

# 2024

## RISK IN FOCUS

Hot topics  
for internal  
auditors

LATINOAMÉRICA

[Leer más](#)



Internal Audit  
**FOUNDATION**



**FLAI**  
Fundación Latinoamericana  
de **Auditores Internos**

# ACERCA DE RISK IN FOCUS

La serie Risk in Focus ofrece investigación práctica y basada en datos para ayudar a auditores internos y sus grupos de interés a comprender el entorno de riesgos actual y preparar planes de auditoría para el próximo año.

Los informes se basan en una encuesta mundial diseñada para identificar los riesgos actuales y emergentes para cada región, así como una serie de mesas redondas y entrevistas con la finalidad de descubrir prácticas líderes para profesionales de auditoría interna.

Se generan dos informes para cada región:

- **Hot Topics para auditores internos** – Informes detallados que recogen los resultados de la encuesta, las mesas redondas y las entrevistas.
- **Board Briefing** – Informes resumidos para que los auditores internos compartan con sus grupos de interés.

Global Risk in Focus es una alianza colaborativa facilitada por la [Internal Audit Foundation](#) con el generoso apoyo de los órganos

regionales de The IIA, Institutos de Auditores Internos y sponsors corporativos. El primer año en que el proyecto se lleva a cabo globalmente es 2024.

La metodología de Risk in Focus originalmente fue creada en 2016 por el European Institutes Research Group (EIRG), que continúa publicando este informe en Europa, a través de la European Confederation of Institutes of Internal Auditing (ECIIA).

Los informes están disponibles en forma gratuita para el público en la [Risk in Focus resource page](#) de The IIA y en los sitios web de todos los grupos regionales afiliados a The IIA: [ACIIA](#) (Asia Pacífico), [AFIIA](#) (África), [ARABCIIA](#) (Medio Oriente), [ECIIA](#) (Europa), [FLAI](#) (Latinoamérica).

## SPONSORS DEL INFORME LATINOAMÉRICA



ALIMENTAMOS UN MUNDO MEJOR

**Patrocinador  
de la traducción**

IIA–Argentina  
IIA–Bolivia  
IIA–Brasil  
IIA–Chile  
IIA–Colombia  
IIA–Costa Rica  
IIA–Dominicana  
IIA–Ecuador  
IIA–El Salvador  
IIA–Guatemala

IIA–Honduras  
IIA–México  
IIA–Nicaragua  
IIA–Panamá  
IIA–Paraguay  
IIA–Perú  
IIA–Uruguay  
IIA–Venezuela



# CONTENIDO

**4** Resumen ejecutivo:  
Construir relaciones para alcanzar el éxito juntos

---

**6** Metodología

---

**7** Resultados de encuesta: Global

---

**14** Resultados de encuesta: Latinoamérica

---

**22** Ciberseguridad:  
Aunar esfuerzos para la ciberseguridad

---

**26** Continuidad del negocio:  
Establecer conexiones para una mayor resiliencia

---

**30** Incertidumbre geopolítica:  
Planificar para cambios de amplio impacto

---



# Contenido

Resumen ejecutivo:  
Construir relaciones para  
alcanzar el éxito juntos

Metodología

Resultados de encuesta: Global

Resultados de encuesta: Latinoamérica

Ciberseguridad:  
Aunar esfuerzos para la ciberseguridad

Continuidad del negocio:  
Establecer conexiones para una  
mayor resiliencia

Incertidumbre geopolítica:  
Planificar para cambios de amplio  
impacto

## RESUMEN EJECUTIVO – LATINOAMÉRICA

### Construir relaciones para alcanzar el éxito juntos

**Los ciclos electorales y la incertidumbre política han complicado el panorama de riesgos emergentes en Latinoamérica, mientras las organizaciones intentan recuperarse de las secuelas de la pandemia. Los países de la región se esfuerzan por entablar relaciones más estrechas para reconstruir sus economías y crear o unificar regulaciones en áreas como la prevención del lavado de activos y la ciberseguridad.**

Risk in Focus Latinoamérica 2024 brinda perspectivas sobre preguntas esenciales para las organizaciones y sus consejos, a saber:

- ¿Cuáles son los principales riesgos que enfrentan las organizaciones en la región? ¿Cómo evolucionarán en los próximos tres años?
- ¿Dónde están invirtiendo los auditores internos más tiempo y esfuerzo?
- ¿Cómo pueden las funciones de auditoría interna ayudar a sus organizaciones?

La ciberseguridad, el cambio regulatorio y la continuidad del negocio son las tres áreas de mayor riesgo citadas por los Directores de Auditoría interna (DEA) de Latinoamérica

para 2024 (Figura 5). Los DEA también asignan el mayor esfuerzo de auditoría interna a las dos primeras categorías (Figura 7). El cambio climático y la disrupción digital son las dos áreas en las que se espera ver el mayor aumento en el nivel de riesgo en los próximos tres años en las organizaciones de Latinoamérica, y ambas también son señaladas como las áreas con la expectativa de un marcado incremento del esfuerzo que auditoría interna les dedica (Figuras 6 y 8).

Entre los encuestados a nivel mundial, las tres áreas de mayor riesgo identificadas fueron la ciberseguridad, el capital humano y la continuidad del negocio (Figura 1). En todas las regiones, el consenso es notable: la disrupción digital y el cambio climático son las dos áreas en las que se espera ver el mayor aumento, tanto en el nivel de riesgo como en el esfuerzo de auditoría (Figura 3).

### Participación de Latinoamérica en la investigación

- 956 respuestas de DEA y directores
- 25 países/territorios participantes
- 2 mesas redondas con 18 participantes
- 5 entrevistas en profundidad



# Contenido

Resumen ejecutivo:  
Construir relaciones para  
alcanzar el éxito juntos

---

Metodología

---

Resultados de encuesta: Global

---

Resultados de encuesta: Latinoamérica

---

Ciberseguridad:  
Aunar esfuerzos para la ciberseguridad

---

Continuidad del negocio:  
Establecer conexiones para una  
mayor resiliencia

---

Incertidumbre geopolítica:  
Planificar para cambios de amplio  
impacto

---

## RESUMEN EJECUTIVO – LATINOAMÉRICA

Los informes Risk in Focus Latinoamérica describen en detalle desafíos y soluciones para las áreas de riesgo más urgentes y se basan en la experiencia, la especialización y el conocimiento de múltiples líderes de auditoría interna de toda la región. Los temas que se destacan en los informes para la región Latinoamérica son los siguientes:

**Ciberseguridad** – Cuando faltan marcos locales de ciberseguridad, los DEA recurren a normas internacionales para impulsar la madurez cibernética de sus organizaciones.

**Continuidad del negocio** – Los planes de continuidad se utilizan no solo para hacer frente

a los riesgos emergentes, sino también para identificar nuevas oportunidades y resolver problemas inesperados.

**Incertidumbre geopolítica y fraude** – El juego de roles con distintos escenarios ha ayudado a los consejos a planificar respuestas estratégicas a cambios políticos que pueden desarrollarse a gran velocidad y a gran escala.

**Si desea ver un resumen de las conclusiones para compartir con el consejo y los grupos de interés, consulte [Risk in Focus Latinoamérica 2024 – Board Briefing](#). Para ver informes sobre otras regiones, consulte la [página de recursos Risk in Focus](#).**



# Contenido

Resumen ejecutivo:  
Construir relaciones para  
alcanzar el éxito juntos

Metodología

Resultados de encuesta: Global

Resultados de encuesta: Latinoamérica

Ciberseguridad:  
Aunar esfuerzos para la ciberseguridad

Continuidad del negocio:  
Establecer conexiones para una  
mayor resiliencia

Incertidumbre geopolítica:  
Planificar para cambios de amplio  
impacto

## METODOLOGÍA

La metodología Risk in Focus comienza con una encuesta en la que participan DEA y responsables de auditoría interna para identificar riesgos actuales y emergentes para cada región. Los principales riesgos identificados en la encuesta se abordan luego en mesas redondas de seguimiento y entrevistas con DEA, académicos y otros expertos de industria.

La encuesta presenta 16 categorías de riesgo, que se muestran a continuación. Los participantes deben elegir las 5 categorías principales que representan el mayor nivel de riesgo y las 5 categorías principales que insumen mayor tiempo y esfuerzo del equipo de auditoría interna, tanto en la actualidad como su expectativa a tres años. En los informes, se hace referencia a las categorías por sus nombres abreviados.

Para el proyecto Risk in Focus 2024 a nivel mundial, la encuesta fue respondida por 4,207 DEA y directores en 111 países/territorios, entre el 15 de febrero y 12 de julio de 2023. Asimismo, se realizaron 18 mesas redondas con 152 participantes, seguidas de 40 entrevistas en profundidad.

### Categorías de riesgo incluidas en el estudio Risk in Focus 2024

Tema de riesgo	Descripción del riesgo utilizada en la encuesta
Continuidad del negocio	Continuidad del negocio, resiliencia operativa, gestión de crisis y respuesta a desastres
Cambio climático	Cambio climático, biodiversidad y sostenibilidad ambiental
Comunicaciones/reputación	Comunicaciones, reputación y relaciones con grupos de interés
Ciberseguridad	Ciberseguridad y seguridad de datos
Disrupción digital	Disrupción digital, nuevas tecnologías e inteligencia artificial
Liquidez financiera	Riesgos financieros, de liquidez e insolvencia
Fraude	Fraude, sobornos y explotación delictiva de la disrupción
Incertidumbre geopolítica	Incertidumbre macroeconómica y geopolítica
Gobierno/informes corporativos	Gobierno organizativo e informes corporativos
Salud y seguridad	Salud y seguridad física y lógica
Capital humano	Capital humano, diversidad y gestión y retención de talento
Cambios del mercado	Cambios en el mercado/competencia y comportamiento de clientes
Fusiones y adquisiciones	Fusiones y adquisiciones
Cultura organizacional	Cultura de la organización
Cambio regulatorio	Cambios en leyes y regulaciones
Cadena de suministro y outsourcing	Cadena de suministro, outsourcing y riesgo de terceros y otras partes

111  
países/  
territorios

4,207  
respuestas de  
encuestas  
DEA

18  
mesas redondas  
152  
participantes

40  
entrevistas



## Contenido

Resumen ejecutivo:  
Construir relaciones para  
alcanzar el éxito juntos

Metodología

Resultados de encuesta: Global

Resultados de encuesta: Latinoamérica

Ciberseguridad:  
Aunar esfuerzos para la ciberseguridad

Continuidad del negocio:  
Establecer conexiones para una  
mayor resiliencia

Incertidumbre geopolítica:  
Planificar para cambios de amplio  
impacto

# RESULTADOS DE LA ENCUESTA – GLOBAL

## Comparaciones regionales

La participación mundial en la encuesta Risk in Focus ofrece una oportunidad única para comparar la planificación de riesgos y auditorías entre diferentes regiones.

### Cómo usar los resultados de la encuesta

Los resultados del estudio Risk in Focus se presentan en una serie de gráficos que muestran las respuestas a la encuesta sobre niveles de riesgo y esfuerzos de auditoría, tanto actuales como dentro de tres años. A continuación, se resumen los hallazgos clave. Se alienta a los lectores a revisar los gráficos en detalle para obtener más información.

El primer conjunto de gráficos muestra resultados generales para los encuestados de todo el mundo, en comparación con la región. El segundo conjunto de gráficos muestra resultados detallados correspondientes a la región sobre la que trata este informe.

