AMÉRICA LATINA 2026/2027

Temas de alto interés para auditores internos

RISK in FOCUS



Fundación Latinoamericana de Auditores Internos

Internal Audit FOUNDATION 1976-2026

ACERCA DE «GLOBAL RISK IN FOCUS»

Conoce tus riesgos. Planifica de forma estratégica.

«Risk in Focus» es la principal iniciativa anual de la Fundación de Auditoría Interna destinada a identificar los cinco riesgos más significativos que afectan a las organizaciones de todo el mundo.

Conozca qué dicen los auditores internos sobre:

- Los cinco riesgos más importantes en su región
- Cinco prioridades fundamentales para auditoría interna
- Consideraciones clave para los Consejos de Administración y los Comités de Auditoría

«Risk in Focus» utiliza los resultados de encuestas, mesas redondas regionales y entrevistas con expertos locales para ofrecer información clave desde la perspectiva única de la auditoría interna.

La Fundación de Auditoría Interna agradece sinceramente el trabajo de los institutos nacionales del IIA y organismos regionales del IIA que han hecho posible esta investigación: Federación Africana de Institutos de Auditores Internos (AFIIA), Confederación Árabe de Auditores Internos (ARABCIA), la Confederación Asiática de Institutos de Auditores Internos (ACIIA), la Confederación Europea de Institutos de Auditoría Interna (ECIIA) y la Fundación Latinoamericana de Auditores Internos (FLAI).

Queremos expresar nuestro especial agradecimiento al Grupo de Investigación de Institutos Europeos (EIRG), que desarrolló el enfoque de investigación «Risk in Focus» en 2016 y sigue publicando el informe para Europa a través de la ECIIA.

Todos los informes y las sesiones informativas de la junta directiva son de acceso gratuito para el público:

- África
- Asia-Pacífico
- Europa
- América Latina
- Oriente Medio
- América del Norte
- Resumen global

Visita el Centro de conocimientos «Risk in Focus» para obtener más información.

Internal Audit FOUNDATION 1976-2026

Visita el Centro de conocimiento «Risk in Focus» para obtener informes gratuitos y sesiones informativas para el consejo de administración (theiia.org/RiskInFocus).

PARTICIPACIÓN EN LA ENCUESTA MUNDIAL

132 países/territorios

3,285 respuestas de la encuesta

17 mesas redondas con **149** participantes

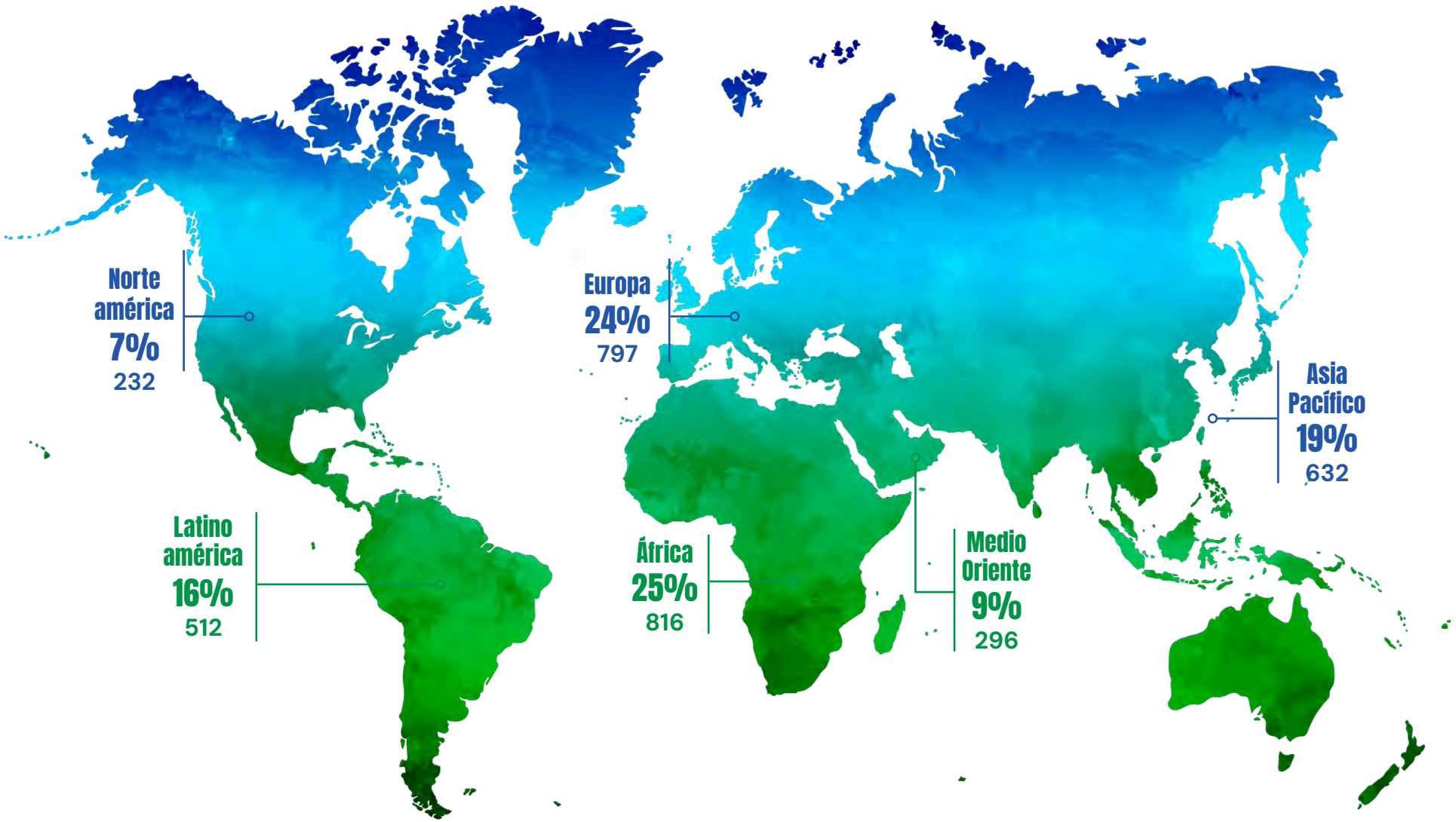
12 entrevistas a fondo

PARTICIPACIÓN EN LA ENCUESTA MUNDIAL

TOTALES GLOBALES

3.285. encuestados

132 países/lugares



Metodología de la encuesta

Se recibieron respuestas a la encuesta de 3.285 directores de auditoría y consejeros, en representación de 132 países y ubicaciones. La Fundación de Auditoría Interna llevó a cabo la encuesta en línea del 24 de marzo al 6 de mayo de 2026 para todas las regiones, excepto Europa. La encuesta para Europa fue realizada por el European Institutes Research Group entre el 2 de marzo y el 7 de abril de 2026.

CONTENIDO

Resumen ejecutivo 5

Sección 1. Entorno de riesgo 6

Sección 2. Prioridades de auditoría interna 14

Sección 3. Madurez y cobertura del riesgo 22

Conclusión 28

Apéndice A. Metodología 29

Apéndice B. Datos demográficos 30

Apéndice C. Resumen de riesgos globales 32

Apéndice D. Recursos del IIA 35

Agradecimientos

Fundación de Auditoría Interna 36

Socios de la Fundación de Auditoría Interna 37

Fundación Latinoamericana de Auditores Internos (FLAI) 38

El IIA 39



RESUMEN EJECUTIVO

De la conciencia del riesgo a las acciones de una auditoría estratégica.

El panorama de riesgos en América Latina ya no se caracteriza por amenazas aisladas. La ciberseguridad, la disrupción digital, la incertidumbre geopolítica, el fraude, el talento, la regulación y la liquidez funcionan ahora como un sistema de riesgos interconectado. El reto para los directores de auditoría consiste en convertir esa conciencia del riesgo en cobertura de auditoría, asesoramiento y acciones a nivel del Consejo de Administración.

Los resultados del informe «Risk in Focus 2026/2027» de Latinoamérica muestran una región que se enfrenta a un panorama de riesgos más digital, volátil e interconectado. La ciberseguridad sigue siendo la principal preocupación, el 80 % de los encuestados la ha seleccionado como uno de los cinco principales riesgos y el 82 % la ha calificado como de alto riesgo.

Sin embargo, lo más relevante es la rapidez y el alcance de los cambios que se están produciendo a su alrededor.

La disrupción digital, incluida la inteligencia artificial, ocupa ahora el segundo puesto entre los cinco principales riesgos, con un 61 %, mientras que el 75 % la calificó como de alto riesgo. La incertidumbre geopolítica y macroeconómica le sigue de cerca, el 52 % la ha seleccionado como uno de los cinco principales riesgos y el 71 % la ha calificado como alta.

De esta investigación se destacan cinco conclusiones:

- La ciberseguridad se ha convertido en una cuestión de resiliencia empresarial y de confianza. Los participantes en las mesas redondas describieron el riesgo cibernético no solo como un riesgo tecnológico, sino también como un riesgo para las operaciones, las infraestructuras críticas, la confianza de los clientes, la reputación, el cumplimiento normativo y la capacidad de recuperación.
- La disrupción digital avanza más rápido que la gobernanza. La inteligencia artificial, la automatización, los bots, las herramientas «low-code», los servicios en la nube y el análisis de datos están transformando los procesos empresariales a un ritmo más rápido que aquel con el que muchas organizaciones pueden actualizar sus controles, políticas, competencias y estructuras de responsabilidad.
- La incertidumbre geopolítica y macroeconómica debe traducirse en impactos relevantes para la auditoría. En el caso de América Latina, este riesgo se manifiesta a través de las cadenas de suministro, el tipo de cambio, los precios de los combustibles, la ubicación de la nube, los cambios normativos, las operaciones transfronterizas, las infraestructuras públicas y la continuidad del negocio.
- Las prioridades de la auditoría interna siguen siendo más tradicionales que el panorama de riesgos. La ciberseguridad, el fraude, los aspectos financieros y de liquidez, los cambios normativos y la transformación digital son las cinco principales prioridades de auditoría. Sin embargo, siguen existiendo importantes brechas en lo que respecta a la incertidumbre geopolítica y macroeconómica, los cambios en los mercados, el clima y el medio ambiente, el capital humano, la cultura y la disrupción digital, en relación con el nivel de riesgo y la madurez en materia de gobernanza.
- La madurez y la cobertura son la próxima frontera. La disrupción digital presenta el nivel más bajo de madurez en materia de gestión de riesgos, y, sin embargo, constituye uno de los riesgos más relevantes. Además, presenta el nivel más bajo de cobertura total de auditoría interna. Esta discrepancia supone un llamamiento a la acción para los DEA.

El mensaje principal para los Directores de Auditoría es claro: La profesión no puede basarse únicamente en programas de auditoría ya conocidos y en categorías de riesgo tradicionales. Los DEA deben ayudar a los Consejos de Administración y a los equipos ejecutivos a comprender cómo los riesgos emergentes se relacionan con la estrategia, las operaciones, el personal, la tecnología, el fraude, la normativa y la resiliencia. En 2027, las funciones de auditoría interna más destacadas no se definirán por el número de auditorías realizadas, sino por su capacidad para centrar los escasos recursos en los riesgos que podrían afectar en mayor medida al valor de la organización.

AMÉRICA LATINA PARTICIPACIÓN DE INVESTIGACIÓN

512 respuestas a la encuesta

18 países/lugares

2 mesas redondas con **23** participantes

4 entrevistas en profundidad

AUTOR DEL INFORME

Renato Trisciuzzi, CIA, QIAL, CCSA, CRMA, MSc, PhD

SOCIO DE INVESTIGACIÓN

Fundación Latinoamericana de Auditores Internos

1. ENTORNO DE RIESGO

Un panorama de riesgos más interconectado y menos indulgente

Los resultados del informe «Risk in Focus» 2026/2027 para América Latina muestran una clara concentración de la preocupación en torno a tres riesgos: la ciberseguridad, la disrupción digital y la incertidumbre geopolítica y macroeconómica.

Estos riesgos no son nuevos, pero las conversaciones mantenidas con los responsables de auditoría de toda la región sugieren que los factores que los provocan han cambiado. La ciberseguridad ya no se considera únicamente un riesgo informático. La disrupción digital ya no se limita a la estrategia tecnológica. La incertidumbre geopolítica ya no es un riesgo externo lejano. Cada uno de ellos tiene ahora repercusiones directas en las operaciones, la gobernanza, la resiliencia, el cumplimiento normativo, el fraude, la reputación y el talento.

Riesgo de ciberseguridad

Como se muestra en el anexo 1.1, la ciberseguridad es, con diferencia, el mayor riesgo. El 80 % de los encuestados lo seleccionó como uno de los cinco principales riesgos y el 82 % lo calificó como «alto». Esto confirma que los riesgos cibernéticos siguen siendo el principal riesgo para los consejos de administración, la dirección y la auditoría interna de la región. Los participantes en las mesas redondas describieron un entorno de riesgo en el que las amenazas cibernéticas son cada vez más sofisticadas, más frecuentes y están más estrechamente vinculadas al fraude, la identidad, la protección de datos, la tecnología operativa y la continuidad del negocio. La inteligencia artificial puede mejorar la defensa, pero también mejora la capacidad de ataque. Los estafadores pueden automatizar el phishing, crear identidades falsas, imitar voces, generar mensajes realistas y aprovechar las vulnerabilidades con mayor rapidez.

