AMÉRICA LATINA 2026/2027

Assuntos Relevantes para auditores internos

RISK in FOCUS



Fundación Latinoamericana de Auditores Internos

Internal Audit FOUNDATION 1976-2026

SOBRE A GLOBAL RISK IN FOCUS

Conheça seus riscos. Planeje estrategicamente.

O Risk in Focus é a principal iniciativa anual da Fundação de Auditoria Interna para identificar os cinco riscos mais significativos que impactam o mundo.

Saiba o que os auditores internos estão dizendo sobre:

- Os cinco maiores riscos na sua região
- As cinco principais prioridades para os esforços de auditoria interna
- As principais considerações para o Conselho e Comitê de Auditoria

O Risk in Focus utiliza resultados de pesquisas, painéis regionais e entrevistas com especialistas locais para revelar insights cruciais sob a perspectiva única da auditoria interna.

A Fundação de Auditoria Interna agradece sinceramente o trabalho dos Institutos Nacionais do IIA e dos órgãos regionais do IIA que tornam esta pesquisa possível: Federação Africana de Institutos de Auditores Internos (AFIIA), Confederação Árabe de Auditores Internos (ARABCIA), Confederação Asiática de Institutos de Auditores Internos (ACIIA), Confederação Europeia de Institutos de Auditores Internos (ECIIA) e a Fundação Latino-Americana de Auditores Internos (FLAI).

Um agradecimento especial ao Grupo de Pesquisa dos Institutos Europeus (EIRG), que desenvolveu a abordagem de pesquisa Risk in Focus em 2016 e continua a publicar o relatório para a Europa por meio da ECIIA.

Todos os relatórios e comunicações ao Conselho são de acesso gratuito ao público:

- África
- Ásia Pacífico
- Europa
- América Latina
- Oriente Médio
- América do Norte
- Sumário global

Acesse o Centro de Conhecimento Risk in Focus para saber mais.

Internal Audit FOUNDATION 1976-2026

Visite o Centro de Conhecimento Risk in Focus para obter relatórios gratuitos e relatórios executivos para o conselho (theiia.org/RiskInFocus).

PARTICIPAÇÃO NA PESQUISA GLOBAL

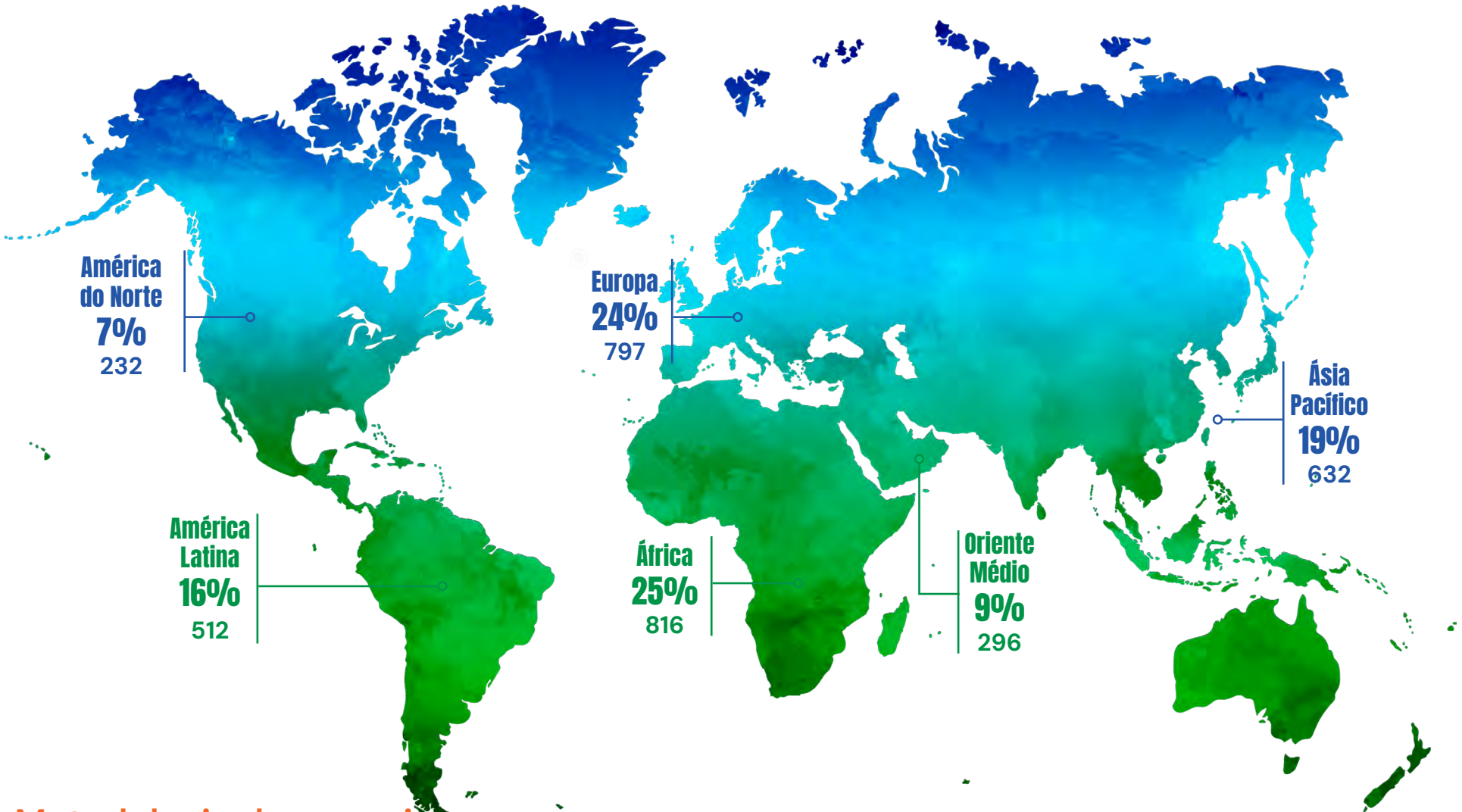


PARTICIPAÇÃO NA PESQUISA GLOBAL

TOTAIS GLOBAIS

3.285 respondentes

132 países/regiões



Metodologia da pesquisa

Foram recebidas respostas de 3.285 diretores e chefes de auditoria interna, representando 132 países e regiões. A Fundação de Auditoria Interna realizou a pesquisa online de 24 de março a 6 de maio de 2026, para todas as regiões, exceto a Europa. A pesquisa para a Europa foi realizada pelo Grupo de Pesquisa dos Institutos Europeus entre 2 de março e 7 de abril de 2026.

CONTEÚDO

Resumo executivo 5

Seção 1. Ambiente de riscos 6

Seção 2. Prioridades da Auditoria Interna 14

Seção 3. Maturidade e cobertura de riscos 22

Conclusão 28

Apêndice A. Metodologia 29

Apêndice B. Dados demográficos 30

Apêndice C. Visão geral dos riscos globais 32

Apêndice D. Recursos do IIA 35

AGRADECIMENTOS

Fundação de Auditoria Interna 36

Parceiros da Fundação de Auditoria Interna 37

Fundação Latino-Americana de Auditores Internos (FLAI) 38

O IIA 39



RESUMO EXECUTIVO

Da consciência dos riscos à ação estratégica de Auditoria

O cenário de riscos da América Latina não é mais definido por ameaças isoladas. Cibersegurança, disrupção digital, incerteza geopolítica, fraude, talentos, regulação e liquidez agora operam como um sistema de riscos interconectado. O desafio para os chefes executivos de auditoria é transformar essa conscientização em cobertura de auditoria, insights consultivos e ações no âmbito do conselho.

Os resultados do Risk in Focus 2026/2027 para a América Latina mostram uma região que enfrenta um cenário de riscos mais digital, volátil e interconectado. A cibersegurança continua sendo a preocupação dominante, selecionada por 80% dos respondentes como um dos cinco principais riscos e classificada como alta por 82%.

No entanto, o ponto mais relevante é a velocidade e a amplitude da mudança ao seu redor.

A disrupção digital, incluindo a inteligência artificial, é agora o segundo maior risco entre os cinco principais, com 61%, enquanto 75% a classificaram como alta. A incerteza geopolítica/macroeconômica vem logo atrás, selecionada como um dos cinco principais riscos por 52% e classificada como alta por 71%.

Cinco conclusões se destacam nesta pesquisa:

- A cibersegurança tornou-se uma questão de resiliência dos negócios e confiança. Os participantes dos painéis regionais descreveram o risco cibernético não apenas como um risco tecnológico, mas também como um risco para as operações, infraestrutura crítica, confiança do cliente, reputação, conformidade regulatória e capacidade de recuperação.
- A disrupção digital está se acelerando mais rapidamente do que a governança. A IA, a automação, os bots, as ferramentas low-code, os serviços em nuvem e a análise de dados estão transformando os processos de negócios mais rapidamente do que muitas organizações conseguem atualizar seus controles, políticas, competências e estruturas de responsabilização.
- A incerteza geopolítica e macroeconômica deve ser traduzida em impactos relevantes para a auditoria. Para a América Latina, esse risco se manifesta por meio das cadeias de suprimentos, da taxa de câmbio, dos preços dos combustíveis, da localização na nuvem, das mudanças regulatórias, das operações transfronteiriças, da infraestrutura pública e da continuidade dos negócios.
- As prioridades da auditoria interna permanecem mais tradicionais do que o próprio panorama de riscos. Cibersegurança, fraude, riscos financeiros/de liquidez, mudanças regulatórias e disrupção digital são as cinco principais prioridades de auditoria. No entanto, permanecem lacunas significativas relacionadas à incerteza geopolítica/macroeconômica, às mudanças de mercado, ao clima/meio ambiente, ao capital humano, à cultura e à disrupção digital, quando comparadas ao nível de risco e à maturidade da governança.
- A maturidade e a cobertura representam a próxima fronteira. A disrupção digital apresenta o menor nível de maturidade na governança de riscos, embora seja um dos riscos mais elevados. Também apresenta o menor nível de cobertura integral por parte da auditoria interna. Essa discrepância constitui um chamado à ação para os Chefes Executivos de Auditoria.

A principal mensagem para os Chefes Executivos de Auditoria é clara: a profissão não pode depender apenas de programas de auditoria já conhecidos e de categorias de risco tradicionais. Os Chefes Executivos de Auditoria devem ajudar os conselhos de administração e as equipes executivas a compreender como os riscos emergentes se conectam à estratégia, às operações, às pessoas, à tecnologia, à fraude, à regulamentação e à resiliência. Em 2027, as principais funções de auditoria interna não serão definidas pelo número de auditorias realizadas, mas pela sua capacidade de direcionar recursos escassos para os riscos que possam afetar de forma mais significativa o valor da organização.

PARTICIPAÇÃO NA PESQUISA – AMÉRICA LATINA

512 respostas à pesquisa

18 países/locais

2 mesas-redondas com **23** participantes

4 entrevistas em profundidade

AUTOR DO RELATÓRIO

Renato Trisciuzzi, CIA, QIAL, CCSA, CRMA, M.Sc., Ph.D.

PARCEIRO DE PESQUISA

Fundación Latinoamericana de Auditores Internos

1 AMBIENTE DE RISCOS

Um cenário de riscos mais conectado e menos tolerante

Os resultados do Risk in Focus de 2026/2027 para a América Latina mostram uma clara concentração de preocupação em torno de três riscos: cibersegurança, disrupção digital e incerteza geopolítica/macroeconômica.

Esses riscos não são novos, mas as conversas com líderes de auditoria em toda a região sugerem que os fatores que os impulsionam mudaram. A cibersegurança não é mais vista apenas como um risco de TI. A disrupção digital não está mais limitada à estratégia de tecnologia. A incerteza geopolítica não é mais um risco externo distante. Cada um deles agora tem implicações diretas para as operações, a governança, a resiliência, a conformidade, a fraude, a reputação e a gestão de talentos.

Risco de cibersegurança

Conforme mostrado na Figura 1.1, a cibersegurança é, de longe, o risco mais significativo. Foi escolhido como um dos cinco principais riscos por 80% dos respondentes e classificado como um risco elevado por 82% deles. Isso confirma que a cibersegurança continua sendo o risco determinante para os conselhos de administração, a diretoria executiva e a auditoria interna na região. Os participantes da mesa-redonda descreveram um ambiente de risco onde as ameaças cibernéticas estão se tornando mais sofisticadas, mais frequentes e mais intimamente ligadas à fraude, identidade, proteção de dados, tecnologia operacional e continuidade de negócios. A IA pode melhorar a defesa, mas também melhora a capacidade de ataque. Os fraudadores podem automatizar o phishing, criar identidades sintéticas, imitar vozes, gerar mensagens realistas e explorar vulnerabilidades com mais rapidez.

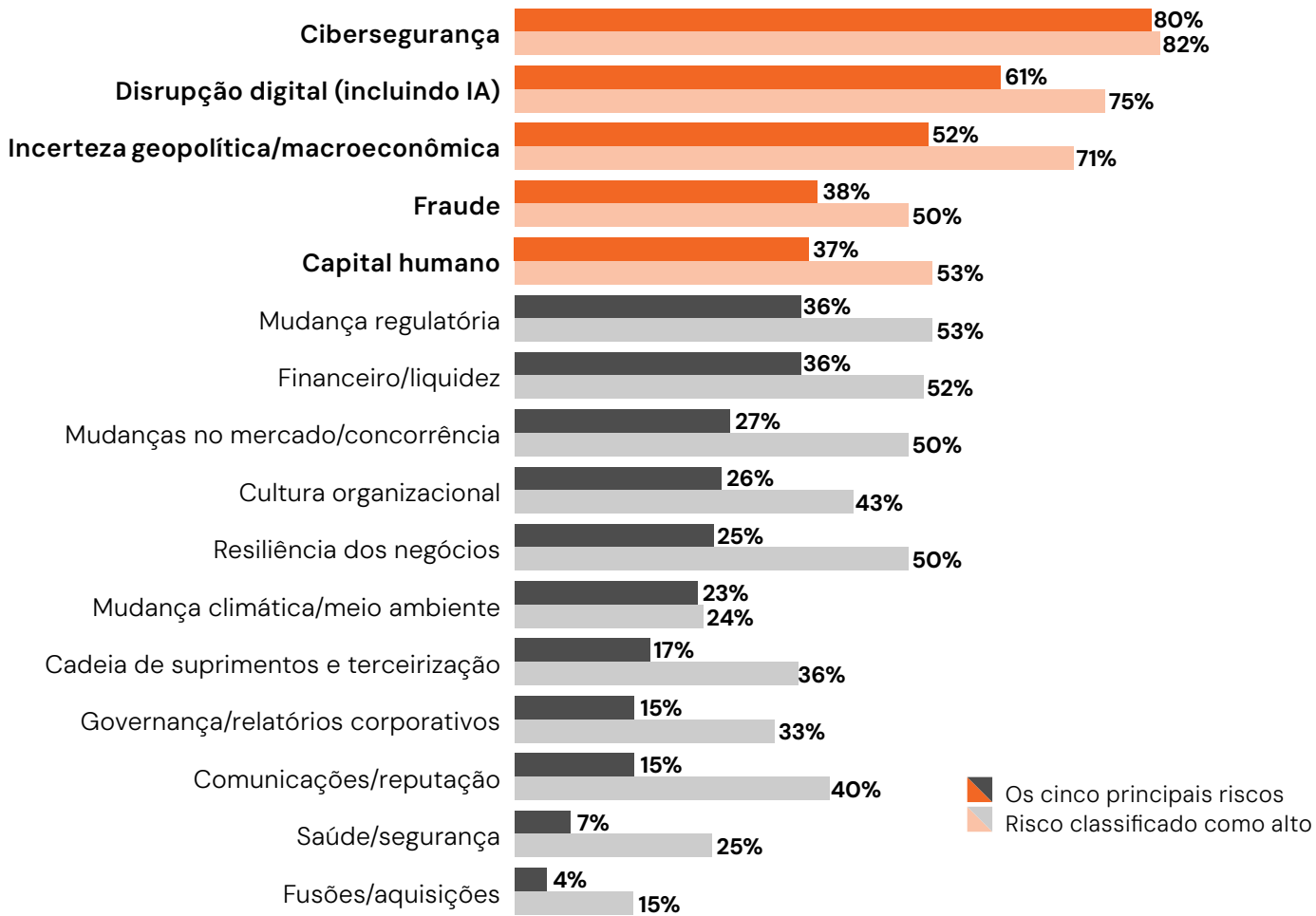
Para muitas organizações, o perímetro de risco cibernético se expandiu. Agora inclui ambientes em nuvem, provedores de tecnologia terceirizados, automação industrial, canais digitais, aplicativos móveis, acesso remoto, data lakes, ferramentas de inteligência artificial e tecnologia operacional.