Los porcentajes muestran cuántos eligieron un área de auditoría determinada como una de las cinco principales para el nivel de riesgo o el esfuerzo de auditoría en sus organizaciones. En los gráficos, los resultados para los niveles de riesgo se muestran en color azul, mientras que los resultados para el esfuerzo de auditoría se muestran en color verde. Los niveles actuales se presentan en tonos más oscuros y los niveles futuros en tonos más claros.

### Figura 1: Los 5 riesgos principales por región – Global

Existe un amplio consenso en todo el mundo de que las tres áreas de mayor riesgo para las organizaciones donde trabajan los DEA son:

1. Ciberseguridad
2. Capital humano
3. Continuidad del negocio

Para la mayoría de las regiones, el cambio regulatorio también se ubica como uno de los 5 principales riesgos, con la excepción de África y Medio Oriente, donde la liquidez financiera tiene más prioridad. Como reflejo de los acontecimientos actuales y las preocupaciones futuras, la inestabilidad geopolítica encabezó la lista para Latinoamérica y Europa. Los cambios del mercado se consideraron un riesgo importante en Asia Pacífico y Norteamérica, pero no en otras regiones.

### Encuesta Global – Respuestas por región

África	808
Asia Pacífico	1,035
Latinoamérica & Caribe	956
Europa	799
Norteamérica	442
Medio Oriente	167
<b>Total</b>	<b>4,207</b>



## Contenido

Resumen ejecutivo:  
Construir relaciones para  
alcanzar el éxito juntos

Metodología

Resultados de encuesta: Global

Resultados de encuesta: Latinoamérica

Ciberseguridad:  
Aunar esfuerzos para la ciberseguridad

Continuidad del negocio:  
Establecer conexiones para una  
mayor resiliencia

Incertidumbre geopolítica:  
Planificar para cambios de amplio  
impacto

# RESULTADOS DE LA ENCUESTA – GLOBAL

Finalmente, África fue la única región que señaló el fraude como una de las 5 preocupaciones principales, mientras que Medio Oriente fue la única región que clasificó la gobernanza/los informes corporativos entre las 5 preocupaciones principales.

Otra forma de ver los datos es considerar qué región exhibió el mayor riesgo dentro de cada área de auditoría. Por ejemplo, los riesgos de cambio climático se calificaron como los más altos en Europa, en comparación con otras regiones. Algunos puntos notables sobre las calificaciones más altas por área de auditoría incluyen:

- Los encuestados norteamericanos dieron a la ciberseguridad (85%) y al capital humano (65%) las calificaciones de riesgo más altas en comparación con otras regiones.
- Para Europa, mientras que la ciberseguridad se ubicó casi tan alto como para Norteamérica (84%), otras áreas de gran preocupación fueron la incertidumbre geopolítica (43%) y el cambio climático (31%). Europa fue la única región donde el cambio climático fue superior al 30%.
- Latinoamérica compartió la preocupación de Europa por la incertidumbre geopolítica (42%), pero también registró una alta calificación para el riesgo de cambios regulatorios (48%) y disrupción digital (38%).

- Asia Pacífico mostró particular inquietud por la continuidad del negocio (61%) y el cambio del mercado (47%), en comparación con otras regiones.
- Medio Oriente registró niveles de riesgo mucho más altos para la gobernanza/informes corporativos (45%) que otras regiones y también asignó una calificación ligeramente mayor a comunicaciones/reputación (28%).
- Finalmente, África presentó una combinación única de riesgos que eran más altos que otras regiones, que incluyen la liquidez financiera (47%), el fraude (46%) y la cultura organizacional (34%).

### Figura 2: Los 5 esfuerzos de auditoría principales por región – Global

Aunque los niveles de riesgo pueden variar de una región a otra, las áreas de mayor esfuerzo para la auditoría interna son notablemente similares, generalmente en este orden:

1. Ciberseguridad
2. Gobierno/informes corporativos
3. Comunidad de negocio
4. Cambios regulatorios
5. Liquidez financiera
6. Fraude

Si bien los niveles de riesgo pueden variar de una región a otra, las áreas de mayor esfuerzo para la auditoría interna presentan similitudes notables.

La principal área de diferencia fue el cambio regulatorio, donde los porcentajes de esfuerzo de auditoría fueron notablemente más bajos para África (35%) y Medio Oriente (35%) que para otras regiones, que fueron del 50% o más.

Otras diferencias específicas fueron:

- Asia Pacífico asignó un porcentaje menor a la liquidez financiera (35%) que el promedio mundial (45%).
- Latinoamérica registró un porcentaje menor que otras regiones al esfuerzo invertido en gobierno/informes corporativos (46% para Latinoamérica frente a 55% del promedio mundial).
- Norteamérica dio una calificación muy inferior al promedio mundial al esfuerzo en materia de fraude (26% para Norteamérica frente al 42% del promedio mundial).



# Contenido

Resumen ejecutivo:  
Construir relaciones para  
alcanzar el éxito juntos

---

Metodología

---

Resultados de encuesta: Global

---

Resultados de encuesta: Latinoamérica

---

Ciberseguridad:  
Aunar esfuerzos para la ciberseguridad

---

Continuidad del negocio:  
Establecer conexiones para una  
mayor resiliencia

---

Incertidumbre geopolítica:  
Planificar para cambios de amplio  
impacto

---

## RESULTADOS DE LA ENCUESTA – GLOBAL

Otra forma de ver los datos es considerar qué región reflejó el mayor esfuerzo de auditoría dentro de cada área de auditoría. En muchas áreas de auditoría, la diferencia de esfuerzo entre regiones es pequeña. Pero hubo algunas áreas de auditoría donde las diferencias fueron notables:

- En Norteamérica, la auditoría estuvo mucho más enfocada en ciberseguridad (84%) que otras regiones, con la excepción de Europa (79%).
- En África, los 5 principales esfuerzos estuvieron más dirigidos hacia el fraude (57%) y la liquidez financiera (53%), en comparación con las demás regiones.
- En Europa, se registró un porcentaje para el cambio climático como uno de los 5 principales esfuerzos de auditoría (19%) que es casi el doble del promedio mundial (11%).

### Figura 3: Cambio esperado en el nivel de riesgo en 3 años – Global

Existe un consenso en todo el mundo de que los niveles de riesgo aumentarán en los próximos tres años en las áreas de disrupción digital y cambio climático. Ambas áreas experimentaron aumentos de alrededor de 20 puntos porcentuales entre los niveles de riesgo actuales y los esperados para el futuro. Aún más notable es el aumento en el ranking para el cambio climático, que sube del decimocuarto al quinto puesto en cuanto a expectativa de nivel de riesgo.

### Figura 4: Cambio esperado en el esfuerzo de auditoría en 3 años – Global

Dado que se espera que aumenten los niveles de riesgo para la disrupción digital y el cambio climático, también se espera un incremento en la cantidad de tiempo y esfuerzo que la auditoría interna invertirá en estas áreas. El porcentaje de directores de auditoría que espera que la disrupción digital esté entre las 5 principales áreas de esfuerzo de auditoría creció a más del doble: del 22% al 52%. Asimismo, se aprecia un dato notable el porcentaje que considera que el cambio climático será una de las 5 principales áreas de esfuerzo, que se triplicó: del 11% al 34%.

Hay consenso a nivel mundial de que los niveles de riesgo aumentarán en los próximos tres años en las áreas de disrupción digital y cambio climático.



## Contenido

Resumen ejecutivo:  
Construir relaciones para  
alcanzar el éxito juntos

Metodología

Resultados de encuesta: Global

Resultados de encuesta: Latinoamérica

Ciberseguridad:  
Aunar esfuerzos para la ciberseguridad

Continuidad del negocio:  
Establecer conexiones para una  
mayor resiliencia

Incertidumbre geopolítica:  
Planificar para cambios de amplio  
impacto

Figura 1:

# Los 5 riesgos principales por región

Riesgos  
más altos  
por región

■ Existe un amplio consenso en todo el mundo de que las tres áreas de mayor riesgo son ciberseguridad, capital humano y continuidad del negocio.

¿Cuáles son los 5 riesgos principales que su organización enfrenta actualmente?

Área de Auditoría	Promedio total regiones	Asia Pacífico	Latinoamérica	África	Norteamérica	Medio oriente	Europa
Ciberseguridad	<b>73%</b>	<b>66%</b>	<b>75%</b>	<b>58%</b>	<b>85%</b>	<b>70%</b>	<b>84%</b>
Capital Humano	<b>51%</b>	<b>59%</b>	<b>44%</b>	<b>39%</b>	<b>65%</b>	<b>47%</b>	<b>50%</b>
Continuidad de engocio	<b>47%</b>	<b>61%</b>	<b>47%</b>	<b>52%</b>	<b>36%</b>	<b>53%</b>	<b>35%</b>
Cambio regulatorio	<b>39%</b>	<b>35%</b>	<b>48%</b>	<b>32%</b>	<b>43%</b>	<b>33%</b>	<b>43%</b>
Disrupción digital	<b>34%</b>	30%	38%	33%	36%	32%	33%
Liquidez financiera	<b>32%</b>	21%	33%	<b>47%</b>	28%	<b>38%</b>	26%
Cambios del mercado	<b>32%</b>	<b>47%</b>	26%	21%	<b>41%</b>	26%	30%
Incertidumbre geopolítica	<b>30%</b>	28%	<b>42%</b>	25%	28%	16%	<b>43%</b>
Gobierno/ informes corporativos	<b>27%</b>	24%	18%	36%	16%	<b>45%</b>	22%
Cadena de suministro y outsourcing	<b>26%</b>	27%	16%	19%	36%	28%	30%
Cultura organizacional	<b>26%</b>	23%	26%	34%	21%	30%	20%
Fraude	<b>24%</b>	22%	30%	<b>46%</b>	9%	26%	13%
Comunicaciones/reputación	<b>21%</b>	18%	22%	27%	21%	28%	12%
Cambio climático	<b>19%</b>	22%	22%	19%	12%	10%	31%
Salud y seguridad	<b>11%</b>	12%	8%	10%	17%	9%	13%
Fusiones y adquisiciones	<b>6%</b>	4%	3%	3%	8%	10%	8%

Nota: La Encuesta Global de Risk in Focus del IIA, n=4,207. Porcentajes indican quienes seleccionaron el área como una de las principales 5 en nivel de riesgo. Azul oscuro sombreado indica las 5 áreas de mayor riesgo para esa región.



# Contenido

Resumen ejecutivo:  
Construir relaciones para  
alcanzar el éxito juntos

Metodología

Resultados de encuesta: Global

Resultados de encuesta: Latinoamérica

Ciberseguridad:  
Aunar esfuerzos para la ciberseguridad

Continuidad del negocio:  
Establecer conexiones para una  
mayor resiliencia

Incertidumbre geopolítica:  
Planificar para cambios de amplio  
impacto

## Figura 2: Los 5 áreas de mayor tiempo de auditoría

Áreas de  
mayor tiempo  
por región

Las áreas de mayor tiempo para la auditoría interna son notablemente similares

¿Cuáles son los 5 riesgos principales a los que la auditoría interna dedica más tiempo y esfuerzo?

