el software o aspectos que pueden ser explotados en él, y la IA va a brindar la oportunidad de explotarlos antes de que ninguna organización se dé cuenta de que existe alguna amenaza", afirma John Messina, Consultor de TI y Ex Director de Informática del Gobierno Canadiense.

Los líderes empresariales también están divididos sobre cómo evolucionará el riesgo cibernético. Si bien el 35 % de los directores ejecutivos y líderes tecnológicos coinciden en que el riesgo cibernético es el principal en la actualidad, solo el 29 % de los directores ejecutivos cree que seguirá siéndolo durante los próximos cinco años, en comparación con el 41 % de los líderes tecnológicos.

Esta discrepancia sugiere una falsa sensación de seguridad, creyendo que la ciberseguridad siempre irá al ritmo de la transformación empresarial y tecnológica.

"Las organizaciones no operan de esa manera, y con la rápida implementación de la tecnología , esto introduce un mayor riesgo", afirma Galletto.

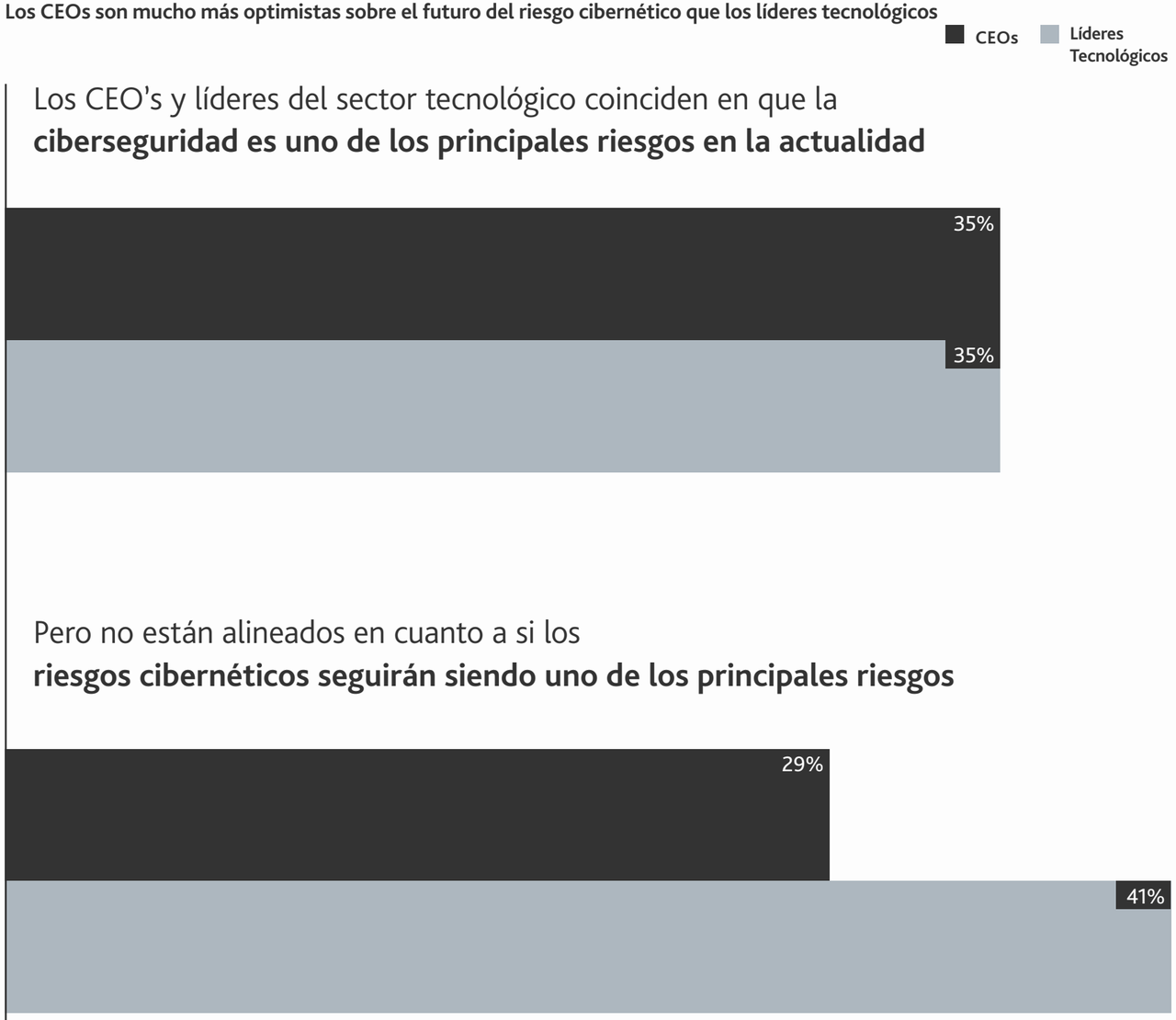
Aunque la mayoría de las organizaciones creen que invierten lo suficiente en ciberdefensa (solo el 23 % de los directores ejecutivos afirma que su empresa invierte menos de lo necesario en ciberseguridad), determinar el nivel de inversión adecuado sigue siendo un reto.

"Si te encuentras en un proceso de transformación continua, probablemente deberías invertir más para mantener el ritmo", afirma Galletto. "Si tu gasto en ciberseguridad está por debajo del promedio de tu sector, es probable que no estés invirtiendo de forma responsible".

Ante el continuo aumento de los ciberataques, los líderes empresariales se preguntan si se debe a que la inversión en ciberseguridad no crece lo suficientemente rápido como para mitigar el riesgo o a que se ven limitados por procesos obsoletos, añade Galletto. En cualquier caso, las organizaciones deben aceptar que lo que funcionó en el pasado no funcionará en el futuro . Las estrategias de ciberseguridad deben adaptarse a esta nueva era de riesgos.