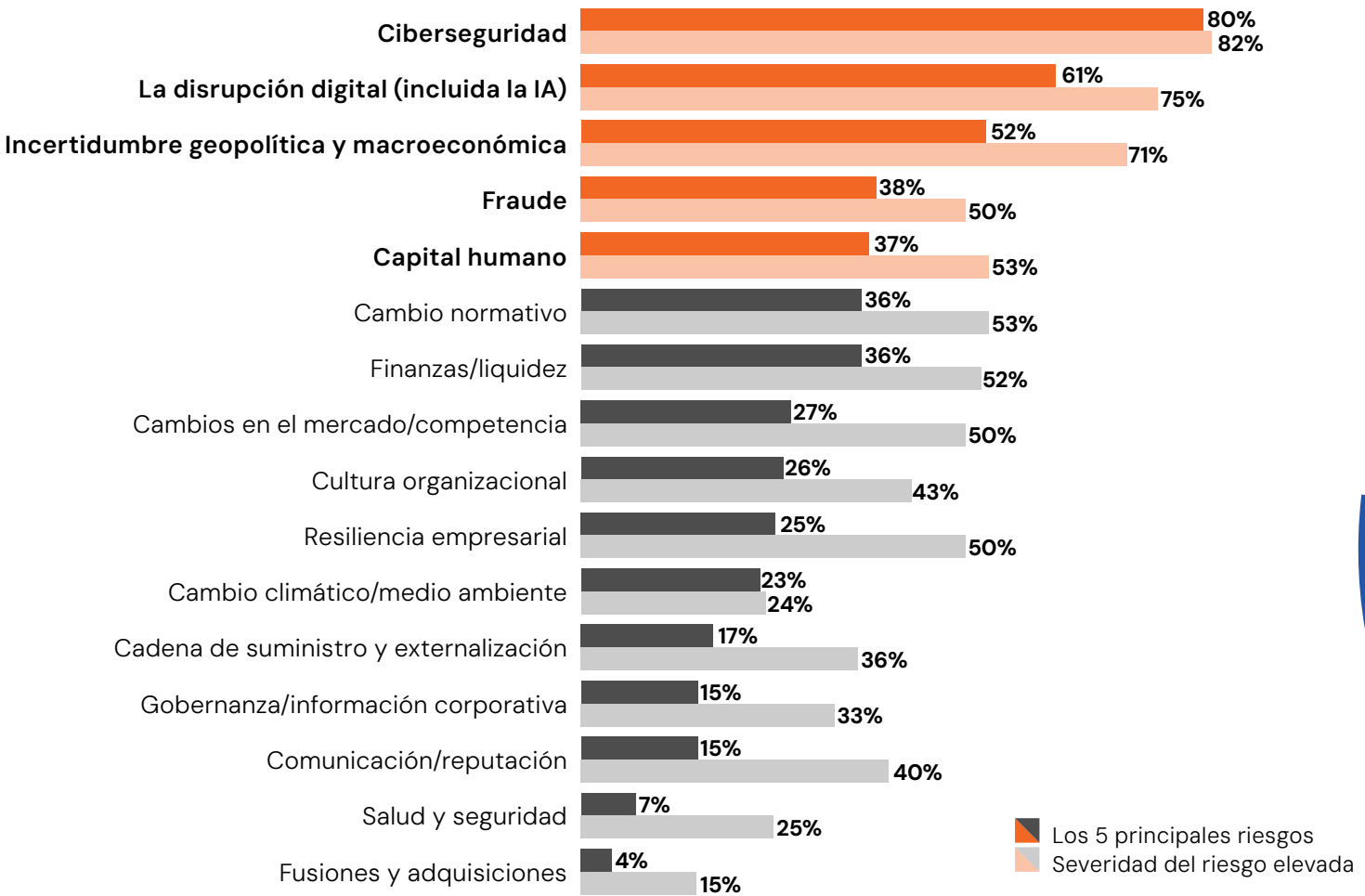
Para muchas organizaciones, el perímetro de riesgo cibernético se ha ampliado. Ahora incluye entornos en la nube, proveedores de tecnología externalizados, automatización industrial, canales digitales, aplicaciones móviles, acceso remoto, data lakes, herramientas de inteligencia artificial y tecnología operativa.

Al mismo tiempo, las consideraciones sobre los riesgos de ciberseguridad deben ir más allá de las operaciones tradicionales de tecnologías de la información. Por ejemplo, uno de los participantes en la mesa redonda describió el reto que supone la ciberseguridad para las operaciones industriales altamente automatizadas, en las que la tecnología de producción ha evolucionado a lo largo de muchos años, pero los controles de seguridad no han seguido el mismo ritmo. Esta es una señal importante para los directores de auditoría interna (DEA): el riesgo cibernético no debe evaluarse únicamente desde el punto de vista de las tecnologías de la información de la empresa. También debe evaluarse a través de las operaciones, los terceros, los productos digitales, los canales de atención al cliente y las infraestructuras críticas.

La ciberseguridad siguió ocupando los primeros puestos en las clasificaciones de riesgos, con **el 80 %** de los directores de auditoría interna de América Latina la calificó como uno de sus cinco principales riesgos.

Anexo 1.1. América Latina: los 5 principales riesgos frente a la severidad de los riesgos elevados

Pregunta 1 de la encuesta: **¿Cuáles son los cinco principales riesgos a los que se enfrenta actualmente tu organización? (Elige 5.)**
Pregunta 2 de la encuesta: **En una escala del 1 al 7, evalúe el nivel actual de riesgo en su organización para cada una de las siguientes áreas de riesgo.**



Cómo interpretar el gráfico
Colores oscuros indican quiénes han seleccionado ese riesgo como uno de los cinco más importantes de su organización (los cinco principales riesgos). **Colores claros** indican quiénes han calificado el riesgo con un 5, un 6 o un 7 en una escala del 1 al 7 (alto nivel de gravedad del riesgo). **Naranja** indica las cinco puntuaciones más altas en ambas medidas de riesgo.

Nota: Encuesta «Risk in Focus», realizada en línea a nivel mundial entre el 2 de marzo y el 6 de mayo de 2026. n = 512 para Latinoamérica.

ENTORNO DE RIESGO

Riesgo de disrupción digital

La disrupción digital, incluida la inteligencia artificial, es el segundo riesgo más importante de entre los cinco principales, seleccionado por el 61 % de los encuestados y calificado como «alto» por el 75 %. Además, el riesgo de disrupción digital aumentó considerablemente en comparación con el año anterior (Anexo 1.2). Esto podría ser el cambio más importante en el panorama del riesgo en América Latina.

Las oportunidades que ofrece la inteligencia artificial son considerables: automatización, productividad, análisis de datos, experiencia del cliente, detección de fraudes y apoyo a la toma de decisiones. Pero el riesgo es igualmente importante: resultados inexactos, modelos sesgados, fugas de datos, vulnerabilidades cibernéticas, IA en la sombra, incumplimientos normativos, exposición de la propiedad intelectual y una responsabilidad poco clara.

La cuestión no es si las organizaciones deberían adoptar nuevas tecnologías. En muchos sectores, la presión competitiva para adoptar la inteligencia artificial y las herramientas digitales ya es ineludible. La cuestión es si las organizaciones pueden adoptarlas con el nivel adecuado de gobernanza, rendición de cuentas, transparencia, resiliencia y control. Los entrevistados señalaron que los directivos reconocen cada vez más la importancia de la transformación digital, pero que las presiones operativas del día a día suelen retrasar la adopción de medidas. Esto genera una brecha entre la concientización sobre los riesgos y la respuesta ante los mismos.

El grado de madurez de la gobernanza organizacional en materia de IA varía. Algunas organizaciones están creando comités de IA, modelos de gobernanza, políticas, procesos de aprobación y controles de datos. Hay quienes aún se están dando cuenta de que algunas unidades de negocio ya han adoptado herramientas de inteligencia artificial sin un marco de gobernanza formal. En lo que respecta a la auditoría interna, el auge mundial de la inteligencia artificial implica que las metodologías de auditoría deben evolucionar rápidamente. Los auditores necesitan criterios para evaluar la gobernanza de la IA, pero también métodos prácticos para comprobar los controles relacionados con los datos, el acceso, la supervisión, la gestión de proveedores, los resultados de los modelos y la supervisión humana.

Riesgo de incertidumbre geopolítica

La incertidumbre geopolítica y macroeconómica ocupa el tercer lugar, el 52 % la ha seleccionado como uno de los cinco principales riesgos y el 71 % la ha calificado como «alta». En comparación con el año pasado, el riesgo derivado de la incertidumbre geopolítica aumentó considerablemente, probablemente debido, en parte, al conflicto que se desencadenó el 28 de febrero de 2026, cuando Estados Unidos e Israel lanzaron un ataque conjunto contra Irán. La incertidumbre geopolítica se situó, junto con la disrupción digital, como uno de los dos riesgos de más rápido crecimiento en la región (Figura 1.2).

En años anteriores, la incertidumbre geopolítica solía abordarse como un riesgo externo general. Este año, los debates han sido más prácticos y concretos. El riesgo geopolítico en América Latina debe analizarse tanto desde una perspectiva externa como interna. Entre los factores externos se encuentran la política comercial, los aranceles, los conflictos armados, la normativa transfronteriza, los precios de las materias primas y las dependencias tecnológicas a nivel mundial. Entre los factores internos se encuentran los ciclos electorales, la estabilidad institucional, los cambios en la política económica, las decisiones fiscales, el malestar social y los cambios en el papel del Estado en la economía. Ambos tipos de factores pueden influir en las tasas de interés, la propensión a la inversión, la liquidez, el mercado de divisas, las agendas de los reguladores y la continuidad operacional. En otras palabras, el riesgo geopolítico pasa a ser relevante para la auditoría cuando se traduce en repercusiones concretas para la empresa.

"Los riesgos más relevantes en América Latina ya no son casos aislados. La ciberseguridad, la inteligencia artificial, el fraude, la liquidez, el talento y la geopolítica forman ahora parte del mismo debate sobre el riesgo."

– Renato Trisciuzzi, Brasil

Anexo 1.2. América Latina: las 5 principales tendencias en materia de riesgos

Pregunta de la encuesta: **¿Cuáles son los cinco principales riesgos a los que se enfrenta actualmente tu organización? (Elige 5.)**

2023	2024	2025	2026	Variación de 2025 a 2026	Variación	Áreas de riesgo
75%	**74%**	**76%**	**80%**		**+4**	**Ciberseguridad**
38%	**37%**	**54%**	**61%**		**+7**	**Disrupción digital (incluida la IA)**
42%	**37%**	**45%**	**52%**		**+7**	**Incertidumbre geopolítica y macroeconómica**
30%	**32%**	**32%**	**38%**		**+6**	**Fraude**
44%	46%	40%	37%		-3	Capital humano
48%	45%	49%	36%		-13	Cambio normativo
33%	**33%**	**32%**	**36%**		**+4**	**Finanzas/liquidez**
26%	26%	24%	27%		+3	Cambios en el mercado/competencia
26%	28%	28%	26%		-2	Cultura organizacional
47%	49%	35%	25%		-10	Resiliencia empresarial
22%	29%	25%	23%		-2	Cambio climático/medio ambiente
16%	17%	15%	17%		+2	Cadena de suministro y externalización
18%	18%	16%	15%		-1	Gobernanza/información corporativa
22%	17%	19%	15%		-4	Comunicación/reputación
8%	9%	6%	7%		+1	Salud y seguridad
3%	4%	5%	4%		-1	Fusiones y adquisiciones

Aumento del riesgo con respecto al año anterior Disminución del riesgo con respecto al año anterior

Cómo interpretar el gráfico
El texto en naranja indica un aumento de 4 puntos porcentuales o más en comparación con el año anterior. El naranja y azul muestran la diferencia en las valoraciones entre 2025 y 2026. La columna titulada «variación» muestra la diferencia en puntos porcentuales entre 2025 y 2026.

Nota: Encuesta «Risk in Focus», realizada en línea a nivel mundial entre el 2 de marzo y el 6 de mayo de 2026. n = 512 para América Latina.

ENTORNO DE RIESGO

En el sector aéreo, la incertidumbre geopolítica puede afectar a las rutas, el acceso a los aeropuertos, las autorizaciones reglamentarias, los precios del combustible, los impuestos y la demanda de pasajeros. En el sector de los servicios financieros, puede afectar a la liquidez, el riesgo de crédito, el fraude, los ciberataques, la normativa y el comportamiento de los clientes. En el ámbito de la salud y los seguros, puede afectar a los medicamentos, los productos sanitarios, los equipos, la logística y los planes de continuidad. En el sector público y en las infraestructuras críticas, puede afectar a la prestación de servicios, a la resiliencia a nivel nacional, a la confianza de la ciudadanía y a la capacidad de respuesta.

Los participantes en las mesas redondas hicieron hincapié en que el riesgo geopolítico suele manifestarse a través de consecuencias operacionales. Estas consecuencias varían según el sector, pero la función del DEA es similar: ayudar a la Alta Dirección y al Consejo de Administración a comprender los escenarios, las dependencias, los puntos de activación y los planes de respuesta.

Riesgo de fraude

El fraude fue seleccionado como uno de los cinco principales riesgos por el 38 % y calificado como «alto» por el 50 %. Este resultado debe analizarse en el contexto de la ciberseguridad, la disrupción digital, la presión macroeconómica y el capital humano.

El riesgo de fraude se ve cada vez más favorecido por los canales digitales, la manipulación de la identidad, la ingeniería social, las brechas de seguridad cibernética, las dificultades económicas, los terceros y una gobernanza de datos deficiente. El auge de la IA también da lugar a nuevos escenarios de fraude, entre los que se incluyen las identidades sintéticas, los «deepfakes», el phishing automatizado, la manipulación de indicaciones y una explotación más rápida de las vulnerabilidades. La frontera entre el riesgo cibernético y el riesgo de fraude es cada vez menos clara. Para los directores de auditoría interna (DEA), esto significa que deben coordinarse los planes de auditoría cibernética y de fraude. La identidad digital, la gestión de accesos, la supervisión de transacciones, la respuesta ante incidentes y la comunicación con los clientes deben evaluarse de forma conjunta.

El riesgo de fraude en América Latina también está estrechamente relacionado con el riesgo financiero y de liquidez, así como con las presiones macroeconómicas. La inestabilidad económica puede aumentar los incentivos y las oportunidades para cometer fraude. Las dificultades de liquidez pueden debilitar la disciplina de control. La inflación puede influir en el comportamiento en materia de compras, el riesgo de existencias, las decisiones sobre precios y la solvencia de los clientes. Las organizaciones del sector público pueden verse sometidas a una presión adicional en lo que respecta a la transparencia, la continuidad del servicio y la confianza de los ciudadanos.

Capital humano, cambios normativos, riesgo financiero y de liquidez

El capital humano, los cambios normativos y el riesgo financiero y de liquidez constituyen el siguiente nivel de preocupación. El capital humano fue seleccionado como uno de los cinco principales riesgos por el 37 % y calificado como de alto riesgo por el 53 %. El cambio normativo fue seleccionado entre los cinco principales por el 36 % y recibió una valoración alta por parte del 53 %. El riesgo financiero o de liquidez fue seleccionado como uno de los cinco principales riesgos por el 36 % de los encuestados y calificado como «alto» por el 52 %. El capital humano también debe analizarse desde una perspectiva geopolítica y macroeconómica. En las economías en desarrollo, los profesionales altamente calificados en ciberseguridad, datos, automatización, inteligencia artificial, finanzas y gestión de riesgos pueden tener oportunidades en mercados globales más amplios o mediante el teletrabajo para organizaciones fuera de la región. Esta tendencia puede agravar las carencias en materia de capacidades de las organizaciones latinoamericanas. Para los directores generales y los Consejos de Administración, la fuga de talentos no es solo una cuestión de recursos humanos; puede afectar a la ejecución de la transformación, la resiliencia cibernética, el cumplimiento normativo, la innovación y la capacidad de auditoría interna.

Una compleja red de riesgos

Estos resultados ponen de manifiesto que la región no está pasando de los «riesgos antiguos» a los «riesgos nuevos». Por el contrario, los riesgos tradicionales y los emergentes están cada vez más interrelacionados, lo que da lugar a una compleja red de riesgos con repercusiones para la organización en su conjunto. La transformación digital requiere nuevos talentos. La ciberseguridad requiere inversión. La incertidumbre geopolítica puede dar lugar a cambios normativos. Las dificultades económicas pueden favorecer el fraude. Las carencias de talento pueden limitar la capacidad de transformación de la organización.