Área de Auditoría	Promedio total regiones	Asia Pacífico	Latinoamérica	África	Norteamérica	Medio oriente	Europa
Ciberseguridad	<b>68%</b>	<b>66%</b>	<b>66%</b>	<b>54%</b>	<b>84%</b>	<b>61%</b>	<b>79%</b>
Gobierno/ informes corporativos	<b>55%</b>	<b>54%</b>	46%	<b>52%</b>	<b>55%</b>	<b>64%</b>	<b>61%</b>
Continuidad de engocio	<b>54%</b>	<b>59%</b>	<b>53%</b>	<b>56%</b>	<b>53%</b>	<b>53%</b>	<b>50%</b>
Cambio regulatorio	<b>46%</b>	<b>56%</b>	<b>50%</b>	35%	<b>53%</b>	35%	<b>50%</b>
Liquidez financiera	<b>45%</b>	35%	<b>50%</b>	<b>53%</b>	<b>46%</b>	<b>44%</b>	<b>45%</b>
Fraude	<b>42%</b>	<b>42%</b>	<b>47%</b>	<b>57%</b>	26%	<b>43%</b>	36%
Cadena de suministro y outsourcing	<b>34%</b>	33%	28%	32%	38%	39%	36%
Capital humano	<b>30%</b>	33%	28%	33%	26%	35%	26%
Cultura organizacional	<b>24%</b>	23%	29%	27%	17%	27%	21%
Disrupción digital	<b>22%</b>	19%	24%	24%	25%	20%	21%
Comunicaciones/reputación	<b>20%</b>	21%	23%	25%	20%	23%	11%
Salud y seguridad	<b>17%</b>	18%	12%	13%	21%	16%	19%
Cambios del mercado	<b>16%</b>	23%	17%	15%	14%	16%	10%
Cambio climático	<b>11%</b>	10%	8%	11%	9%	7%	19%
Incertidumbre geopolítica	<b>9%</b>	6%	13%	12%	4%	8%	8%
Fusiones y adquisiciones	<b>6%</b>	3%	5%	2%	10%	8%	9%

Nota: La Encuesta Global de Risk in Focus del IIA, n=4,207. Porcentajes indican quienes seleccionaron el área como una de las principales 5 en nivel de riesgo. Verde oscuro sombreado indica las 5 áreas de mayor esfuerzo de auditoría para esa región.



# Contenido

Resumen ejecutivo:  
Construir relaciones para  
alcanzar el éxito juntos

Metodología

Resultados de encuesta: Global

Resultados de encuesta: Latinoamérica

Ciberseguridad:  
Aunar esfuerzos para la ciberseguridad

Continuidad del negocio:  
Establecer conexiones para una  
mayor resiliencia

Incertidumbre geopolítica:  
Planificar para cambios de amplio  
impacto

Cambio  
esperado en  
el riesgo

Figura 3:

## Figura 3: Cambio esperado en el riesgo en 3 años - Global

- El riesgo de cambio climático aumenta dramáticamente al quinto lugar, desde el decimocuarto lugar.
- Disrupción digital se espera que incremente del 34% al 55% para quienes lo ven como uno de los 5 riesgos principales.

¿Cuáles son los 5 riesgos principales que su organización enfrenta actualmente?

¿Cuáles son los 5 riesgos principales que su organización enfrentará en 3 años?

1. Ciberseguridad	73%	1. Ciberseguridad	67%
2. Capital humano	51%	2. <b>Disrupción digital</b>	55%
3. Continuidad del negocio	47%	3. Capital humano	46%
4. Cambio regulatorio	39%	4. Continuidad del negocio	41%
5. <b>Disrupción digital</b>	34%	5. <b>Cambio climático</b>	39%
6. Liquidez financiera	32%	6. Cambio regulatorio	39%
7. Cambios del mercado	32%	7. Incertidumbre geopolítica	34%
8. Incertidumbre geopolítica	30%	8. Cambios del mercado	33%
9. Gobierno/informes corporativos	27%	9. Cadena de suministro y outsourcing	25%
10. Cadena de suministro y outsourcing	26%	10. Liquidez financiera	23%
11. Cultural organizacional	26%	11. Cultural organizacional	21%
12. Fraude	24%	12. Gobierno/informes corporativos	20%
13. Comunicaciones/reputación	21%	13. Fraude	20%
14. <b>Cambio climático</b>	19%	14. Comunicaciones/reputación	15%
15. Salud y seguridad	11%	15. Salud y seguridad	11%
16. Fusiones y adquisiciones	6%	16. Fusiones y adquisiciones	11%

Nota: La Encuesta Global de Risk in Focus del IIA, n=4,207. Porcentajes quienes seleccionaron el área como una de las principales 5 a nivel de riesgo en su organización.



# Contenido

Resumen ejecutivo:  
Construir relaciones para  
alcanzar el éxito juntos

Metodología

Resultados de encuesta: Global

Resultados de encuesta: Latinoamérica

Ciberseguridad:  
Aunar esfuerzos para la ciberseguridad

Continuidad del negocio:  
Establecer conexiones para una  
mayor resiliencia

Incertidumbre geopolítica:  
Planificar para cambios de amplio  
impacto

Cambio  
esperado en  
el tiempo

## Figura 4: Cambio de tiempo de auditoría esperado en 3 años - Global

Se espera un aumento pronunciado para la actividad de auditoría interna relacionada a disrupción digital y cambio climático.

¿Cuáles son los 5 riesgos a los que la auditoría interna dedica más tiempo y esfuerzo?

¿Cuáles son los 5 riesgos a los que piensa que la auditoría interna dedicará más tiempo y esfuerzo en 3 años?

1. Ciberseguridad	68%	1. Ciberseguridad	73%
2. Gobierno/informes corporativos	55%	2. <b>Disrupción digital</b>	<b>52%</b>
3. Continuidad del negocio	54%	3. Continuidad del negocio	49%
4. Cambio regulatorio	46%	4. Cambio regulatorio	37%
5. Liquidez financiera	45%	5. Gobierno/informes corporativos	36%
6. Fraude	42%	6. Capital humano	35%
7. Cadena de suministro/outsourcing	34%	7. <b>Cambio climático</b>	<b>34%</b>
8. Capital humano	30%	8. Fraude	29%
9. Cultura organizacional	24%	9. Liquidez financiera	28%
10. <b>Disrupción digital</b>	<b>22%</b>	10. Cadena de suministro y outsourcing	28%
11. Comunicaciones/reputación	20%	11. Cultural organizacional	24%
12. Salud y seguridad	17%	12. Cambios del mercado	22%
13. Cambios del mercado	16%	13. Comunicaciones/reputación	16%
14. <b>Cambio climático</b>	<b>11%</b>	14. Incertidumbre política	16%
15. Incertidumbre geopolítica	9%	15. Salud y seguridad	15%
16. Fusiones y adquisiciones	6%	16. Fusiones y adquisiciones	8%

Nota: La Encuesta Global de Risk in Focus del IIA, n=4,207. Porcentaje quienes seleccionaron el área como una de las mayores 5 en esfuerzo y tiempo.



# Contenido

Resumen ejecutivo:  
Construir relaciones para  
alcanzar el éxito juntos

Metodología

Resultados de encuesta: Global

Resultados de encuesta: Latinoamérica

Ciberseguridad:  
Aunar esfuerzos para la ciberseguridad

Continuidad del negocio:  
Establecer conexiones para una  
mayor resiliencia

Incertidumbre geopolítica:  
Planificar para cambios de amplio  
impacto

# RESULTADOS DE ENCUESTA – LATINOAMÉRICA

## Cómo interpretar los resultados de la encuesta

A continuación, se resumen los hallazgos clave para Latinoamérica. Se alienta a los lectores a revisar los gráficos detallados que figuran en las páginas siguientes para obtener más información.

Los porcentajes muestran cuántos encuestados eligieron un área de auditoría determinada como una de las cinco principales para el nivel de riesgo en su organización. Los resultados de los niveles de riesgo se presentan en color azul y los resultados relativos al esfuerzo de auditoría se presentan verdes. Los niveles actuales se muestran en tonos más oscuros y los niveles futuros, en tonos más claros

## Respuestas a la encuesta por país – Latinoamérica y Caribe

A los fines de este estudio, los países y la mayoría de los territorios del Caribe se incluyen dentro de la región Latinoamérica.

**Figura 5: Niveles de riesgo actuales versus niveles de riesgo futuros**

- La ciberseguridad se destaca por encabezar el listado del panorama de riesgos para Latinoamérica en 2024.
- En los próximos 3 años, la disrupción digital y el cambio climático son los riesgos con mayores expectativas de incrementarse.

**Figura 6: Cambio esperado en el panorama de riesgos a 3 años**

- Se espera que la disrupción digital pase al segundo lugar: el 56% de los encuestados señala que este riesgo será uno de los 5 principales.

- Los riesgos relacionados con el clima pasan a la quinta posición: el 41% de los encuestados señala que este riesgo será uno de los 5 principales.

**Figura 7: Esfuerzo de auditoría actual versus esfuerzo de auditoría futuro**

- Los DEA latinoamericanos fueron los más propensos a elegir la ciberseguridad como una de sus 5 principales áreas para el esfuerzo de auditoría interna (66%).
- Una amplia variedad de áreas siguió de cerca a la ciberseguridad en cuanto a la expectativa de esfuerzo de auditoría interna, incluida la continuidad del negocio, la liquidez financiera y el cambio regulatorio.

México	140	República Dominicana	27
Colombia	121	Uruguay	27
Argentina	78	El Salvador	25
Brasil	69	Paraguay	21
Venezuela	67	Trinidad y Tobago	15
Costa Rica	59	Honduras	13
Nicaragua	54	Barbados	3
Ecuador	52	Jamaica	3
Bolivia	43	Aruba	1
Guatemala	38	Bahamas	1
Chile	35	Islas Caimán	1
Panamá	31	Saint Kitts and Nevis	1
Perú	31	<b>TOTAL</b>	<b>956</b>

Note: For reporting purposes, countries and territories in the Caribbean are included with Latin America.



# Contenido

Resumen ejecutivo:  
Construir relaciones para  
alcanzar el éxito juntos

Metodología

Resultados de encuesta: Global

Resultados de encuesta: Latinoamérica

Ciberseguridad:  
Aunar esfuerzos para la ciberseguridad

Continuidad del negocio:  
Establecer conexiones para una  
mayor resiliencia

Incertidumbre geopolítica:  
Planificar para cambios de amplio  
impacto

## RESULTADOS DE ENCUESTA – LATINOAMÉRICA

**Figura 8: Cambio esperado en el tiempo de auditoría en 3 años**

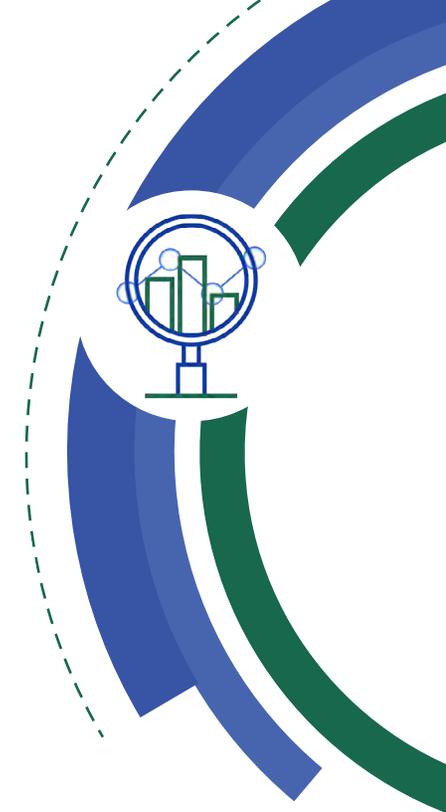
- Se esperan marcados aumentos en la actividad para hacer frente a la disrupción digital y el cambio climático.
- Los aumentos se compensan con reducciones en la expectativa en cuanto a liquidez financiera, cambios regulatorios y fraude.