En la práctica, esto implica una estrategia más dinámica que garantice que el gasto en ciberseguridad se mantenga al ritmo de la transformación tecnológica, al tiempo que se centra en la resiliencia y la respuesta de forma más específica . Los seres humanos siguen siendo el eslabón más débil en las defensas cibernéticas de una organización, por lo que la estrategia también debe garantizar la responsabilidad individual en todos los departamentos.

Los CEOs son mucho más optimistas sobre el futuro del riesgo cibernético que los líderes tecnológicos



La acción cibernética sigue centrándose en la respuesta y el cumplimiento
Las cinco principales prioridades de ciberseguridad para las empresas en los próximos dos años

#1
Mejorar la detección de amenazas 53%

#2
Nuevas medidas de cumplimiento 52%

#3
Mejorar la protección/ privacidad de los datos 49%

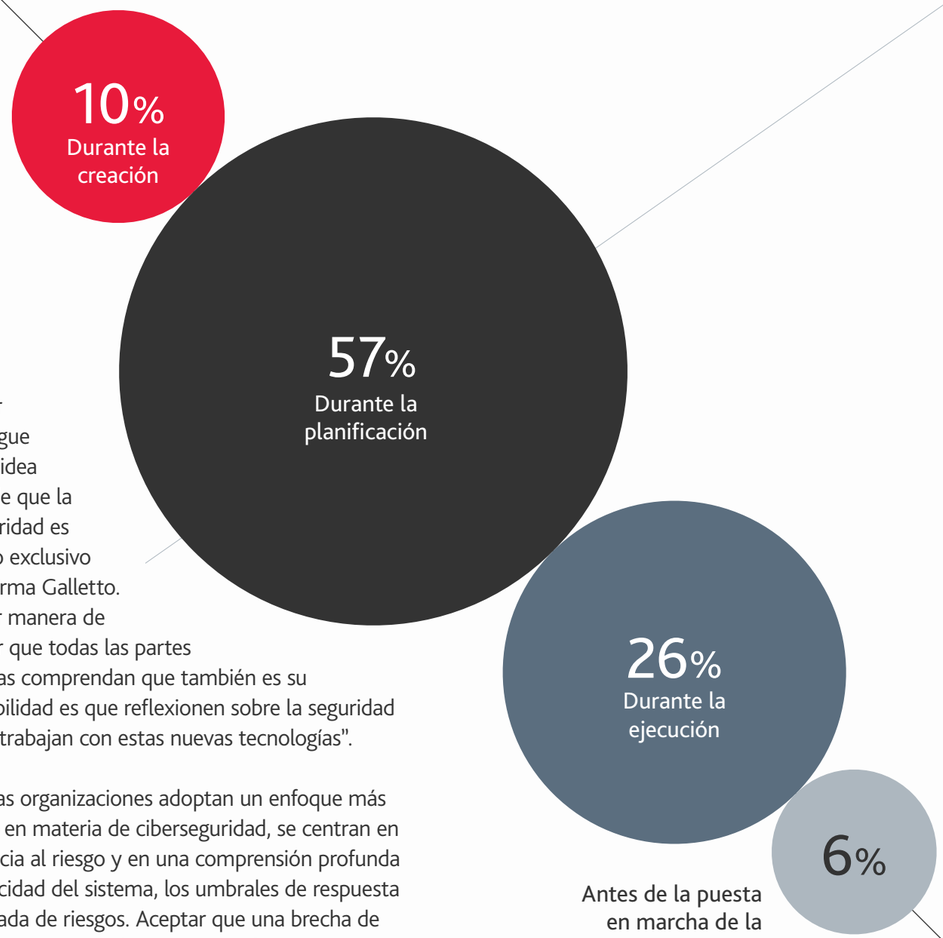
#4
Actualización de los planes de respuesta ante incidentes 48%

#5
Preparación para los riesgos impulsados por la IA 46%

La respuesta a incidentes y la IA están ganando terreno, pero la formación está quedando en segundo plano
Las tres principales medidas que los líderes empresariales tomarán en los próximos dos años para reducir el riesgo cibernético

Y a menudo se les pide a los equipos de ciberseguridad que protejan decisiones que ya se han tomado

Cuándo suelen participar los equipos cibernéticos en las iniciativas de transformación



"El mayor desafío sigue siendo la idea errónea de que la ciberseguridad es un asunto exclusivo de TI", afirma Galletto. "La mejor manera de garantizar que todas las partes interesadas comprendan que también es su responsabilidad es que reflexionen sobre la seguridad mientras trabajan con estas nuevas tecnologías".

Cuando las organizaciones adoptan un enfoque más proactivo en materia de ciberseguridad, se centran en la tolerancia al riesgo y en una comprensión profunda de la criticidad del sistema, los umbrales de respuesta y la escalada de riesgos. Aceptar que una brecha de seguridad es cuestión de tiempo, no de si ocurrirá, implica pasar de intentar protegerlo todo con un plan general a una planificación más estratégica centrada en la resiliencia.

INSIGHT

No trates lo cibernético como algo secundario

Los equipos de ciberseguridad deben participar en las decisiones desde el primer día

Rocco Galletto
Partner and Global Cybersecurity Leader at BDO Canada

La etapa ideal para que los equipos de ciberseguridad se involucren en las transformaciones empresariales es la fase de ideación, cuando se define la estrategia y la dirección. Esto tiene una buena razón: permite anticipar posibles amenazas e integrar la seguridad desde el principio. Si se involucra demasiado tarde, se corre el riesgo de quedarse atrás indefinidamente, y al ritmo que se mueven las empresas hoy en día, es imposible ponerse al día.