Anexo 1.3. América Latina: los 5 principales riesgos por sector

Pregunta de la encuesta: **¿Cuáles son los cinco principales riesgos a los que se enfrenta actualmente tu organización? (Elige 5.)**

Zonas de riesgo	Total América Latina	Servicios financieros	Sector público	Sector de capital privado	Cotiza en bolsa
Ciberseguridad	**80 %**	**88 %**	**70 %**	**78 %**	**79 %**
Disrupción digital (incluida la IA)	**61 %**	**74 %**	43 %	**62 %**	**55 %**
Incertidumbre geopolítica y macroeconómica	**52 %**	**52 %**	40 %	**53 %**	**69 %**
Fraude	**38 %**	41 %	**46 %**	32 %	33 %
Capital humano	**37 %**	32 %	**46 %**	**39 %**	36 %
Cambio normativo	36 %	**43 %**	**47 %**	29 %	19 %
Finanzas/liquidez	36 %	**42 %**	21 %	35 %	**38 %**
Cambios en el mercado/competencia	27 %	24 %	11 %	**37 %**	**38 %**
Cultura organizacional	26 %	17 %	**46 %**	27 %	12 %
Resiliencia empresarial	25 %	28 %	23 %	23 %	26 %
Cambio climático/medio ambiente	23 %	20 %	21 %	27 %	26 %
Cadena de suministro y externalización	17 %	13 %	10 %	23 %	33 %
Gobernanza/información corporativa	15 %	10 %	32 %	11 %	12 %
Comunicación/reputación	15 %	12 %	28 %	11 %	10 %
Salud y seguridad	7 %	2 %	7 %	11 %	10 %
Fusiones y adquisiciones	4 %	2 %	10 %	3 %	5 %

Los 5 riesgos más importantes

Nota: Encuesta «Risk in Focus», realizada en línea a nivel mundial del 2 de marzo al 6 de mayo de 2026. n = 512 para América Latina.

ENTORNO DE RIESGO

Diferencias entre sectores

Las diferencias entre sectores son un factor importante a la hora de comprender la «red de riesgos» de una organización, tal y como se muestra en el anexo 1.3.

- En todos los sectores, la ciberseguridad sigue siendo un riesgo común, aunque el grado de exposición varía. En el sector de los servicios financieros, la ciberseguridad y la transformación digital están estrechamente relacionadas con la identidad digital, el fraude, la seguridad de los datos, la confianza de los clientes, la resiliencia y las exigencias normativas. Sin embargo, la ciberseguridad de la tecnología operativa (OT) está cobrando cada vez más importancia en los sectores de la fabricación, la alimentación y las bebidas, la pasta de papel y el papel, la minería, la energía, el petróleo y el gas, los servicios públicos y otros entornos industriales, donde un incidente cibernético puede interrumpir la producción, poner en peligro la seguridad, afectar a las infraestructuras críticas o interrumpir la prestación de servicios.
- En las empresas que cotizan en bolsa, la incertidumbre geopolítica y macroeconómica, así como los cambios en los mercados, tienen mayor relevancia.
- En las empresas privadas, la disrupción digital, la incertidumbre macroeconómica, el capital humano y la competencia en el mercado se perfilan como importantes preocupaciones estratégicas.
- En el sector público, el perfil de riesgo se distribuye entre una amplia gama de áreas de riesgo, entre las que destacan la ciberseguridad, los cambios normativos, el fraude y el capital humano, aunque el riesgo también es elevado en lo que respecta a la disrupción digital, la incertidumbre geopolítica y la gobernanza.

Cambio climático/riesgos medioambientales

El 23 % considera que el cambio climático y el medio ambiente se encuentran entre los cinco principales riesgos, y solo el 24 % lo calificó como un riesgo elevado. Esta posición relativamente baja en la calificación regional debe interpretarse con cautela. En muchas organizaciones latinoamericanas, los riesgos climáticos y medioambientales compiten con otras prioridades más inmediatas, como el crecimiento económico, la inflación, la liquidez, la seguridad, las infraestructuras, el empleo y los cambios normativos. La exposición también varía considerablemente según el país, la zona geográfica y el sector. Para algunos sectores, como el energético, el agrícola, el del transporte, el de las infraestructuras públicas, el de los seguros, el minero, el manufacturero y el público, los riesgos climáticos y medioambientales pueden ser relevantes. Sin embargo, en otras organizaciones, es posible que el riesgo aún no se haya traducido plenamente en repercusiones operacionales, financieras, de cumplimiento normativo, de seguros, de protección de activos, de la cadena de suministro o de resiliencia. Para los directores de auditoría interna (DEA), la cuestión clave no es si el riesgo climático es elevado para todas las organizaciones, sino si se evalúa adecuadamente en aquellos casos en los que la exposición es significativa.

Riesgos de comunicación y reputación

Solo el 15 % considera que las comunicaciones y la reputación se encuentran entre los cinco principales riesgos, pero el 40 % les otorga una puntuación alta. Esta brecha merece nuestra atención. Es posible que la reputación no siempre figure como una categoría independiente dentro del ámbito de auditoría, pero a menudo es consecuencia de fallos en materia de ciberseguridad, fraude, seguridad, experiencia del cliente, normativa, ética, criterios ESG y continuidad operacional. En el caso de los bancos digitales, las empresas fintech, las aerolíneas, los servicios públicos y las empresas de consumo, el daño a la reputación puede producirse rápidamente y extenderse a través de las redes sociales antes de que la dirección tenga tiempo de reaccionar.

Resumen

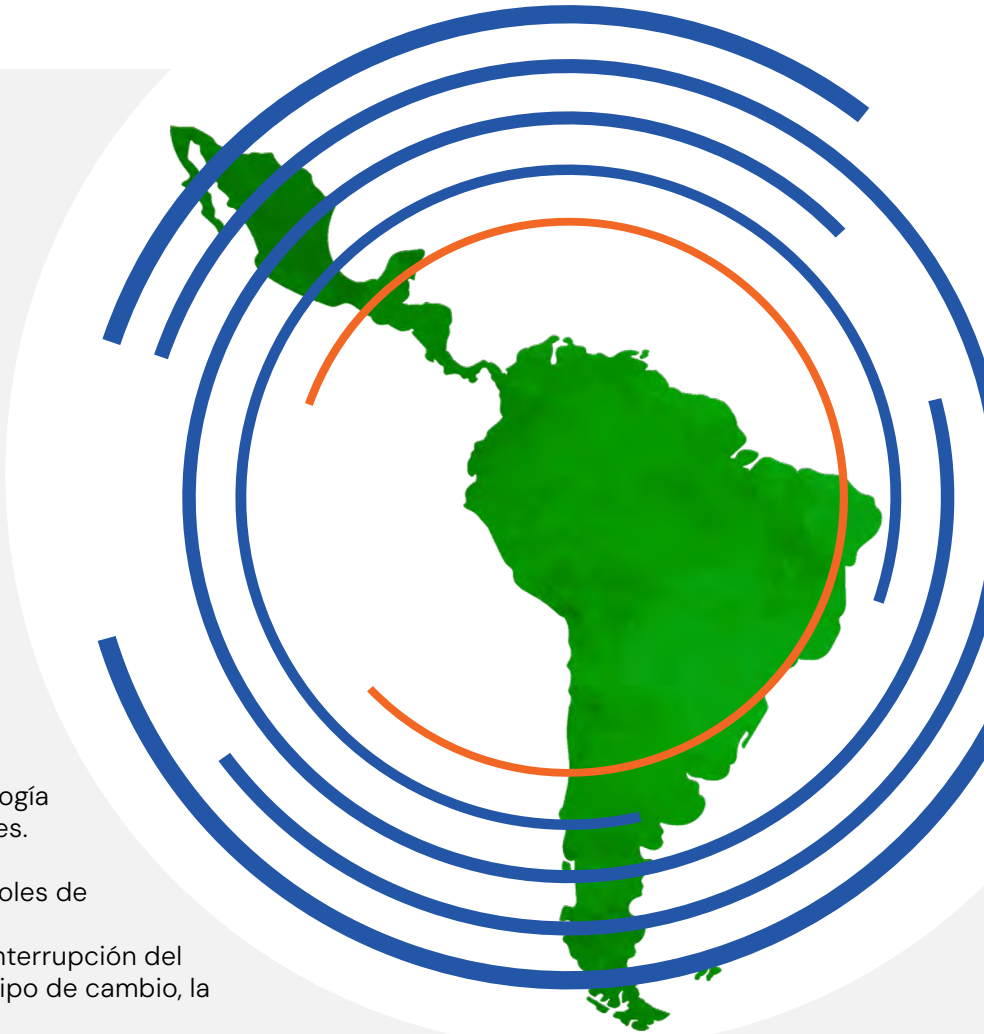
La tendencia general es clara: El entorno de riesgo de América Latina está pasando de la gestión de riesgos individuales a la gestión de riesgos interrelacionados. Los riesgos más elevados no deben analizarse de forma aislada. La ciberseguridad, la inteligencia artificial, el fraude, el talento, los terceros, la liquidez, la regulación, la continuidad y la reputación deben evaluarse de forma conjunta, ya que los incidentes que causan mayor daño suelen combinar varios de estos riesgos.

El entorno de riesgo en América Latina está pasando de la gestión de riesgos individuales a la gestión de riesgos interrelacionados.

PUNTOS CLAVE

Conclusiones de la encuesta

- La ciberseguridad sigue siendo el principal riesgo en América Latina, pero la tendencia general es la convergencia entre la tecnología, la incertidumbre macroeconómica, el fraude, la regulación y el capital humano.
- La disrupción digital y la inteligencia artificial se están convirtiendo en ámbitos de alto riesgo, ya que su implantación avanza más rápido que los mecanismos de gobernanza.
- La incertidumbre geopolítica y macroeconómica es elevada porque ya no es algo abstracto; afecta a las cadenas de suministro, la estrategia de la nube, el mercado de divisas, el combustible, la liquidez, la normativa y la continuidad.



Estrategias de auditoría interna

- Los directores de auditoría interna (DEA) deberían actualizar el universo de auditoría para que refleje los riesgos interrelacionados, en lugar de categorías aisladas.
- Las auditorías de ciberseguridad deben abarcar la nube, los terceros, la tecnología operativa, la protección de datos, la resiliencia y la recuperación ante incidentes.
- La disrupción digital debe evaluarse teniendo en cuenta la gobernanza de la inteligencia artificial, la calidad de los datos, el riesgo de los modelos, los controles de automatización, el uso ético y la rendición de cuentas.
- El riesgo geopolítico debe traducirse en escenarios auditables, tales como la interrupción del suministro, las tensiones de liquidez, los cambios normativos, la exposición al tipo de cambio, la dependencia de infraestructuras críticas y la continuidad del negocio.

2. PRIORIDADES DE LA AUDITORÍA INTERNA

La brecha de cobertura: Cuando el riesgo avanza más rápido que los planes de auditoría

Los resultados de la encuesta sobre las prioridades de la auditoría interna muestran que los directores de auditoría interna (DEA) de América Latina están respondiendo al panorama de riesgos, aunque no siempre al mismo ritmo ni con la misma intensidad con la que cambian los niveles de riesgo.

El anexo 2.1 muestra que la ciberseguridad es, a la vez, el mayor riesgo y la máxima prioridad de auditoría. El 74 % de los encuestados lo seleccionó como una de las cinco principales prioridades de auditoría. Esta alineación es adecuada y previsible. Sin embargo, la conclusión más importante se encuentra en las discrepancias entre las áreas de alto riesgo y los niveles más bajos de esfuerzo en materia de auditoría interna.

El fraude, los riesgos financieros y de liquidez, los cambios normativos y la disrupción digital completan las cinco principales prioridades de auditoría en América Latina. El 56 % señaló el fraude como una de las cinco principales prioridades de auditoría; el 53 %, las cuestiones financieras y de liquidez; el 53 %, los cambios normativos; y el 47 %, la disrupción digital. Estos resultados ponen de manifiesto que las funciones de auditoría interna siguen dedicando un esfuerzo considerable a los riesgos que les resultan familiares, que son cuantificables, que están regulados y que, tradicionalmente, se encuentran dentro de su zona de confort.

La disrupción digital como prioridad de auditoría

Es alentador el aumento de la importancia que se concede a la disrupción digital como prioridad de auditoría, ya que es el ámbito de auditoría que ha registrado un mayor incremento en el esfuerzo dedicado, según la encuesta (Figura 2.2). Sin embargo, su prioridad sigue siendo inferior a su nivel de riesgo.

El 61 % consideró la disrupción digital como uno de los cinco principales riesgos, mientras que el 47 % la consideró una prioridad de auditoría. La diferencia se hace aún más evidente cuando se analiza junto con los datos sobre madurez y cobertura que figuran en la sección 3.
La disrupción digital es uno de los mayores riesgos, pero también uno de los ámbitos en los que menor madurez presenta la gobernanza y menor es la cobertura de auditoría. Esta es una de las conclusiones más importantes del informe.

Los participantes en las mesas redondas y los entrevistados ofrecieron varias explicaciones. En primer lugar, algunas organizaciones reconocen que la disrupción digital reviste una importancia estratégica, pero las presiones operativas prevalecen en la toma de decisiones diaria. En el sector minorista, por ejemplo, los directivos deben seguir gestionando las ventas, la tesorería, la logística, las pérdidas por merma, los márgenes y la experiencia del cliente, al tiempo que transforman los procesos y la tecnología. Tal y como describió Magy Fuentes, el reto consiste en «actuar y transformar» al mismo tiempo.

La disrupción digital obtuvo una puntuación alta en cuanto al riesgo (**61 %**), pero relativamente baja en cuanto a la prioridad de auditoría (**47 %**). Además, es una de las áreas con menor nivel de madurez en materia de gobernanza y cobertura completa de auditoría.

"La transformación digital y la ciberseguridad se reconocen claramente como cuestiones relevantes. El problema es que, en muchas organizaciones, siguen siendo más una preocupación que una ocupación."

– Magy Fuentes, Argentina

PRIORIDADES DE LA AUDITORÍA INTERNA

Anexo 2.1. América Latina: los 5 principales riesgos frente a las 5 principales prioridades de auditoría

Pregunta 1 de la encuesta: **¿Cuáles son los cinco principales riesgos a los que se enfrenta actualmente tu organización? (Elige 5.)**
Pregunta 2 de la encuesta: **¿Cuáles son las cinco principales áreas de auditoría en las que la auditoría interna dedica más tiempo y esfuerzo? (Elige 5.)**



Nota: Encuesta «Risk in Focus», realizada en línea a nivel mundial entre el 2 de marzo y el 6 de mayo de 2026. n = 512 para América Latina.

En segundo lugar, algunos equipos de auditoría interna carecen de las competencias necesarias para auditar la inteligencia artificial, la nube, la automatización, la gobernanza de datos, los algoritmos, la ciberseguridad, la tecnología operativa o los productos digitales. No se trata únicamente de una cuestión de personal. También es una cuestión de metodología. Es posible que los programas de auditoría tradicionales no sean suficientes para evaluar el desarrollo ágil, los modelos de aprendizaje automático, los bots, los agentes de IA, el linaje de los datos, la identidad digital, la resiliencia en la nube o los ecosistemas de plataformas. Los responsables de auditoría interna (CAE) deberían plantearse desarrollar o mantener capacidades multidisciplinares dentro de la función de auditoría interna, entre las que se incluyen las tecnologías de la información, la ciberseguridad, la automatización, el análisis de datos, la inteligencia artificial, la tecnología operativa, los procesos y los conocimientos especializados en el ámbito empresarial. Cuando no sea viable contar con personal fijo, puede ser necesario recurrir a acuerdos permanentes de co-sourcing o al acceso a expertos especializados en la materia. Incluso cuando se vean sometidos a la presión de realizar auditorías tradicionales, los responsables de auditoría interna (CAE) deben reservar un espacio específico en el plan de auditoría anual para los riesgos emergentes mediante actividades de verificación específicas, evaluaciones del grado de preparación, revisiones de asesoramiento, seguimiento continuo o auditorías piloto.