Ao mesmo tempo, as considerações de risco de cibersegurança precisam ir além das operações tradicionais de tecnologia da informação. Por exemplo, um participante da mesa-redonda descreveu o desafio da cibersegurança para operações industriais altamente automatizadas, onde a tecnologia de produção evoluiu ao longo de muitos anos, mas os controles de segurança não acompanharam o mesmo ritmo. Esse é um sinal importante para os Chefes Executivos de Auditoria: o risco cibernético não deve ser avaliado apenas por meio da TI corporativa. Isso também deve ser avaliado por meio de operações, terceiros, produtos digitais, canais de clientes e infraestrutura crítica.

A cibersegurança continuou a dominar os rankings de risco, com **80%** dos Chefes Executivos de Auditoria da América Latina classificando-a como um dos seus cinco principais riscos.

Figura 1.1. América Latina – Os cinco Principais Riscos vs. Severidade de Risco Alto

Pergunta 1 da pesquisa: Quais são os cinco principais riscos que sua organização enfrenta atualmente? (Escolha 5.)
Pergunta 2 da pesquisa: Em uma escala de 1 a 7, classifique o nível atual de risco em sua organização para cada uma das seguintes áreas de risco.



Como interpretar o gráfico
As cores escuras mostram quem escolheu o risco como um dos 5 maiores em sua organização (Os 5 principais riscos).
As cores claras mostram quem classificou o risco como 5, 6 ou 7 em uma escala de 1 a 7 (alta gravidade do risco).
O laranja indica as cinco classificações mais altas para ambas as medidas de risco.

Nota: Pesquisa Risk in Focus, realizada online em todo o mundo de 2 de março a 6 de maio de 2026. n = 512 para a América Latina.

AMBIENTE DE RISCO

Risco de disrupção digital

A disrupção digital, incluindo a IA, é o segundo maior risco entre os cinco principais, escolhida por 61% dos respondentes e classificada como "alta" por 75% deles. Além disso, o risco de disrupção digital aumentou substancialmente em comparação com o ano anterior (Figura 1.2). Essa pode ser a mudança mais importante no cenário de riscos da América Latina.

As oportunidades criadas pela IA são significativas: automação, produtividade, análise de dados, experiência do cliente, detecção de fraudes e apoio à tomada de decisões. Mas o risco é igualmente significativo: resultados imprecisos, modelos tendenciosos, vazamento de dados, vulnerabilidades cibernéticas, uso de IA sem aprovação ou supervisão formal da organização (shadow AI), violações regulatórias, exposição da propriedade intelectual e falta de clareza na responsabilização.

A questão não é se as organizações devem adotar novas tecnologias. Em muitos setores, a pressão competitiva para adotar a IA e as ferramentas digitais já é inevitável. A questão é se as organizações conseguem adotá-las com governança, responsabilidade, transparência, resiliência e controle suficientes. Os respondentes observaram que os executivos reconhecem cada vez mais a importância da transformação digital, mas as pressões operacionais do dia a dia muitas vezes atrasam a ação. Isso cria uma lacuna entre a conscientização dos riscos e a resposta a eles.

A maturidade da governança organizacional para IA varia. Algumas organizações estão criando comitês de IA, modelos de governança, políticas, processos de aprovação e controles de dados. Outras ainda estão descobrindo que as unidades de negócios já adotaram ferramentas de IA sem uma governança formal. Para a auditoria interna, o avanço global da IA significa que as metodologias de auditoria devem evoluir rapidamente.

Os auditores precisam de critérios para avaliar a governança da IA, mas também de formas práticas para testar os controles relacionados a dados, acesso, monitoramento, gestão de fornecedores, resultados dos modelos e supervisão humana.

Risco de incerteza geopolítica

A incerteza geopolítica/macroeconômica ocupa o terceiro lugar, sendo selecionada por 52% como um dos cinco principais riscos e classificada como alta por 71%. Em comparação com o ano passado, o risco de incerteza geopolítica aumentou substancialmente, provavelmente devido, em parte, ao conflito que começou em 28 de fevereiro de 2026, quando os EUA e Israel iniciaram um ataque conjunto contra o Irã. A incerteza geopolítica empatou com a disrupção digital como um dos dois riscos de crescimento mais rápido na região (Figura 1.2).

Nos anos anteriores, a incerteza geopolítica era frequentemente discutida como um risco externo de caráter geral. Este ano, as discussões foram mais práticas e específicas. O risco geopolítico na América Latina deve ser analisado tanto sob a ótica externa quanto doméstica. Entre os fatores externos estão a política comercial, as tarifas, os conflitos armados, a regulamentação transfronteiriça, os preços das commodities e as dependências tecnológicas globais. Entre os fatores internos estão os ciclos eleitorais, a estabilidade institucional, as mudanças na política econômica, as decisões fiscais, a agitação social e as mudanças no papel do Estado na economia. Ambos os tipos de fatores podem afetar as taxas de juros, o apetite por investimentos, a liquidez, o mercado de câmbio, as agendas regulatórias e a continuidade operacional. Em outras palavras, o risco geopolítico torna-se relevante para a auditoria quando se traduz em impactos de negócios específicos.

"Os riscos mais relevantes na América Latina não são mais isolados. Cibersegurança, IA, fraude, liquidez, talento e geopolítica agora fazem parte da mesma discussão sobre riscos."

– Renato Trisciuzzi, Brasil

Figura 1.2. América Latina – Tendência dos cinco principais riscos

Pergunta da pesquisa: Quais são os cinco principais riscos que sua organização enfrenta atualmente? (Escolha 5.)

2023	2024	2025	2026	Variação de 2025 para 2026	Variação	Áreas de risco
75%	**74%**	**76%**	**80%**		**+4**	**Cibersegurança**
38%	**37%**	**54%**	**61%**		**+7**	**Disrupção digital (incluindo IA)**
42%	**37%**	**45%**	**52%**		**+7**	**Incerteza geopolítica/macroeconômica**
30%	**32%**	**32%**	**38%**		**+6**	**Fraude**
44%	46%	40%	37%		-3	Capital humano
48%	45%	49%	36%		-13	Mudança regulatória
33%	**33%**	**32%**	**36%**		**+4**	**Financeiro/liquidez**
26%	26%	24%	27%		+3	Mudanças no mercado/concorrência
26%	28%	28%	26%		-2	Cultura organizacional
47%	49%	35%	25%		-10	Resiliência dos negócios
22%	29%	25%	23%		-2	Mudança climática/meio ambiente
16%	17%	15%	17%		+2	Cadeia de suprimentos e terceirização
18%	18%	16%	15%		-1	Governança/relatórios corporativos
22%	17%	19%	15%		-4	Comunicações/reputação
8%	9%	6%	7%		+1	Saúde/segurança
3%	4%	5%	4%		-1	Fusões/aquisições

Aumento de risco em relação ao ano anterior Redução de risco em relação ao ano anterior

Como interpretar o gráfico
O laranja indica um aumento de 4 pontos percentuais ou mais em relação ao ano anterior. As barras laranja e azul mostram a diferença nas avaliações de 2025 para 2026. A coluna identificada como "variação" mostra a diferença em pontos percentuais de 2025 para 2026.

Nota: Pesquisa Risk in Focus realizada online em todo o mundo entre 2 de março e 6 de maio de 2026. n = 512 para a América Latina.

AMBIENTE DE RISCO

No setor aéreo, a incerteza geopolítica pode afetar rotas, acesso a aeroportos, autorizações regulatórias, preços dos combustíveis, impostos e a demanda dos passageiros. Nos serviços financeiros, pode afetar a liquidez, o risco de crédito, a fraude, os ataques cibernéticos, a regulamentação e o comportamento do cliente. Na saúde e seguros, pode afetar medicamentos, insumos médicos, equipamentos, logística e planos de continuidade. No setor público e infraestrutura crítica, pode afetar a prestação de serviços, a resiliência nacional, a confiança pública e a capacidade de resposta.

Os participantes da mesa-redonda enfatizaram que o risco geopolítico é frequentemente sentido por meio de consequências operacionais. Essas consequências diferem por setor, mas o papel do Chefe executivo de auditoria é semelhante: ajudar a administração e o conselho a compreender cenários, dependências, pontos de gatilho e planos de resposta.

Risco de fraude

A fraude foi selecionada como um dos cinco principais riscos por 38% e classificada como alta por 50%. Esse resultado deve ser lido em conjunto com a cibersegurança, a disrupção digital, a pressão macroeconômica e o capital humano.

O risco de fraude é cada vez mais facilitado por canais digitais, manipulação de identidade, engenharia social, violações cibernéticas, estresse econômico, terceiros e governança de dados deficiente. O crescimento da IA também introduz novos cenários de fraude, incluindo identidades sintéticas, deepfakes, phishing automatizado, manipulação de comandos (prompts) e exploração mais rápida de vulnerabilidades. A fronteira entre o risco cibernético e o risco de fraude está se tornando cada vez menos clara. Para os Chefes Executivos de Auditoria, isso significa que os planos de auditoria cibernética e de fraude devem ser coordenados. A identidade digital, a gestão de acesso, o monitoramento de transações, a resposta a incidentes e a comunicação com o cliente devem ser avaliados em conjunto.

O risco de fraude na América Latina também possui uma forte relação com o risco financeiro/de liquidez e com a pressão macroeconômica. A volatilidade econômica pode aumentar os incentivos e as oportunidades para fraudes. O estresse de liquidez pode enfraquecer a disciplina de controle. A inflação pode alterar o comportamento nas compras, o risco de estoque, as decisões de preços e a qualidade de crédito do cliente. As organizações do setor público podem enfrentar pressões adicionais relacionadas à transparência, à continuidade dos serviços e à confiança pública.

Capital humano, mudanças regulatórias, risco financeiro/de liquidez

O capital humano, as mudanças regulatórias e o risco financeiro/de liquidez constituem a próxima camada de preocupações. O capital humano foi apontado como um dos cinco principais riscos por 37% e classificado como de alto risco por 53%. A mudança regulatória foi selecionada como um dos cinco principais riscos por 36% e classificada como alta por 53%. O risco financeiro/de liquidez foi selecionado como um dos cinco principais por 36% dos respondentes e classificado como alto por 52%. O capital humano também deve ser analisado sob uma perspectiva geopolítica e macroeconômica. Em economias em desenvolvimento, profissionais altamente qualificados em cibersegurança, dados, automação, inteligência artificial, finanças e gestão de riscos podem ter oportunidades em mercados globais maiores ou por meio de trabalho remoto para organizações fora da região. Esse movimento pode aprofundar as lacunas de capacidade para as organizações latino-americanas. Para os CEOs e conselhos de administração, a fuga de talentos não é apenas um problema de RH; ela pode afetar a execução da transformação, a resiliência cibernética, a conformidade, a inovação e a capacidade de auditoria interna.

Uma rede de riscos complexa

Estes resultados mostram que a região não está mudando de “riscos antigos” para “novos riscos”. Em vez disso, os riscos tradicionais e emergentes estão se tornando mais conectados, criando uma rede de riscos complexa, com implicações para a organização como um todo. A disrupção digital exige novos talentos. A cibersegurança exige investimentos. A incerteza geopolítica pode desencadear mudanças regulatórias. O estresse financeiro pode aumentar as fraudes. As lacunas de talento podem limitar a capacidade da organização de se transformar.



Figura 1.3. América Latina – Os cinco principais riscos por setor

Pergunta da pesquisa: Quais são os cinco principais riscos que sua organização enfrenta atualmente? (Escolha 5.)

Áreas de risco	Toda a América Latina	Serviços financeiros	Setor público	De capital fechado	Com capital aberto
Cibersegurança	**80%**	**88%**	**70%**	**78%**	**79%**
Disrupção digital (incluindo IA)	**61%**	**74%**	43%	**62%**	**55%**
Incerteza geopolítica/macroeconômica	**52%**	**52%**	40%	**53%**	**69%**
Fraude	**38%**	41%	**46%**	32%	33%
Capital humano	**37%**	32%	**46%**	**39%**	36%
Mudança regulatória	36%	**43%**	**47%**	29%	19%
Financeiro/liquidez	36%	**42%**	21%	35%	**38%**
Mudanças no mercado/concorrência	27%	24%	11%	**37%**	**38%**
Cultura organizacional	26%	17%	**46%**	27%	12%
Resiliência de negócios	25%	28%	23%	23%	26%
Mudança climática/meio ambiente	23%	20%	21%	27%	26%
Cadeia de suprimentos e terceirização	17%	13%	10%	23%	33%
Governança/relatórios corporativos	15%	10%	32%	11%	12%
Comunicações/reputação	15%	12%	28%	11%	10%
Saúde/segurança	7%	2%	7%	11%	10%
Fusões/aquisições	4%	2%	10%	3%	5%

Os 5 maiores riscos

Nota: Pesquisa Risk in Focus, realizada online em todo o mundo entre 2 de março e 6 de maio de 2026. n = 512 para a América Latina.

AMBIENTE DE RISCO

Diferenças setoriais

As diferenças setoriais são um fator importante para a compreensão da "rede de riscos" de uma organização, conforme ilustrado na Figura 1.3.

