



# Auditoria Interna em Foco: Ano Fiscal 2024

Uma perspectiva de auditoria interna sobre os principais riscos enfrentados pelas organizações



Agosto de 2023

[kpmg.com.br](http://kpmg.com.br)

**Para promover a confiança e agregar valor, a auditoria interna deve permanecer ágil e abordar os riscos contemporâneos. A equipe de auditoria interna da KPMG tem trabalhado nas áreas de foco mais importantes, que a Auditoria Interna devera considerar no Ano Fiscal de 2024 (FY24).**

---

# Auditoria Interna em Foco FY24

## Macroeconomia

No Brasil, o crescimento real do Produto Interno Bruto (PIB) sofreu desaceleração no período de 2022 (3%) para 2023 (projeção de 0,8%). Essa retração foi gradativa, com a economia encolhendo um pouco mais a cada trimestre. Enquanto isso, o presidente Luiz Inácio Lula da Silva assumiu seu terceiro mandato como chefe do Executivo, em um clima bem diferente daquele que encontrou em 2002 e 2006, quando foi eleito e reeleito, consecutivamente. Agora, inserido em um cenário doméstico menos sereno e em condições geopolíticas mais complexas, ele traz uma agenda focada em programas sociais que podem manter o consumo em alta a curto prazo, porém acarretando alta inflacionária mais adiante.

Entre outras medidas, Lula prolongou estímulos fiscais relacionados à pandemia. A expectativa de seu governo é que os subsídios salariais e de preços, bem como os pagamentos de transferência, apoiem o crescimento em 2023. O governo brasileiro também estabeleceu um déficit orçamentário-alvo, com base no crescimento esperado (que foi cortado em novembro de 2022), tornando improvável que o país melhore em relação ao déficit do ano passado. O pacote de estímulos aumentará os gastos dos consumidores e aumentará os déficits governamentais já inchados.

Hoje, a China é o maior parceiro comercial do Brasil, respondendo por quase um terço das exportações do País, de acordo com o Observatório de Complexidade Econômica (OEC). Espera-se que a reabertura da economia chinesa e o bloqueio no índice de poupança das famílias respaldem o crescimento daquele país. Vale ressaltar que as despesas finais de consumo na China aumentaram em 2022 e é possível que a demanda represada alimente as exportações brasileiras. Quanto aos EUA, é esperado que o país desempenhe um papel menor no equilíbrio da balança comercial brasileira, visto que o governo de John Biden já enfrenta um quadro de desaceleração econômica.

### Resposta da auditoria interna

A auditoria interna deve estar atenta aos riscos emergentes e garantir que a primeira e a segunda linhas continuem a avaliar as forças externas que podem impactar a organização. Também deve monitorar os riscos decorrentes das exposições a fornecedores terceirizados, principalmente no que tange às mudanças econômicas, ao mesmo tempo em que se concentra internamente no controle de custos, no gerenciamento do capital de trabalho e na compreensão dos acordos de dívidas.

Durante cada auditoria, os auditores internos devem identificar potenciais riscos de fraude, avaliar a eficácia dos controles que previnem e reconhecem comportamentos fraudulentos e conduzir análises de dados direcionadas para identificar indicadores de conduta fraudulenta.

## Geopolítica

O Relatório Global de Riscos de 2023 do Fórum Econômico Mundial (WEF, na sigla em inglês) inventou uma nova palavra para descrever a situação em que uma multiplicidade de problemas e dificuldades materiais ocorrem simultaneamente: uma *polycrisis* (em português, algo como “policrises”).

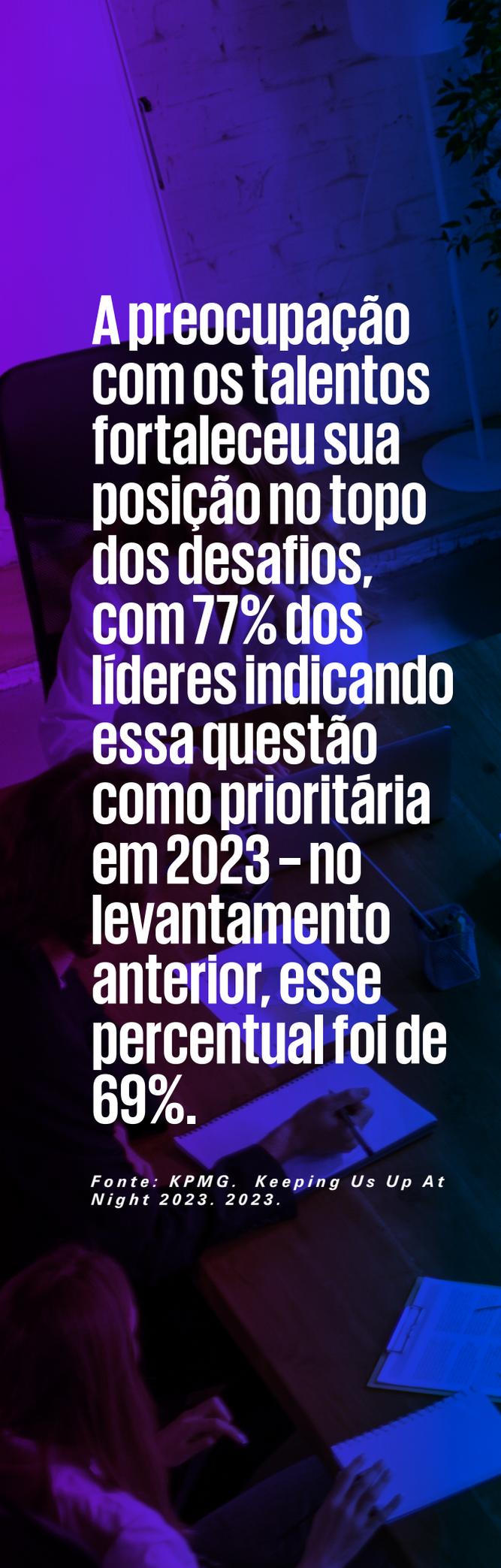
A pandemia continua sendo uma ameaça global (incluindo os efeitos da covid-19 prolongada), bem como a crise climática e o conflito em curso entre Rússia e Ucrânia. Outros riscos e questões emergentes mais proeminentes incluem mudanças demográficas aceleradas na China, crises nas cadeias de suprimentos, respostas da política monetária ao aumento da inflação e os impactos dessas questões sobre custo de vida.