El problema es que las empresas no siempre comprenden el valor de contar con ciberseguridad desde el inicio, ni por qué debería ser un facilitador estratégico en lugar de un añadido de última hora antes de la puesta en marcha. Porque si se lanza un producto sin seguridad integrada, los ciberdelincuentes tienen todo el ciclo de vida del producto para encontrar una forma de infiltrarse.

El fraude: El riesgo mal entendido bajo una ilusión tecnológica

El fraude merece una mayor atención por parte de los directivos de la que recibe actualmente

De un vistazo

Lo que está cambiando:

Los líderes empresariales están menos preocupados por el riesgo de fraude

Por qué es importante:

El fraude sofisticado impulsado por IA está en aumento

Qué hacer:

Invertir en herramientas de IA para mejorar la detección y prevención del fraude

La tecnología deepfake, impulsada por IA, permite a los estafadores automatizar fraudes a gran escala, aumentando el riesgo para las empresas. Sin embargo, resulta alarmante que el fraude esté perdiendo protagonismo en la agenda ejecutiva. Aproximadamente el 93 % de los líderes empresariales no lo consideran una de las principales amenazas para las que no están preparados, lo que sugiere una grave subestimación de la amenaza.

Parte de la razón por la que el fraude se ha convertido en una prioridad menor no es porque el fraude haya disminuido, sino porque el marco de aplicación de la ley se ha relajado, particularmente en los EE. UU. Esto luego tiende a extenderse a otras grandes economías, dice Glenn Pomerantz, Principal & Forensic Leader de BDO USA y Global Forensic Leader.

"Cuando la aplicación de la ley es menos efectiva, simplemente no es una prioridad para los ejecutivos", dice Pomerantz.

Otra explicación es, sencillamente, que el fraude se está agrupando con otros factores de riesgo, en particular los cibernéticos y los relacionados con la inteligencia artificial, que fueron los dos principales riesgos notificados por las empresas este año.

"Cuando se excluyen la IA, la ciberseguridad y cosas como el fraude relacionado con activos digitales , lo que queda son los fraudes genéricos más comunes, que en realidad se parecen más a los fraudes de ayer", dice Pomerantz.

Si bien las empresas son conscientes del riesgo de fraude mediante IA (el 79 % de los líderes empresariales afirmó tener un plan para protegerse contra este tipo de fraude el año pasado), este año solo el 13 % declara estar monitoreando y actualizando activamente sus medidas de seguridad específicamente para el fraude con IA. Dada la rápida evolución de la tecnología subyacente, las organizaciones que no adopten un enfoque más dinámico ante el riesgo de fraude mediante IA serán cada vez más vulnerables.

El fraude es una amenaza que aún se malinterpreta en gran medida.

93%

de los líderes empresariales no cree que el fraude sea un riesgo importante para su organización

79%

de los líderes empresariales afirmaron tener un plan para defenderse del fraude impulsado por IA en 2025

Solo el 13%

está monitoreando y actualizando activamente sus defensas específicamente contra el fraude habilitado por IA en 2026

"Todo el mundo está centrado en la gobernanza de la IA, pero en lo que respecta a la prevención del fraude mediante IA, las empresas se están quedando atrás", afirma Pomerantz. "Los delincuentes se moverán con mayor rapidez, por lo que tendrán que revisar y mejorar constantemente sus medidas de protección contra el fraude".

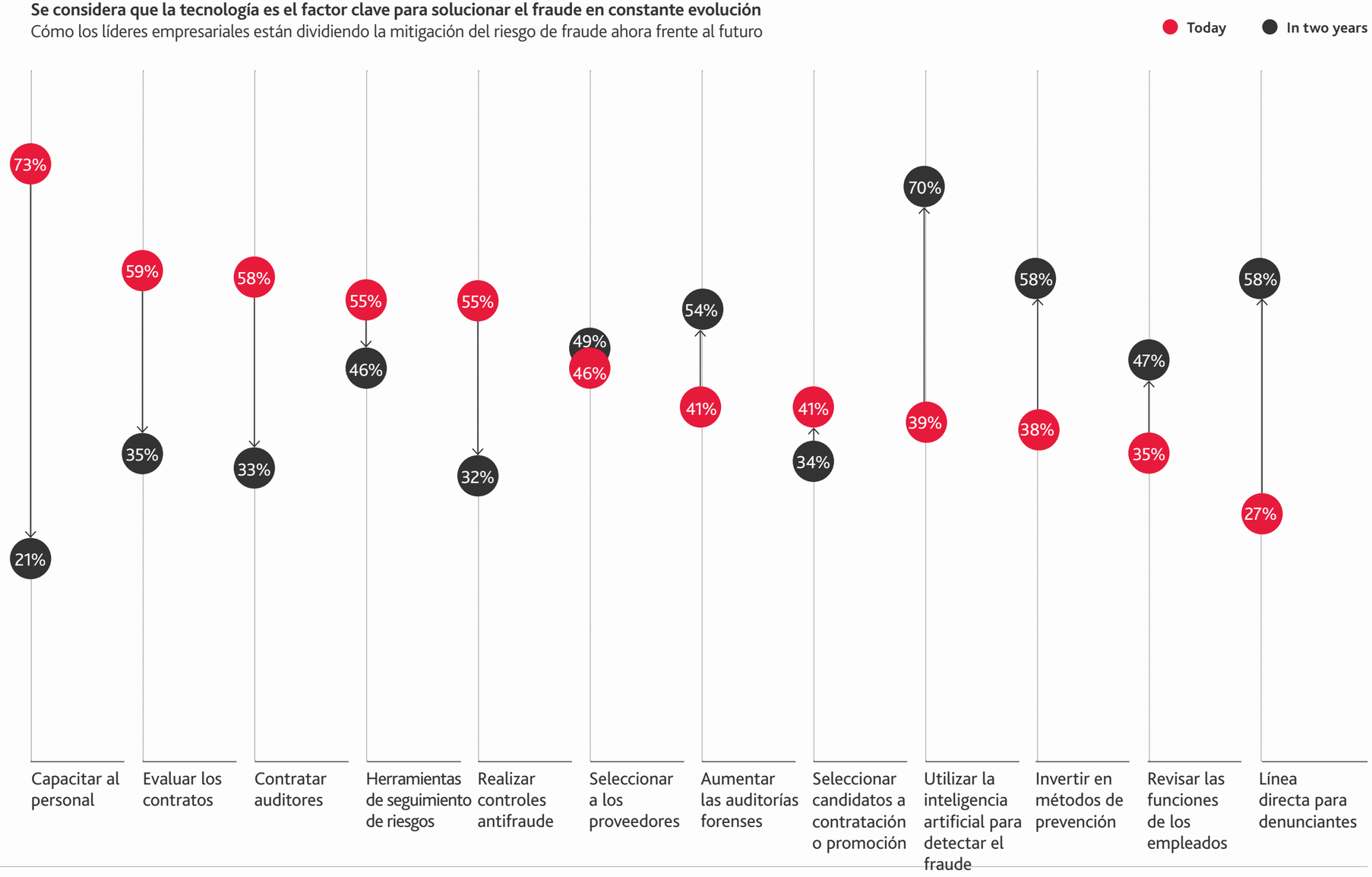
En la actualidad, las empresas están centrando sus esfuerzos para mitigar el riesgo de fraude en la formación del personal, pero esto cambiará en los próximos dos años, ya que la mayoría de los líderes empresariales esperan que sus organizaciones aumenten el uso de la IA para identificar el fraude .