- Em todos os setores, a cibersegurança continua sendo um risco comum, mas a exposição a ela varia. No setor de serviços financeiros, a cibersegurança e a disrupção digital estão estreitamente conectadas à identidade digital, à fraude, à segurança de dados, à confiança do cliente, à resiliência e às expectativas regulatórias. No entanto, a cibersegurança da tecnologia operacional (TO) está se tornando cada vez mais relevante nos setores de manufatura, alimentos e bebidas, celulose e papel, mineração, energia, petróleo e gás, serviços públicos e outros ambientes industriais, onde um incidente cibernético pode interromper a produção, comprometer a segurança, afetar a infraestrutura crítica ou interromper a prestação de serviços.
- Em empresas de capital aberto, a incerteza geopolítica/macroeconômica e as mudanças de mercado são mais proeminentes.
- Em empresas de capital fechado, a disrupção digital, a incerteza macroeconômica, o capital humano e a concorrência no mercado surgem como preocupações estratégicas significativas.
- No setor público, o perfil de risco distribui-se por uma ampla gama de áreas de risco, com destaque para a cibersegurança, mudanças regulatórias, fraude e capital humano; mas o risco também é elevado para disrupção digital, incerteza geopolítica e governança.

Riscos de mudança climática/meio ambiente

A mudança climática/meio ambiente é selecionada como um dos cinco principais riscos por 23% dos respondentes, e apenas 24% o classificaram como alto. Essa classificação regional relativamente baixa deve ser interpretada com cautela. Em muitas organizações latino-americanas, os riscos climáticos e ambientais competem com pressões mais imediatas, incluindo crescimento econômico, inflação, liquidez, segurança, infraestrutura, emprego e mudanças regulatórias. A exposição também varia significativamente por país, região geográfica e setor. Para alguns setores, como energia, agricultura, transporte, infraestrutura pública, seguros, mineração, indústria e governo, o risco climático e ambiental pode ser severo. No entanto, em outras organizações, o risco pode ainda não ter sido totalmente traduzido em impactos operacionais, financeiros, de conformidade, de seguros, de proteção de ativos, da cadeia de suprimentos ou de resiliência. Para os Chefes Executivos de Auditoria, a questão fundamental não é se o risco climático é alto para todas as organizações, mas se ele é avaliado adequadamente nos casos onde a exposição é significativa.

Riscos de comunicação/reputação

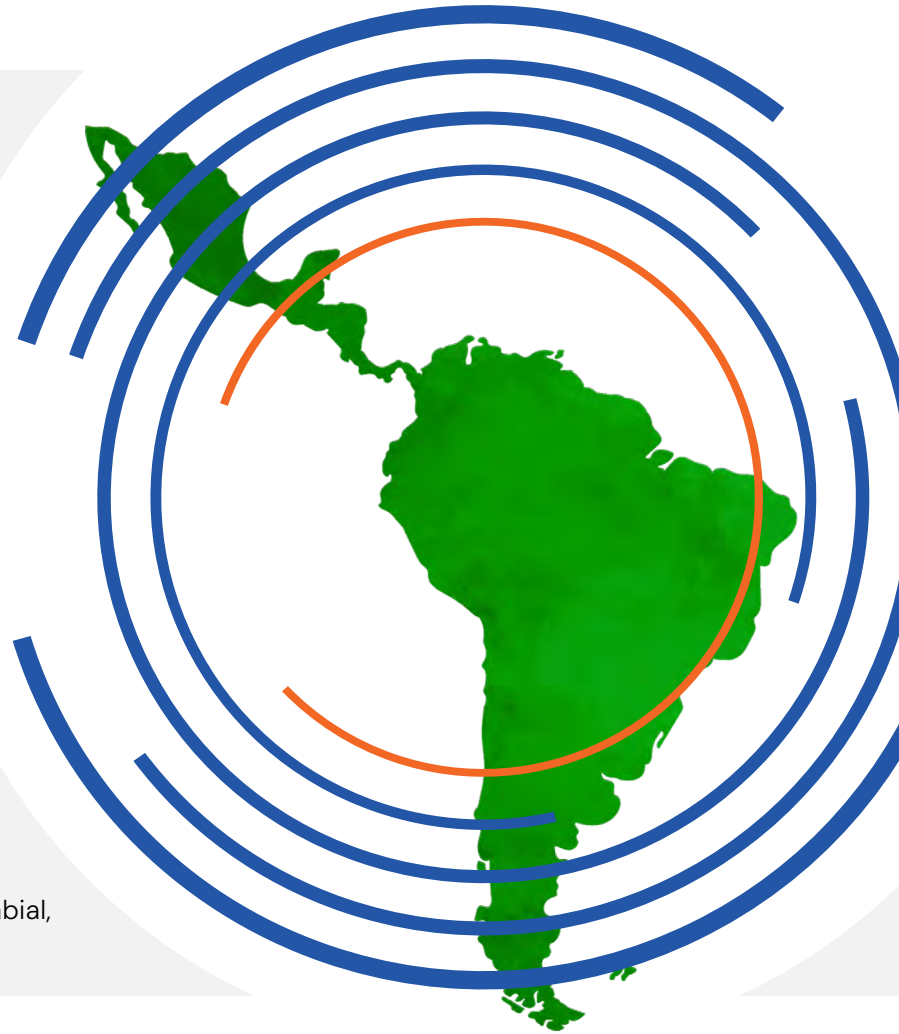
A comunicação/reputação é selecionada como um dos cinco principais riscos por apenas 15%, mas é classificada como alta por 40%. Essa lacuna merece atenção. A reputação pode nem sempre aparecer como uma categoria independente no universo de uma auditoria, mas frequentemente é a consequência de falhas em cibersegurança, fraude, segurança, experiência do cliente, regulamentação, ética, ESG e continuidade operacional. Para bancos digitais, fintechs, companhias aéreas, serviços públicos e empresas do setor de consumo, o dano reputacional pode se materializar rapidamente e se espalhar pelas redes sociais antes que a administração tenha tempo de responder.

Resumo

A tendência geral é clara: O ambiente de riscos da América Latina está mudando da gestão de riscos isolados para a gestão de riscos conectados. Os riscos mais altos não devem ser auditados como silos separados. A cibersegurança, a inteligência artificial, a fraude, os talentos, os terceiros, a liquidez, a regulamentação, a continuidade e a reputação devem ser avaliados em conjunto, porque os eventos que causam os maiores danos frequentemente combinam vários desses riscos.

O ambiente de riscos da América Latina está mudando da gestão de riscos isolados para a gestão de riscos conectados.

PONTOS PRINCIPAIS



Conclusões da pesquisa

- A cibersegurança continua sendo o principal risco na América Latina, mas a tendência mais ampla é a convergência de tecnologia, incerteza macroeconômica, fraude, regulamentação e capital humano.
- A disrupção digital e a IA estão se tornando áreas de alto risco, pois a adoção dessas tecnologias está avançando mais rapidamente do que a governança.
- A incerteza geopolítica/macroeconômica é alta porque não é mais abstrata; ela afeta as cadeias de suprimentos, a estratégia de nuvem, o câmbio, os combustíveis, a liquidez, a regulamentação e a continuidade.

Estratégias de auditoria interna

- Os Chefes Executivos de Auditoria devem atualizar o universo de auditoria para refletir riscos conectados, em vez de categorias isoladas.
- As auditorias de cibersegurança devem incluir nuvem, terceiros, tecnologia operacional, proteção de dados, resiliência e recuperação de incidentes.
- A disrupção digital deve ser avaliada por meio da governança de IA, qualidade dos dados, risco de modelo, controles de automação, uso ético e prestação de contas.
- O risco geopolítico deve ser traduzido em cenários auditáveis, tais como interrupção de suprimentos, teste de estresse de liquidez, mudanças regulatórias, exposição cambial, dependência de infraestrutura crítica e continuidade de negócios.

2 PRIORIDADES DE AUDITORIA INTERNA

A lacuna de cobertura: Quando o risco se move mais rápido do que os planos de auditoria

Os resultados da pesquisa sobre as prioridades da auditoria interna mostram que os Chefes Executivos de Auditoria da América Latina estão se adaptando ao panorama de riscos, mas nem sempre com a mesma velocidade ou intensidade com que os níveis de risco estão mudando.

A Figura 2.1 mostra que a cibersegurança representa tanto o maior risco quanto a maior prioridade de auditoria. Foi selecionada como uma das cinco principais prioridades de auditoria por 74% dos respondentes. Esse alinhamento é adequado e esperado. No entanto, a constatação mais importante está nas discrepâncias entre as áreas de alto risco e os níveis mais baixos de esforço da auditoria interna.

Fraude, questões financeiras/de liquidez, mudanças regulatórias e disrupção digital completam as cinco principais prioridades de auditoria na América Latina. A fraude foi escolhida como uma das cinco principais prioridades de auditoria por 56% dos respondentes; as questões financeiras e de liquidez, por 53%; as mudanças regulatórias, por 53%; e a disrupção digital, por 47%. Esses resultados mostram que as funções de auditoria interna continuam a dedicar esforços significativos a riscos que são conhecidos, mensuráveis, regulamentados e que, tradicionalmente, estão dentro da zona de conforto da auditoria interna.

Disrupção digital como prioridade de auditoria

O aumento da importância da disrupção digital como prioridade de auditoria é encorajador, representando o maior crescimento no volume de trabalho entre todas as áreas de auditoria analisadas na pesquisa (Figura 2.2). No entanto, sua prioridade continua abaixo do seu nível de risco. A disrupção digital foi apontada como um dos cinco principais riscos por 61% dos respondentes, mas como prioridade de auditoria por 47%. Essa disparidade se torna ainda mais acentuada quando analisada em conjunto com os dados sobre maturidade e cobertura apresentados na Seção 3.
A disrupção digital é um dos maiores riscos, mas também uma das áreas com menor maturidade em governança e menor cobertura de auditoria. Essa é uma das principais conclusões do relatório.

Os participantes da mesa-redonda e os respondentes apresentaram várias explicações. Em primeiro lugar, algumas organizações reconhecem a disrupção digital como algo estrategicamente importante, mas as pressões operacionais dominam a tomada de decisões no dia a dia. No varejo, por exemplo, os executivos precisam continuar gerenciando vendas, caixa, logística, perdas, margens e experiência do cliente, ao mesmo tempo em que transformam processos e tecnologia. Como descreveu Magy Fuentes, o desafio é "atuar e transformar" ao mesmo tempo.

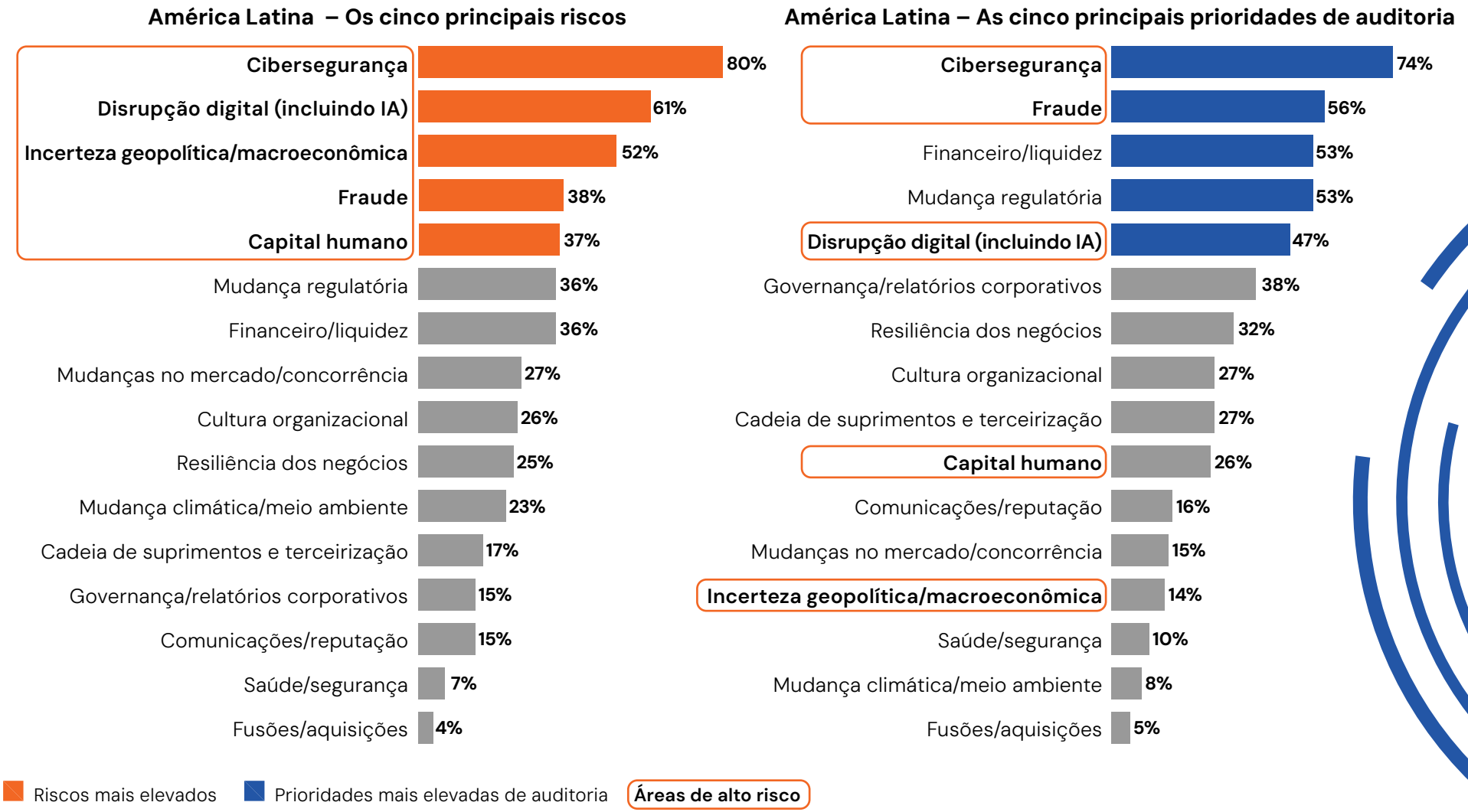
A disrupção digital obteve uma pontuação alta em termos de risco (**61%**), mas relativamente baixa em termos de prioridade de auditoria (**47%**). Além disso, é uma das áreas com menor nível de maturidade em governança e cobertura completa de auditoria.

"A transformação digital e a cibersegurança são claramente reconhecidas como temas relevantes. O desafio é que, em muitas organizações, elas ainda são mais uma preocupação do que uma ocupação."

– Magy Fuentes, Argentina

Figura 2.1. América Latina – Os cinco principais riscos vs. As cinco principais prioridades de auditoria

Pergunta 1 da pesquisa: Quais são os cinco principais riscos que sua organização enfrenta atualmente? (Escolha 5.)
Pergunta 2 da pesquisa: Quais são as cinco principais áreas de auditoria nas quais a auditoria interna gasta mais tempo e esforço? (Escolha 5.)



Nota: Pesquisa Risk in Focus, realizada on-line em todo o mundo de 2 de março a 6 de maio de 2026. n = 512 para a América Latina.