En tercer lugar, es posible que algunos CAE se ciñan demasiado a lo que les resulta familiar. Los entrevistados se mostraron sinceros al hablar de la zona de confort de la profesión. La auditoría de las finanzas, el cumplimiento normativo, las compras, las nóminas o la presentación de informes reglamentarios puede resultar más sencilla, ya que los criterios son más claros y los equipos cuentan con experiencia. La auditoría de la cultura, la innovación, la transformación digital, la exposición geopolítica o la resiliencia estratégica requiere más criterio, más colaboración y una mayor disposición a lidiar con la ambigüedad.

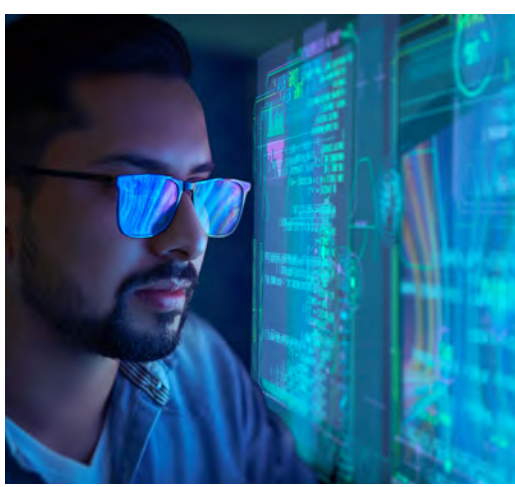
La incertidumbre geopolítica, prioridad en la auditoría

La incertidumbre geopolítica y macroeconómica es la que presenta la mayor discrepancia entre el riesgo y la prioridad de auditoría. El 52 % lo seleccionó como uno de los cinco principales riesgos, pero solo el 14 % lo seleccionó como una de las cinco principales prioridades de auditoría. A primera vista, esto podría parecer una cobertura insuficiente. En la práctica, la cuestión es más compleja. El riesgo geopolítico es difícil de evaluar directamente. La auditoría interna no puede auditar una guerra, unas elecciones, la inflación, un conflicto diplomático ni la volatilidad del mercado de materias primas. No obstante, la auditoría interna puede evaluar cómo la organización se anticipa, supervisa, escala y responde al impacto de estas circunstancias en el entorno de riesgo externo.

Esto significa que los CAE no deberían crear necesariamente una auditoría denominada «riesgo geopolítico». En su lugar, pueden integrar escenarios geopolíticos y macroeconómicos en las áreas de auditoría ya existentes dentro de la organización, tales como la cadena de suministro, la liquidez, la tesorería, la planificación estratégica, la continuidad del negocio, el cumplimiento normativo, el riesgo asociado a terceros, la concentración en la nube, la gestión de crisis y la expansión en el mercado. Por ejemplo, una empresa de tecnología financiera puede traducir el riesgo geopolítico en una estrategia de dependencia de la nube y de recuperación. Una compañía aérea puede interpretarlo en términos de acceso a los aeropuertos, permisos de ruta, exposición al riesgo cambiario y precios del combustible. Una entidad sanitaria o aseguradora podría interpretarlo como la continuidad del suministro de material médico.

"El riesgo geopolítico se convierte en una realidad cuando afecta a los medicamentos, los suministros médicos, los equipos, la logística y la continuidad operativa."

– José Luis Fernández García, Chile



Anexo 2.2. América Latina: Tendencias en las cinco principales prioridades de auditoría

Pregunta de la encuesta: **¿Cuáles son las cinco principales áreas de auditoría a las que la auditoría interna dedica más tiempo y esfuerzo? (Elige 5.)**

2023	2024	2025	2026	Variación de 2025 a 2026	Variación	Áreas de auditoría
66%	**67%**	**69%**	**74%**		**+5**	**Ciberseguridad**
47%	**52%**	**51%**	**56%**		**+5**	**Fraude**
50%	49%	51%	53%		+2	Finanzas/liquidez
50%	47%	53%	53%		0	Cambio normativo
24%	**19%**	**29%**	**47%**		**+18**	**Disrupción digital (incluida la IA)**
46%	46%	48%	38%		-10	Gobernanza/informes corporativos
53%	49%	40%	32%		-8	Resiliencia empresarial
29%	30%	29%	27%		-2	Cultura organizacional
28%	29%	24%	27%		+3	Cadena de suministro y externalización
28%	29%	27%	26%		-1	Capital humano
23%	22%	20%	16%		-4	Comunicación/reputación
17%	17%	16%	15%		-1	Cambios en el mercado/competencia
13%	12%	16%	14%		-2	Incertidumbre geopolítica y macroeconómica
12%	14%	12%	10%		-2	Salud/seguridad
8%	11%	9%	8%		-1	Cambio climático/medio ambiente
5%	7%	6%	5%		-1	Fusiones y adquisiciones

Prioridad de auditoría mayor que la del año anterior Prioridad de auditoría menor que la del año anterior

Cómo interpretar el gráfico
El color naranja indica un aumento de 4 puntos porcentuales o más en comparación con el año anterior. El naranja y el azul muestran la diferencia en las valoraciones entre 2025 y 2026. La columna titulada «variación» muestra la diferencia en puntos porcentuales entre 2025 y 2026.

Nota: Encuesta «Risk in Focus», realizada en línea a nivel mundial entre el 2 de marzo y el 6 de mayo de 2026. n = 512 para América Latina.

PRIORIDADES DE AUDITORÍA INTERNA

Prioridad en la auditoría del capital humano

El capital humano es otro ámbito en el que existe una brecha significativa. El 37 % lo seleccionó como uno de los cinco principales riesgos, pero solo el 26 % lo seleccionó como una de las cinco principales prioridades de auditoría. Esto es comprensible, ya que el capital humano puede resultar difícil de auditar más allá de los procesos tradicionales de recursos humanos. Sin embargo, las entrevistas sugieren que el talento es un factor que influye en casi todos los demás riesgos. Sin el talento adecuado, las organizaciones no pueden gestionar la IA, protegerse frente a las amenazas cibernéticas, llevar a cabo la transformación, mantener los controles, cumplir con la normativa, detectar el fraude ni desarrollar operaciones resilientes.

Por lo tanto, la auditoría interna debería ampliar su visión del capital humano. No se trata únicamente de la rotación de personal, la contratación, la formación o la sucesión. También se trata de la capacidad estratégica. ¿Cuenta la organización con las competencias necesarias para llevar a cabo su estrategia? ¿Se han identificado los puestos clave? ¿Son suficientes las capacidades en materia digital, cibernética, de datos y de gestión de riesgos? ¿Son eficaces la transferencia de conocimientos y los planes de sucesión? ¿Están los incentivos en consonancia con un comportamiento ético y una asunción prudente de riesgos? ¿Favorecen la cultura y los comportamientos de liderazgo la concientización sobre los riesgos?

Prioridad de la auditoría sobre los cambios en el mercado y la competencia

El 27 % ha seleccionado «los cambios en el mercado y la competencia» como uno de los cinco principales riesgos, pero solo el 15 % lo ha seleccionado como una de las cinco principales prioridades de auditoría. Esta brecha puede reflejar otra limitación tradicional: la auditoría interna suele centrarse más en los procesos internos que en la dinámica de los mercados externos. Sin embargo, el riesgo de mercado puede afectar a la fijación de precios, al comportamiento de los clientes, a la calidad crediticia, a las existencias, al diseño de productos, a los canales digitales, a la liquidez y a la ejecución de la estrategia. Los responsables de auditoría interna (CAE) deben evaluar si los cambios en el mercado se tienen en cuenta en las evaluaciones estratégicas de riesgos y si la dirección cuenta con mecanismos eficaces para supervisarlos y dar respuesta a ellos.

Prioridad en materia de cambio climático y auditoría medioambiental

El cambio climático y el medio ambiente siguen un patrón similar. El 23 % lo seleccionó como uno de los cinco principales riesgos, pero solo el 8 % lo seleccionó como prioridad de auditoría. Para muchas organizaciones, esto puede resultar adecuado si el riesgo de exposición es bajo. Sin embargo, para las organizaciones de los sectores de la agricultura, la energía, la minería, el transporte, los seguros, las infraestructuras, el sector público y la industria manufacturera, la baja prioridad de auditoría podría indicar la necesidad de reconsiderar la situación. El riesgo climático debe evaluarse no solo en el marco de los informes de sostenibilidad, sino también en lo que respecta a la resiliencia operativa, la protección de los activos, las interrupciones en la cadena de suministro, la normativa, el costo de los seguros y el impacto en la comunidad.



Anexo 2.3. América Latina: las 5 principales prioridades de auditoría por sector

Pregunta de la encuesta: **¿Cuáles son las cinco principales áreas de auditoría en las que la auditoría interna dedica más tiempo y esfuerzo? (Elige 5.)**

Áreas de auditoría	Todo Latino América	Servicios financieros	Sector público	Sector de capital privado	Cotiza en bolsa
Ciberseguridad	**74 %**	**88 %**	**52 %**	**68 %**	**83 %**
Fraude	**56 %**	**55 %**	46 %	**65 %**	**55 %**
Finanzas/liquidez	**53 %**	**65 %**	34 %	**52 %**	**38 %**
Cambio normativo	**53 %**	**61 %**	**62 %**	**44 %**	29 %
Disrupción digital (incluida la IA)	**47 %**	**58 %**	38 %	**42 %**	**48 %**
Gobernanza/informes corporativos	38 %	34 %	**51 %**	32 %	**38 %**
Resiliencia empresarial	32 %	32 %	26 %	35 %	**38 %**
Cultura organizacional	27 %	15 %	**47 %**	25 %	26 %
Cadena de suministro y externalización	27 %	15 %	13 %	**42 %**	**50 %**
Capital humano	26 %	21 %	**48 %**	22 %	12 %
Comunicación y reputación	16 %	14 %	29 %	14 %	7 %
Cambios en el mercado/competencia	15 %	15 %	10 %	17 %	14 %
Incertidumbre geopolítica y macroeconómica	14 %	17 %	19 %	12 %	7 %
Salud/seguridad	10 %	2 %	10 %	17 %	24 %
Cambio climático/medio ambiente	8 %	5 %	8 %	8 %	24 %
Fusiones y adquisiciones	5 %	2 %	8 %	5 %	7 %

Las 5 prioridades principales de auditoría

Nota 1: Los empates por el quinto puesto aparecen resaltados en un tono más claro.
Nota 2: Encuesta «Risk in Focus» realizada en línea a nivel mundial entre el 2 de marzo y el 6 de mayo de 2026. n = 512 para Latinoamérica.

PRIORIDADES DE AUDITORÍA INTERNA

Diferencias entre sectores

Las diferencias entre sectores ponen de manifiesto que los responsables de auditoría interna (CAE) deben adaptar los planes de auditoría al modelo operativo de la organización (Figura 2.3).

La ciberseguridad y el fraude suelen ser prioridades importantes para la auditoría interna en todos los sectores. En el sector de los servicios financieros, también se concede gran importancia a la situación financiera y la liquidez, los cambios normativos y la transformación digital. Las empresas privadas y las que cotizan en bolsa conceden mayor prioridad a los riesgos de la cadena de suministro, mientras que el sector público otorga una prioridad considerablemente mayor a la gobernanza, la Cultura organizacional y el capital humano.

El análisis sectorial refuerza un mensaje fundamental: las auditorías internas no deben utilizar las clasificaciones regionales de forma mecánica. Las clasificaciones deben utilizarse como una herramienta para retar lo establecido. Los responsables de auditoría interna (CAE) deben comparar los resultados regionales con la evaluación de riesgos, la estrategia, las expectativas de las partes interesadas, el modelo operativo, la dinámica del sector y el mapa de aseguramiento existente de su organización. Los planes de auditoría también deben seguir siendo flexibles. Las condiciones geopolíticas, digitales, cibernéticas, de liquidez, normativas y de mercado pueden cambiar más rápido que el ciclo de planificación anual. Por lo tanto, los responsables de auditoría interna (CAE) deberían incluir puntos de revisión formales de actualidad en el plan de auditoría y mantener la capacidad de reasignar recursos cuando cambie el perfil de riesgo. Los conocimientos y la experiencia del CAE en el sector constituyen valiosos activos intangibles. Cuando se combina con una metodología sólida de planificación de auditoría, este conocimiento del sector ayuda a la auditoría interna a centrarse en los riesgos más relevantes para los objetivos de la organización.

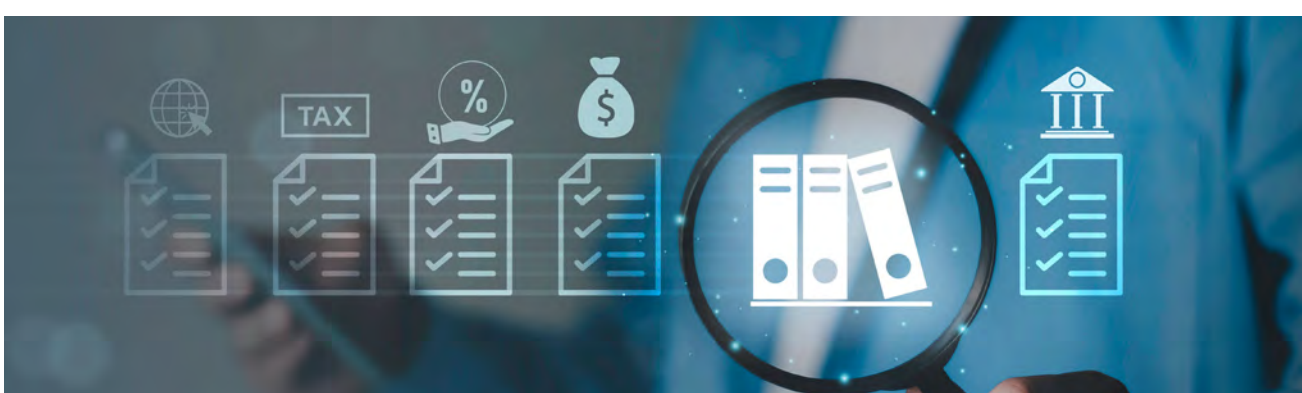
Cuando el riesgo sectorial sea elevado, pero la prioridad de auditoría sea baja, el responsable de auditoría interna (CAE) deberá determinar si dicho riesgo está cubierto por otro proveedor de servicios de aseguramiento, integrado en otras auditorías, abordado a través de servicios de asesoramiento, supervisado mediante actualizaciones periódicas o si, por el contrario, no está suficientemente cubierto.