**Figura 9: Nivel de riesgo actual versus tiempo de auditoría actual**

- El esfuerzo es relativamente alto en comparación con el nivel de riesgo percibido para gobierno/informes corporativos, fraude y liquidez financiera.
- El esfuerzo es relativamente bajo en comparación con el nivel de riesgo percibido para incertidumbre geopolítica, capital humano, disrupción digital y cambio climático, pero el esfuerzo de auditoría para abordarlos puede tener interconexiones con otras áreas.

**Figura 10: Nivel de riesgo futuros versus tiempo de auditoría futuro**

- En 3 años, los DEA esperan que la brecha entre los riesgos clave y el esfuerzo de auditoría interna se reduzca en la mayoría de las áreas. Pero el esfuerzo seguirá siendo relativamente bajo en comparación con el riesgo de incertidumbre geopolítica y capital humano.
- Se espera que la ciberseguridad y la disrupción digital compartan los puestos más altos, tanto para el riesgo como para el esfuerzo de auditoría.



# Contenido

Resumen ejecutivo:  
Construir relaciones para  
alcanzar el éxito juntos

Metodología

Resultados de encuesta: Global

Resultados de encuesta: Latinoamérica

Ciberseguridad:  
Aunar esfuerzos para la ciberseguridad

Continuidad del negocio:  
Establecer conexiones para una  
mayor resiliencia

Incertidumbre geopolítica:  
Planificar para cambios de amplio  
impacto

Figura 5:

## Nivel de riesgo actual versus nivel de riesgo futuro - Latinoamérica



- La ciberseguridad se destaca por encabezar el listado del panorama de riesgos para Latinoamérica en 2024.
- En los próximos 3 años, la disrupción digital y el cambio climático son los riesgos con mayores expectativas de incrementarse.

¿Cuáles son los 5 riesgos principales que su organización enfrenta actualmente?



¿Cuáles son los 5 riesgos principales que su organización enfrentará en 3 años?



# Contenido

Resumen ejecutivo:  
Construir relaciones para  
alcanzar el éxito juntos

Metodología

Resultados de encuesta: Global

Resultados de encuesta: Latinoamérica

Ciberseguridad:  
Aunar esfuerzos para la ciberseguridad

Continuidad del negocio:  
Establecer conexiones para una  
mayor resiliencia

Incertidumbre geopolítica:  
Planificar para cambios de amplio  
impacto

Figura 6:

## Cambio esperado en el riesgo en 3 años - Latinoamérica

Cambio  
esperado  
en riesgos

- Se espera que la **disrupción digital** pase al segundo lugar: el 56% de los encuestados señala que este riesgo será uno de los 5 principales.
- Los riesgos relacionados con el clima pasan a la quinta posición: el 41% de los encuestados señala que este riesgo será uno de los 5 principales.

¿Cuáles son los 5 riesgos principales que su organización enfrenta actualmente?

¿Cuáles son los 5 riesgos principales que su organización enfrentará en 3 años?

1. Ciberseguridad	75%	1. Ciberseguridad	69%
2. Cambio regulatorio	48%	2. <b>Disrupción digital</b>	<b>56%</b>
3. Continuidad del negocio	47%	3. Capital humano	43%
4. Capital humano	44%	4. Continuidad del negocio	43%
5. Incertidumbre geopolítica	42%	5. <b>Cambio climático</b>	<b>41%</b>
6. <b>Disrupción digital</b>	<b>38%</b>	6. Cambio regulatorio	40%
7. Liquidez financiera	33%	7. Incertidumbre geopolítica	40%
8. Fraude	30%	8. Cambios del mercado	28%
9. Cultura organizacional	26%	9. Fraude	27%
10. Cambios del mercado	26%	10. Liquidez financiera	25%
11. Comunicaciones/reputación	22%	11. Cultura organizacional	21%
12. <b>Cambio climático</b>	<b>22%</b>	12. Gobierno/informes corporativos	17%
13. Gobierno/informes corporativos	18%	13. Comunicaciones/reputación	15%
14. Cadena de suministro y outsourcing	16%	14. Cadena de suministro y outsourcing	15%
15. Salud y seguridad	8%	15. Salud y seguridad	11%
16. Fusiones y adquisiciones	3%	16. Fusiones y adquisiciones	9%



# Contenido

Resumen ejecutivo:  
Construir relaciones para  
alcanzar el éxito juntos

Metodología

Resultados de encuesta: Global

Resultados de encuesta: Latinoamérica

Ciberseguridad:  
Aunar esfuerzos para la ciberseguridad

Continuidad del negocio:  
Establecer conexiones para una  
mayor resiliencia

Incertidumbre geopolítica:  
Planificar para cambios de amplio  
impacto

Figura 7:

## Tiempo de auditoría actual versus tiempo de auditoría futuro - Latinoamérica



- Los DEA latinoamericanos fueron los más propensos a elegir la ciberseguridad como una de sus 5 principales áreas para el esfuerzo de auditoría interna (66%).
- Una amplia variedad de áreas siguió de cerca a la ciberseguridad en cuanto a la expectativa de esfuerzo de auditoría interna, incluida la continuidad del negocio, la liquidez financiera y el cambio regulatorio.

¿Cuáles son los 5 riesgos a los que la auditoría dedica más tiempo y esfuerzo?

¿Cuáles son los 5 riesgos a los que piensa que la auditoría interna dedicará más tiempo y esfuerzo en 3 años?



Nota: La Encuesta Global de Risk in Focus del IIA, Latinoamérica n=956. Porcentaje quienes seleccionaron el área como una de las 5 principales en esfuerzo y tiempo.



# Contenido

Resumen ejecutivo:  
Construir relaciones para  
alcanzar el éxito juntos

Metodología

Resultados de encuesta: Global

Resultados de encuesta: Latinoamérica

Ciberseguridad:  
Aunar esfuerzos para la ciberseguridad

Continuidad del negocio:  
Establecer conexiones para una  
mayor resiliencia

Incertidumbre geopolítica:  
Planificar para cambios de amplio  
impacto

Figura 8:

## Cambio en tiempo de auditoría esperado en 3 años - Latinoamérica

Cambio  
esperado en  
el tiempo

- Se esperan aumentos en la actividad para hacer frente a la disrupción digital y el cambio climático.
- Los aumentos se compensan con reducciones en la expectativa en cuanto a liquidez financiera, cambios regulatorios y fraude.

¿Cuáles son los 5 riesgos a los que la auditoría interna dedica más tiempo y esfuerzo actualmente?

¿Cuáles son los 5 riesgos a los que piensa que la auditoría interna dedicará más tiempo y esfuerzo en 3 años?

1. Ciberseguridad	66%	1. Ciberseguridad	73%
2. Continuidad del negocio	53%	2. <b>Disrupción digital</b>	<b>59%</b>
3. Liquidez financiera	50%	3. Continuidad del negocio	51%
4. Cambio regulatorio	50%	4. Cambio regulatorio	36%
5. Fraude	47%	5. Fraude	34%
6. Gobierno/informes corporativos	46%	6. <b>Cambio climático</b>	<b>33%</b>
7. Cultura organizacional	29%	7. Capital humano	33%
8. Cadena de suministro y outsourcing	28%	8. Liquidez financiera	32%
9. Capital humano	28%	9. Cultura organizacional	29%
10. <b>Disrupción digital</b>	<b>24%</b>	10. Gobierno/informes corporativos	24%
11. Comunicaciones/reputación	23%	11. Incertidumbre geopolítica	23%
12. Cambios del mercado	17%	12. Cambios del mercado	22%
13. Incertidumbre geopolítica	13%	13. Comunicaciones/reputación	18%
14. Salud y seguridad	12%	14. Cadena de suministro y outsourcing	18%
15. <b>Cambio climático</b>	<b>8%</b>	15. Salud y seguridad	12%
16. Fusiones y adquisiciones	5%	16. Fusiones y adquisiciones	6%



# Contenido

Resumen ejecutivo:  
Construir relaciones para  
alcanzar el éxito juntos

Metodología

Resultados de encuesta: Global

Resultados de encuesta: Latinoamérica

Ciberseguridad:  
Aunar esfuerzos para la ciberseguridad

Continuidad del negocio:  
Establecer conexiones para una  
mayor resiliencia

Incertidumbre geopolítica:  
Planificar para cambios de amplio  
impacto

Figura 9:

## Nivel de riesgo actual versus nivel de esfuerzo de auditoría actual - Latinoamérica



- El esfuerzo es relativamente alto en comparación con el nivel de riesgo percibido para gobierno/informes corporativos, fraude y liquidez financiera.
- El esfuerzo es relativamente bajo en comparación con el nivel de riesgo percibido para incertidumbre geopolítica, capital humano, disrupción digital y cambio climático, pero el esfuerzo de auditoría para abordarlos puede tener interconexiones con otras áreas.

¿Cuáles son los 5 riesgos principales que su organización enfrenta actualmente?

¿Cuáles son los 5 riesgos a los que la auditoría interna dedica más tiempo y esfuerzo?



Nota: La Encuesta Global de Risk in Focus del IIA, Latinoamérica n=956. Porcentaje quienes seleccionaron el área como una de las 5 principales en riesgo o esfuerzo de auditoría interna.

# Contenido

Resumen ejecutivo:  
Construir relaciones para  
alcanzar el éxito juntos

Metodología

Resultados de encuesta: Global

Resultados de encuesta: Latinoamérica

Ciberseguridad:  
Aunar esfuerzos para la ciberseguridad

Continuidad del negocio:  
Establecer conexiones para una  
mayor resiliencia

Incertidumbre geopolítica:  
Planificar para cambios de amplio  
impacto

Figura 10:

## Nivel de riesgo futuro versus esfuerzo de auditoría futuro - Latinoamérica



- En 3 años, los DEA esperan que la brecha entre los riesgos clave y el esfuerzo de auditoría interna se reduzca en la mayoría de las áreas.
- Se espera que la ciberseguridad y la disrupción digital compartan los puestos más altos en costos tanto para el riesgo como para el esfuerzo de auditoría.

¿Cuáles son los 5 riesgos principales que su organización enfrentará en 3 años?

¿Cuáles son los 5 riesgos principales que piensa que su organización enfrentará en 3 años?



Nota: La Encuesta Global de Risk in Focus del IIA, Latinoamérica n=956. Porcentaje quienes seleccionaron el área como una de las 5 principales en riesgo o esfuerzo de auditoría interna.



## Contenido

Resumen ejecutivo:  
Construir relaciones para  
alcanzar el éxito juntos

Metodología

Resultados de encuesta: Global

Resultados de encuesta: Latinoamérica

Ciberseguridad:  
Aunar esfuerzos para la ciberseguridad

Continuidad del negocio:  
Establecer conexiones para una  
mayor resiliencia

Incertidumbre geopolítica:  
Planificar para cambios de amplio  
impacto

# CIBERSEGURIDAD

## Aunar esfuerzos para la ciberseguridad

**Ante los actuales niveles relativamente bajos de regulaciones en ciberseguridad y seguridad de datos, para generar resiliencia, los DEA están recurriendo a crear relaciones dentro del negocio y con otras organizaciones en la región.**

Los servicios de nube han experimentado un auge en Latinoamérica en los últimos años, con el impulso de la pandemia. Según un estudio de investigación, entre 2019 y 2023, se produjo un crecimiento compuesto del uso de servicios de nube del 22.4%. Los DEA que participaron en la serie de mesas redondas manifestaron que muchas veces las organizaciones implementan nuevos servicios en la nube a un ritmo que no espera que se pongan en marcha los controles necesarios y la capacitación adecuada. Además, algunos transmitieron la inquietud de que las empresas no pueden realizar una diligencia debida exhaustiva en algunos servicios de terceros, o insistieron en la necesidad de cláusulas de derecho a auditoría, frente a la capacidad de las empresas poderosas para negarse.