Em segundo lugar, algumas equipes de auditoria interna não possuem as competências necessárias para auditar IA, nuvem, automação, governança de dados, algoritmos, segurança cibernética, tecnologia operacional ou produtos digitais. Isso não é apenas um problema de pessoal. Trata-se também de um problema de metodologia. Os programas tradicionais de auditoria podem não ser suficientes para avaliar o desenvolvimento ágil, modelos de aprendizado de máquina, bots, agentes de IA, linhagem de dados, identidade digital, resiliência na nuvem ou ecossistemas de plataformas. Os Chefes Executivos de Auditoria devem considerar a criação ou a manutenção de competências multidisciplinares dentro da função de auditoria interna, incluindo tecnologia da informação, cibersegurança, automação, análise de dados, inteligência artificial, tecnologia operacional, processos e conhecimento especializado em negócios. Nos casos em que não for viável contar com uma equipe permanente, pode ser necessário estabelecer acordos permanentes de co-sourcing ou ter acesso a especialistas em áreas específicas. Mesmo sob pressão para realizar auditorias tradicionais, os Chefes Executivos de Auditoria devem reservar espaço específico no plano anual de auditoria para riscos emergentes por meio de trabalhos de avaliação direcionados, avaliações de prontidão, análises consultivas, monitoramento contínuo ou auditorias-piloto.

Em terceiro lugar, alguns Chefes Executivos de Auditoria podem permanecer próximos demais daquilo que lhes é familiar. Os respondentes foram sinceros ao falar sobre a zona de conforto da profissão. A auditoria nas áreas de finanças, conformidade, compras, folha de pagamento ou relatórios regulatórios pode ser mais simples, pois os critérios são mais claros e as equipes possuem experiência. A auditoria da cultura, da inovação, da transformação digital, da exposição geopolítica ou da resiliência estratégica exige mais discernimento, mais colaboração e mais disposição para lidar com a ambiguidade.

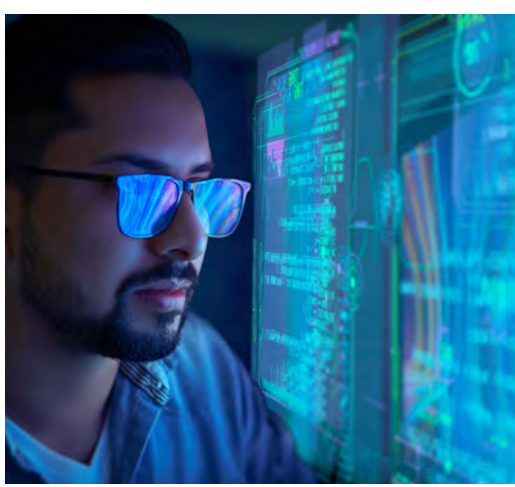
A incerteza geopolítica como prioridade de auditoria

A incerteza geopolítica/macroeconômica representa a maior discrepância entre risco e prioridade de auditoria. Esse risco foi selecionado como um dos cinco principais riscos por 52%, mas apenas 14% o selecionaram como uma das cinco principais prioridades de auditoria. À primeira vista, isso pode parecer uma cobertura insuficiente. Na prática, a questão é mais sutil. É difícil avaliar diretamente o risco geopolítico. A auditoria interna não pode auditar uma guerra, uma eleição, a inflação, um conflito diplomático ou a volatilidade do mercado de commodities. No entanto, a auditoria interna pode avaliar como a organização antecipa, monitora, encaminha para instâncias superiores e responde ao impacto dessas condições no ambiente de risco externo.

Isso significa que os Chefes Executivos de Auditoria não devem necessariamente criar uma auditoria denominada "risco geopolítico". Em vez disso, eles podem incorporar cenários geopolíticos e macroeconômicos às áreas de auditoria já existentes na organização, tais como cadeia de suprimentos, liquidez, tesouraria, planejamento estratégico, continuidade de negócios, conformidade regulatória, risco de terceiros, concentração em nuvem, gestão de crises e expansão de mercado. Por exemplo, uma empresa de fintech pode traduzir o risco geopolítico em estratégia de dependência da nuvem e de recuperação. Uma companhia aérea pode interpretar isso em termos de acesso aos aeroportos, autorizações de rotas, exposição cambial e preços do combustível. Uma organização da área da saúde ou de seguros pode interpretar isso como continuidade no fornecimento de produtos médicos.

"O risco geopolítico se torna real quando afeta medicamentos, suprimentos médicos, equipamentos, logística e a continuidade operacional."

– José Luis Fernández García, Chile



PRIORIDADES DE AUDITORIA INTERNA

Figura 2.2. América Latina – Tendência das cinco principais prioridades de auditoria

Pergunta da pesquisa: Quais são as cinco principais áreas de auditoria nas quais a auditoria interna gasta mais tempo e esforço? (Escolha 5.)

2023	2024	2025	2026	Variação de 2025 a 2026	Variação	Áreas de auditoria
66%	67%	69%	74%		+5	**Cibersegurança**
47%	52%	51%	56%		+5	**Fraude**
50%	49%	51%	53%		+2	Financeiro/liquidez
50%	47%	53%	53%		0	Mudança regulatória
24%	19%	29%	47%		+18	**Disrupção digital (incluindo IA)**
46%	46%	48%	38%		-10	Governança/relatórios corporativos
53%	49%	40%	32%		-8	Resiliência dos negócios
29%	30%	29%	27%		-2	Cultura organizacional
28%	29%	24%	27%		+3	Cadeia de suprimentos e terceirização
28%	29%	27%	26%		-1	Capital humano
23%	22%	20%	16%		-4	Comunicações/reputação
17%	17%	16%	15%		-1	Mudanças no mercado/concorrência
13%	12%	16%	14%		-2	Incerteza geopolítica e macroeconômica
12%	14%	12%	10%		-2	Saúde/segurança
8%	11%	9%	8%		-1	Mudança climática/meio ambiente
5%	7%	6%	5%		-1	Fusões/aquisições

Aumento da prioridade de auditoria em relação ao ano anterior Diminuição da prioridade de auditoria em relação ao ano anterior

Como interpretar o gráfico
Laranja indica um aumento de 4 pontos percentuais ou mais em relação ao ano anterior. As barras laranja e azul mostram a diferença nas classificações de 2025 para 2026. A coluna intitulada "variação" mostra a diferença em pontos percentuais entre 2025 e 2026.

Nota: Pesquisa Risk in Focus, realizada online em todo o mundo entre 2 de março e 6 de maio de 2026. n = 512 para a América Latina.

PRIORIDADES DE AUDITORIA INTERNA

Capital humano como prioridade de auditoria

O capital humano é outra área em que se observa uma lacuna significativa. Foi selecionado como um dos cinco principais riscos por 37%, mas apenas 26% o selecionaram como uma das cinco principais prioridades de auditoria. Isso é compreensível, pois o capital humano pode ser difícil de avaliar além dos processos tradicionais de RH. No entanto, as entrevistas indicam que a disponibilidade de talentos é um fator essencial para a gestão de praticamente todas as demais categorias de risco. Sem os talentos certos, as organizações não conseguem gerenciar a IA, proteger-se contra ameaças cibernéticas, implementar transformações, manter controles, cumprir as regulamentações, detectar fraudes nem construir operações resilientes.

A auditoria interna deve, portanto, ampliar sua visão sobre o capital humano. Não se trata apenas de rotatividade, recrutamento, treinamento ou sucessão. Trata-se também de capacidade estratégica. A organização possui as competências necessárias para executar sua estratégia? As funções essenciais foram identificadas? As capacidades nas áreas digital, cibernética, de dados e de risco são suficientes? A transferência de conhecimento e os planos de sucessão são eficazes? Os incentivos estão alinhados com o comportamento ético e a assunção prudente de riscos? A cultura e os comportamentos de liderança estão promovendo a conscientização sobre os riscos?

Mudanças de mercado/concorrência como prioridade de auditoria

As mudanças no mercado/concorrência foram apontadas como um dos cinco principais riscos por 27%, mas apenas 15% as selecionaram como uma das cinco principais prioridades de auditoria. Essa lacuna pode refletir outra limitação tradicional: a auditoria interna costuma se concentrar mais nos processos internos do que na dinâmica do mercado externo. No entanto, o risco de mercado pode afetar os preços, o comportamento dos clientes, a qualidade de crédito, o estoque, o design dos produtos, os canais digitais, a liquidez e a execução da estratégia. Os Chefes Executivos de Auditoria devem avaliar se as mudanças no mercado são incorporadas às avaliações de risco estratégico e se a administração dispõe de mecanismos eficazes para monitorar e responder a essas mudanças.

Mudanças climáticas/meio ambiente como prioridade de auditoria

As mudanças climáticas e o meio ambiente apresentam um padrão semelhante. Essa área de risco foi selecionada como um dos cinco principais riscos por 23%, mas apenas 8% a escolheram como prioridade de auditoria. Para muitas organizações, isso pode ser adequado caso o risco de exposição seja baixo. No entanto, para organizações dos setores agrícola, energético, de mineração, de transportes, de seguros, de infraestrutura, do setor público e da indústria, a baixa prioridade de auditoria pode indicar a necessidade de uma reavaliação. O risco climático deve ser avaliado não apenas no contexto dos relatórios de sustentabilidade, mas também em termos de resiliência operacional, proteção de ativos, interrupções na cadeia de suprimentos, regulamentação, custo de seguros e impacto na comunidade.



Figura 2.3. América Latina – As cinco principais prioridades de auditoria por setor

Pergunta da pesquisa: Quais são as cinco principais áreas de auditoria nas quais a auditoria interna gasta mais tempo e esforço? (Escolha 5.)

Áreas de auditoria	Toda a América Latina	Serviços financeiros	Setor público	De capital fechado	De capital aberto
Cibersegurança	**74%**	**88%**	**52%**	**68%**	**83%**
Fraude	**56%**	**55%**	46%	**65%**	**55%**
Financeiro/liquidez	**53%**	**65%**	34%	**52%**	**38%**
Mudança regulatória	**53%**	**61%**	**62%**	**44%**	29%
Disrupção digital (incluindo IA)	**47%**	**58%**	38%	**42%**	**48%**
Governança/relatórios corporativos	38%	34%	**51%**	32%	**38%**
Resiliência dos negócios	32%	32%	26%	35%	**38%**
Cultura organizacional	27%	15%	**47%**	25%	26%
Cadeia de suprimentos e terceirização	27%	15%	13%	**42%**	**50%**
Capital humano	26%	21%	**48%**	22%	12%
Comunicações/reputação	16%	14%	29%	14%	7%
Mudanças no mercado/concorrência	15%	15%	10%	17%	14%
Incerteza geopolítica/macroeconômica	14%	17%	19%	12%	7%
Saúde/segurança	10%	2%	10%	17%	24%
Mudança climática/meio ambiente	8%	5%	8%	8%	24%
Fusões/aquisições	5%	2%	8%	5%	7%

As cinco principais prioridades de auditoria

Nota 1: Os empates pelo quinto lugar estão destacados em um tom mais claro.
Nota 2: Pesquisa Risk in Focus, realizada online em todo o mundo de 2 de março a 6 de maio de 2026. n = 512 para a América Latina.

PRIORIDADES DE AUDITORIA INTERNA

Diferenças setoriais

As diferenças setoriais mostram que os Chefes Executivos de Auditoria devem adaptar os planos de auditoria ao modelo operacional da organização (Figura 2.3).

A cibersegurança e a fraude costumam ser prioridades importantes da auditoria interna em todos os setores. No setor de serviços financeiros, questões como finanças/liquidez, mudanças regulatórias e disrupção digital também são prioridades importantes. As organizações de capital fechado e as de capital aberto atribuem maior prioridade aos riscos da cadeia de suprimentos, enquanto o setor público atribui prioridade substancialmente maior à governança, à cultura organizacional e ao capital humano.

A análise setorial reforça uma mensagem central: as auditorias internas não devem utilizar os rankings regionais de forma mecânica. Os rankings devem ser utilizados como uma ferramenta de desafio. Os Chefes Executivos de Auditoria devem comparar os resultados regionais com a avaliação de riscos, a estratégia, as expectativas das partes interessadas, o modelo operacional, a dinâmica do setor e o mapa de cobertura dos serviços de avaliação existente de sua organização. Os planos de auditoria também devem permanecer flexíveis. As condições geopolíticas, digitais, cibernéticas, de liquidez, regulatórias e de mercado podem mudar mais rapidamente do que o ciclo de planejamento anual. Os Chefes Executivos de Auditoria devem, portanto, incluir pontos formais de atualização no plano de auditoria e manter a capacidade de realocar recursos quando o perfil de risco se alterar. O conhecimento e a experiência do Chefe Executivo de Auditoria no setor são ativos intangíveis valiosos. Quando combinada com uma metodologia robusta de planejamento de auditoria, essa visão do setor ajuda a auditoria interna a se concentrar nos riscos mais relevantes para os objetivos da organização. Onde o risco do setor é alto, mas a prioridade de auditoria é baixa, o Chefe Executivo de Auditoria deve determinar se o risco é coberto por outro provedor de avaliação, integrado em outras auditorias, abordado por meio de trabalho de consultoria, monitorado por atualizações periódicas ou insuficientemente coberto.

Resumo

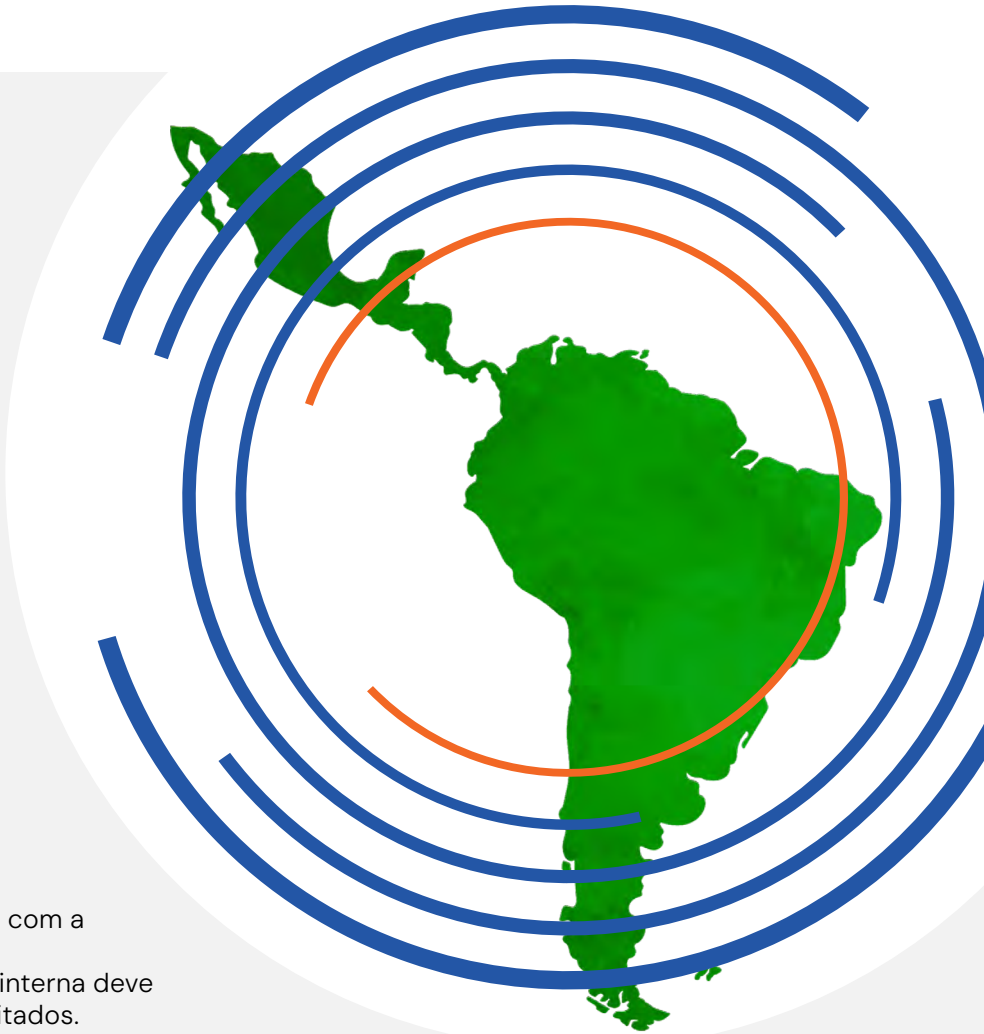
A implicação para os Chefes Executivos de Auditoria não é que todos os riscos devam receber a mesma atenção. Os recursos de auditoria são limitados. Isso significa que o plano de auditoria interna deve explicitar a justificativa para a cobertura da auditoria, levando em consideração a estratégia organizacional, ao mesmo tempo em que se mantém flexível o suficiente para responder a mudanças significativas no ambiente de risco. Quando o risco é alto, mas o esforço de auditoria é baixo, o Chefe Executivo de Auditoria deve ser capaz de explicar o motivo. O risco é coberto por outro provedor de avaliação? A governança da administração é madura? O risco é monitorado por meio de atividades de assessoria? Isso está incluído em outras auditorias? O risco será reavaliado durante uma atualização formal do plano? Ou será que existe realmente uma lacuna devido à capacidade limitada?