Resumen

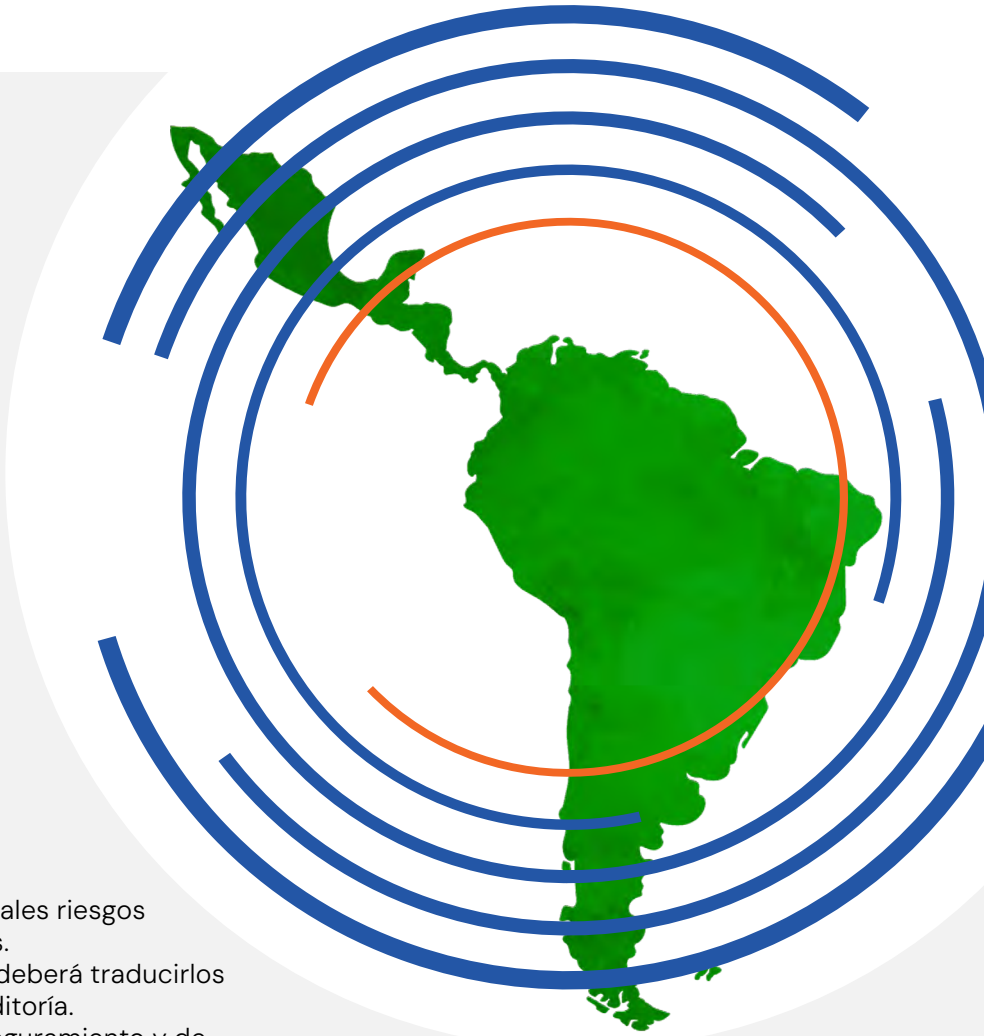
Esto no implica que, en el caso de los CAE, todos los riesgos deban recibir la misma atención. Los recursos de auditoría son limitados. Esto implica que el plan de auditoría interna debe explicar de forma explícita los motivos que justifican la cobertura de determinado riesgo, teniendo en cuenta la estrategia de la organización, sin dejar de ser lo suficientemente flexible como para responder a cambios significativos en el entorno de riesgo. Cuando el riesgo es elevado, pero el esfuerzo de auditoría es reducido, el director de auditoría interna debería poder explicar por qué. ¿Está cubierto ese riesgo por otro proveedor de aseguramiento? ¿Es madura la gobernanza de la gerencia? ¿Se supervisa el riesgo mediante actividades de asesoramiento? ¿Se incluye en otras auditorías? ¿Se volverá a evaluar el riesgo durante una actualización formal del plan? ¿O existe realmente una brecha debida a una capacidad o unos recursos limitados?

"La auditoría interna debe ir más allá de lo que resulta cómodo. La cuestión no es solo si disponemos de recursos, sino si nos estamos preparando para evaluar en qué se está convirtiendo la empresa."

– Ámbar Vargas, Panamá



PUNTOS CLAVE



Conclusiones de la encuesta

- El esfuerzo de auditoría interna sigue siendo más intenso en:
  - Ciberseguridad
  - Fraude
  - Finanzas/liquidez
  - Cambio normativo
  - La disrupción digital (incluida la IA)

Esto refleja tanto la importancia de los riesgos como las fortalezas históricas de la profesión.

- Las mayores deficiencias se dan en ámbitos que resultan más difíciles de auditar directamente:
  - Incertidumbre geopolítica y macroeconómica
  - Cambios en el mercado/competencia
  - Cambio climático/medio ambiente
  - Capital humano
  - Cultura organizacional
  - Algunos aspectos de la disrupción digital

Estrategias de auditoría interna

- Los responsables de auditoría interna (CAE) deben comparar los cinco principales riesgos con la cobertura actual de auditoría e identificar las deficiencias no explicadas.
- Cuando los riesgos sean difíciles de auditar directamente, la auditoría interna deberá traducirlos en procesos, decisiones, escenarios y controles que puedan ser objeto de auditoría.
- Los planes de auditoría deben incluir un equilibrio entre las actividades de aseguramiento y de asesoramiento y deben documentar de forma explícita cómo se abordan los riesgos elevados, ya sea mediante auditorías directas, un alcance integrado en otra auditoría, un seguimiento continuo, apoyo en funciones de segunda línea o la presentación de informes al Consejo de Administración.

3. MADUREZ Y COBERTURA DEL RIESGO

Los riesgos más elevados no siempre son los más maduros ni los mejor cubiertos

Los nuevos datos sobre la madurez de la gobernanza y la cobertura de auditoría interna constituyen uno de los aspectos más destacados del informe de este año.

El nivel de riesgo por sí solo no indica si una organización está preparada para gestionar dicho riesgo. La prioridad de auditoría por sí sola no indica si la cobertura de la auditoría interna es suficiente. Al comparar el nivel de riesgo, la madurez de la gobernanza y la cobertura de la auditoría, los directores de auditoría interna (CAE) pueden identificar en qué ámbitos la organización puede estar más expuesta.

Madurez en la gobernanza del riesgo

En la encuesta se pidió a los encuestados que valoraran el grado de madurez de la gobernanza del riesgo en cada área de riesgo. El anexo 3.1 muestra que el ámbito financiero y de liquidez presenta el nivel más alto de madurez en materia de gobernanza, ya que el 59 % lo califica como «gestionado» u «optimizado». Le siguen los cambios normativos, con un 47 %; la gobernanza y la información corporativa, con un 44 %; las comunicaciones y la reputación, con un 41 %; y el fraude, con un 40 %. Se trata de ámbitos en los que las organizaciones suelen contar con marcos establecidos, responsabilidades bien definidas, requisitos normativos, políticas y una supervisión periódica.

Por el contrario, la disrupción digital es la que presenta un nivel de gobernanza más bajo. Solo el 19 % consideró que la gestión de la disrupción digital estaba controlada u optimizada, mientras que el 57 % la consideró en fase inicial o en fase de infraestructura. El ámbito del cambio climático y el medio ambiente también presenta un bajo nivel de madurez, con un 20 % en fase de gestión u optimización y un 56 % en fase inicial o de infraestructura. La incertidumbre geopolítica y macroeconómica, el capital humano, la cultura y la cadena de suministro también presentan niveles de madurez relativamente modestos.

Este patrón es comprensible, pero arriesgado. La gobernanza madura suele darse en aquellas organizaciones que han tenido muchos años para desarrollar procesos y en las que las consecuencias normativas o financieras están claras. Los riesgos emergentes suelen evolucionar más rápido que los mecanismos de gobernanza. La IA, por ejemplo, puede ser adoptada por las unidades de negocio antes de que la organización haya definido políticas, procesos de aprobación de modelos, la titularidad de los datos, los requisitos de supervisión o los protocolos de escalamiento. Es posible que el riesgo geopolítico se debata en el Consejo de Administración, pero que no se traduzca en indicadores de riesgo, escenarios o planes de respuesta operativos.

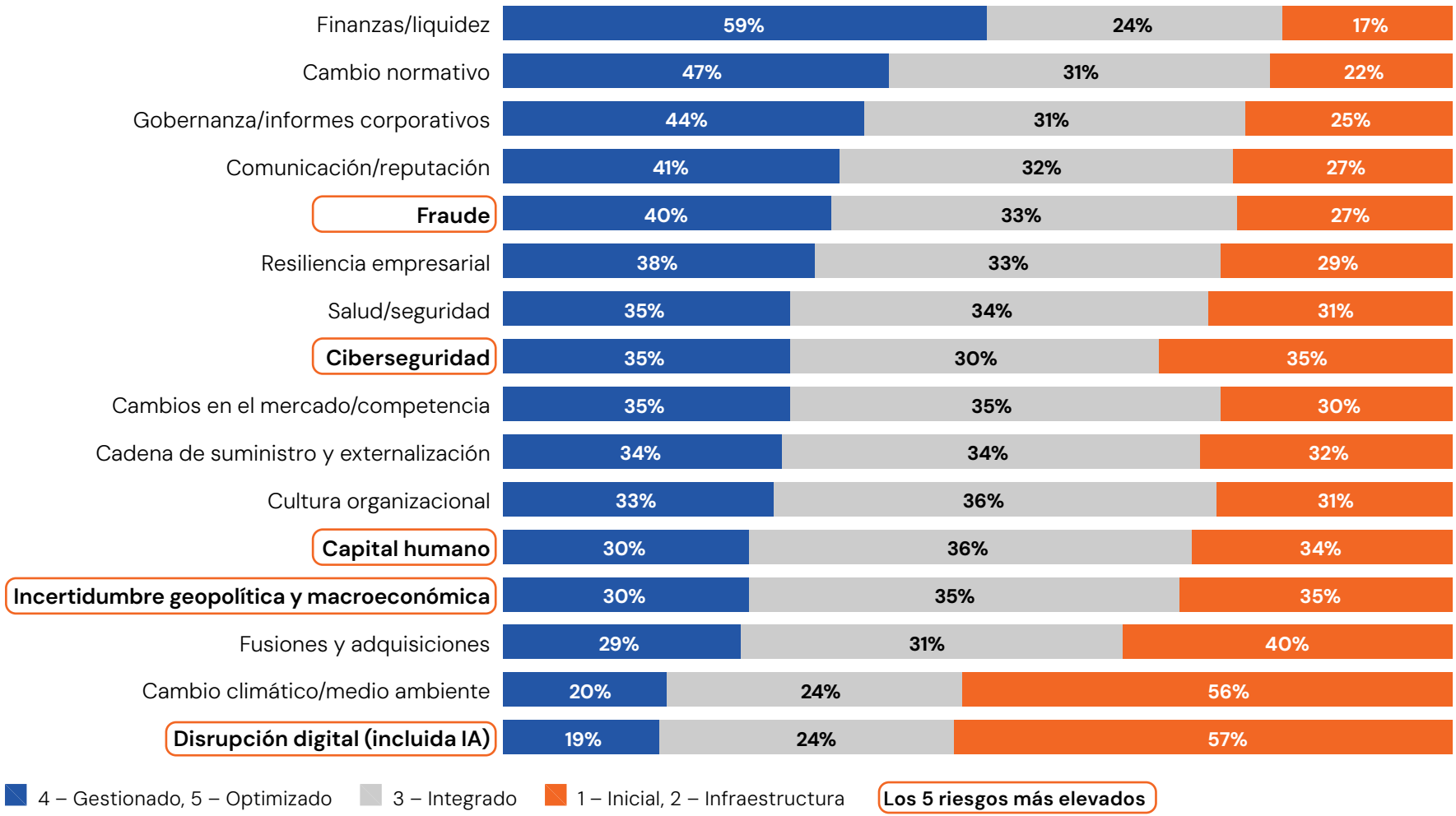
Las directrices del IIA sobre la evaluación de los procesos de gestión de riesgos refuerzan la importancia de la madurez. La madurez en la gestión de riesgos no consiste únicamente en contar con políticas, sino en que la identificación, la evaluación, la respuesta, el seguimiento, la comunicación y la rendición de cuentas en materia de riesgos estén integradas en la toma de decisiones. Un entorno con bajo grado de madurez requiere un enfoque diferente de la auditoría interna. En ámbitos muy consolidados, la auditoría interna puede evaluar la eficacia del diseño y del funcionamiento. En las áreas con un bajo grado de madurez, es posible que la auditoría interna tenga que evaluar en primer lugar el diseño del sistema de gobernanza, las funciones y responsabilidades, el apetito de riesgo, la disponibilidad de datos, los procedimientos de escalamiento y el seguimiento.

AI

La disrupción digital presenta el nivel más bajo de madurez en materia de gestión de riesgos, con solo **el 19 %** de los responsables de auditoría interna (CAE) latinoamericanos que la califican como controlada u optimizada.

Anexo 3.1. América Latina – Madurez en la gestión de riesgos

Pregunta de la encuesta: **En una escala del 1 al 5, valora el nivel actual de madurez de la gobernanza del riesgo en tu organización para cada una de las siguientes áreas de riesgo.**



Nota: Encuesta «Risk in Focus», realizada en línea a nivel mundial entre el 2 de marzo y el 6 de mayo de 2026. n = 512 para América Latina.

MADUREZ Y COBERTURA DEL RIESGO

Alcance de auditoría interna

El anexo 3.2 refleja una preocupación similar en cuanto a la cobertura de auditoría interna. El ámbito financiero y de liquidez presenta el nivel más alto de cobertura total, con un 45 %, seguido de los cambios normativos, con un 39 %; el gobierno corporativo y la información empresarial, con un 37 %; el fraude, con un 30 %; y la ciberseguridad, con un 26 %. Se trata de ámbitos de cobertura conocidos y necesarios.

Sin embargo, la cobertura total es menor en el caso de la disrupción digital, con tan solo un 8 %. La cobertura de la incertidumbre geopolítica y macroeconómica también es baja, con un 11 %; la relacionada con el cambio climático y el medio ambiente, del 13 %; la derivada de los cambios en el mercado y la competencia, del 14 %; la relacionada con la Cultura organizacional, del 20 %; la del capital humano, del 20 %; y la de la cadena de suministro, del 21 %. El porcentaje de empresas que consideran que su cobertura es insuficiente es mayor en el caso de la disrupción digital (45 %), el clima y el medio ambiente (37 %), la incertidumbre geopolítica y macroeconómica (35 %) y los cambios en el mercado y la competencia (29 %).

Esto pone de manifiesto un claro mensaje de riesgo: algunas de las áreas con mayor relevancia estratégica son las que presentan una menor madurez en materia de gobernanza y una cobertura de auditoría interna más débil. La disrupción digital es el ejemplo más evidente. Es el segundo riesgo más importante de los cinco principales y el 75 % lo califica como «alto», pero presenta el nivel más bajo de madurez en materia de gobernanza y la cobertura de auditoría más reducida. Para los Consejos de Administración, esto debería ser una señal de alarma. Para los CAE, debería ser una prioridad en la planificación.

Repensar la cobertura

La solución no consiste necesariamente en realizar un gran número de nuevas auditorías. Muchas funciones de auditoría interna en América Latina cuentan con una dotación y un presupuesto limitados. La solución consiste en replantearse la cobertura. En lo que respecta a la disrupción digital, la auditoría interna puede llevar a cabo revisiones de carácter consultivo sobre la gobernanza de la inteligencia artificial, la gobernanza de los datos, los riesgos relacionados con la nube, los controles de automatización, los riesgos tecnológicos de terceros, la ciberseguridad desde el diseño y la gestión del cambio. También puede integrar cuestiones relacionadas con los riesgos digitales en las auditorías de ventas, finanzas, operaciones, compras, recursos humanos y cumplimiento normativo.