## El atraso en materia regulatoria obstaculiza la respuesta al riesgo

Los ataques de hackers se han vuelto moneda corriente en la región, debido a las vulnerabilidades que a menudo se introducen en las conexiones con terceros. Según IBM, el país en el que más respondió a casos de hacking en 2023 fue Brasil, seguido de lejos por Colombia y México. Las industrias que prefieren los hackers son las de comercio minorista y mayorista, finanzas y seguros, y energía.<sup>2</sup>

Resultados  
de encuesta–  
Ciberseguridad

1. – NIVEL DE RIESGO

75%  
lo clasificó  
entre los 5  
principales  
en nivel de riesgo

1. – ESFUERZO DE AUDITORÍA

66%  
lo clasificó  
entre los 5  
principales  
en esfuerzo de  
auditoría

<sup>1</sup> Para obtener más información sobre la actividad global de computación en la nube, consulte <https://aag-it.com/the-latest-cloud-computing-statistics/>

<sup>2</sup> Para obtener más información sobre las amenazas mundiales, consulte IBM Security X-Force Threat Intelligence Index 2023 en <https://www.ibm.com/reports/threat-intelligence>



# Contenido

Resumen ejecutivo:  
Construir relaciones para  
alcanzar el éxito juntos

Metodología

Resultados de encuesta: Global

Resultados de encuesta: Latinoamérica

Ciberseguridad:  
Aunar esfuerzos para la ciberseguridad

Continuidad del negocio:  
Establecer conexiones para una  
mayor resiliencia

Incertidumbre geopolítica:  
Planificar para cambios de amplio  
impacto

## CIBERSEGURIDAD

El DEA en un banco boliviano manifestó que la falta de regulaciones específicas en ciberseguridad obstaculiza la defensa efectiva en toda la región. Las regulaciones de ciberseguridad exigirían procedimientos y procesos mínimos de seguridad cibernética y vendrían con marcos de control recomendados, mejores prácticas de gobierno y, a veces, sanciones por incumplimiento. Las regulaciones gubernamentales también podrían establecer un sistema para alertar a las organizaciones sobre nuevas amenazas cibernéticas. Sin un sistema de este tipo, señaló el ejecutivo, las organizaciones a menudo no tienen relaciones efectivas para el intercambio de información. “Como no compartimos información sobre ataques de ciberseguridad, estamos ciegos”, expresó.

Los DEA coincidieron en que no pueden esperar a que se establezcan regulaciones, especialmente en áreas en rápida evolución como la IA (inteligencia artificial). Como resultado, las organizaciones están utilizando marcos reconocidos internacionalmente, como el que ofrece el NIST de EE. UU., para combatir esta amenaza. El DEA de una empresa de servicios financieros en Panamá fue claro sobre su experiencia con el uso de las normas NIST: “Nuestro análisis mostró dónde nos encontramos en el nivel de madurez en comparación

con otras empresas, nos permitió definir qué pasos debíamos adoptar para cerrar las brechas y nos proporcionó una hoja de ruta para llegar al estado deseado”.

### Las relaciones fortalecen las defensas

Las funciones de auditoría interna están invirtiendo en impulsar el conocimiento y mantenerse al día en tecnologías disruptivas, como la Inteligencia Artificial (AI), donde la organización puede estar ansiosa por implementar software. “Decidimos bloquear Open AI”, comentó Pamela Vago, DEA en Genneia, una compañía de energía en Argentina. “Es parte de la ética de nuestra empresa capacitar a las personas antes de permitir el uso de estas tecnologías, para asegurar que entiendan qué información de la compañía pueden utilizar y qué información no pueden divulgar”.

La ejecutiva mencionó que es clave para los DEA construir relaciones con las líneas de negocios que están introduciendo nuevas tecnologías para que la auditoría interna pueda dar asesoramiento estratégico sobre riesgos y controles antes de la implementación. Estar en estrecho

contacto con la gerencia de primera línea también puede contribuir a identificar posibles puntos débiles. “Asignamos nuestros esfuerzos de investigación adonde el riesgo es más alto, y si vemos que el riesgo no se está gestionando en algún lugar de la empresa, debemos llevarlo a los líderes y garantizar que se establezca un plan de acción para mitigarlo”, señaló.

Ese enfoque puede ser difícil cuando las empresas operan en varios países, sea en Sudamérica o en otras regiones. La madurez cibernética es a menudo desigual, y enfrenta obstáculos en países con menos recursos. El DEA de un banco boliviano comentó que había creado un programa de auditoría interna corporativa para estandarizar el conocimiento en las diferentes regiones del negocio. “Compartimos experiencias entre todos los auditores de la corporación”, señaló. “También hemos creado comités de especialistas para compartir los problemas que identificamos en todos los países en los que operamos.”



# Contenido

Resumen ejecutivo:  
Construir relaciones para  
alcanzar el éxito juntos

---

Metodología

---

Resultados de encuesta: Global

---

Resultados de encuesta: Latinoamérica

---

Ciberseguridad:  
Aunar esfuerzos para la ciberseguridad

---

Continuidad del negocio:  
Establecer conexiones para una  
mayor resiliencia

---

Incertidumbre geopolítica:  
Planificar para cambios de amplio  
impacto

---

## CIBERSEGURIDAD

### Reconfigurar el gobierno corporativo para enfrentar la velocidad del riesgo

En vista de la velocidad y ferocidad del panorama del riesgo cibernético, los DEA que participaron en mesas redondas señalaron que algunas estrategias efectivas son:

- Reconfigurar las estructuras de gobierno corporativo para permitir un mejor aseguramiento combinado entre las tres líneas.
- Crear comités de riesgo adicionales en toda la empresa dedicados a la amenaza.
- Realzar a los comités de auditoría y los consejos mediante el requisito de que tengan al menos un director no ejecutivo con una especialidad en ciberseguridad.

El DEA de un banco brasileño dijo que asignó al área de TI la responsabilidad por el riesgo cibernético, incluyéndola efectivamente en el sistema de gobierno como cuarta línea. “Esto ha sido súper saludable para la organización y ha generado mucho valor”, comentó.

### Para la ciberdefensa, se requiere conocimiento

La concientización de los ataques cibernéticos es alta, pero también lo es la escasez de talento para las habilidades clave de TI y cibernéticas. La mayoría de las funciones de auditoría interna se beneficiarían de un experto en ciberseguridad, pero los puestos son difíciles de cubrir o implican un costo demasiado alto. En vista de estos desafíos, la capacitación y la sensibilización han pasado a ocupar el centro de atención, según mencionaron los DEA en las mesas redondas. Los DEA están alentando a los auditores a certificarse en áreas de TI.

Si bien la creación de una cultura cibersegura se ha hecho más difícil por la mayor rotación de personal durante y después de la pandemia, los DEA que participaron en los debates comentaron que estaban aprovechando la capacitación en línea para compartir recursos y conocimientos. Algunos también aportaron que utilizan sus relaciones con los proveedores de TI operativos para proporcionar actualizaciones y capacitación de forma gratuita. Una vez capacitado, se suele pedir al personal que transmita los conocimientos adquiridos a otros integrantes del negocio.

## Recursos

[Assessing Cybersecurity Operations: Prevention and Detection \(The IIA\)](#)

[The IIA's Three Lines Model](#)

El Modelo de las Tres Líneas explica las funciones de la primera, segunda y tercera líneas en el gobierno corporativo.

“Estamos realizando mucha más capacitación para que todos en la organización estén más informados, porque si los empleados no conocen cómo funcionan los ataques de phishing, es muy fácil para los hackers ingresar en la empresa”, señaló José Gabriel Calderón, DEA de la multinacional mexicana de alimentos Grupo Bimbo.



# Contenido

Resumen ejecutivo:  
Construir relaciones para  
alcanzar el éxito juntos

---

Metodología

---

Resultados de encuesta: Global

---

Resultados de encuesta: Latinoamérica

---

Ciberseguridad:  
Aunar esfuerzos para la ciberseguridad

---

Continuidad del negocio:  
Establecer conexiones para una  
mayor resiliencia

---

Incertidumbre geopolítica:  
Planificar para cambios de amplio  
impacto

---

## CIBERSEGURIDAD

### Cómo puede la auditoría interna ayudar a la organización

1. Incluya auditorías de ciberseguridad en el plan de auditoría de forma recurrente e informe los resultados al consejo y a la dirección ejecutiva.
2. Si las regulaciones regionales de ciberseguridad son débiles o inexistentes, aliente a la organización a utilizar marcos alternativos de ciberseguridad, como el que ofrece el NIST.
3. Evalúe en qué medida la dirección comprende las tecnologías disruptivas, como la IA, antes de que sean implementadas, y genere relaciones dentro de la organización para poder hacer aportes sobre los riesgos emergentes.
4. Evalúe la eficacia de las estructuras de gobierno corporativo para ayudar a optimizar la colaboración entre las tres líneas en temas de ciberseguridad y seguridad de datos.
5. Evalúe los programas de capacitación y concientización sobre ciberseguridad y en qué medida dichas campañas se difunden a toda la organización.



## Contenido

Resumen ejecutivo:  
Construir relaciones para  
alcanzar el éxito juntos

Metodología

Resultados de encuesta: Global

Resultados de encuesta: Latinoamérica

Ciberseguridad:  
Aunar esfuerzos para la ciberseguridad

Continuidad del negocio:  
Establecer conexiones para una  
mayor resiliencia

Incertidumbre geopolítica:  
Planificar para cambios de amplio  
impacto

# CONTINUIDAD DEL NEGOCIO

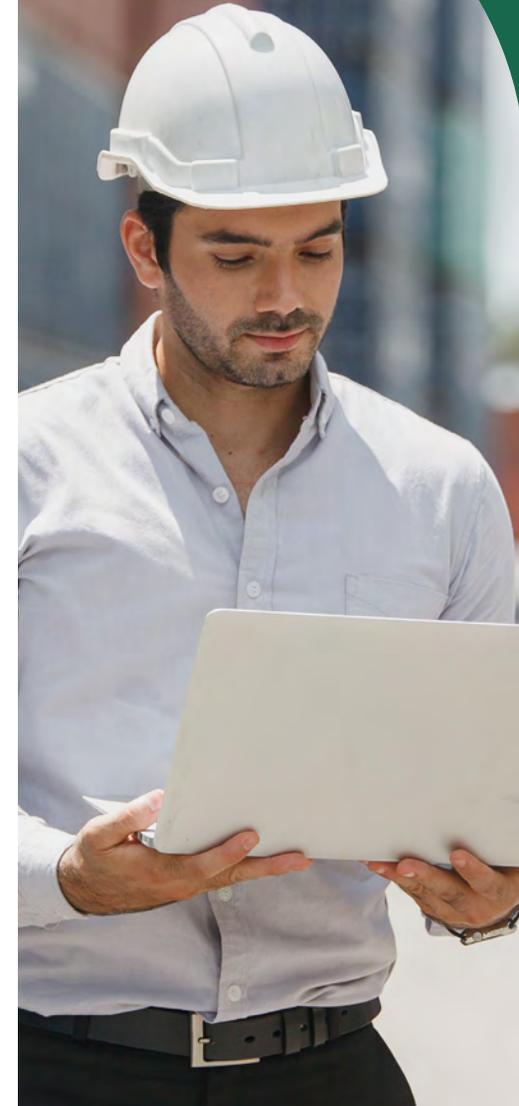
## Establecer conexiones para una mayor resiliencia

**En un panorama de riesgos dinámico e interconectado, trabajar en equipo y actuar de manera rápida y decisiva son las claves para recuperarse después del deterioro o cierre de las operaciones.**

Si bien la falla operacional es una amenaza importante en sí misma, sus causas potenciales se cruzan con otros riesgos principales que enfrentan las organizaciones en Latinoamérica. Los ataques de ransomware, los cambios inesperados en leyes y regulaciones, y la incertidumbre macro-económica, el cambio climático y las disrupciones en la cadena de suministro crean una variedad compleja de riesgos que pueden causar cierres parciales o totales de las operaciones comerciales.