"A auditoria interna deve ir além do que é confortável. A questão não é apenas se dispomos de recursos, mas se estamos nos preparando para avaliar o que a empresa está se tornando."

– Ámbar Vargas, Panamá



PONTOS PRINCIPAIS



Conclusões da pesquisa

- O esforço de auditoria interna continua sendo mais intenso em:
  - Cibersegurança
  - Fraude
  - Financeiro/liquidez
  - Mudança regulatória
  - Disrupção digital (incluindo IA)

Isso reflete tanto a relevância do risco quanto os pontos fortes históricos da profissão.

- As maiores lacunas estão em áreas que são mais difíceis de auditar diretamente:
  - Incerteza geopolítica/macroeconômica
  - Mudanças no mercado/concorrência
  - Mudanças climáticas/meio ambiente
  - Capital humano
  - Cultura organizacional
  - Alguns aspectos da disrupção digital

Estratégias de auditoria interna

- Os Chefes Executivos de Auditoria devem comparar os cinco principais riscos com a cobertura atual da auditoria e identificar lacunas não explicadas.
- Nos casos em que os riscos sejam difíceis de auditar diretamente, a auditoria interna deve traduzi-los em processos, decisões, cenários e controles que possam ser auditados.
- Os planos de auditoria devem incluir um equilíbrio entre os trabalhos de avaliação e consultoria, e devem documentar explicitamente como os riscos elevados são abordados, seja por meio de auditorias diretas, cobertura integrada, monitoramento contínuo, confiança em funções de segunda linha ou relatórios ao nível do conselho de administração.

3 MATURIDADE E COBERTURA DE RISCOS

Os riscos mais elevados nem sempre são os mais maduros ou os mais bem cobertos

Os novos dados de maturidade de governança e cobertura da auditoria interna fornecem uma das principais conclusões do relatório deste ano.

O nível de risco, por si só, não indica se uma organização está preparada para gerenciar o risco. A prioridade de auditoria, por si só, não indica se a cobertura da auditoria interna é suficiente. Ao comparar o nível de risco, a maturidade da governança e a cobertura da auditoria, os Chefes Executivos de Auditoria podem identificar onde a organização pode estar mais exposta.

Maturidade da governança de riscos

A pesquisa solicitou aos participantes que classificassem o nível de maturidade da governança de riscos para cada área de risco. A Figura 3.1 mostra que a área financeira/de liquidez apresenta o nível mais alto de maturidade em governança, com 59% classificando-a como gerenciada ou otimizada. Em seguida, vêm as mudanças regulatórias, com 47%; governança e relatórios corporativos, com 44%; comunicações e reputação, com 41%; e fraudes, com 40%. Essas são áreas nas quais as organizações geralmente contam com estruturas estabelecidas, responsabilidades bem definidas, expectativas regulatórias, políticas e supervisão contínua.

Em contrapartida, a disrupção digital apresenta o nível mais baixo de governança madura. Apenas 19% classificaram a governança para a disrupção digital como gerenciada ou otimizada, enquanto 57% a classificaram como inicial ou de infraestrutura. A área de mudanças climáticas/meio ambiente também apresenta baixo nível de maturidade, com 20% em fase de gestão ou otimização e 56% em fase inicial ou de infraestrutura. A incerteza geopolítica/macroeconômica, o capital humano, a cultura e a cadeia de suprimentos também apresentam níveis de maturidade relativamente modestos.

Esse padrão é compreensível, mas arriscado. Uma governança madura tende a existir em organizações que tiveram muitos anos para desenvolver processos e nas quais as consequências regulatórias ou financeiras são claras. Os riscos emergentes costumam evoluir mais rapidamente do que as estruturas de governança. A IA, por exemplo, pode ser adotada por unidades de negócios antes que a organização tenha definido políticas, processos de aprovação de modelos, propriedade dos dados, requisitos de monitoramento ou protocolos de escalonamento. O risco geopolítico pode ser discutido no nível do conselho, mas não traduzido em indicadores de risco, cenários ou planos de resposta operacional.

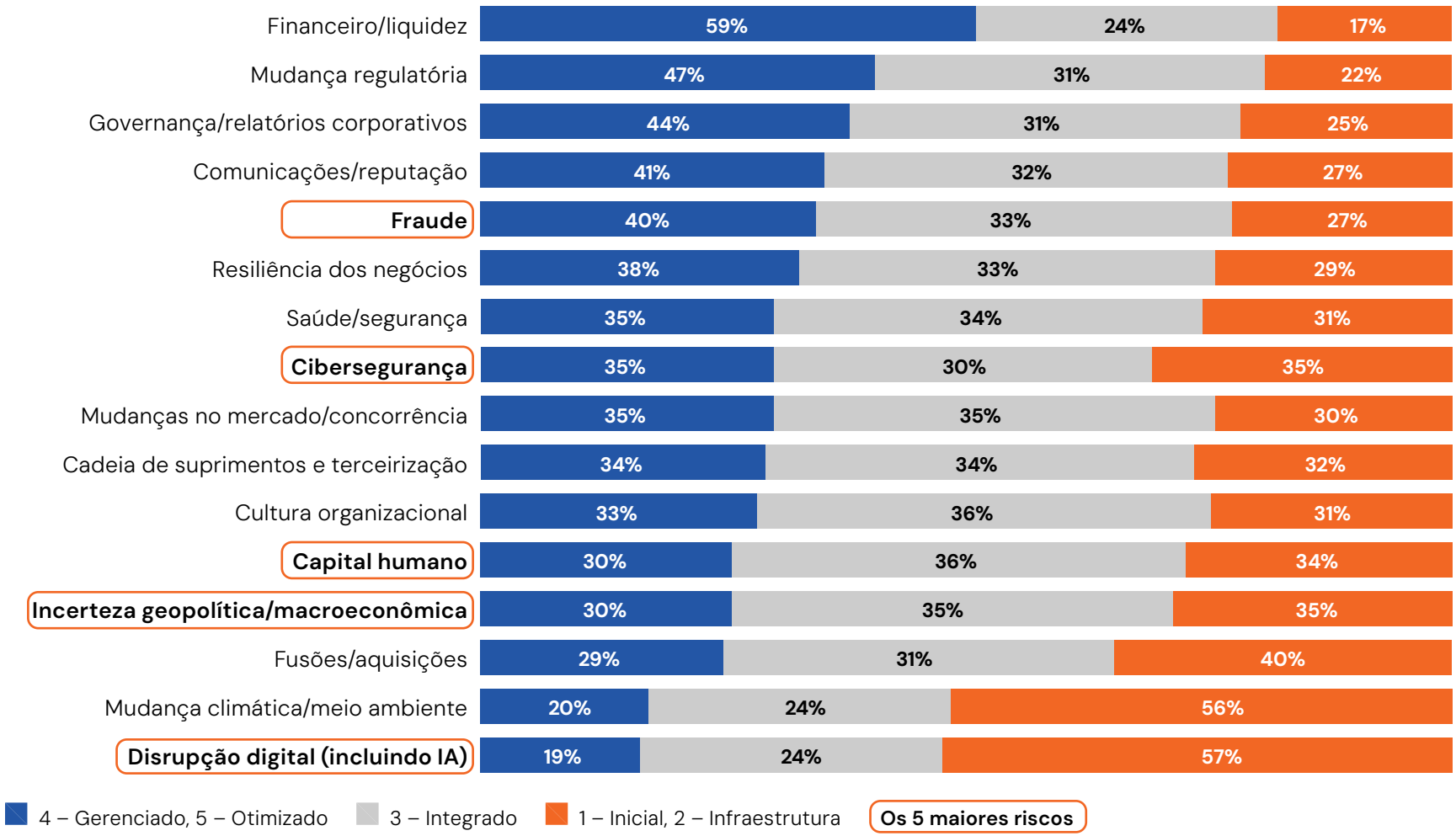
Os guias do IIA sobre a avaliação dos processos de gestão de riscos reforçam a importância da maturidade. A maturidade na gestão de riscos não se resume apenas à existência de políticas; trata-se de saber se a identificação, a avaliação, a resposta, o monitoramento, a comunicação e a prestação de contas em relação aos riscos estão integrados ao processo de tomada de decisão. Um ambiente com baixo nível de maturidade exige uma abordagem diferente da auditoria interna. Em áreas de alta maturidade, a auditoria interna pode testar a eficácia do desenho e da operação. Em áreas com baixo grau de maturidade, a auditoria interna pode precisar, em primeiro lugar, avaliar a estrutura de governança, as funções e responsabilidades, o apetite a risco, a disponibilidade de dados, o processo de escalonamento e o monitoramento.

AI

A disrupção digital apresenta o nível mais baixo de maturidade em governança de riscos, com apenas **19%** dos Chefes Executivos de Auditoria latino-americanos classificando-a como gerenciada ou otimizada.

Figura 3.1. América Latina – Maturidade na governança de riscos

Pergunta da pesquisa: Em uma escala de 1 a 5, avalie o nível atual de maturidade da governança de riscos na sua organização para cada uma das seguintes áreas de risco.



Nota: Pesquisa Risk in Focus, realizada online em todo o mundo de 2 de março a 6 de maio de 2026. n = 512 para a América Latina.

MATURIDADE E COBERTURA DE RISCO

Cobertura da auditoria interna

A Figura 3.2 mostra uma preocupação semelhante em relação à cobertura da auditoria interna. A área financeira/liquidez apresenta o maior nível de cobertura total, com 45%, seguida por mudanças regulatórias, com 39%; governança/relatórios corporativos, com 37%; fraudes, com 30%; e cibersegurança, com 26%. Essas são áreas de cobertura conhecidas e necessárias.

No entanto, a cobertura total é menor no caso da disrupção digital, ficando em apenas 8%. A incerteza geopolítica/macroeconômica também é baixa, com 11%, as mudanças climáticas/meio ambiente com 13%, as mudanças de mercado/concorrência com 14%, a cultura organizacional com 20%, o capital humano com 20% e a cadeia de suprimentos, com 21%. A porcentagem de empresas que consideram a cobertura insuficiente é mais alta no caso da disrupção digital (45%), seguida por clima/meio ambiente (37%), incerteza geopolítica/macroeconômica (35%) e mudanças no mercado/concorrência (29%).

Isso transmite uma mensagem clara sobre os riscos: algumas das áreas com maior relevância estratégica apresentam o menor nível de maturidade em governança e a cobertura de auditoria interna mais fraca. A disrupção digital é o exemplo mais visível. É o segundo maior risco entre os cinco principais e é classificado como "alto" por 75%; no entanto, apresenta o nível mais baixo de maturidade de governança e a menor cobertura de auditoria completa. Para os conselhos isso deve ser um sinal de alerta. Para os Chefes Executivos de Auditoria, isso deve ser uma prioridade no planejamento.

Repensando a cobertura

A solução não consiste necessariamente em realizar um grande número de novas auditorias. Muitas funções de auditoria interna na América Latina operam com equipe e orçamento limitados. A solução é repensar a cobertura. Para a disrupção digital, a auditoria interna pode realizar serviços de consultoria em governança de IA, governança de dados, risco de nuvem, controles de automação, risco de tecnologia de terceiros, cibersegurança desde a concepção e gestão de mudanças. Além disso, pode integrar questões relacionadas a riscos digitais nas auditorias das áreas de vendas, finanças, operações, compras, RH e conformidade.