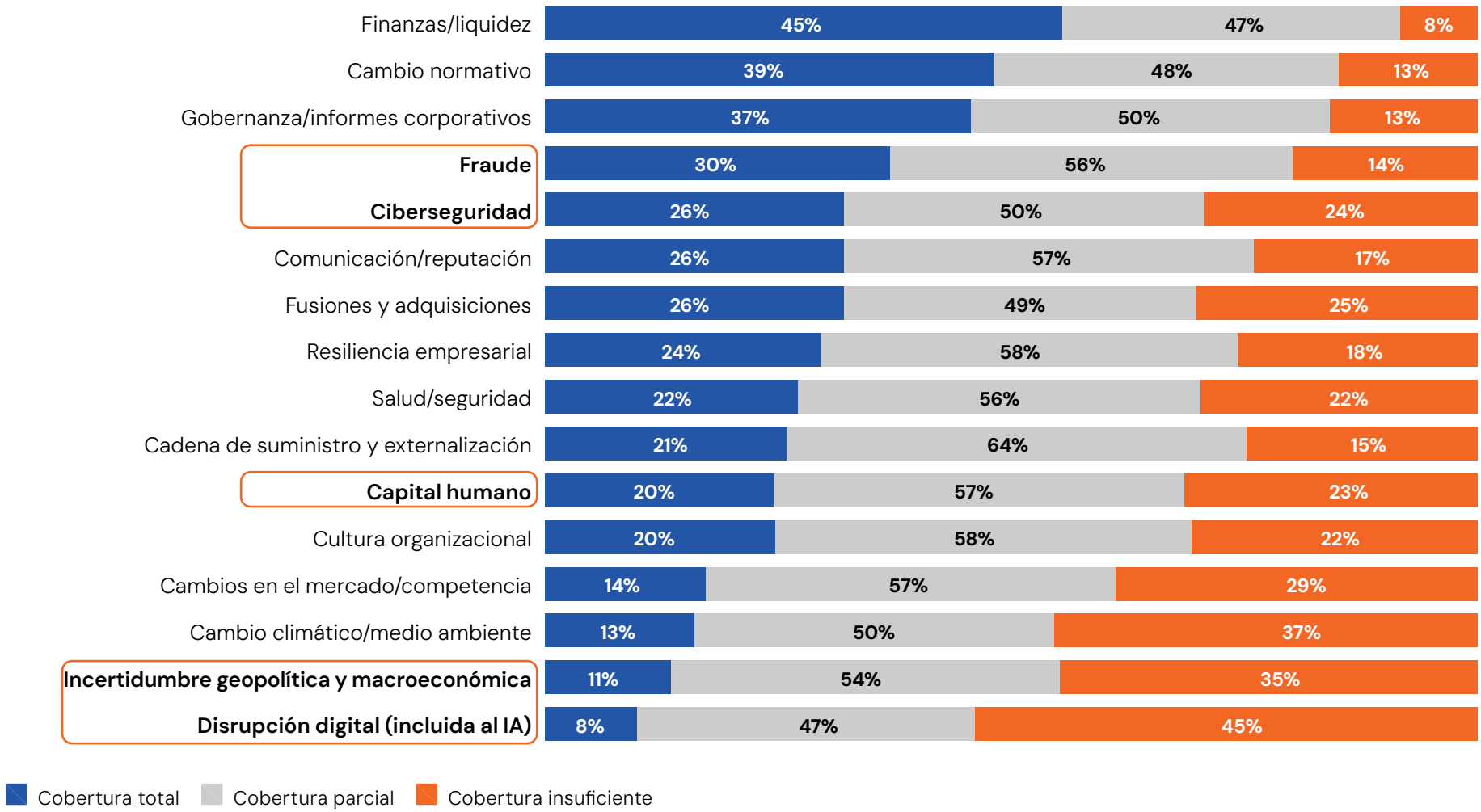
Ante la incertidumbre geopolítica y macroeconómica, la auditoría interna puede examinar la planificación de escenarios, las pruebas de resistencia, la continuidad del negocio, la gestión de crisis, la tesorería, la cadena de suministro, la planificación estratégica y el seguimiento regulatorio. En lo que respecta al clima y el medio ambiente, la auditoría interna puede centrarse en la exposición a riesgos físicos, el cumplimiento de la normativa medioambiental, los controles de los informes de sostenibilidad, la resiliencia de los activos, los seguros y los planes de continuidad. En lo que respecta al capital humano, la auditoría interna puede evaluar la planificación estratégica de la plantilla, los puestos clave, la sucesión, la formación, la retención, la cultura, los incentivos y las brechas en las competencias.

"Muchos planes de auditoría siguen reflejando lo que los auditores saben auditar, en lugar de lo que supone una mayor amenaza para la estrategia."

– Ámbar Vargas, Panamá

Anexo 3.2. América Latina – Alcance de auditoría interna

Pregunta de la encuesta: **Indique, por favor, si la cobertura actual de auditoría interna de estas áreas de riesgo es adecuada en su organización.**



Nota: Encuesta «Risk in Focus» realizada en línea a nivel mundial entre el 2 de marzo y el 6 de mayo de 2026. n = 512 para América Latina.

MADUREZ Y COBERTURA DEL RIESGO

Coordinación con la segunda línea

Los datos sobre madurez y cobertura también ponen de relieve la importancia de la coordinación con la segunda línea. La auditoría interna no tiene por qué encargarse de todas las actividades de gestión de riesgos. No obstante, el CAE debe comprender quién asume el riesgo, cómo se supervisa, qué garantías existen y si el Consejo de Administración recibe información confiable. En áreas con un bajo grado de madurez, la labor de asesoramiento puede resultar más valiosa que la auditoría tradicional a corto plazo, siempre que se garantice la objetividad.

Servicios de asesoramiento

Varios participantes en la mesa redonda plantearon la cuestión de la independencia cuando la auditoría interna presta apoyo en materia de asesoramiento en ámbitos emergentes. Esta preocupación es legítima, pero no debería convertirse en una excusa para la inacción. Las Normas Globales de Auditoría Interna™ permiten que la auditoría interna preste servicios de asesoramiento, siempre que el responsable de auditoría interna (CAE) gestione los posibles riesgos que puedan afectar a la objetividad y evite asumir responsabilidades de gestión. En la práctica, la auditoría interna puede ayudar a la dirección a comprender las mejores prácticas, formular preguntas más acertadas, evaluar el grado de preparación e identificar deficiencias sin tener que diseñar ni asumir la responsabilidad de los controles.

Esto es especialmente importante en el ámbito de la inteligencia artificial y la transformación digital. Esperar a que las medidas de control se hayan aplicado por completo podría ser demasiado tarde. La auditoría interna puede aportar valor añadido en una fase más temprana mediante la revisión del diseño de los mecanismos de gobernanza, los criterios de decisión, las evaluaciones de riesgos, la debida diligencia de proveedores, las pruebas de aprobaciones, la protección de datos y los planes de seguimiento. La participación en etapas tempranas no implica responsabilidad en la gestión. Esto supone ofrecer aseguramiento y asesoramiento oportunos en un ámbito en el que los riesgos evolucionan rápidamente.

Resumen

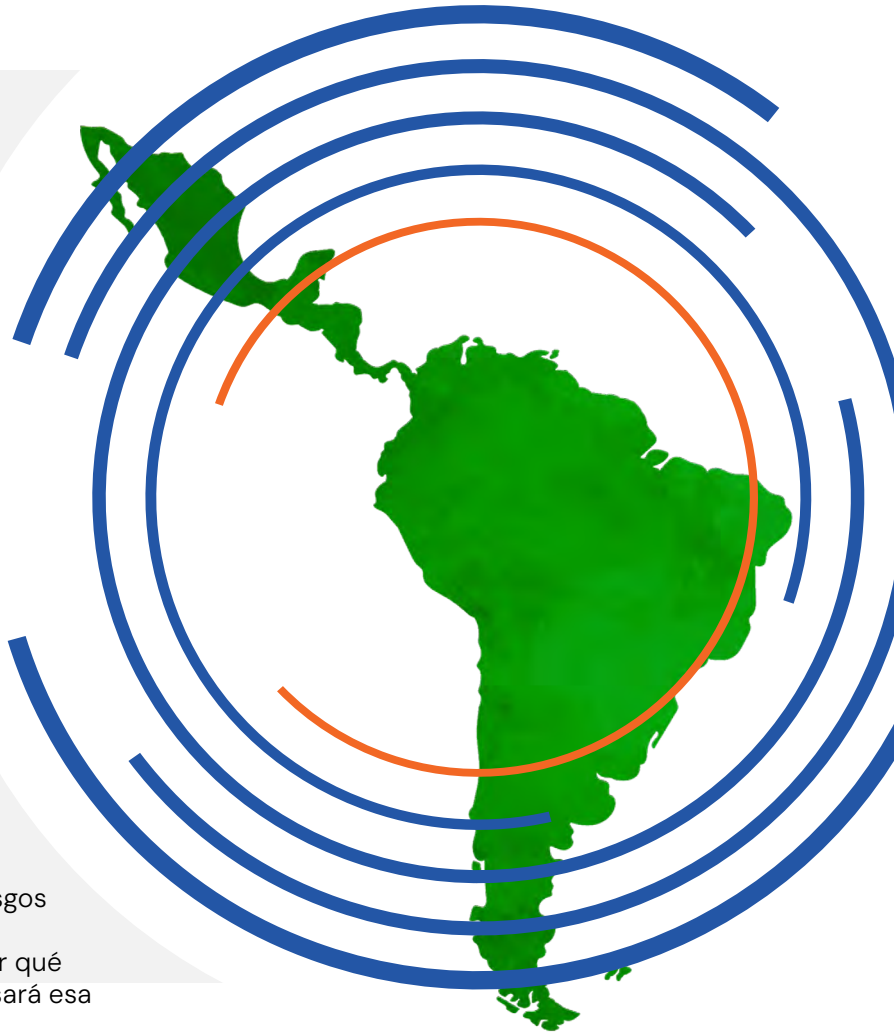
En el caso de los responsables de auditoría interna (CAE), el análisis de la madurez y la cobertura debería formar parte de la reunión anual de planificación de la auditoría con el Consejo de Administración. El CAE debería poner de manifiesto no solo los riesgos más elevados, sino también aquellas áreas en las que la gobernanza es inmadura y la cobertura es insuficiente. Esto permite al consejo de administración detectar dónde se pueden estar acumulando riesgos de forma silenciosa.



PUNTOS CLAVE

Conclusiones de la encuesta

- El mayor grado de madurez en materia de gobernanza y la mayor cobertura de auditoría se concentran en ámbitos más tradicionales, como las finanzas y la liquidez, los cambios normativos, la gobernanza y la información corporativa, el fraude y la ciberseguridad.
- Los aspectos que presentan un menor grado de madurez y cobertura son los relacionados con ámbitos emergentes o estratégicos, como la disrupción digital, la incertidumbre geopolítica y macroeconómica, el clima y el medio ambiente, los cambios en los mercados, la cultura y el capital humano.
- La disrupción digital destaca como la carencia más urgente, ya que supone un riesgo elevado y, al mismo tiempo, es un ámbito con un bajo nivel de madurez y una cobertura reducida.



Estrategias de auditoría interna

- Los responsables de auditoría interna (CAE) deberían elaborar un informe sobre «riesgo, madurez y cobertura» para el Consejo de Administración. Se deben abordar de forma explícita las áreas de alto riesgo con bajo nivel de madurez y escasa cobertura de auditoría. La auditoría interna debería recurrir a trabajos de asesoramiento, evaluaciones del grado de preparación, procedimientos de auditoría integrados en otras auditorías y aseguramiento coordinado para hacer frente a los riesgos emergentes antes de que se conviertan en fallos de control.
- Los planes de auditoría deben identificar no solo qué se va a auditar, sino también por qué determinadas áreas de alto riesgo reciben una cobertura limitada y cómo se supervisará esa deficiencia.

CONCLUSIÓN

El CAE como traductor del riesgo, la estrategia y la acción

Los resultados del informe «Risk in Focus» de Latinoamérica para 2026/2027 muestran que la región está entrando en una fase exigente en lo que respecta a la gestión de riesgos y el liderazgo en auditoría interna.

Los principales riesgos son evidentes. La ciberseguridad, la disrupción digital, la incertidumbre geopolítica y macroeconómica, el fraude, el capital humano, la normativa y la liquidez ya están en el punto de mira de los responsables de auditoría interna, los ejecutivos y los Consejos de Administración. El reto ya no es solo la concientización. El reto es pasar a la acción.

En el ámbito de la auditoría interna, esto supone pasar de una mentalidad centrada en la clasificación de riesgos a una mentalidad centrada en la respuesta a los riesgos. Un riesgo elevado que no influya en la planificación de la auditoría, la cobertura de aseguramiento, la actividad de asesoramiento, la estrategia de talento o el diálogo con el Consejo de Administración no pasa de ser un simple resultado de una encuesta. El valor de «Risk in Focus» se pone de manifiesto cuando los responsables de auditoría interna (CAE) lo utilizan para analizar su ámbito de auditoría, poner a prueba sus hipótesis y plantearse si la función se está centrando en los riesgos que más influyen en el valor de la organización. Las conclusiones apuntan a tres prioridades para los responsables de auditoría interna (CAE) en América Latina:

1. La auditoría interna debe abordar los riesgos que se relacionan. La ciberseguridad, la inteligencia artificial, el fraude, los datos, la regulación, los terceros, la liquidez, la reputación y la continuidad no deberían auditarse únicamente como aspectos aislados. Los sucesos más devastadores suelen producirse en la intersección de varios riesgos. Un incidente cibernético puede derivar en un caso de fraude, un incumplimiento normativo, un problema de liquidez o una crisis de reputación. Un acontecimiento geopolítico puede convertirse en un problema relacionado con la cadena de suministro, con la resiliencia de la nube, con el tipo de cambio o con la continuidad del negocio.
2. Los responsables de auditoría interna deben reducir la brecha entre los riesgos emergentes y la capacidad de auditoría. La disrupción digital se ha convertido en uno de los mayores riesgos de la región, pero el nivel de madurez en materia de gobernanza y la cobertura de las auditorías siguen siendo bajos. Esta carencia no se puede resolver únicamente contratando a especialistas, aunque las competencias especializadas son importantes. También requiere nuevas metodologías, formación, externalización compartida, análisis de datos, auditorías continuas, una mayor coordinación con la segunda línea y un diálogo más estratégico con la gerencia.
3. La auditoría interna debe reforzar su relación con el consejo y la dirección ejecutiva. El DEA debe estar lo suficientemente cerca de la estrategia como para comprender hacia dónde se dirige la organización, al tiempo que mantiene la objetividad necesaria para evaluar si los riesgos se gestionan adecuadamente. Este equilibrio no supone una falta de independencia, sino que es un requisito para mantener la relevancia.