Existe un inconveniente. Al esperar a que las herramientas avanzadas de IA combatan el fraude en lugar de rediseñar los controles para adaptarlos a las amenazas actuales, es probable que las organizaciones permanezcan en modo reactivo . Esto significa que el fraude solo se convertirá en una prioridad cuando (y no si) los estafadores logren atacar con éxito a la empresa. Esto recuerda las actitudes iniciales hacia el riesgo cibernético, donde los equipos directivos no comprendieron los beneficios de invertir en ciberseguridad hasta que sufrieron un incidente cibernético, afirma Richard Liao de Hwa-Hsia Glass.

"Se necesita paciencia y tiempo para que la gente comprenda la magnitud del problema antes de que se sumen a él", añade Liao.

Ante el aumento del riesgo provocado por la IA y el fraude cibernético, los líderes empresariales deben replantearse sus prioridades y renovar su enfoque para la mitigación del fraude hoy mismo, en lugar de simplemente esperar que la tecnología proporcione una mejor solución en el futuro.

Se considera que la tecnología es el factor clave para solucionar el fraude en constante evolución
Cómo los líderes empresariales están dividiendo la mitigación del riesgo de fraude ahora frente al futuro



El riesgo de fraude está aumentando en un mundo cada vez más volátil

Glenn Pomerantz
Principal & Forensic Market Leader at BDO USA

Áreas en las que las herramientas de IA pueden reducir el riesgo de fraude

Nuestros datos muestran que las herramientas de IA para la mitigación del fraude se utilizarán con mayor frecuencia dentro de dos años que ahora, probablemente debido al presupuesto necesario y a la necesidad de una formación adecuada del personal. Estas soluciones también deben personalizarse para cada negocio, en lugar de adquirir soluciones estándar.

La debida diligencia de terceros es un buen ejemplo de dónde la IA está empezando a desempeñar un papel importante. Si ya utiliza la IA para el trabajo de investigación en inteligencia corporativa global, el siguiente paso es aplicarla al cumplimiento normativo y a la verificación de terceros. También podríamos verla surgir en la selección y verificación de altos directivos, donde las empresas

Markus Brinkmann
Partner and Head of Forensic, Risk & Compliance at BDO Germany

La prevención del fraude es cada vez más dinámica

Los retos geopolíticos actuales están generando volatilidad e incertidumbre en toda la economía mundial, lo que aumenta drásticamente la probabilidad de que se produzcan fraudes. Las empresas operan en un entorno en el que factores como las interrupciones en las cadenas de suministro, las tensiones geopolíticas, el cambio climático y las presiones normativas cambiantes hacen que los riesgos sean más difíciles de predecir y de supervisar de forma sistemática. Al mismo tiempo, las organizaciones dependen de sistemas y procesos digitales cada vez más complejos que pueden generar vulnerabilidades adicionales si la gobernanza no se adapta al ritmo de estos cambios.

Los riesgos ya no pueden tratarse como algo estático. En un entorno volátil, las empresas deben identificar y reevaluar los riesgos de forma continua, ya que las amenazas pueden evolucionar muy rápidamente, sobre todo a medida que las tácticas de fraude se vuelven más sofisticadas y están impulsadas por la tecnología.

AI: Del auge a la aplicación práctica, con un control desigual

Por qué la gobernanza de la IA debe avanzar al mismo ritmo que su

De un vistazo

Qué está cambiando:

El optimismo en materia de IA crece a medida que los proyectos piloto pasan a una implementación más amplia

Por qué es importante:

El riesgo aumenta a medida que se amplía el uso de la IA, lo que amplifica cualquier debilidad en la gobernanza y el control

Qué hacer:

Asegurarse de que el riesgo de la IA se comparta entre todas las funciones, y no recaiga únicamente sobre los equipos técnicos

El optimismo en torno a la IA está en auge. Sin embargo, esto podría estar impidiendo que los líderes empresariales vean los riesgos potenciales que se amplifican cuando los sistemas de IA se integran en toda la organización.