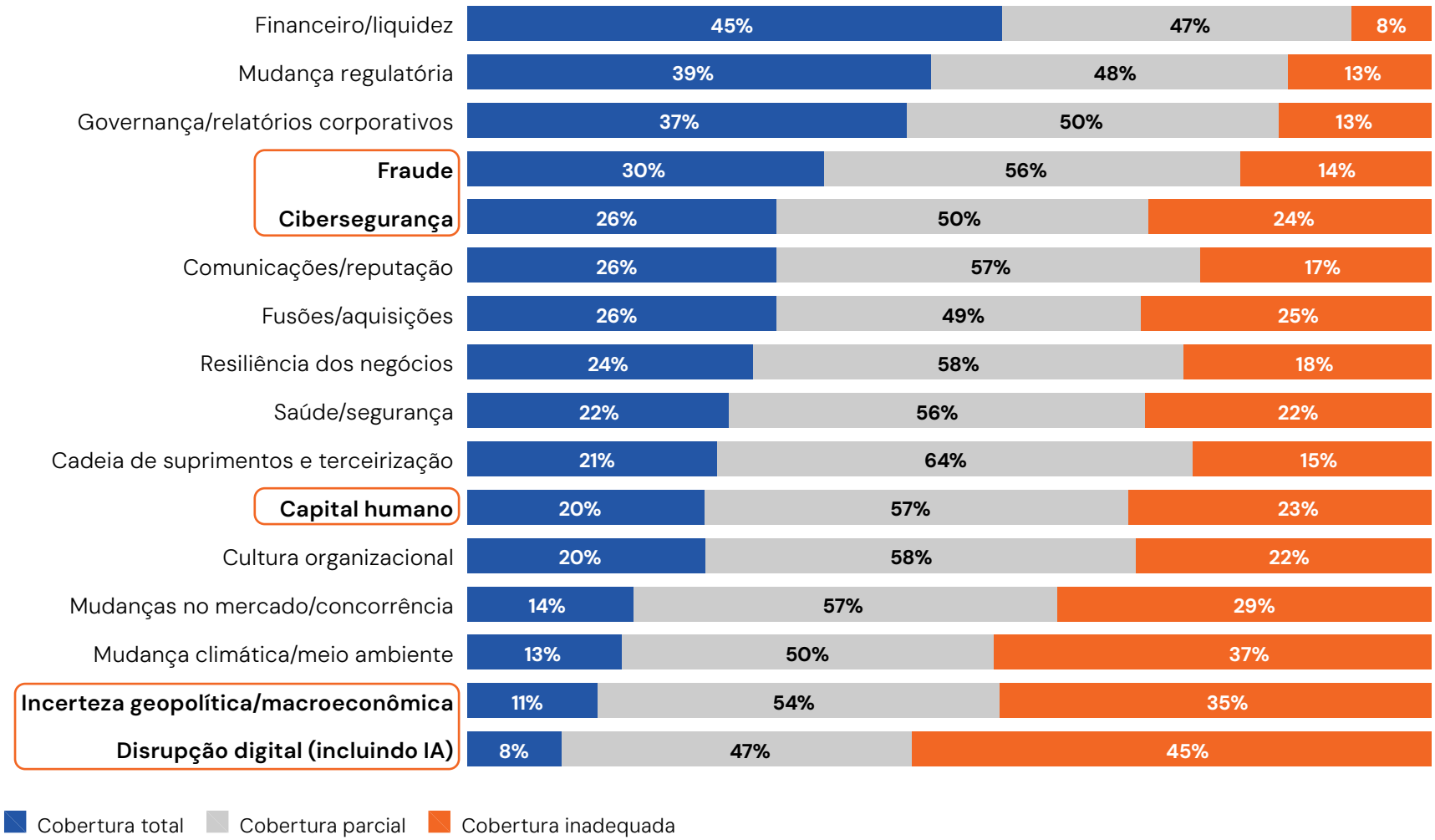
Para a incerteza geopolítica/macroeconômica, a auditoria interna pode analisar o planejamento de cenários, os testes de estresse, a continuidade dos negócios, a gestão de crises, a tesouraria, a cadeia de suprimentos, o planejamento estratégico e o monitoramento regulatório. Para o clima/meio ambiente, a auditoria interna pode se concentrar na exposição a riscos físicos, conformidade ambiental, controles de relatórios de sustentabilidade, resiliência de ativos, seguros e planejamento de continuidade. Para o capital humano, a auditoria interna pode avaliar o planejamento estratégico da força de trabalho, cargos críticos, sucessão, treinamento, retenção, cultura, incentivos e lacunas de competências.

"Muitos planos de auditoria ainda refletem o que os auditores sabem como auditar, em vez do que mais ameaça a estratégia."

– Ámbar Vargas, Panamá

Figura 3.2. América Latina – Cobertura da auditoria interna

Pergunta da pesquisa: Indique se a cobertura atual da auditoria interna dessas áreas de risco em sua organização é adequada.



Nota: Pesquisa Risk in Focus, realizada online em todo o mundo de 2 de março a 6 de maio de 2026. n = 512 para a América Latina.

MATURIDADE E COBERTURA DE RISCOS

Coordenação com a segunda linha

Os dados de maturidade e cobertura também destacam a importância da coordenação com a segunda linha. A gestão é responsável pelo gerenciamento dos riscos. A auditoria interna deve compreender essas responsabilidades e coordenar sua atuação com a segunda linha e outros prestadores de avaliação. No entanto, o Chefe Executivo de Auditoria deve compreender quem detém o risco, como ele é monitorado, qual avaliação existe e se o conselho recebe informações confiáveis. Em áreas com baixo nível de maturidade, o trabalho de consultoria pode ser mais valioso do que a auditoria tradicional no curto prazo, desde que a objetividade seja salvaguardada.

Serviços de consultoria/assessoria

Vários participantes da mesa-redonda levantaram a questão da independência quando a auditoria interna presta apoio consultivo em áreas emergentes. Essa preocupação é válida, mas não deve se tornar uma desculpa para a inação. As Normas Globais de Auditoria Interna™ permitem que a auditoria interna preste serviços de consultoria, desde que o Chefe Executivo de Auditoria gerencie possíveis comprometimentos da objetividade e evite assumir responsabilidades gerenciais. Na prática, a auditoria interna pode ajudar a administração a compreender as melhores práticas, formular perguntas mais pertinentes, avaliar o grau de preparação e identificar lacunas, sem assumir o desenho dos controles ou a responsabilidade por eles.

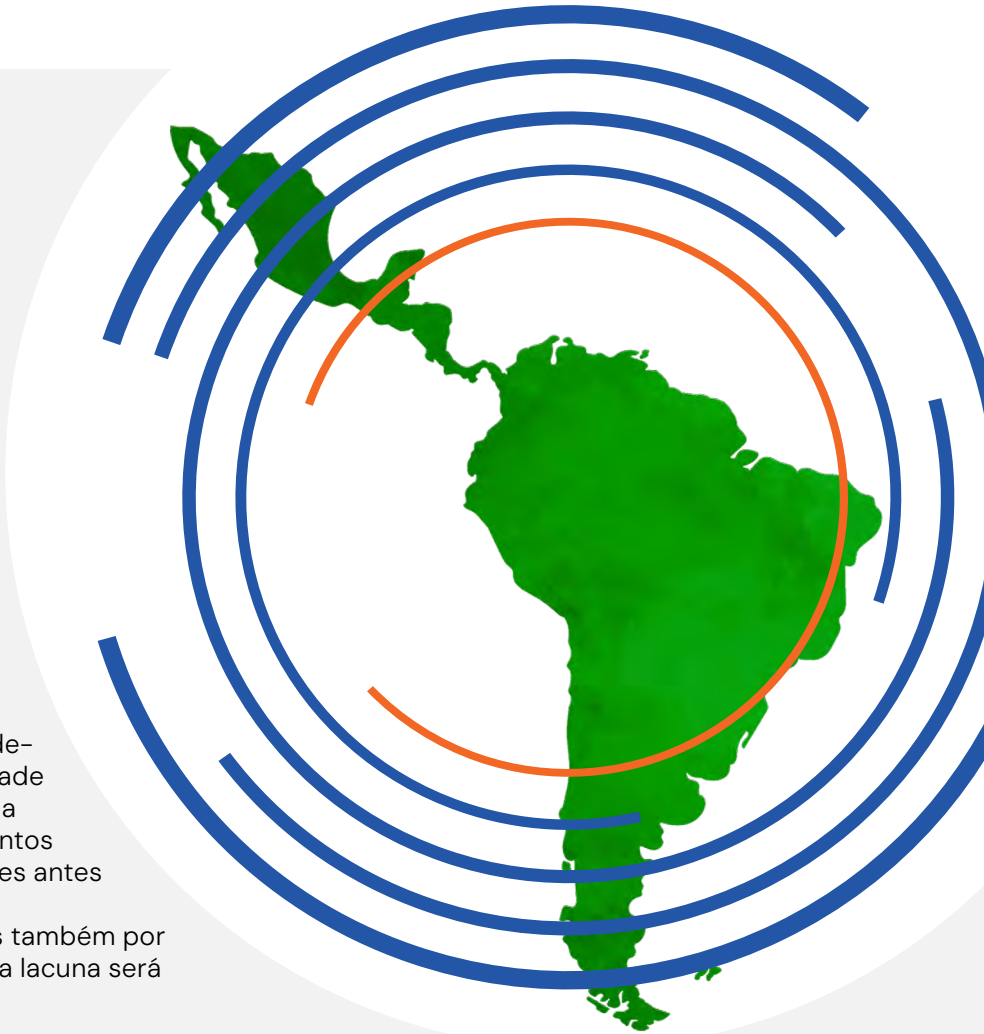
Isso é especialmente importante para a IA e a transformação digital. Esperar até que as medidas de controle estejam totalmente implementadas pode ser tarde demais. A auditoria interna pode agregar valor desde o início, ao analisar a estrutura de governança, os critérios de decisão, as avaliações de risco, a due diligence de fornecedores, as aprovações de testes, a proteção de dados e os planos de monitoramento. O envolvimento desde o início não implica responsabilidade pela gestão. Isso significa prestar serviços de avaliação e consultoria em tempo oportuno em uma área em que os riscos evoluem rapidamente.

Resumo

Para os Chefes Executivos de Auditoria, a análise de maturidade e cobertura deve se tornar parte da conversa anual de planejamento de auditoria com o conselho. O chefe executivo de auditoria deve apresentar ao conselho não apenas os riscos mais elevados, mas também as áreas em que a governança é imatura e a cobertura é insuficiente. Isso permite que o conselho identifique onde o risco pode estar se acumulando de forma imperceptível.



PONTOS PRINCIPAIS



Conclusões da pesquisa

- A maior maturidade em governança e a mais ampla cobertura de auditoria concentram-se em áreas mais tradicionais, como finanças/liquidez, mudanças regulatórias, governança/relatórios corporativos, fraudes e cibersegurança.
- Os pontos mais fracos em termos de maturidade e cobertura estão em áreas emergentes ou estratégicas, como a disrupção digital, a incerteza geopolítica/macroeconômica, o clima/meio ambiente, as mudanças no mercado, a cultura e o capital humano.
- A disrupção digital se destaca como a lacuna mais urgente, pois se trata tanto de uma área de alto risco quanto de baixa maturidade e baixa cobertura.

Estratégias de auditoria interna

- Os Chefes Executivos de Auditoria devem criar uma visão de "risco-maturidade-cobertura" para o conselho. As áreas de alto risco com baixo nível de maturidade e baixa cobertura de auditoria devem ser discutidas explicitamente. A auditoria interna deve usar serviços de consultoria, avaliações de prontidão, procedimentos de auditoria integrados e avaliação coordenada para abordar riscos emergentes antes que se traduzam em falhas de controle.
- Os planos de auditoria devem identificar não apenas o que será auditado, mas também por que determinadas áreas de alto risco recebem cobertura limitada e como essa lacuna será monitorada.

CONCLUSÃO

O Chefe Executivo de Auditoria como tradutor de risco, estratégia e ação

Os resultados do estudo Risk in Focus 2026/2027 da América Latina mostram que a região está entrando em uma fase desafiadora no que diz respeito à gestão de riscos e à liderança em auditoria interna.

Os principais riscos são evidentes. A cibersegurança, a disrupção digital, a incerteza geopolítica e macroeconômica, a fraude, o capital humano, a regulamentação e a liquidez já estão no radar dos Chefes Executivos de Auditoria, executivos e conselhos. O desafio já não se resume apenas à conscientização. O desafio é a ação.

Para a auditoria interna, isso significa passar de uma mentalidade de classificação de riscos para uma mentalidade de resposta a riscos. Um risco alto que não influencia o planejamento de auditoria, a cobertura da avaliação, a atividade de consultoria, a estratégia de talentos ou o diálogo com o conselho continua sendo apenas um resultado da pesquisa. O valor do Risk in Focus se concretiza quando os Chefes Executivos de Auditoria o utilizam para questionar seu universo de auditoria, testar premissas e avaliar se a função está se concentrando nos riscos que mais importam para o valor da organização. Os resultados apontam para três prioridades para os Chefes Executivos de Auditoria na América Latina:

1. A auditoria interna deve abordar os riscos relacionados. A cibersegurança, a inteligência artificial, a fraude, os dados, a regulamentação, terceiros, a liquidez, a reputação e a continuidade não devem ser auditados apenas como áreas isoladas. Os eventos mais prejudiciais costumam ocorrer na interseção entre os riscos. Um incidente cibernético pode se transformar em um caso de fraude, uma violação regulatória, um problema de liquidez e uma crise de reputação. Um evento geopolítico pode se tornar um problema para a cadeia de suprimentos, um problema de resiliência da nuvem, um problema cambial e um problema de continuidade dos negócios.
2. Os Chefes Executivos de Auditoria devem fechar a lacuna entre os riscos emergentes e a capacidade de auditoria. A disrupção digital tornou-se um dos maiores riscos na região, mas o nível de maturidade da governança e a cobertura das auditorias continuam baixos. Essa lacuna não pode ser resolvida apenas com a contratação de especialistas, embora as competências especializadas sejam importantes. Isso também exige novas metodologias, treinamento, co-sourcing, análise de dados, auditoria contínua, maior coordenação com a segunda linha e diálogos mais estratégicos com a administração.
3. A auditoria interna deve fortalecer seu relacionamento com o conselho e a diretoria executiva. O Chefe Executivo de Auditoria deve estar suficientemente próximo da estratégia para compreender para onde a organização está indo, ao mesmo tempo em que mantém a objetividade necessária para avaliar se os riscos estão sendo gerenciados de forma adequada. Esse equilíbrio não é uma falha na independência; é um requisito para a relevância.

A próxima geração de líderes de auditoria interna na América Latina será caracterizada pela capacidade de transformar a volatilidade em decisões. Os conselhos de administração precisam de Chefes Executivos de Auditoria capazes de explicar como as tendências globais afetam as operações locais, como as tecnologias emergentes alteram os ambientes de controle, como a falta de talentos afeta a execução estratégica e como a cobertura de auditoria deve evoluir.

A questão mais importante para 2027 não é se a auditoria interna compreende o panorama de riscos. A questão é se a auditoria interna está preparada para tomar medidas a respeito.

"A auditoria interna não pode indicar o caminho certo se não compreender para onde a organização está indo."

– Héctor Trujeque, Argentina

APÊNDICE A. METODOLOGIA

Pesquisa, mesas-redondas e entrevistas

A Fundação de Auditoria Interna coletou respostas à pesquisa de 24 de março a 6 de maio de 2026, em todas as regiões, exceto na Europa. As respostas da Europa foram coletadas pelo Grupo de Pesquisa dos Institutos Europeus entre 2 de março e 7 de abril de 2026.