Las tensiones políticas en la región pueden desencadenar cambios inesperados en el

sector empresarial, según comentaron los DEA en las mesas redondas. Por ejemplo, el gobierno nicaragüense nacionalizó una importante compañía de gasolineras en 2023 en aparente represalia contra las sanciones de Estados Unidos, lo cual planteó grandes desafíos para otras empresas y organizaciones.<sup>4</sup> Argentina, Brasil, Chile, Colombia, México y Perú enfrentan posibles huelgas y disturbios políticos en 2023, lo que amenaza aún más la continuidad del negocio. <sup>5</sup>Y las elecciones en varios países son otro elemento que suma incertidumbre política.



**Resultados  
de Encuesta –  
Continuidad  
del Negocio**

3. – NIVEL DE RIESGO

**47%**  
lo clasificó  
entre los 5  
principales  
en nivel de riesgo

2. – ESFUERZO DE AUDITORÍA

**53%**  
lo clasificó  
entre los 5  
principales  
en esfuerzo de  
auditoría

<sup>4</sup>Para más información sobre la nacionalización de la compañía de gasolineras, consulte <https://www.reuters.com/article/us-nicaragua-ortega-idUSKBN1YI0LV>

<sup>5</sup>Para más información sobre los disturbios políticos en Latinoamérica, consulte <https://www.lexology.com/library/detail.aspx?g=17706d05-173b-474a-a928-97ab1385493d>



# Contenido

Resumen ejecutivo:  
Construir relaciones para  
alcanzar el éxito juntos

Metodología

Resultados de encuesta: Global

Resultados de encuesta: Latinoamérica

Ciberseguridad:  
Aunar esfuerzos para la ciberseguridad

Continuidad del negocio:  
Establecer conexiones para una  
mayor resiliencia

Incertidumbre geopolítica:  
Planificar para cambios de amplio  
impacto

## CONTINUIDAD DEL NEGOCIO

### La continuidad del negocio se basa en las relaciones

La pandemia contribuyó a construir relaciones clave necesarias para responder a las crisis, y al mismo tiempo se tomó conciencia de lo esencial que es la planificación para la continuidad del negocio.

Un DEA de la industria aérea en El Salvador comentó que su compañía pudo mantener los vuelos durante la pandemia debido a la cooperación y el diálogo con el gobierno nacional. El impacto de la pandemia de COVID-19 subrayó la necesidad de planificar para eventos improbables. “El episodio cambió la mentalidad de la alta dirección, que antes solía demorar las recomendaciones de la auditoría interna para crear planes de recuperación de desastres”, comentó. “COVID-19 ayudó a comprender que, si bien estos riesgos tienen muy poca probabilidad de materializarse, cuando lo hacen, el resultado puede ser catastrófico”.

Cuando los ejercicios de recuperación de desastre fortalecen la relación entre la

auditoría interna y la dirección, es más probable que ambos grupos colaboren para lanzar una respuesta rápida cuando los objetivos estratégicos se ven amenazados. Por ejemplo, cuando Panamá cerró sus fronteras a ciertos bienes importados, interrumpiendo las cadenas de suministro establecidas, las exportaciones se vieron afectadas de la noche a la mañana. El DEA de un productor de lácteos costarricense, cuyo negocio se vio afectado por el hecho, comentó que la dirección recurrió a la auditoría interna para ayudar al negocio a buscar nuevos acuerdos de fabricación en Panamá, y así se reanudaron las operaciones.

Los planes de respuesta a desastres deben ser acordados por la auditoría interna y la dirección. “En todo plan de continuidad del negocio, se necesita un apoyo claro de la alta dirección para asegurar que se cuenta con su aceptación del proyecto; de lo contrario sólo se van a tratar las cuestiones a nivel operativo”, señaló Fábio Pimpão, director de auditoría interna de Whirlpool Latinoamérica.

Una vez establecido, cada plan debe ser lo suficientemente detallado como para considerar todas las variables potenciales

(incluso los riesgos interconectados) y estar bien documentado y probado a fondo, según señaló. Eso incluye prestar mucha atención a la infraestructura crítica de la cadena de suministro.

“COVID-19 ayudó a comprender que, si bien estos riesgos tienen muy poca probabilidad de materializarse, cuando lo hacen, el resultado puede ser catastrófico”.



# Contenido

Resumen ejecutivo:  
Construir relaciones para  
alcanzar el éxito juntos

Metodología

Resultados de encuesta: Global

Resultados de encuesta: Latinoamérica

Ciberseguridad:  
Aunar esfuerzos para la ciberseguridad

Continuidad del negocio:  
Establecer conexiones para una  
mayor resiliencia

Incertidumbre geopolítica:  
Planificar para cambios de amplio  
impacto

## CONTINUIDAD DEL NEGOCIO

### Integrar controles en todas las operaciones

Para lograr la resiliencia operativa, la continuidad del negocio debe integrarse en todos los aspectos de las operaciones de una organización, y los análisis de impacto y las evaluaciones de riesgos deben mantenerse actualizados. Según los testimonios de la mesa redonda, la auditoría interna debe cubrir tanto los riesgos emergentes, tales como blockchain e IA, como los que existen desde hace muchos años, como la inestabilidad política, el fraude y el riesgo regulatorio. Puede ser tentador centrarse solo en amenazas nuevas y emergentes, pero las consecuencias de riesgos bien conocidos también pueden destruir las operaciones. Defender continuamente la necesidad de planificar para la continuidad del negocio es esencial para evitar que la alta dirección vuelva a caer en el pensamiento complaciente previo a la pandemia.

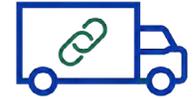
En áreas de rápida evolución como la ciberseguridad, los DEA deben conocer las metodologías de ciberataque de vanguardia, comentaron los DEA reunidos en mesa redonda, con evaluaciones de riesgo

cibernético, pruebas de controles y monitoreo activo como parte de cada tarea. Es esencial trabajar en estrecha colaboración con el área TI y las funciones de gestión de riesgos y, dado que los ataques de ingeniería social se basan en el desconocimiento del personal, dar capacitación es fundamental. “No solo facilitamos la capacitación, también asistimos a ella”, comentó el DEA de una empresa financiera en Guatemala, “porque necesitamos estar al tanto de lo que está sucediendo”.

La gestión de riesgos empresariales (ERM) de alta calidad es fundamental para todos los planes de continuidad del negocio y resiliencia operativa. “La continuidad efectiva del negocio debe ser colaborativa y basarse en un ERM fuerte y sólido”, manifestó el DEA de una compañía minera peruana. “Bromeo con el consejo diciendo que, si tuviera que hacer solo una auditoría por año, auditaría ERM.”

### Equipos diversos, mayor resiliencia

Dada la amplia gama de riesgos que intervienen en el trabajo de auditoría interna sobre la continuidad del negocio, adquirir el equilibrio adecuado de habilidades



## Recursos

[Auditing Third-Party Risk Management \(The IIA\)](#)

[Business Continuity Management \(The IIA\)](#)

es sumamente difícil. En tres años, los encuestados dijeron que esperan que la disrupción digital pase al segundo lugar como un riesgo clave, y que el cambio climático salte al quinto lugar (Figura 2). Los DEA dijeron que estaban tratando de diversificar sus equipos cuanto antes para estar listos para estos desafíos, a pesar de la escasez de habilidades técnicas, particularmente para pequeñas funciones de auditoría y el sector público.



# Contenido

Resumen ejecutivo:  
Construir relaciones para  
alcanzar el éxito juntos

---

Metodología

---

Resultados de encuesta: Global

---

Resultados de encuesta: Latinoamérica

---

Ciberseguridad:  
Aunar esfuerzos para la ciberseguridad

---

Continuidad del negocio:  
Establecer conexiones para una  
mayor resiliencia

---

Incertidumbre geopolítica:  
Planificar para cambios de amplio  
impacto

---

## CONTINUIDAD DEL NEGOCIO

### Cómo puede la auditoría interna ayudar a la organización

1. Construya relaciones con la dirección ejecutiva y el comité de auditoría y trabajen juntos para mejorar el desarrollo y las pruebas de los planes de continuidad del negocio.
2. Evalúe en qué medida se han documentado y probado los planes de continuidad del negocio.
3. Evalúe si el conocimiento de la organización sobre sus riesgos clave está actualizado y cubre todo el universo de riesgos, en lugar de centrarse demasiado en los riesgos emergentes.
4. Evalúe los requisitos futuros de capital humano de la organización en función de los resultados de la planificación de la continuidad del negocio.
5. Según corresponda, incluya una auditoría de los planes de continuidad de la organización en el plan de auditoría.



## Contenido

Resumen ejecutivo:  
Construir relaciones para  
alcanzar el éxito juntos

Metodología

Resultados de encuesta: Global

Resultados de encuesta: Latinoamérica

Ciberseguridad:  
Aunar esfuerzos para la ciberseguridad

Continuidad del negocio:  
Establecer conexiones para una  
mayor resiliencia

Incertidumbre geopolítica:  
Planificar para cambios de amplio  
impacto

# INCERTIDUMBRE GEOPOLÍTICA

## Planificar para cambios de amplio impacto

**La incertidumbre política ha aumentado el riesgo de cambios regulatorios en algunos países, pero los DEA están asegurándose de que estos problemas se incluyan en las agendas de riesgo de las organizaciones.**

La disrupción política ha caracterizado a muchos países latinoamericanos en los últimos años en que Argentina, Guatemala y Paraguay tuvieron elecciones. Es parte de lo que se considera un superciclo, que se extiende de 2021 a 2024 e incluye elecciones en todos los países de la región.<sup>6</sup>

“La disrupción política marcada por cambios de gobierno está afectando significativamente la liquidez de las empresas, y la inflación está afectando a los mercados locales”, explicó un DEA en una institución financiera guatemalteca.

Algunos países de la región pueden experimentar cambios gubernamentales que alteran las políticas económicas o restringen la actividad económica. Los DEA pueden ayudar a los consejos a prepararse para los cambios políticos que podrían poner en riesgo su negocio ayudando a encontrar planes alternativos para permitir la continuidad de su negocio a largo plazo y buscando apoyo experto, como especialistas legales y de comercio exterior.

Resultados  
de Encuesta –  
Incertidumbre  
geopolítica

5. – NIVEL DE RIESGO

**42%**  
lo clasificó  
entre los 5  
principales  
en nivel de riesgo

13. – ESFUERZO DE AUDITORÍA

**13%**  
lo clasificó  
entre los 5  
principales  
en esfuerzo de  
auditoría



# Contenido

Resumen ejecutivo:  
Construir relaciones para  
alcanzar el éxito juntos

Metodología

Resultados de encuesta: Global

Resultados de encuesta: Latinoamérica

Ciberseguridad:  
Aunar esfuerzos para la ciberseguridad

Continuidad del negocio:  
Establecer conexiones para una  
mayor resiliencia

Incertidumbre geopolítica:  
Planificar para cambios de amplio  
impacto

## INCERTIDUMBRE GEOPOLÍTICA

### El plan para prevenir crisis de flujos de fondos

Los cambios en las leyes y regulaciones pueden ser a gran escala, rápidos e impactantes. En esta apreciación coincidieron los DEA presentes en la mesa redonda.