Se necesita un enfoque más equilibrado.

“Las organizaciones que tratan la IA como una mera oportunidad son ingenuas, y aquellas que la tratan como un mero riesgo en algún momento serán superadas o derrotadas por la competencia", dice Matteo De Renzi de Gett.

A medida que los proyectos piloto avanzan hacia una implementación más estructurada, está surgiendo una brecha cada vez mayor entre quienes ven la IA como una oportunidad y quienes proceden con mayor cautela.

Las preocupaciones sobre los riesgos no se refieren a la tecnología en sí, sino a las repercusiones operativas que podrían exponer las debilidades existentes, y la prisa por integrar la IA podría estar enmascarando una creciente brecha de gobernanza.

“Si vas a utilizar inteligencia artificial, la lección clave que debes aprender de antemano es que tus datos tienen que estar en muy buen estado”, afirma el consultor informático John Messina.

Esto es importante porque si la propiedad de los datos no está clara o los controles de calidad son deficientes, es probable que la IA amplifique esos defectos.

“En mi opinión, la IA no corrige esos problemas . En cambio, los incorpora a las decisiones automatizadas, a menudo a gran escala, lo que dificulta su detección y solución una vez que están en producción”, afirma Karen Schuler, Principal & Cyber Market Leader de BDO USA y Global Privacy, Data & AI Leader. “Si su sistema no estaba en orden, la situación solo empeorará y se agravará tras la implementación de la IA”.

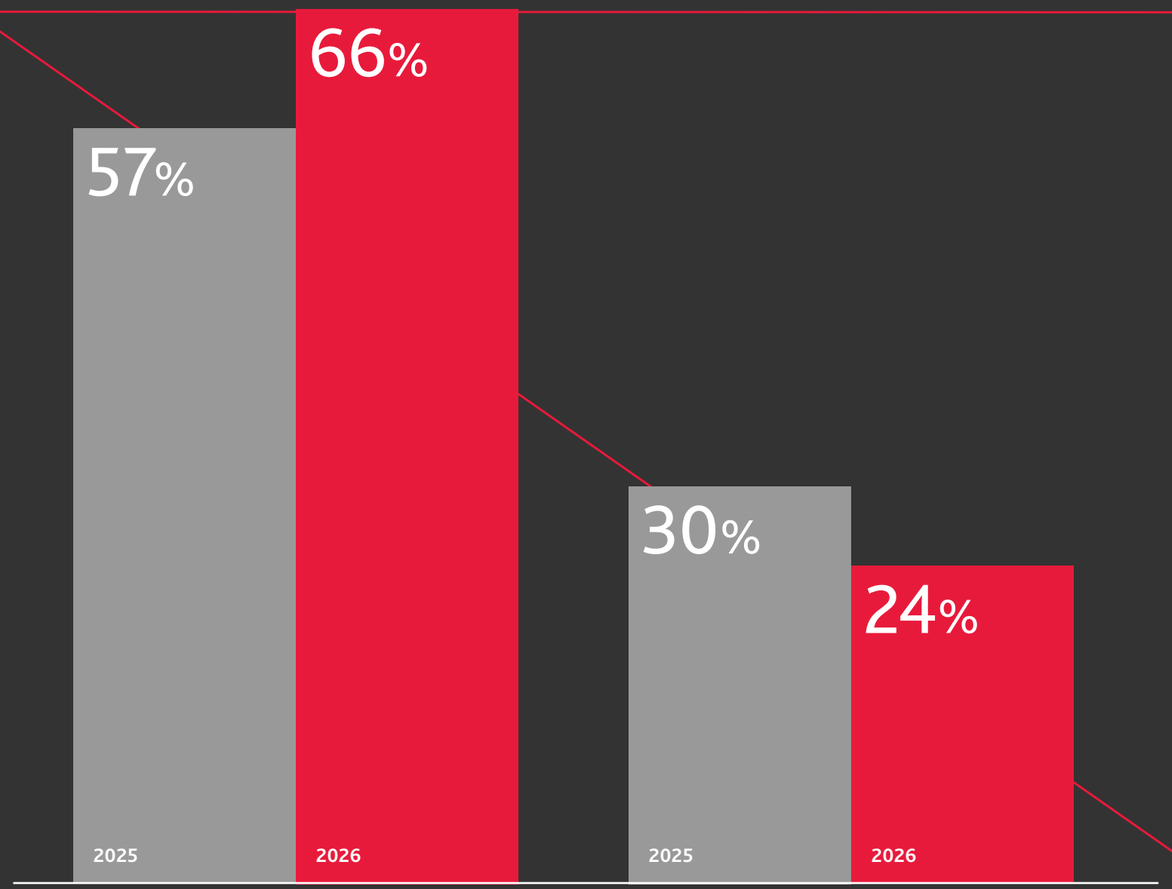
“Desde mi punto de vista, dado que la IA abarca diversas funciones, se trata esencialmente de una prueba de estrés para la capacidad organizativa, que revela si la gobernanza y los controles están realmente integrados y se aplican de forma coherente.”

Schuler sostiene que un nivel de riesgo claramente definido permite a las organizaciones establecer los parámetros de esta prueba de estrés con antelación, en lugar de descubrir sus límites solo cuando algo sale mal. “Estas deficiencias no son nuevas; existen desde hace mucho tiempo, pero la IA las hace más visibles y con mayores consecuencias”, añade.

Ese impacto interfuncional también significa que, en su opinión, la responsabilidad en materia de riesgos de la IA debe compartirse en toda la empresa y no dejarse únicamente en manos de los equipos de tecnología.