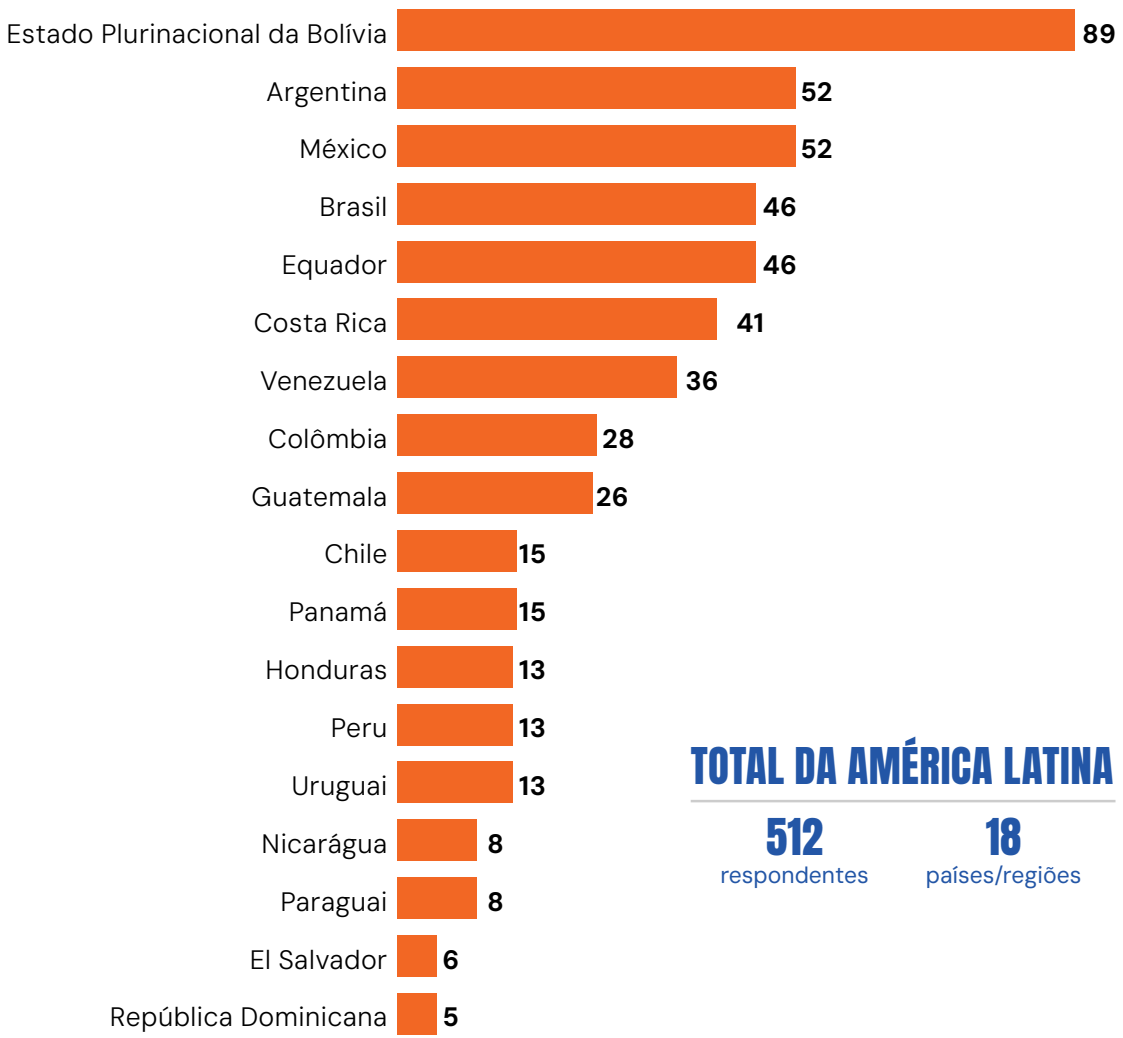
Foram recebidos questionários preenchidos por 3.285 auditores internos, que confirmaram ser os auditores internos de mais alto escalão em suas organizações. Eles representavam 132 países/locais. A pesquisa foi realizada on-line por meio de contatos ligados aos Institutos Nacionais do IIA e aos órgãos regionais. Além disso, foram realizadas mesas-redondas e entrevistas para cada relatório regional.

As 16 áreas de risco usadas na pesquisa são mostradas abaixo. Foi feita aos respondentes uma série de perguntas sobre níveis de risco, planejamento de auditoria e maturidade da governança de risco.

Nome do risco	Descrição de risco usada na pesquisa
Resiliência dos negócios	Continuidade dos negócios, resiliência operacional, gerenciamento de crises e resposta a desastres
Mudança climática/meio ambiente	Mudanças climáticas, biodiversidade e sustentabilidade ambiental
Comunicações/reputação	Comunicações, reputação e relacionamentos com as partes interessadas
Cibersegurança	Cibersegurança e segurança de dados
Disrupção digital (incluindo IA)	Disrupção digital, nova tecnologia e IA (inteligência artificial)
Financeiro/liquidez	Riscos financeiros, de liquidez e de insolvência
Fraude	Fraude, suborno e exploração criminosa de interrupções
Incerteza geopolítica/macroeconômica	Incerteza macroeconômica, social e geopolítica
Governança/relatórios corporativos	Governança organizacional e relatórios corporativos
Saúde/segurança	Saúde, segurança e proteção
Capital humano	Capital humano, diversidade, gerenciamento e retenção de talentos
Mudanças no mercado/concorrência	Mudanças no mercado/concorrência e comportamento do cliente
Fusões/aquisições	Fusões e aquisições
Cultura organizacional	Cultura organizacional
Mudança regulatória	Mudança nas leis e regulamentos
Cadeia de suprimentos e terceirização	Cadeia de suprimentos, terceirização e risco da "enésima" parte

APÊNDICE B: DADOS DEMOGRÁFICOS

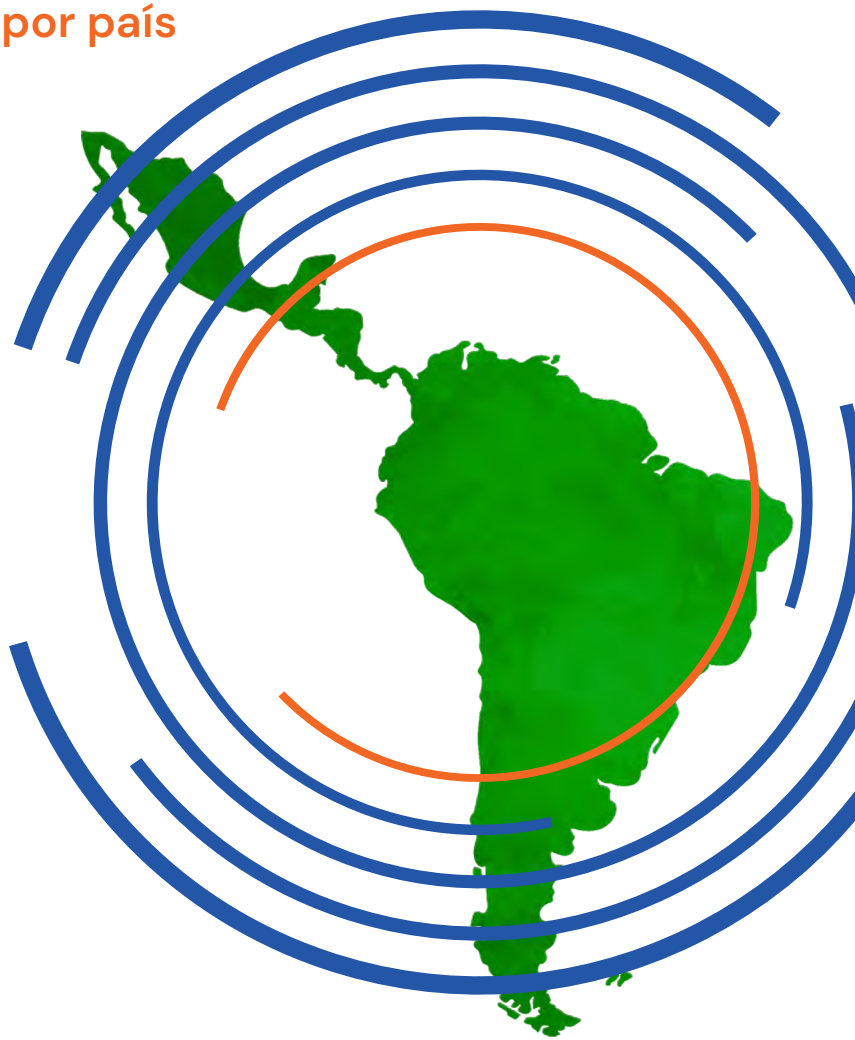
Anexo B.1. América Latina – Número de respondentes por país



TOTAL DA AMÉRICA LATINA

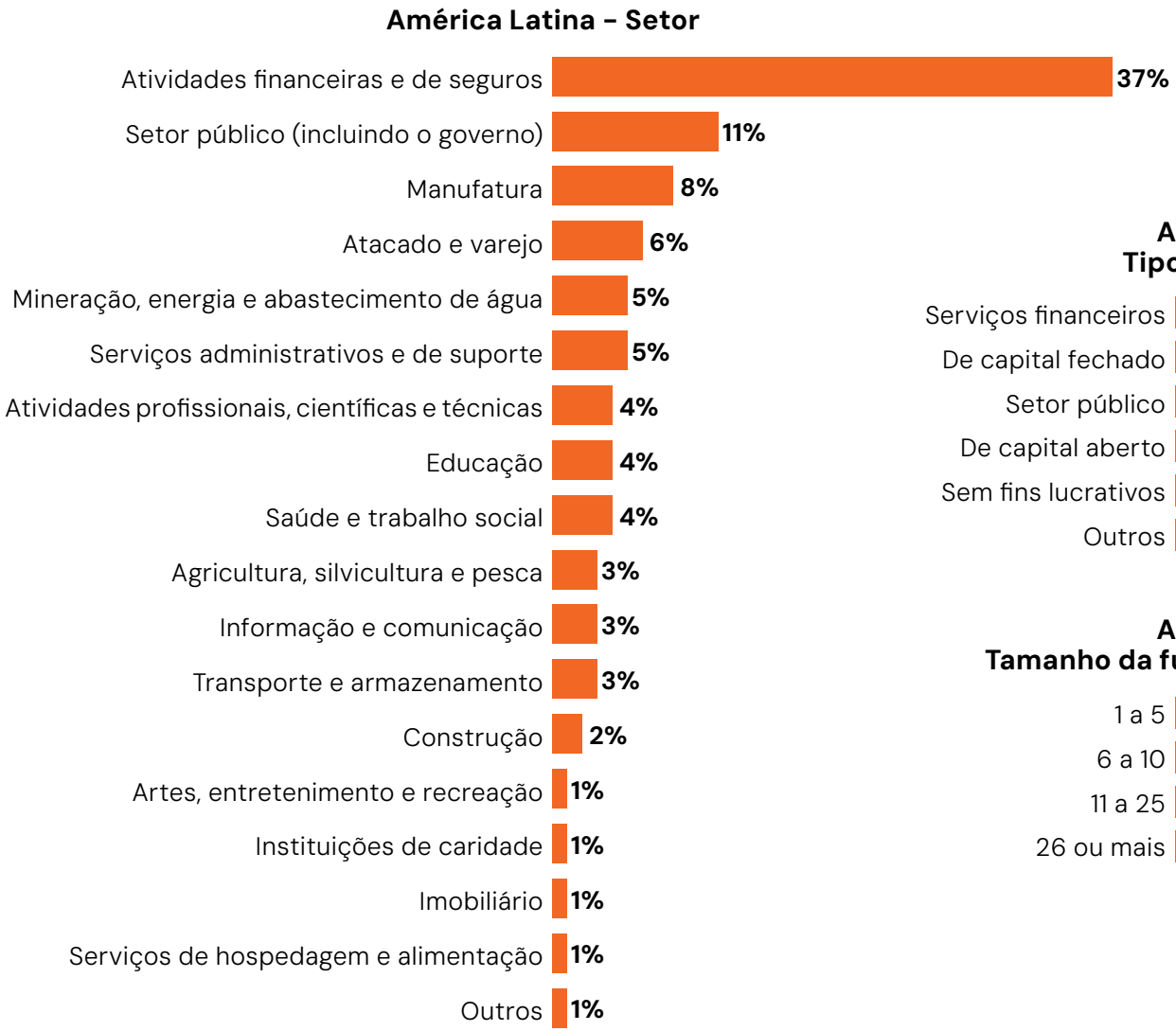
512 respondentes

18 países/regiões

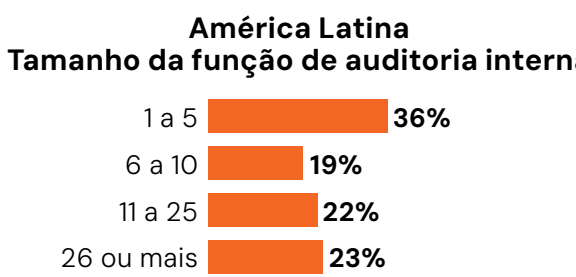


Nota: Pesquisa Risk in Focus, realizada online em todo o mundo de 2 de março a 6 de maio de 2026. n = 512 para a América Latina.

Anexo B.2. América Latina – Setor, Tipo de organização, Tamanho da auditoria interna







Nota: Pesquisa Risk in Focus, realizada online em todo o mundo de 2 de março a 6 de maio de 2026. n = 512 para a América Latina.

APÊNDICE C. VISÃO GERAL DOS RISCOS GLOBAIS

A América Latina em um padrão global de aceleração

O cenário de risco na América Latina faz parte de uma tendência global mais ampla. O panorama global é relevante para os Chefes Executivos de Auditoria na América Latina, pois muitas organizações da região atuam além das fronteiras, dependem de fornecedores globais de tecnologia, importam insumos essenciais, utilizam mercados financeiros internacionais e são afetadas por agentes de ameaças cibernéticas globais. Mesmo as organizações que atuam localmente estão expostas à propagação de riscos globais por meio da inflação, do câmbio, das plataformas em nuvem, dos fornecedores de software, das redes de crimes cibernéticos, da regulamentação e do comportamento do consumidor.

Os resultados da pesquisa mostram que regiões em todo o mundo estão apresentando tendências de risco semelhantes (Figura C.1 e Figura C.2):

- As classificações de risco relacionadas à disrupção digital aumentaram em todas as regiões do mundo.
- A cibersegurança e a incerteza geopolítica aumentaram em todas as regiões, com exceção de uma: a América do Norte.
- Os riscos de fraude e os riscos financeiros e de liquidez aumentaram na África, na Ásia-Pacífico e na América Latina.
- O risco na cadeia de suprimentos aumentou na África, na Ásia-Pacífico e no Oriente Médio.

Obtendo perspectiva a partir do contexto global

O contexto global não deve levar os Chefes Executivos de Auditoria a copiar as prioridades globais sem adaptá-las. Em vez disso, deveria ajudá-los a questionar os pressupostos locais. Uma tendência global pode não representar um risco elevado para todas as organizações, mas deve ser levada em conta na avaliação de riscos. Por exemplo, o clima/meio ambiente pode ter uma prioridade menor para a América Latina como um todo do que a cibersegurança ou a inteligência artificial, mas, para os setores de energia, agricultura, infraestrutura, transporte, mineração, seguros e governo, pode ser um risco estratégico. Da mesma forma, o risco na cadeia de suprimentos pode não ser alto no caso do abastecimento de alimentos a bordo de uma companhia aérea, mas pode ser crítico nos setores de saúde, varejo, manufatura ou energia.

Para conselhos de administração e comitês de auditoria, o valor da comparação global reside na análise comparativa. Isso ajuda a responder a três perguntas: Estamos vendo os mesmos riscos que os nossos pares? Estamos avançando mais rápido ou mais devagar do que o mercado? Existem riscos crescentes em nível global que ainda não incorporamos à nossa estratégia? Os Chefes Executivos de Auditoria devem utilizar as comparações globais não como um substituto para a avaliação de riscos da empresa, mas como um mecanismo de desafio para aprimorá-la.