“Los auditores internos deben estar bien informados sobre los cambios políticos o las modificaciones en las leyes y regulaciones”, señaló Francisco Ramón Aráuz Rodríguez, Presidente de la Fundación Latinoamericana de Auditores Internos (FLAI). “Los DEA deben poder alertar a sus organizaciones de manera oportuna, evaluando y determinando el impacto de tales eventos y regulaciones”.

El objetivo es que el DEA trabaje en asociación con el comité de auditoría para discutir cómo los eventos del entorno político y económico podrían afectar el negocio, y así poder reaccionar en consecuencia, agregó. Además, los DEA deben supervisar proactivamente los riesgos emergentes y sus impactos en los clientes y las cadenas de suministro y evaluar cómo interactúan.

“La política, el medio ambiente, las barreras comerciales, los riesgos

macroeconómicos... es necesario combinar estas amenazas y tener una visión holística para poder asesorar a la dirección sobre cómo actuar”, comentó Fábio Pimpão, director de auditoría interna de Whirlpool Latinoamérica. En particular, el DEA debe crear escenarios y simulaciones para comprender mejor las interrelaciones entre los riesgos y tener un plan en marcha, antes de que llegue la crisis.

El desarrollo de situaciones hipotéticas puede proporcionar al DEA posibles temas a tratar en la auditoría estratégica y operativa, así como ayuda para identificar áreas donde se necesitan seguros, además de oportunidades para mejorar el gobierno operativo en toda la empresa y formas de asegurar que el negocio no se quede sin fondos en caso de que ocurra una crisis.



Pimpão explicó: “Al final, lo que determina que una empresa quiebre no es la cuenta de ganancias y pérdidas, ni sus resultados ni sus fallas en los informes, sino el flujo de caja”, y agregó: “Los escenarios de riesgo emergente pueden ayudar a determinar cuándo la auditoría interna debe centrarse en la gestión de efectivo, por ejemplo, para dar algunas recomendaciones estratégicas que ayuden a la toma de decisiones corporativas y que sean útiles para evitar potenciales desastres.”



# Contenido

Resumen ejecutivo:  
Construir relaciones para  
alcanzar el éxito juntos

Metodología

Resultados de encuesta: Global

Resultados de encuesta: Latinoamérica

Ciberseguridad:  
Aunar esfuerzos para la ciberseguridad

Continuidad del negocio:  
Establecer conexiones para una  
mayor resiliencia

Incertidumbre geopolítica:  
Planificar para cambios de amplio  
impacto

## INCERTIDUMBRE GEOPOLÍTICA

### Actualizaciones en materia de lavado de activos

Si bien puede haber cambios rápidos en el liderazgo político, el lavado de activos, el lavado de dinero y el fraude son problemas profundamente arraigados en muchos de los países de la región. “El lavado de dinero se percibe como un problema que se encuentra todo a nuestro alrededor”, comentó José Lago Rodríguez, vicepresidente de FLAI.

Muchas organizaciones en Latinoamérica no cuentan con procedimientos detallados de cumplimiento para la prevención del lavado de dinero. En general, solo existen procedimientos para entidades de servicios financieros, organizaciones que cotizan en bolsa y empresas globales. Cuando falten procedimientos, el DEA debería considerar la creación de una taxonomía de riesgo que incluya lavado de activos, lavado de dinero y fraude; y luego hacer un mapa de los riesgos en toda la empresa.

Los DEA deben ser conscientes de las diferencias en los requisitos de cumplimiento

contra el lavado de dinero de un país a otro y garantizar que existan procedimientos de control apropiados. En los últimos años, el Grupo de Acción Financiera de Latinoamérica ha desarrollado recursos para ayudar a las organizaciones de la región a navegar por el laberinto de requisitos regulatorios.<sup>7</sup>

En equipos pequeños donde el mandato de la auditoría interna está estrechamente definido, el DEA también puede tener la tarea de educar y persuadir al consejo de que la auditoría interna puede agregar valor al abordar los riesgos relacionados con el lavado de dinero.

Países como Argentina también han lanzado medidas específicas para permitir a las empresas mejorar la madurez de sus procesos anticorrupción y fraude, y los auditores internos están ayudando a integrarlas. Pamela Vago, DEA de Genneia, una compañía de energía en Argentina,<sup>8</sup> comentó: “Hemos estado trabajando con la compañía para desarrollar procedimientos y capacitación en las nuevas regulaciones.”



“Al final, lo que determina que una empresa quiebre no es la cuenta de ganancias y pérdidas, ni sus resultados ni sus fallas en los informes, sino el flujo de caja”



<sup>7</sup> Para más información sobre los esfuerzos contra el lavado de dinero en América Latina, consulte <https://latinlawyer.com/guide/the-guide-corporate-compliance/second-edition/article/17-anti-money-laundering-and-counter-terrorist-financing-in-latin-america>

<sup>8</sup> Para más información sobre los esfuerzos de Argentina contra la corrupción, consulte [https://www.globalcompliance.com/2023/01/06/https-in-sightplus-bakermckenzie-com-bm-investigations-compliance-ethics-argentina-the-registry-of-integrity-and-transparency-of-companies-and-entities-finally-launched\\_01042023/](https://www.globalcompliance.com/2023/01/06/https-in-sightplus-bakermckenzie-com-bm-investigations-compliance-ethics-argentina-the-registry-of-integrity-and-transparency-of-companies-and-entities-finally-launched_01042023/)

# Contenido

Resumen ejecutivo:  
Construir relaciones para  
alcanzar el éxito juntos

---

Metodología

---

Resultados de encuesta: Global

---

Resultados de encuesta: Latinoamérica

---

Ciberseguridad:  
Aunar esfuerzos para la ciberseguridad

---

Continuidad del negocio:  
Establecer conexiones para una  
mayor resiliencia

---

Incertidumbre geopolítica:  
Planificar para cambios de amplio  
impacto

---

## INCERTIDUMBRE GEOPOLÍTICA

La auditoría interna proporciona aseguramiento en torno a los procesos de gobierno corporativo, las políticas y la segregación de funciones que se establecen para prevenir el fraude. Si bien los controles duros son importantes, los controles blandos, como el código de ética, las líneas directas y los canales de quejas, también pueden ayudar, siempre que sean confiables. “Puede haber un temor de represalias por hablar. Por lo tanto, los empleados deben poder confiar en que las personas que administran la línea directa no sean cómplices del fraude”, señaló Vago.

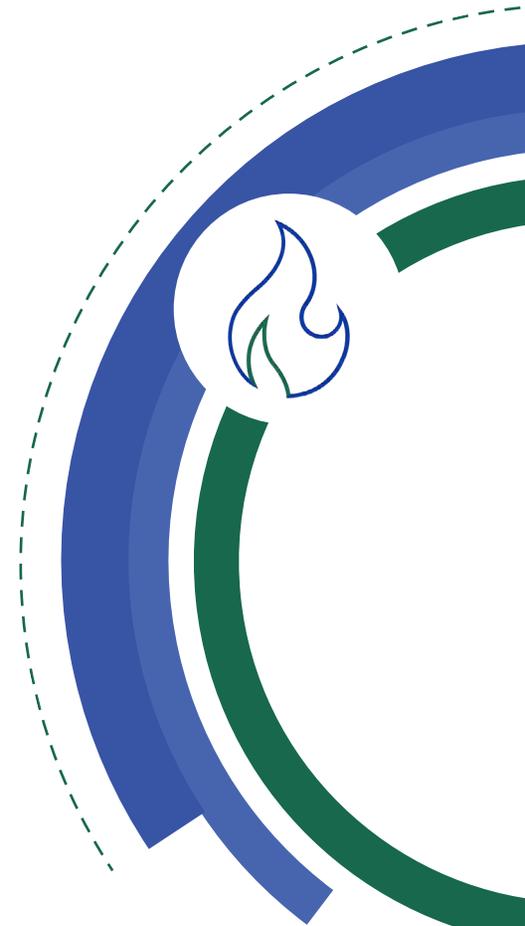
Ante los aumentos de precios que se producen en muchos países, las organizaciones necesitarán tener controles establecidos para reducir la tentación de malversar fondos

Si bien no se niega la importancia de los controles duros, los controles blandos -como el código de ética, las líneas directas y los canales de quejas -también pueden ayudar, siempre que sean confiables.

o activos. “Algunas áreas pueden no ser materiales, como la caja chica en una gran empresa, pero la presencia activa de la función de auditoría interna puede desalentar a las personas de cometer fraude”, expresó Vago.

### Una mayor coordinación entre países

La desaceleración del crecimiento, el aumento de la inflación y la crisis del costo de vida ejercen presión en los gobiernos para que actúen, pero la corrupción y cierta debilidad de las instituciones dificultan resolver los problemas sociales que afectan a la región. Se han realizado múltiples esfuerzos para fomentar una mayor integración entre los países sudamericanos, como una reunión encabezada por el presidente de Brasil reciente, en mayo de 2023, con la esperanza de fomentar la estabilidad política y económica en una región que en forma colectiva representa la quinta economía mundial más grande.<sup>9</sup>



# Contenido

Resumen ejecutivo:  
Construir relaciones para  
alcanzar el éxito juntos

---

Metodología

---

Resultados de encuesta: Global

---

Resultados de encuesta: Latinoamérica

---

Ciberseguridad:  
Aunar esfuerzos para la ciberseguridad

---

Continuidad del negocio:  
Establecer conexiones para una  
mayor resiliencia

---

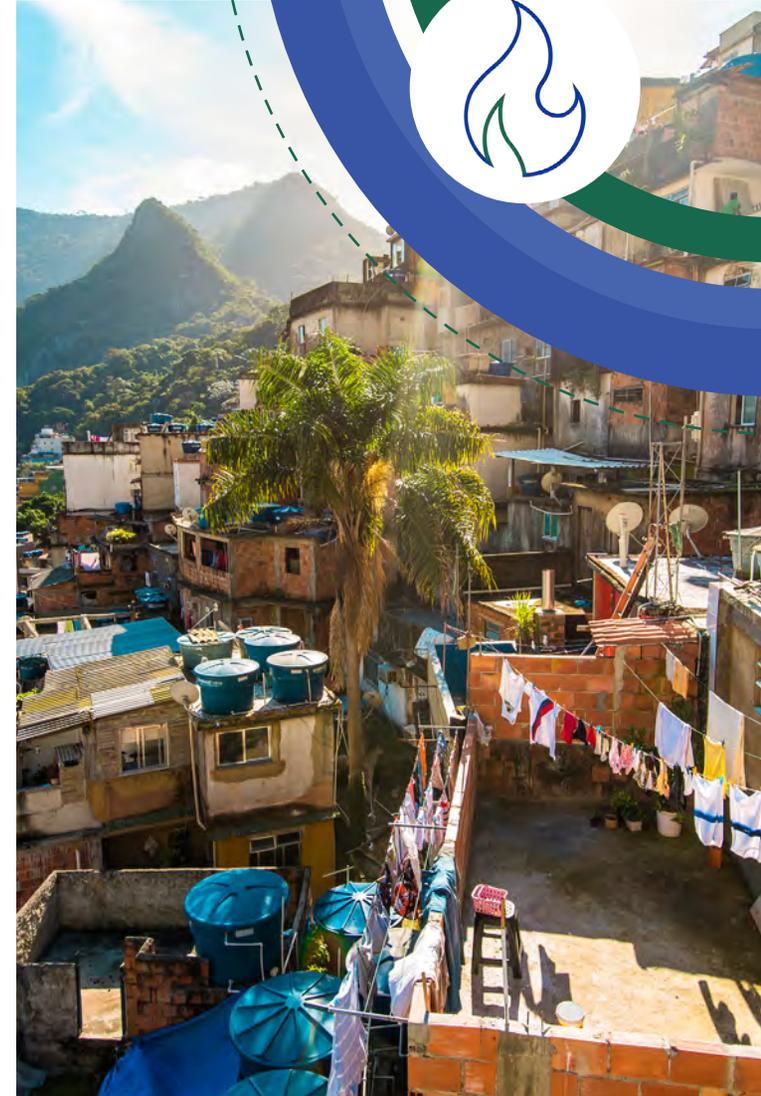
Incertidumbre geopolítica:  
Planificar para cambios de amplio  
impacto