“La IA supone una prueba de resistencia para la capacidad de la organización, ya que pone de manifiesto si la gobernanza y los controles están realmente integrados y se aplican de forma coherente.”

La confianza en la IA está aumentando a medida que los casos de uso se vuelven más concretos



Schuler señala: “Las organizaciones necesitan desarrollar un entendimiento común sobre cómo gestionar el riesgo de la IA a gran escala . No es necesario que todos sean científicos de datos, pero sí se requiere un nivel básico de conocimientos sobre IA en los equipos directivos para que puedan transmitir ese conocimiento a sus equipos”.

Para mejorar la capacidad organizativa, los líderes empresariales deben contar con la cultura de riesgo adecuada. Además, necesitan estar dispuestos a adoptar el cambio organizativo.

Casi uno de cada nueve directores ejecutivos de las 1.500 mayores empresas que cotizan en bolsa fueron reemplazados el año pasado, la cifra más alta desde al menos 2010, según el Wall Street Journal. Esta transformación es una señal de que las viejas formas de pensar ya no son suficientes en este nuevo entorno operativo.

“Los líderes que se aferran a sus costumbres y se resisten al cambio no van a ser la respuesta a hacia dónde debe ir el negocio”, dice Ric Opal, Principal & National Leader, IT Solutions de BDO USA y Global Digital Leader.

Para afrontar este desafío, las empresas deberían adoptar un marco de trabajo de IA basado en la creación, la seguridad y el crecimiento, que les permita mejorar la agilidad en entornos de incertidumbre y, en última instancia, fortalecer la resiliencia empresarial.

Los principales riesgos de la IA residen en los datos, el cumplimiento normativo y la integración
Los cinco principales riesgos de la IA que más preocupan a los líderes empresariales

#1 | Privacidad de datos

#2 | Desafíos de cumplimiento

#3 | Ciberseguridad

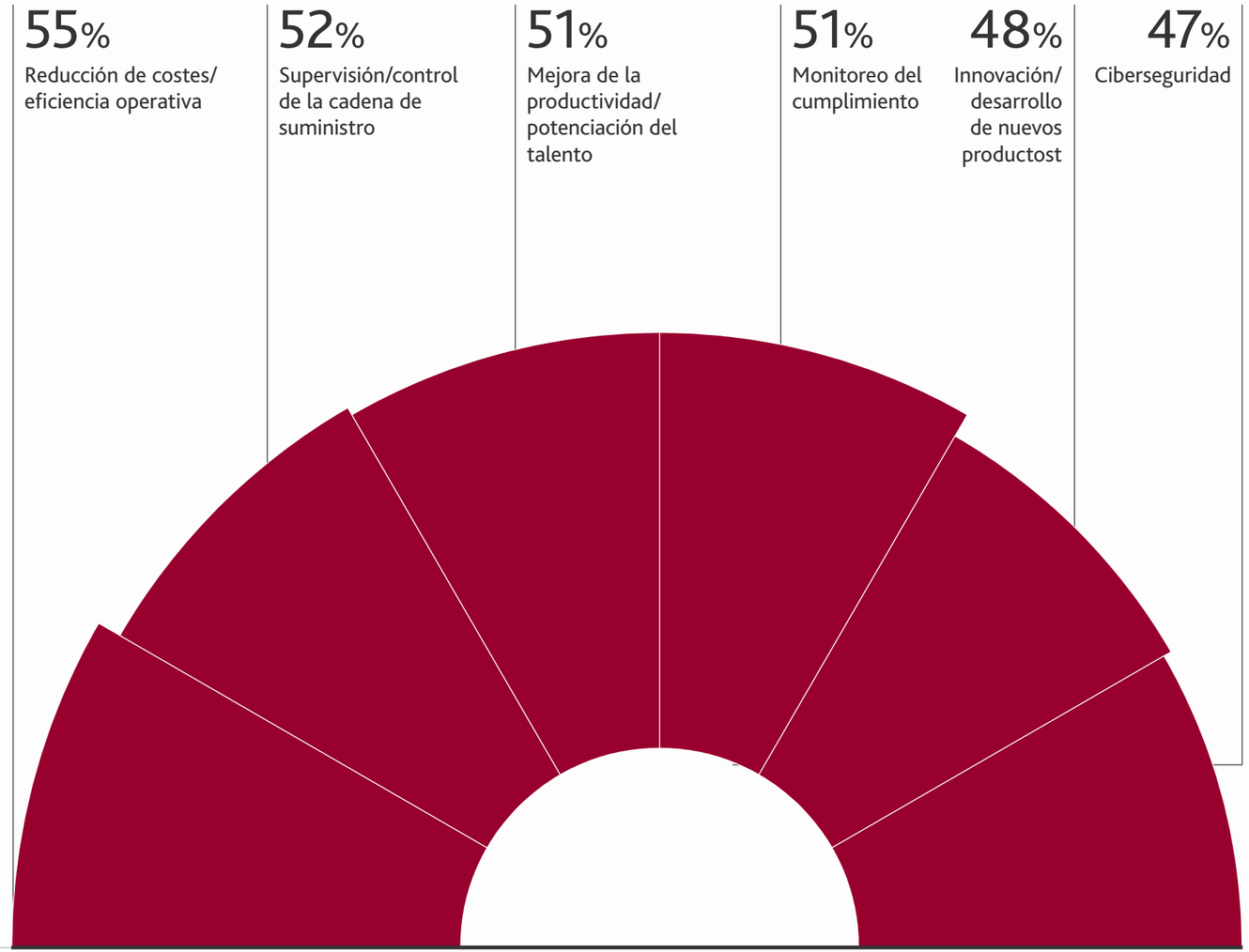
#4 | Desafíos de la integración

#5 | Predicciones inexactas

Nuestro informe 2025 Techtonic States reveló que , para 2028, el 62 % de los líderes prevé que la adopción de la IA se generalice en todas las áreas de su negocio. Implementar la gobernanza, los controles y la resiliencia adecuados será fundamental para que las organizaciones escalen su adopción de la IA con confianza.