La próxima generación de líderes de la auditoría interna en Latinoamérica se caracterizará por su capacidad para convertir la volatilidad en decisiones. Los consejos de administración necesitan directores de auditoría interna (DEA) capaces de explicar cómo las tendencias globales afectan a las operaciones locales, cómo las tecnologías emergentes transforman los entornos de control, cómo la falta de talento influye en la ejecución estratégica y cómo debe evolucionar la cobertura de la auditoría.

La cuestión más importante para 2027 no es si la auditoría interna comprende el panorama de riesgos. La cuestión es si la auditoría interna está preparada para actuar al respecto.



"La auditoría interna no puede marcar el rumbo adecuado si no comprende hacia dónde se dirige la organización."

– Héctor Trujeque, Argentina

APÉNDICE A. METODOLOGÍA

Encuestas, mesas redondas y entrevistas

La Fundación de Auditoría Interna recopiló las respuestas a la encuesta entre el 24 de marzo y el 6 de mayo de 2026 en todas las regiones, excepto en Europa. El Grupo de Investigación de Institutos Europeos recopiló las respuestas procedentes de Europa entre el 2 de marzo y el 7 de abril de 2026.

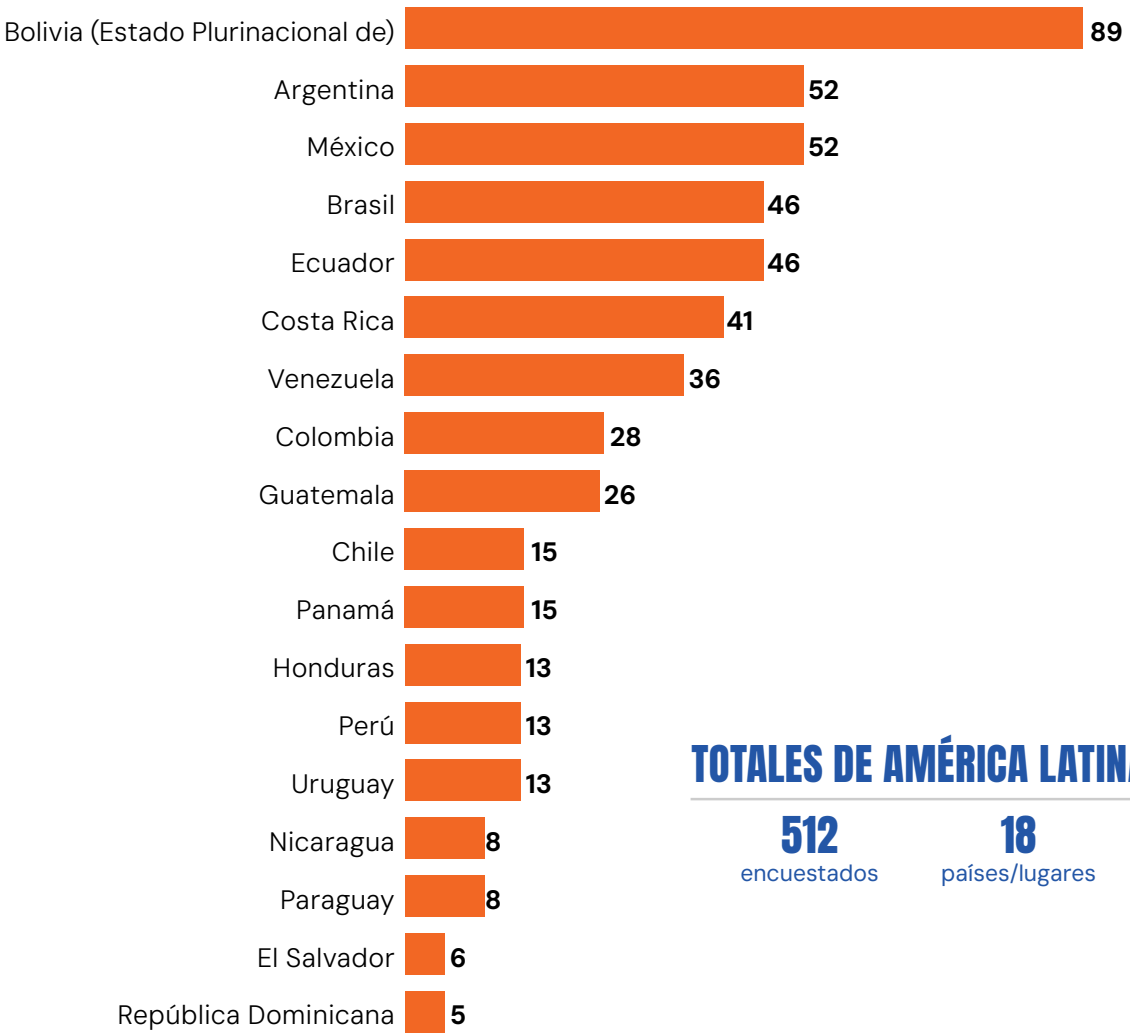
Se recibieron cuestionarios completados por 3.285 auditores internos que confirmaron ser los auditores internos de mayor rango en sus organizaciones. Representaban a 132 países o localidades. La encuesta se llevó a cabo en línea a través de contactos vinculados a los Institutos Nacionales del IIA y a los organismos regionales. Además, se organizaron mesas redondas y entrevistas para cada informe regional.

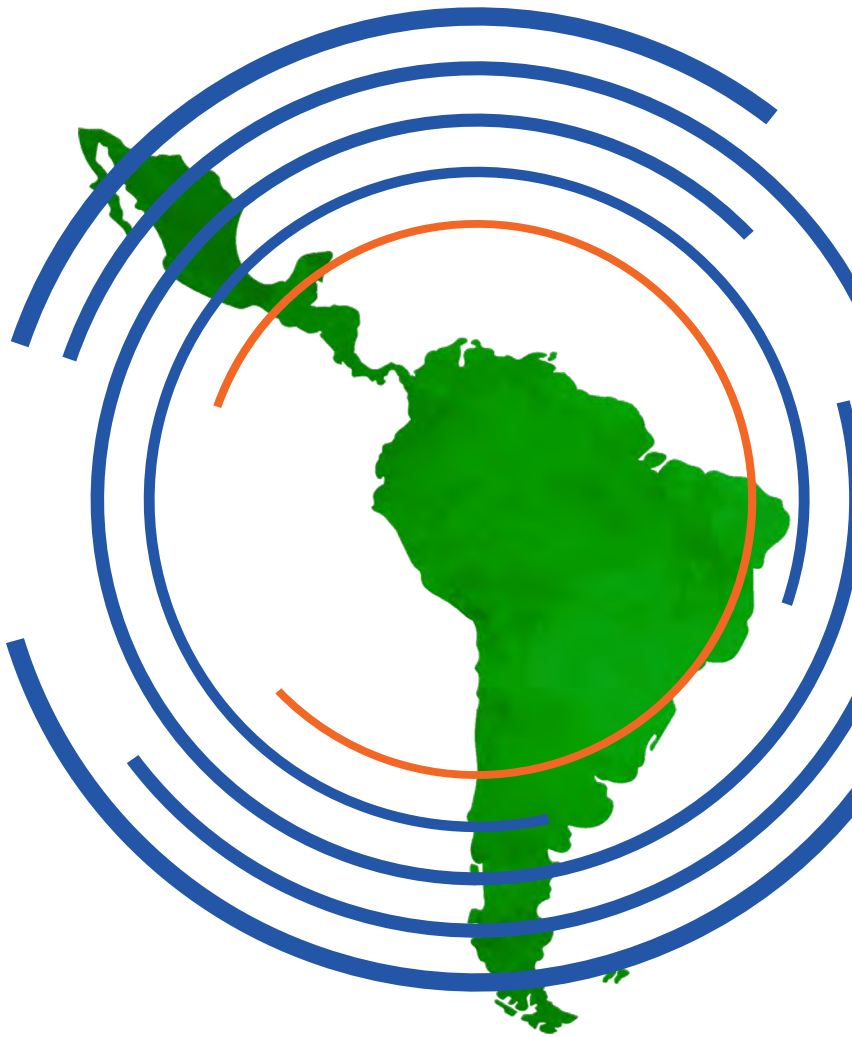
A continuación se indican las 16 áreas de riesgo utilizadas en la encuesta. A los encuestados se les plantearon diversas preguntas sobre los niveles de riesgo, la planificación de la auditoría y el grado de madurez de la gestión del riesgo.

Nombre del riesgo	Descripción del riesgo utilizada en la encuesta
Resiliencia empresarial	Continuidad del negocio, resiliencia operativa, gestión de crisis y respuesta ante catástrofes
Cambio climático/medio ambiente	Cambio climático, biodiversidad y sostenibilidad medioambiental
Comunicación/reputación	Comunicación, reputación y relaciones con las partes interesadas
Ciberseguridad	Ciberseguridad y seguridad de los datos
Disrupción digital (incluida la IA)	La disrupción digital, las nuevas tecnologías y la IA (inteligencia artificial)
Finanzas/liquidez	Riesgos financieros, de liquidez y de insolvencia
Fraude	El fraude, el soborno y la explotación delictiva de situaciones de disrupción
Incertidumbre geopolítica y macroeconómica	Incertidumbre macroeconómica, social y geopolítica
Gobernanza/información corporativa	Gobernanza organizativa y presentación de informes corporativos
Salud y seguridad	Salud, seguridad y protección
Capital humano	Capital humano, diversidad y gestión y retención del talento
Cambios en el mercado/competencia	Cambios en el mercado, competencia y comportamiento de los clientes
Fusiones y adquisiciones	Fusiones y adquisiciones
Cultura organizacional	Cultura organizacional
Cambio normativo	Modificaciones en la legislación y las regulaciones
Cadena de suministro y externalización	Cadena de suministro, externalización y riesgo de “enésima” parte

APÉNDICE B. DATOS DEMOGRÁFICOS

Anexo B.1. América Latina – Índice de respuesta





TOTALES DE AMÉRICA LATINA

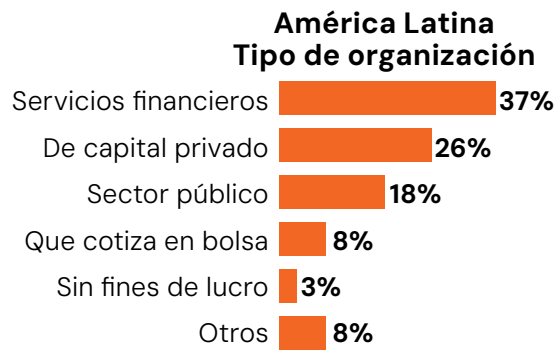
512 encuestados

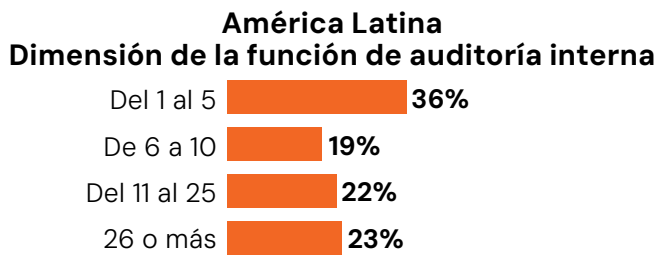
18 países/lugares

Nota: Encuesta «Risk in Focus», realizada en línea a nivel mundial entre el 2 de marzo y el 6 de mayo de 2026. n = 512 para América Latina.

Anexo B.2. América Latina: sector, tipo de organización, tamaño del departamento de auditoría interna







Nota: Encuesta «Risk in Focus», realizada en línea a nivel mundial entre el 2 de marzo y el 6 de mayo de 2026. n = 512 para Latinoamérica.

APÉNDICE C. RESUMEN DEL RIESGO GLOBAL

América Latina en un contexto mundial de aceleración

El entorno de riesgo de América Latina forma parte de una tendencia mundial más amplia. El panorama mundial es relevante para las directores ejecutivos de auditoría (DEA) de América Latina, ya que muchas organizaciones de la región operan a nivel transfronterizo, dependen de proveedores de tecnología internacionales, importan suministros esenciales, recurren a los mercados financieros internacionales y se ven afectadas por actores que representan amenazas cibernéticas a escala mundial. Incluso las organizaciones que operan a nivel local están expuestas a la transmisión de riesgos a escala mundial a través de la inflación, los tipos de cambio, las plataformas en la nube, los proveedores de software, las redes de ciberdelincuencia, la normativa y el comportamiento de los consumidores.

Los resultados de la encuesta muestran que las regiones de todo el mundo están experimentando tendencias de riesgo similares (Anexo C.1 y Anexo C.2):

- Las calificaciones de riesgo relacionadas con la disrupción digital aumentaron en todas las regiones del mundo.
- La ciberseguridad y la incertidumbre geopolítica aumentaron en todas las regiones, salvo en una: América del Norte.
- Los riesgos de fraude y los riesgos financieros y de liquidez aumentaron en África, Asia-Pacífico y América Latina.
- El riesgo en la cadena de suministro ha aumentado en África, Asia-Pacífico y Oriente Medio.

Adquirir una perspectiva desde el contexto global

El contexto mundial no debería llevar a los DEA a copiar las prioridades globales sin adaptarlas. Más bien, debería ayudarles a cuestionar las ideas preconcebidas locales.

Puede que una tendencia global no suponga un riesgo elevado para todas las organizaciones, pero debe tenerse en cuenta en la evaluación de riesgos. Por ejemplo, es posible que, en el conjunto de América Latina, el clima y el medio ambiente ocupen un lugar menos relevante que la ciberseguridad o la inteligencia artificial, pero en sectores como la energía, la agricultura, las infraestructuras, el transporte, la minería, los seguros y la administración pública, pueden suponer un riesgo estratégico. Del mismo modo, es posible que el riesgo de la cadena de suministro no sea elevado en el caso del abastecimiento de comida a bordo de una aerolínea, pero puede resultar crítico en los sectores sanitario, minorista, manufacturero o energético.

Para los consejos y los comités de auditoría, el valor de la comparación a nivel mundial radica en la evaluación comparativa. Ayuda a responder a tres preguntas: ¿Nos enfrentamos a los mismos riesgos que nuestras empresas del sector? ¿Avanzamos más rápido o más lento que el mercado? ¿Existen riesgos que están aumentando a nivel mundial y que aún no hemos incorporado a nuestra estrategia? Los DEA deberían utilizar las comparativas globales no como sustituto de la evaluación de riesgos de la empresa, sino como un mecanismo de cuestionamiento para mejorarla.

La auditoría interna también puede recurrir a comparativas globales para respaldar los debates sobre recursos. Si la disrupción digital, la ciberseguridad y la incertidumbre geopolítica van en aumento en todo el mundo, pero la función de auditoría interna carece de competencias tecnológicas, análisis de datos, conocimientos especializados en ciberseguridad o capacidad para gestionar riesgos estratégicos, el director de auditoría interna (DEA) tiene argumentos más sólidos para justificar la inversión. La conversación con el consejo de administración debería pasar de «necesitamos más recursos» a «nuestro perfil de riesgo ha cambiado y nuestras capacidades deben adaptarse a ello».

MÁS RECURSOS GLOBALES

Consulta el Informe «Risk in Focus» Informe de resumen global para consultar datos y análisis sobre las tendencias regionales.