A auditoria interna também pode recorrer a comparações globais para fundamentar discussões sobre recursos. Se a disrupção digital, a cibersegurança e a incerteza geopolítica estão aumentando em todo o mundo, mas a função de auditoria interna carece de competências tecnológicas, análise de dados, conhecimento em cibersegurança ou capacidade de gestão de riscos estratégicos, o Chefe Executivo de Auditoria tem argumentos ainda mais sólidos para justificar o investimento. A conversa com o conselho deve passar de "precisamos de mais recursos" para "nosso perfil de risco mudou, e nossas capacidades devem mudar junto com ele".

MAIS RECURSOS GLOBAIS

Consulte o relatório Resumo Global do Risk in Focus para obter dados e análises sobre tendências regionais.

Anexo C.1. Global – Os cinco principais riscos por região

Pergunta da pesquisa: Quais são os cinco principais riscos que sua organização enfrenta atualmente? (Escolha 5.)

Áreas de risco	Média das regiões	África	Ásia Pacífico	Europa	América Latina	Oriente Médio	América do Norte
Cibersegurança	**80%** ↑	**73%** ↑	**72%** ↑	**86%** ↑	**80%** ↑	**81%** ↑	**85%**
Disrupção digital (incluindo IA)	**58%** ↑	**50%** ↑	**59%** ↑	**52%** ↑	**61%** ↑	**58%** ↑	**69%** ↑
Incerteza geopolítica/macroeconômica	**48%** ↑	**35%** ↑	**48%** ↑	**51%** ↑	**52%** ↑	**60%** ↑	**43%**
Capital humano	**38%**	30%	**41%**	**39%**	**37%**	34%	**45%**
Resiliência dos negócios	**35%**	28%	**43%**	37%	25%	**47%**	29%
Financeiro/liquidez	34%	**49%** ↑	**28%** ↑	28%	**36%** ↑	**42%** ↑	24%
Mudança regulatória	32%	28%	24%	**40%**	36%	20%	**42%**
Mudanças no mercado/concorrência	29%	20%	37%	32%	27%	20%	**41%** ↑
Fraude	29%	**50%** ↑	**28%** ↑	16%	**38%** ↑	22%	**18%** ↑
Cadeia de suprimentos e terceirização	**27%** ↑	**21%** ↑	**33%** ↑	26%	17%	**35%** ↑	33%
Governança/relatórios corporativos	20%	27%	21%	13%	15%	27%	14%
Mudança climática/meio ambiente	19%	**31%** ↑	20%	21%	23%	15%	7%
Cultura organizacional	19%	26%	19%	17%	26%	13%	16%
Comunicações/reputação	15%	18%	13%	**17%** ↑	15%	13%	16%
Saúde/segurança	10%	12%	8%	12%	7%	10%	11%
Fusões/aquisições	5%	2%	6%	5%	4%	3%	7%

Os 5 maiores riscos

Como interpretar o gráfico
As **setas vermelhas** ↑ indicam um aumento de 4 pontos percentuais ou mais em relação ao ano anterior.

Nota: Pesquisa Risk in Focus, realizada online em todo o mundo de 2 de março a 6 de maio de 2026. n = 3.285.

Anexo C.2. Global – Tendência dos cinco principais riscos

Pergunta da pesquisa: Quais são os cinco principais riscos que sua organização enfrenta atualmente? (Escolha 5.)

2023	2024	2025	2026	Variação de 2025 para 2026	Variação	Áreas de risco
73%	71%	73%	80%		+7	**Cibersegurança**
34%	39%	48%	58%		+10	**Disrupção digital (incluindo IA)**
30%	28%	38%	48%		+10	**Incerteza geopolítica/macroeconômica**
51%	49%	43%	38%		-5	Capital humano
47%	54%	47%	35%		-12	**Resiliência dos negócios**
32%	32%	31%	34%		+3	Financeiro/liquidez
39%	37%	41%	32%		-9	**Mudança regulatória**
32%	32%	31%	29%		-2	**Mudanças no mercado/concorrência**
24%	27%	23%	29%		+6	**Fraude**
26%	22%	24%	27%		+3	Cadeia de suprimentos (incluindo terceiros)
27%	26%	24%	20%		-4	Governança/relatórios corporativos
19%	21%	18%	19%		+1	Mudança climática/meio ambiente
26%	25%	24%	19%		-5	Cultura organizacional
21%	21%	19%	15%		-4	Comunicações/reputação
11%	11%	10%	10%		0	Saúde/segurança
6%	6%	5%	5%		0	Fusões/aquisições

Aumento do risco em relação ao ano anterior Redução do risco em relação ao ano anterior

Como interpretar o gráfico
O texto em laranja indica um aumento de 4 pontos percentuais ou mais em relação ao ano anterior. As barras **laranja** e **azul** mostram a diferença nas avaliações de 2025 a 2026. A coluna intitulada "variação" mostra a diferença em pontos percentuais entre 2025 e 2026.

Nota: Pesquisa Risk in Focus, realizada online em todo o mundo de 2 de março a 6 de maio de 2026. n = 3.285.

APÊNDICE D. RECURSOS DO IIA

O IIA oferece uma variedade de recursos para apoiar os auditores internos na avaliação de riscos e no planejamento de auditorias por meio do site, do departamento de Normas e Orientações. A maioria desses recursos está disponível gratuitamente para os membros do IIA em todo o mundo, e alguns também estão à disposição do público em geral. Para conferir os lançamentos mais recentes, visite a página de recursos de Orientações Globais e a página de lançamentos de Posicionamentos .

Ambiente de risco

- **Avaliação do Processo de Gestão de Riscos, 2ª edição** (The IIA, Guia de Práticas Globais, 2024)
- **O papel da função de auditoria interna na gestão de riscos empresariais** (IIA, Declaração de Posição, 2026)

Prioridades de auditoria

- **Ferramentas de suporte à estrutura de IA** (IIA, Ferramentas de Auditoria, 2026)
- **Estrutura de Auditoria em Inteligência Artificial** (IIA, 2024)
- **Auditoria das operações de cibersegurança: Prevenção e Detecção, 2ª edição** (IIA, Guia de Práticas Globais, 2025)
- **Auditoria de Riscos de Privacidade e Proteção de Dados, 3ª edição** (IIA, Guia de Práticas Globais, 2026)
- **Auditoria Interna e Fraude, 3ª edição** (The IIA, Guia de Práticas Globais, 2024)
- **Requisito Temático de Resiliência Organizacional** (IIA, Requisito Temático, 2026)

Maturidade da Governança de Riscos e Cobertura da Auditoria Interna

- **Desenvolvimento de um Plano de Auditoria Interna Baseado em Riscos, 2ª edição** (IIA, Guia de Práticas Globais, 2025)
- **Desenvolvimento de uma Estratégia de Auditoria Interna** (IIA, Guia de Práticas Globais, 2025)
- **Modelo das Três Linhas** (IIA, Declaração de Posição, 2026)

Normas Globais de Auditoria Interna

- **Normas Globais Completas de Auditoria Interna**
- **Normas Globais de Auditoria Interna em Versão Resumida**



FUNDAÇÃO DE AUDITORIA INTERNA

A Internal Audit Foundation é o principal recurso global, em parceria estratégica com o IIA, dedicado a elevar e capacitar a profissão de auditoria interna por meio do desenvolvimento de pesquisas e programas de ponta. Há 50 anos, a Fundação ajuda os auditores internos atuais e futuros a se manterem atualizados, desenvolvendo e aprimorando suas habilidades e conhecimentos, garantindo que as organizações estejam preparadas para criar, proteger e sustentar valor a longo prazo. Visite theiia.org/Foundation.

Conselho de Curadores da Fundação de Auditoria Interna, 2026-27

Presidente:
Glenn Ho, CIA, CRMA

Vice-presidente sênior de Estratégia
Shirley Livhuwani Machaba, CCSA, CRMA

Vice-presidente de Finanças e Desenvolvimento
Michael A. Smith, CIA

Vice-presidente de Conteúdo
Nora Zeid Kelani, CIA, CRMA

Curadores
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

Funcionário de ligação: Laura LeBlanc, Vice-presidente da Fundação de Auditoria Interna e dos Percursos Profissionais

Comitê de Consultores de Pesquisa e Educação, 2026-27

Presidente:
Nora Zeid Kelani, CIA, CRMA

Membros
Christopher Calvin, PhD, CIA
Joseph Ian Canlas, CIA, CRMA
Andrew Dahle, CIA, CRMA
André Domingos
Marc Eulerich, PhD, CIA
Ivony Kudzayi Katsande-Zezekwa, DBL, CIA, CRMA
Tabborrah Labor, CIA
Roberto Leon Pacheco, PhD, CIA, CCSA, CRMA
Ayaka Mitsunari, CIA
Ahmed Mohammed, DBA, CIA
Grace Mubako, PhD, CIA
Nisha Nair, CIA
Millicent Lindiwe Ndaba, CIA
Shintaro Okada, PhD, CIA
Emmanuel Pascal, CIA, CRMA
Brad Schafer, PhD, CIA
Brian Tremblay, CIA
Stacy Wright, CIA

Internal Audit FOUNDATION 1976-2026

Equipe de Pesquisa

Coordenadora de pesquisa
Deborah Poulalion, Gerente sênior de Pesquisa e Análises, The IIA

Gerente de projeto:
Candace Sacher

Designers gráficos
Sergio Analco e Cathy Watanabe

PARCEIROS DA FUNDAÇÃO DE AUDITORIA INTERNA

PARCEIROS DE DIAMANTE

bakertilly

Deloitte.

Grant Thornton

KPMG

Optro

The Institute of Internal Auditors

The Institute of Internal Auditors Chicago

Wolters Kluwer

PARCEIROS GOLD

- Carr, Riggs & Ingram
- Fundação Latino-Americana de Auditores Internos
- IIA – Seção de Houston
- IIA – Japão
- IIA – Seção de Nova York
- IIA – Seção de São Francisco

CÍRCULO DO PRESIDENTE

(Doadores individuais)

- 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

FUNDAÇÃO LATINO-AMERICANA DE AUDITORES INTERNOS (FLAI)

Conselho da FLAI

Presidente
Geraldine Giachello, CIA, CPA
Vice-presidente
Manuel Quezada, CPA, MBA
Secretário e ex-presidente
Francisco Arauz, CIA, CCSA, CPA
Tesoureira
Maritza Barzola, CRMA, CPCC
Membros do Conselho
Javier Ferrer, Contador Certificado, CPA, Mestre em Gestão Executiva
Marcia Pereira, CIA, CCSA
Jim Romero, CIA, CCSA, CRMA, CPA

Diretor Executivo da FLAI

Roberto Loo

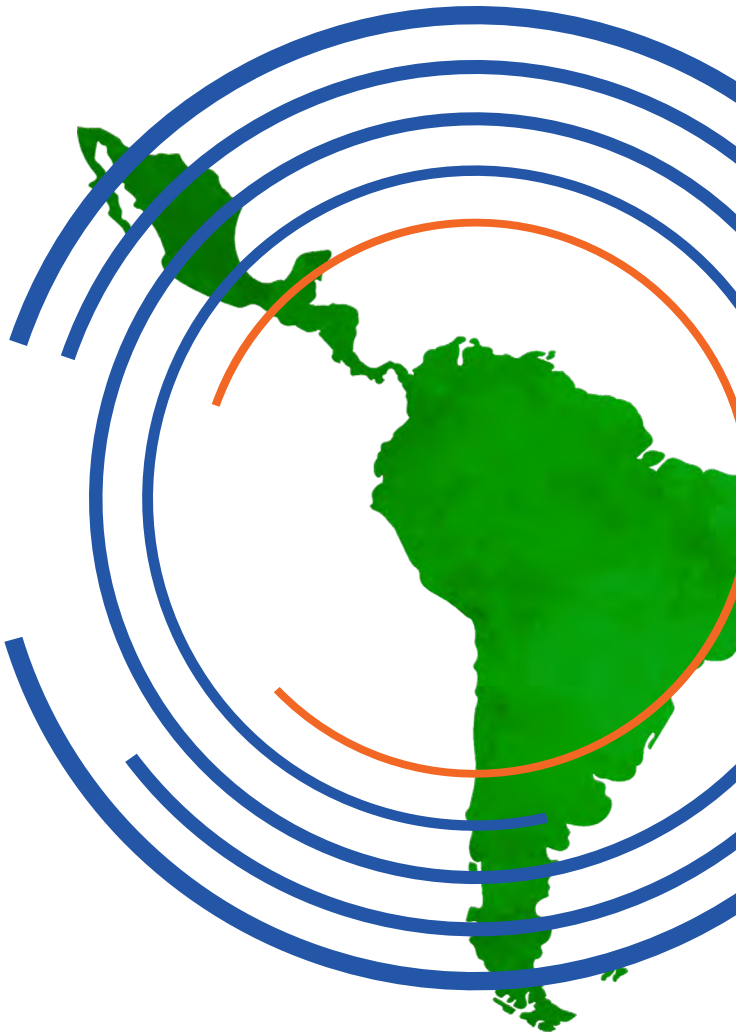
Escritor:

Renato Trisciuzzi,
CIA, QIAL, CCSA, CRMA, M.Sc., Ph.D.

Moderadores da Mesa-Redonda Risk in Focus

Savio Jannuzzi, Brasil

Alejandro Rembado, Argentina



OBRIGADO.

A equipe de pesquisa e desenvolvimento agradece aos líderes de auditoria interna de toda a América Latina que participaram da pesquisa, das mesas-redondas e das entrevistas. Suas percepções práticas ajudaram a transformar os resultados da pesquisa em uma compreensão mais útil sobre como os riscos estão evoluindo na região e como as funções de auditoria interna podem responder com maior relevância, agilidade e impacto estratégico.

Fundación Latinoamericana
de Auditores Internos

O IIA

O Instituto de Auditores Internos (IIA) é uma associação profissional internacional sem fins lucrativos que atende a mais de 265.000 membros em todo o mundo e já concedeu mais de 200.000 certificações de Auditor Interno Certificado (CIA) globalmente. Fundado em 1941, o The IIA é reconhecido em todo o mundo como o líder da profissão de auditoria interna em normas, certificações, educação, pesquisa e orientação técnica. Para obter mais informações, visite theiia.org.

Isenção de responsabilidade e direitos autorais
O IIA publica este documento para fins informativos e educacionais. Este material não tem a intenção de fornecer respostas definitivas para circunstâncias individuais específicas e, portanto, deve ser usado apenas como um guia. O IIA recomenda que se busque uma consultoria especializada independente relacionada diretamente a qualquer situação específica. O IIA não se responsabiliza por qualquer pessoa que confie exclusivamente neste material.

Copyright © 2026 by the Internal Audit Foundation. Todos os direitos reservados. Para obter permissão para republicar, entre em contato com Copyright@theiia.org.

Setembro de 2026

The Institute of
Internal Auditors

Sede Global | Instituto de Auditores Internos
1035 Greenwood Blvd., Suíte 401 | Lake Mary, FL 32746, EUA
Telefone: +1-407-937-1111 | Fax: +1-407-937-1101
Site: theiia.org