“Si eres resiliente, deberías estar en una mejor posición en cuanto a riesgos”, añade Opal.

El valor de la IA se está capturando primero dentro del modelo operativo
Donde se espera que la IA tenga un impacto significativo en el próximo año



El riesgo de la IA está evolucionando más rápido de lo que las empresas pueden seguir el ritmo

Karen Schuler
Principal & Cyber Market Leader at BDO USA and Global Privacy, Data & AI Leader

Cómo la adopción de la IA está superando la preparación de las organizaciones

Cuando una tecnología emergente llega al mercado, las empresas tienden a adoptarla y a considerar los riesgos a posteriori. Esto significa que el riesgo evoluciona más rápido de lo que los líderes perciben, mientras que la adopción se acelera más que la gobernanza y la preparación organizacional. Los líderes se centran en las ventajas: eficiencia, velocidad y ventaja competitiva. Sin embargo, subestiman la rapidez con la que cambian los perfiles de riesgo una vez que la IA pasa de la fase piloto a la operativa. Esta transición de la experimentación al uso integrado representa un punto de inflexión donde el riesgo se vuelve sistémico en lugar de aislado.

Ric Opal,
Principal & National Leader, Cyber, IT Solutions at BDO USA and Global Digital Leader

El uso indebido de la IA merece tanta atención como las oportunidades que ofrece

También existe una falta generalizada de comprensión del uso de la IA en los negocios. Por mucho que planees utilizar la IA para crecer más rápido y ser más rentable, alguien más la usará en tu contra. Los riesgos relacionados con la velocidad y la sofisticación de la IA aún no se comprenden del todo.

Impulsar una gestión de riesgos que actúe, no que reaccione

Los líderes empresariales comprenden que ya no pueden simplemente esperar a que regrese la estabilidad. La incertidumbre es la nueva normalidad y las antiguas formas de gestionar el riesgo se están volviendo cada vez más obsoletas.

Solo integrando la gestión de riesgos en los procesos operativos de todas las funciones, las organizaciones pueden mejorar la concienciación sobre los riesgos y, al mismo tiempo, comprender mejor su situación general de riesgo. Esto les permite mantener la agilidad necesaria para asumir riesgos calculados en el momento oportuno, garantizando que los líderes empresariales puedan actuar con decisión incluso en un contexto de gran incertidumbre.

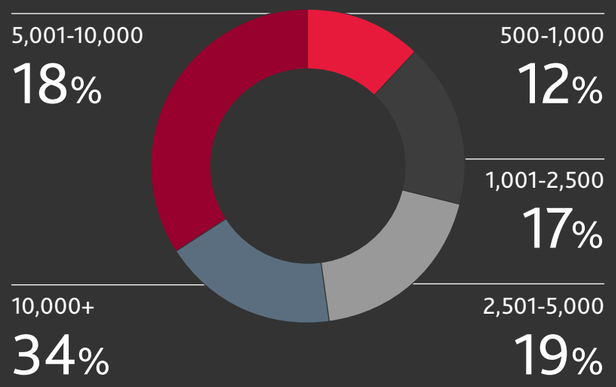
Pero la agilidad requiere claridad. Las organizaciones que definen su tolerancia al riesgo desde el principio están mejor posicionadas para distinguir entre los riesgos que vale la pena asumir y aquellos que requieren mitigación, en lugar de optar por una cautela generalizada.

Este enfoque constituye, en efecto, un nuevo modelo operativo, donde el riesgo no es un enemigo que deba evitarse, sino un facilitador comercial que puede convertirse en una ventaja competitiva.

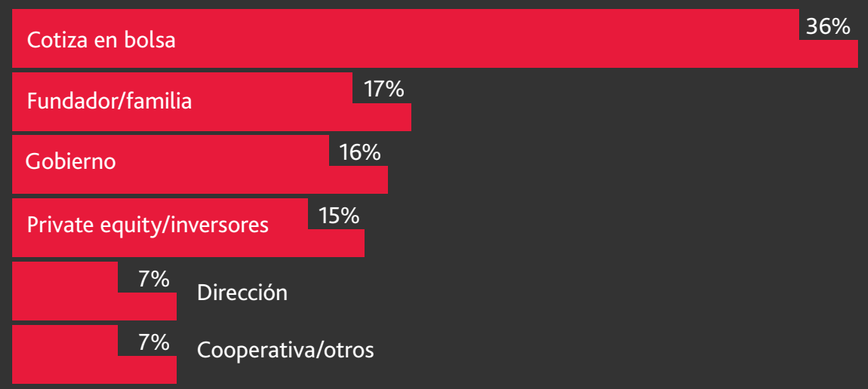
Metodología y datos demográficos

BDO y alan. agency encuestaron a 500 altos ejecutivos (incluidos CEOs, CFOs, CROs y CTOs) de empresas de diversos sectores a nivel mundial, como servicios financieros, energía y servicios públicos, salud y ciencias de la vida, manufactura, capital privado y otros. Todas las empresas contaban con al menos 500 empleados y generaban ingresos anuales de al menos 100 millones de dólares. El trabajo de campo se realizó entre diciembre de 2025 y enero de 2026.