Anexo C.1. A nivel mundial: los 5 principales riesgos por región

Pregunta de la encuesta: **¿Cuáles son los cinco principales riesgos a los que se enfrenta actualmente tu organización? (Elige 5.)**

Áreas de riesgo	Media de las regiones	África	Asia Pacífico	Europa	América Latina	Medio Oriente	América del Norte
Ciberseguridad	**80 % ↑**	**73 % ↑**	**72 % ↑**	**86 % ↑**	**80 % ↑**	**81 % ↑**	**85 %**
Disrupción digital (incluida la IA)	**58 % ↑**	**50 % ↑**	**59 % ↑**	**52 % ↑**	**61 % ↑**	**58 % ↑**	**69 % ↑**
Incertidumbre geopolítica y macroeconómica	**48 % ↑**	**35 % ↑**	**48 % ↑**	**51 % ↑**	**52 % ↑**	**60 % ↑**	**43 %**
Capital humano	**38 %**	30 %	**41 %**	**39 %**	**37 %**	34 %	**45 %**
Resiliencia empresarial	**35 %**	28 %	**43 %**	37 %	25 %	**47 %**	29 %
Finanzas/liquidez	34 %	**49 % ↑**	**28 % ↑**	28 %	**36 % ↑**	**42 % ↑**	24 %
Cambio normativo	32 %	28 %	24 %	**40 %**	36 %	20 %	**42 %**
Cambios en el mercado/competencia	29 %	20 %	37 %	32 %	27 %	20 %	**41 % ↑**
Fraude	29 %	**50 % ↑**	**28 % ↑**	16 %	**38 % ↑**	22 %	**18 % ↑**
Cadena de suministro y externalización	**27 % ↑**	**21 % ↑**	**33 % ↑**	26 %	17 %	**35 % ↑**	33 %
Gobernanza/información corporativa	20 %	27 %	21 %	13 %	15 %	27 %	14 %
Cambio climático/medio ambiente	19 %	**31 % ↑**	20 %	21 %	23 %	15 %	7 %
Cultura organizacional	19 %	26 %	19 %	17 %	26 %	13 %	16 %
Comunicación/reputación	15 %	18 %	13 %	**17 % ↑**	15 %	13 %	16 %
Salud y seguridad	10 %	12 %	8 %	12 %	7 %	10 %	11 %
Fusiones y adquisiciones	5 %	2 %	6 %	5 %	4 %	3 %	7 %

Los 5 riesgos más importantes

Cómo interpretar el gráfico
Las **flechas rojas ↑** indican un aumento de 4 puntos porcentuales o más en comparación con el año anterior.

Nota: Encuesta «Risk in Focus», realizada en línea a nivel mundial del 2 de marzo al 6 de mayo de 2026. n = 3.285.

Anexo C.2. A nivel mundial – Tendencia de los 5 principales riesgos

Pregunta de la encuesta: **¿Cuáles son los cinco principales riesgos a los que se enfrenta actualmente tu organización? (Elige 5.)**

2023	2024	2025	2026	Cambio de 2025 a 2026	Cambiar	Zonas de riesgo
73%	71%	73%	80%		+7	**Ciberseguridad**
34%	39%	48%	58%		+10	**Disrupción digital (incluida la IA)**
30%	28%	38%	48%		+10	**Incertidumbre geopolítica y macroeconómica**
51%	49%	43%	38%		-5	Capital humano
47%	54%	47%	35%		-12	**Resiliencia empresarial**
32%	32%	31%	34%		+3	Finanzas/liquidez
39%	37%	41%	32%		-9	**Cambio normativo**
32%	32%	31%	29%		-2	**Cambios en el mercado/competencia**
24%	27%	23%	29%		+6	**Fraude**
26%	22%	24%	27%		+3	Cadena de suministro (incluidos terceros)
27%	26%	24%	20%		-4	Gobernanza/información corporativa
19%	21%	18%	19%		+1	Cambio climático/medio ambiente
26%	25%	24%	19%		-5	Cultura organizacional
21%	21%	19%	15%		-4	Comunicación/reputación
11%	11%	10%	10%		0	Salud y seguridad
6%	6%	5%	5%		0	Fusiones y adquisiciones

Aumento del riesgo con respecto al año anterior Disminución del riesgo con respecto al año anterior

Cómo interpretar el gráfico
El color naranja indica un aumento de 4 puntos porcentuales o más en comparación con el año anterior. El **naranja** y **azules** muestran la diferencia en las valoraciones entre 2025 y 2026. La columna titulada «cambio» muestra la diferencia en puntos porcentuales entre 2025 y 2026.

Nota: Encuesta «Risk in Focus», realizada en línea a nivel mundial entre el 2 de marzo y el 6 de mayo de 2026. n = 3.285.

APÉNDICE D. RECURSOS DEL IIA

El IIA ofrece diversos recursos para ayudar a los auditores internos en la evaluación de riesgos y la planificación de auditorías a través del departamento de Normas y Orientaciones. La mayoría de estos recursos están disponibles de forma gratuita para los miembros del IIA de todo el mundo, y algunos también están a disposición del público en general. Para ver las últimas novedades, visita la página de recursos de Global Guidance y la página de comunicados de posición.



Entorno de riesgo

- **Evaluación del proceso de gestión de riesgos, 2.ª edición** (El IIA, Guía de prácticas globales, 2024)
- **El papel de la función de auditoría interna en la gestión de riesgos empresariales** (El IIA, Declaración de posición, 2026)

Prioridades de auditoría

- **Herramientas de apoyo al marco de IA** (El IIA, Herramientas de auditoría, 2026)
- **Marco de auditoría de la inteligencia artificial** (El IIA, 2024)
- **Auditoría de las operaciones de ciberseguridad: Prevención y detección, 2.ª edición** (El IIA, Guía de prácticas globales, 2025)
- **Auditoría de los riesgos relacionados con la privacidad y la protección de datos, 3.ª edición** (El IIA, Guía de prácticas globales, 2026)
- **Auditoría interna y fraude, 3.ª edición** (El IIA, Guía de prácticas globales, 2024)
- **Requisito temático sobre resiliencia organizativa** (El IIA, Requisito temático, 2026)

Madurez en la gestión de riesgos y alcance de la auditoría interna

- **Elaboración de un plan de auditoría interna basado en el riesgo, 2.ª edición** (El IIA, Guía de prácticas globales, 2025)
- **Elaboración de una estrategia de auditoría interna** (El IIA, Guía de prácticas globales, 2025)
- **Modelo de las tres líneas** (El IIA, Declaración de posición, 2026)

Normas Internacionales de Auditoría Interna

- **Normas globales completas de auditoría interna**
- **Normas Internacionales de Auditoría Interna (resumen)**

FUNDACIÓN DE AUDITORÍA INTERNA

La Fundación de Auditoría Interna es la principal entidad mundial, en colaboración estratégica con el IIA, dedicada a potenciar y reforzar la profesión de la auditoría interna mediante el desarrollo de investigaciones y programas de vanguardia. Desde hace 50 años, la Fundación ha ayudado a los auditores internos actuales y futuros a mantenerse al día mediante el desarrollo y la mejora de sus habilidades y conocimientos, garantizando así que las organizaciones estén preparadas para crear, proteger y mantener el valor a largo plazo.
Visita theiia.org/Foundation.

Consejo de la Fundación de Auditoría Interna de la Fundación de Auditoría Interna, 2026-27

Presidente
Glenn Ho, CIA, CRMA

Vicepresidente sénior de Estrategia
Shirley Livhuwani Machaba, CCSA, CRMA

Vicepresidente de Finanzas y Desarrollo
Michael A. Smith, CIA

Vicepresidente de Contenidos
Nora Zeid Kelani, CIA, CRMA

Miembros del consejo de administración
Mohammed Al Qahtani, CIA
José Gabriel Calderón, CIA, CRMA
Susan Haseley, CIA
Dawn Jones, CIA, CRMA
Tshepo Mofokeng, CIA, CRMA
Anthony J. Pugliese, CIA
Nicholas C. Saracco, CIA
Bhaskar Subramanian

Persona de contacto del personal: Laura LeBlanc, vicepresidenta de la Fundación de Auditoría Interna y de los itinerarios profesionales de la Asociación de es ( )

Comité de Asesores de Investigación y Educación, 2026-27

Presidente
Nora Zeid Kelani, CIA, CRMA

Miembros
Christopher Calvin, doctor, CIA
Joseph Ian Canlas, CIA, CRMA
Andrew Dahle, CIA, CRMA
André Domingos
Marc Eulerich, doctor, CIA
Ivony Kudzayi Katsande-Zezekwa, DBL, CIA, CRMA
Tabborrah Labor, CIA
Roberto León Pacheco, doctor, CIA, CCSA, CRMA
Ayaka Mitsunari, CIA
Ahmed Mohammed, Doctor en Administración de Empresas (DBA), CIA
Grace Mubako, doctora, CIA
Nisha Nair, CIA
Millicent Lindiwe Ndaba, CIA
Shintaro Okada, doctor, CIA
Emmanuel Pascal, CIA, CRMA
Brad Schafer, doctor, CIA
Brian Tremblay, CIA
Stacy Wright, CIA

Internal Audit FOUNDATION 1976-2026

Equipo de investigación

Responsable de investigación
Deborah Poulalion, directora sénior de Investigación y Análisis del IIA

Responsable de proyectos
Candace Sacher

Diseñadores gráficos
Sergio Analco y Cathy Watanabe

SOCIOS DE LA FUNDACIÓN DE AUDITORÍA INTERNA

SOCIOS DIAMANTE

bakertilly

Deloitte.

Grant Thornton

KPMG

Optro

The Institute of Internal Auditors

The Institute of Internal Auditors Chicago

Wolters Kluwer

SOCIOS ORO

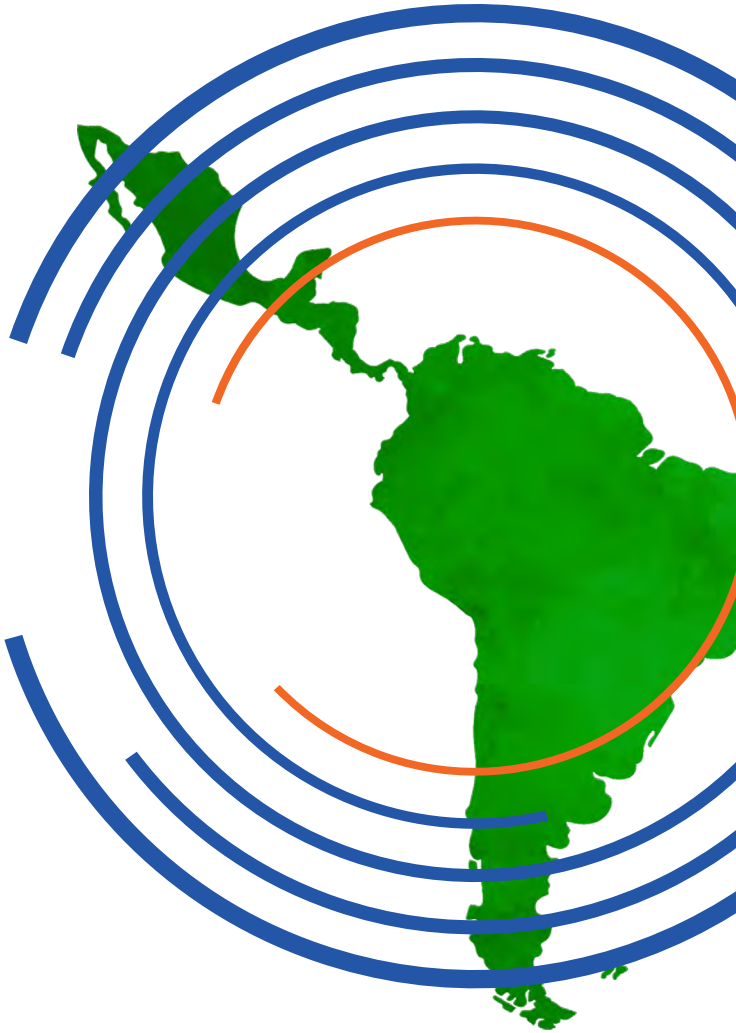
- Carr, Riggs &, Ingram
- Fundación Latinoamericana de Auditores Internos
- IIA – Delegación de Houston
- IIA–Japón
- IIA – Delegación de Nueva York
- IIA – Delegación de San Francisco

CÍRCULO DEL PRESIDENTE

(Donantes particulares)

- Larry Harrington, CIA, QIAL, CRMA
- Glenn Ho, CIA, CRMA
- Keith Kahl, CIA, CRMA
- Doug Mims, CIA, CRMA
- Jessica Rodgers, CIA
- Stacey Schabel, CIA
- Michael A. Smith, CIA
- Warren Stippich, CIA, CRMA

FUNDACIÓN LATINOAMERICANA DE AUDITORES INTERNOS (FLAI)



Junta Directiva de la FLAI

Presidenta
Geraldine Giachello, CIA, CPA
Vicepresidente
Manuel Quezada, CPA, MBA
Secretario y expresidente
Francisco Arauz, CIA, CCSA, CPA
Tesorera
Maritza Barzola, CRMA, CPCC
Miembros del Consejo de Administración
Javier Ferrer, CPA, Máster en Gestión Ejecutiva
Marcia Pereira, CIA, CCSA
Jim Romero, CIA, CCSA, CRMA, CPA

Director ejecutivo de la FLAI

Roberto Loo

Autor

Renato Trisciuzzi, CIA, QIAL, CCSA, CRMA, máster en Ciencias, doctor

Moderadores de la mesa redonda «Risk in Focus»

Savio Jannuzzi, Brasil
Alejandro Rembado, Argentina

¡GRACIAS!

El equipo de investigación y desarrollo agradece a los responsables de auditoría interna de toda América Latina que participaron en la encuesta, las mesas redondas y las entrevistas. Sus aportes prácticos ayudaron a convertir los resultados de la encuesta en una visión más útil sobre cómo están evolucionando los riesgos en la región y cómo las funciones de auditoría interna pueden responder con mayor pertinencia, agilidad e impacto estratégico.

Fundación Latinoamericana
de Auditores Internos

EL IIA

El Instituto de Auditores Internos (IIA) es una asociación profesional internacional sin fines de lucro que presta servicio a más de 265 000 miembros en todo el mundo y ha concedido más de 200 000 certificaciones de Auditor Interno Certificado (CIA) a nivel mundial. Fundado en 1941, el IIA es reconocido en todo el mundo como el líder de la profesión de auditoría interna en normas, certificaciones, educación, investigación y orientación técnica. Para más información puede visitar: theiia.org.

Aviso legal y derechos de autor
El IIA publica este documento con fines informativos y educativos. Este material no pretende dar respuestas definitivas a circunstancias individuales específicas y, como tal, sólo pretende servir de guía. El IIA recomienda buscar asesoramiento experto independiente relacionado directamente con cualquier situación específica. El IIA no acepta ninguna responsabilidad por cualquier persona que confíe exclusivamente en este material.

Copyright © 2026 de la Fundación de Auditoría Interna. Reservados todos los derechos
Para solicitar permiso para volver a publicar, ponte en contacto con Copyright@theiia.org.

Septiembre de 2026

The Institute of
Internal Auditors

Sede central mundial | El Instituto de Auditores Internos
1035 Greenwood Blvd., Suite 401 | Lake Mary, FL 32746, EE. UU.
Teléfono: +1-407-937-1111 | Fax: +1-407-937-1101
Web: theiia.org