---

## INCERTIDUMBRE GEOPOLÍTICA

### Cómo puede la auditoría interna ayudar a la organización

1. Tenga en cuenta el impacto en el negocio si, como consecuencia de un cambio político, asume un gobierno que restringe las actividades económicas.
2. Prepárese para cualquier cambio político que pueda poner en riesgo el negocio, ayudando a encontrar planes alternativos para permitir la continuidad a largo plazo y buscando apoyo experto, como especialistas legales y de comercio exterior.
3. Evalúe la situación de la organización y los procesos de simulación para riesgos emergentes y determine en qué grado se tienen en cuenta para definir el plan de auditoría interna.
4. Evalúe si la organización cuenta con los procesos adecuados contra el lavado de dinero para cumplir con las regulaciones y para permitir un mapeo de riesgos en toda la empresa.
5. Evalúe los controles blandos de la empresa en torno a la prevención y detección de fraude.
6. Revise la elaboración de documentos, como el Código de Ética, que deben contar con el firme apoyo del directorio, la dirección y el DEA.



# AGRADECIMIENTOS - INTERNAL AUDIT FOUNDATION

## Equipo de Desarrollo Risk in Focus

### Directores del proyecto

**Laura LeBlanc** –

Directora Senior, Internal Audit Foundation

**Deborah Poulalion** –

Gerente Senior, Research and Insights, The IIA

**Emely Katz** –

Directora, Afiliada Engagement, The IIA

### Análisis de encuestas y desarrollo de contenido

**Deborah Poulalion** –

Gerente Senior, Research and Insights, The IIA

### Redacción de investigación

**Arthur Piper** – Smith de Wint, Reino Unido

### Diseño gráfico

**Cathy Watanabe**

## Internal Audit Foundation Consejo 2023–24

### Presidente

**Warren W. Stippich Jr.**, CIA, CRMA

### Vicepresidente Senior – Estrategia

**Glenn Ho**, CIA, CRMA

### Vicepresidente – Finanzas y Desarrollo

**Sarah Fedele**, CIA, CRMA

### Vicepresidente – Contenido

**Yulia Gurman**, CIA

### Miembros

**Hossam El Shaffei**, CCSA, CRMA

**Reyes Fuentes Ortea**, CIA, CCSA, CRMA

**Nora Kelani**, CIA, CRMA

**Shirley Livhuwani Machaba**, CCSA, CRMA

**Raoul Ménès**, CIA, CCSA, CRMA

**Hiroshi Naka**, CIA

**Anthony J. Pugliese**, CIA

**Bhaskar Subramanian**

### Enlace del Staff

**Laura LeBlanc** –

Directora Senior, Internal Audit Foundation

## Internal Audit Foundation Asesores del Comité de Investigación y Educación 2023–24

### Presidente

**Yulia Gurman**, CIA

### Vicepresidente

**Jane Traub**, CIA, CCSA, CRMA

### Miembros

**Tonya Arnold-Tornquist**, CIA, CRMA

**Christopher Calvin**, CIA

**Jiin-Feng Chen**, CIA

**Andre Domingos**

**Christina Duquette**, CRMA

**Marc Eulerich**, CIA

**Dagmar Flores**, CIA, CCSA, CRMA

**Anargul Kairulla**, CIA

**Ayaka Mitsunari**

**Ahmed Mohammed**, CIA

**Grace Mubako**, CIA

**Ruth Doreen Mutebe**, CIA

**Erika C. Ray**, CIA

**Brian Tremblay**, CIA

**Koji Watanabe**

### Enlace del Staff

**Deborah Poulalion** –

Gerente Senior, Research and Insights, The IIA



# FUNDACIÓN LATINOAMERICANA DE AUDITORES INTERNOS (FLAI)

## Consejo 2021-2024

### Presidente

**Francisco Ramón Aráuz Rodríguez**, CIA, CCSA

### Vicepresidente

**José Lago Rodríguez**, CIA, CFSA

### Secretario

**Gabriel Benavides**

### Tesorero

**Máximo Perdomo**, CIA

### Directores

**Renato Trisciuzzi**, CIA, QIAL, CRMA, CCSA

**Maritza Barzola**

## Informe sobre Latinoamérica Equipo de Desarrollo

### Enlaces regionales

**Roberto Loo**, Director Ejecutivo, Fundación Latinoamericana de Auditores Internos

**Jorge Badillo Ayala**, CIA, QIAL, CCSA, CGAP, CRMA, CFE, CISA – Director, Global Services (IRC) IIA Global

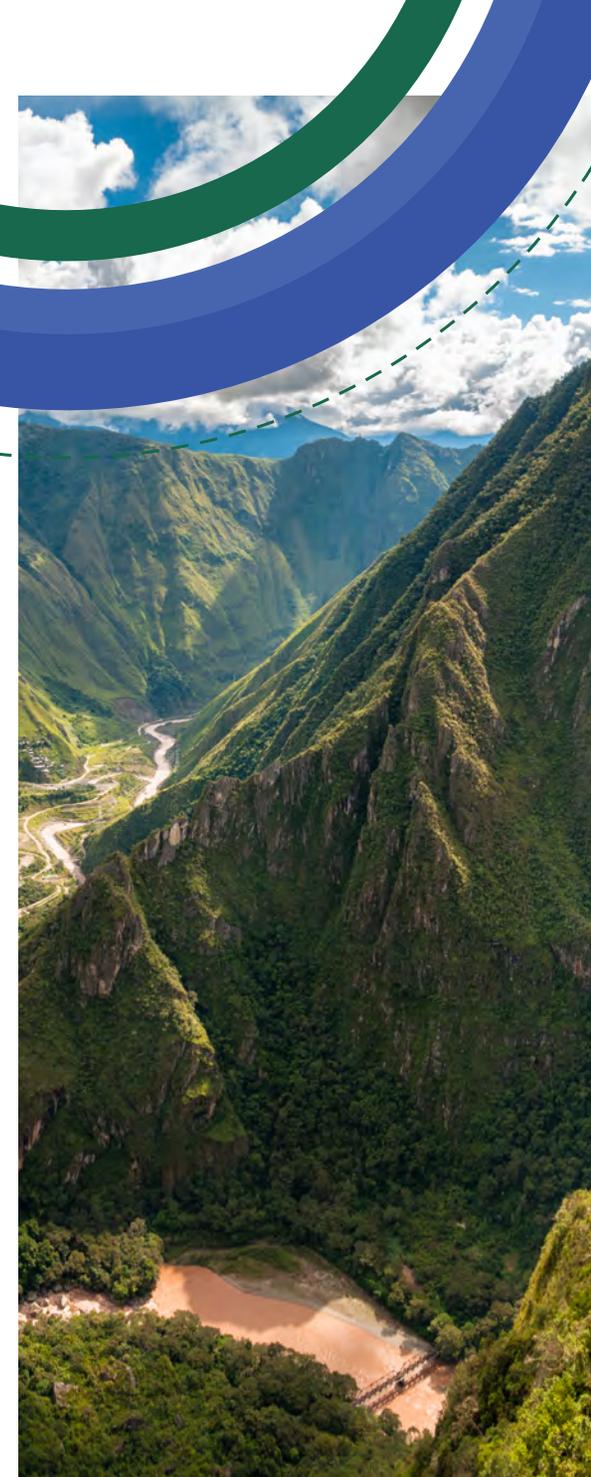
### Moderadores de mesas redondas

**Fábio Pimpão**, Director de Auditoría Interna en Whirlpool Latinoamérica

**José Gabriel Calderón**, Director de Auditoría Interna en Grupo Bimbo

### Patrocinio de la traducción

**Grupo Bimbo**  
(Corporativo Bimbo, S.A. de C.V.)



# SOCIOS

## SOCIOS ESTRATÉGICOS DE LA FUNDACIÓN



## Socios de la Fundación



## Socios Oro

**Larry Harrington**  
CIA, QIAL, CRMA

**Stacey Schabel**  
CIA



## SOCIOS RISK IN FOCUS

- |                   |                 |                 |
|-------------------|-----------------|-----------------|
| IIA – Argentina   | IIA – Guatemala | IIA – Filipinas |
| IIA – Australia   | IIA – Hong Kong | IIA – Ruanda    |
| IIA – Bolivia     | IIA – Indonesia | IIA – Singapur  |
| IIA – Brasil      | IIA – Japón     | IIA – Sudáfrica |
| IIA – Chile       | IIA – Kenia     | IIA – Tanzania  |
| IIA – Colombia    | IIA – Malaysia  | IIA – Uganda    |
| IIA – Costa Rica  | IIA – México    | IIA – Uruguay   |
| IIA – Dominicana  | IIA – Nicaragua | IIA – Venezuela |
| IIA – Ecuador     | IIA – Panamá    |                 |
| IIA – El Salvador | IIA – Paraguay  |                 |
| IIA – Gana        | IIA – Perú      |                 |



# ACERCA DE THE IIA

The Institute of Internal Auditors (IIA) es una asociación profesional internacional sin fines de lucro que brinda servicios a más de 235,000 miembros globales y ha otorgado más de 190,000 certificaciones Certified Internal Auditor (CIA) a nivel mundial. Fundada en 1941, The IIA es reconocida en todo el mundo como la institución líder en normas, certificaciones, educación, investigación y asesoramiento técnico para la profesión de auditoría interna. Más información: [theiia.org](http://theiia.org).

## Acerca de The Internal Audit Foundation

The Internal Audit Foundation ofrece perspectivas a profesionales de auditoría interna y sus grupos de interés, mediante la promoción y el avance del valor de la profesión de auditoría interna a nivel global. A través del Fondo Académico, la Fundación apoya el futuro de la profesión mediante becas para apoyar la educación en auditoría interna en instituciones de estudios superiores. Más información: [theiia.org/Foundation](http://theiia.org/Foundation).

## Aviso legal y derechos de autor

The IIA publica este documento con fines informativos y educativos. Este material no tiene por fin dar respuestas definitivas a circunstancias individuales específicas y no está destinado a ser utilizado como una guía. The IIA recomienda buscar asesoramiento experto independiente que tenga relación directa con una situación específica. The IIA no acepta responsabilidad alguna en caso de que este material se use como único recurso.

Copyright © 2023 de The Internal Audit Foundation. Reservados todos los derechos. Por permisos de reproducción, contacte a [Copyright@theiia.org](mailto:Copyright@theiia.org).



Global Headquarters | The Institute of Internal Auditors  
1035 Greenwood Blvd., Suite 401 | Lake Mary, FL 32746, USA  
Teléfono: +1-407-937-1111 | Fax: +1-407-937-1101  
Sitio web: [theiia.org](http://theiia.org)