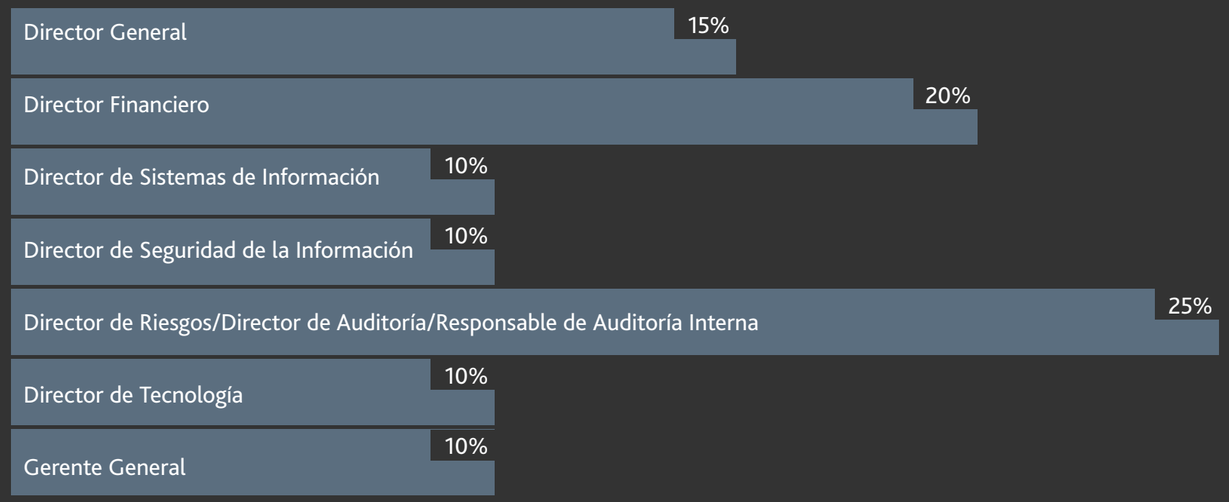
Empleados



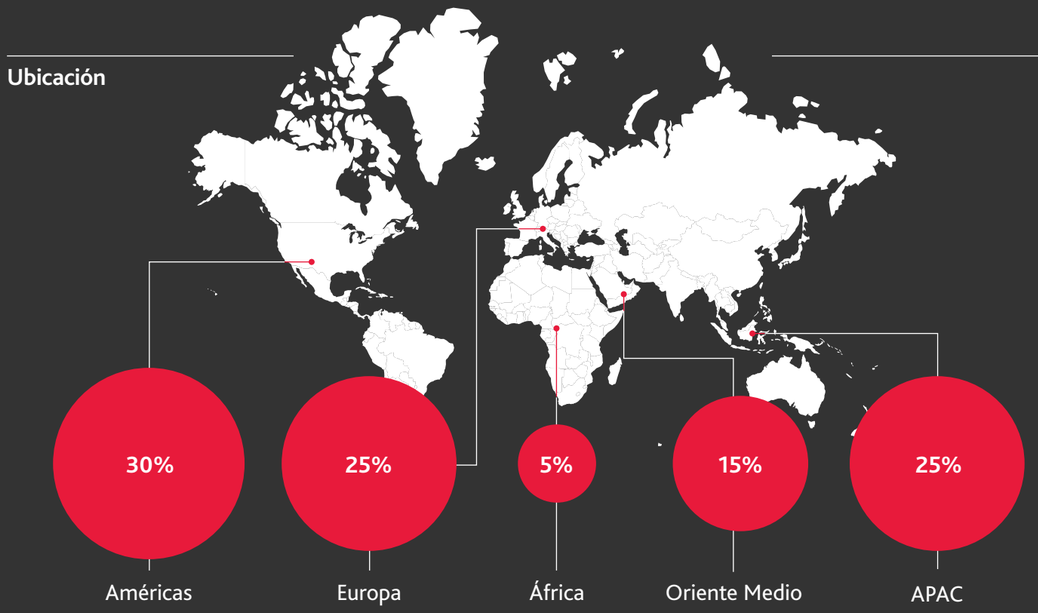
Propiedad de la empresa



Puesto de trabajo



Ubicación



Colaboradores

Colaboradores BDO

Koen Claessens
Global Head of
BDO Risk Advisory

Alisa Voznaya
Partner and Head of Risk
Consulting at BDO UK

Ricky Cheng
Director and Head of Risk
Advisory at BDO Hong Kong

Richard Walker
Head of Risk Advisory Services
at BDO South Africa

Gonzalo García-Liñán
Risk Advisory Services
Partner at BDO Spain

Ziad Akkaoui
Partner and National Risk
Advisory Practice Leader
at BDO Canada

Erin Sells
Principal, Risk Advisory
Services at BDO USA

Rocco Galletto
Partner and Global Cybersecurity
Leader at BDO Canada

Glenn Pomerantz
Principal & Forensic Market
Leader at BDO USA

Markus Brinkmann
Partner and Head of Forensic,
Risk & Compliance
at BDO Germany

Karen Schuler
Principal & Cyber Market Leader
at BDO USA and Global Privacy,
Data & AI Leader

Ric Opal
Principal & National Leader,
Cyber, IT Solutions at BDO USA
and Global Digital Leader

Colaboradores Externos

Matteo De Renzi
CEO at Gett

Johanna Pudda
CEO at Staci Americas

Richard Liao
CEO at Hwa-Hsia Glass

John Messina
IT consultant and former
CIO of the Canadian
government

FOR MORE INFORMATION

KOEN CLAESSENS
Global Head of Risk Advisory Services,
BDO Belgium

koen.claessens@bdo.be

Traducción al español realizada por Evelin Folgar y Victoria Ramírez de BDO Guatemala. Adaptación gráfica al español realizada por Luccia Berolatti de BDO Chile.

www.bdo.global