Os mercados de energia e a transição energética continuarão sendo afetados, inclusive pela interrupção contínua do comércio de energia devido à guerra na Ucrânia, resultando em políticas governamentais que limitem o aumento dos preços de energia e afetem a competição entre os países pela captura de valor na transição para fontes mais limpas de energia.

### Resposta da auditoria interna

A auditoria interna deve identificar e abordar potenciais vulnerabilidades relacionadas ao cumprimento de sanções internacionais, bem como avaliar de que maneiras os fatores geopolíticos-chave podem impactar as operações de uma organização, em questões como: decisões de investimento; relações com clientes no exterior; e/ou interrupções nas cadeias de suprimentos, como energia, matérias-primas ou componentes tecnológicos.

Também deve apoiar as organizações para que estas permaneçam vigilantes em relação às incertezas geopolíticas. Deve também garantir que as organizações compreendam e avaliem com clareza os impactos causados por perturbações políticas, sociais e econômicas, por meio de análise de cenários, modelagem e compreensão das interdependências entre os riscos geopolíticos e outros aspectos.



**A preocupação com os talentos fortaleceu sua posição no topo dos desafios, com 77% dos líderes indicando essa questão como prioritária em 2023 – no levantamento anterior, esse percentual foi de 69%.**

Fonte: KPMG. *Keeping Us Up At Night 2023. 2023.*

## Pessoas e talentos

A covid-19 acelerou o trabalho remoto e flexível, ao mesmo tempo em que afetou a livre circulação de trabalhadores. Isso resultou em níveis mais altos de participação da força de trabalho. Embora existam incertezas relativas aos possíveis impactos macroeconômicos associados a uma desaceleração nas atividades de consumo e investimento, incluindo congelamentos de contratação e redução de pessoal, a questão do “talento” continua sendo uma questão-chave para as organizações, que estão lidando com diversos desafios de curto prazo relacionados a pessoas e talentos. Por exemplo:

- **Cultura** – novo modelo híbrido de local de trabalho e manutenção da conexão, do engajamento e do trabalho em prol de um objetivo comum.
- **Aprendizagem** – a natureza da aprendizagem e do desenvolvimento em um mundo virtual e a necessidade de efetuar ajustes nos métodos tradicionais de troca de ensino.
- **Retorno ao escritório** – equilibrar a flexibilidade proporcionada pelo trabalho em casa e o retorno ao escritório.
- **Tecnologia** – aumento de exposição a riscos devido ao trabalho remoto (no que se refere à segurança cibernética) e capacitação da força de trabalho para enfrentar um futuro mais digitalizado.
- **Retenção de talentos** – os aumentos salariais não têm acompanhado a elevação do custo de vida, o que amplia os riscos relacionados à retenção dos talentos existentes e à gestão dos orçamentos de remuneração.
- **Aquisição de talentos** – o desemprego continua baixo, resultando em escassez contínua de habilidades e talentos. As organizações dispõem de cada vez menos talentos; ao mesmo tempo, os funcionários estão mais exigentes, pleiteando flexibilidade no trabalho, remuneração atrativa e alinhamento pessoal com o propósito e a responsabilidade social da organização.
- **Bem-estar e obrigações psicossociais** – as empresas lidam com os impactos da pandemia no bem-estar dos funcionários e com as novas legislações focadas em gestão de riscos psicossociais no ambiente corporativo. Os riscos psicossociais podem ser baseados em eventos (*bullying* e violência, por exemplo) ou podem ser cumulativos (demandas do trabalho, falta de suporte, baixo reconhecimento etc.).

### Resposta da auditoria interna

A auditoria interna desempenha papel fundamental na avaliação dos riscos relacionados a pessoas e talentos, incluindo:

- Atividades estratégicas de planejamento de força de trabalho alinhadas à estratégia futura da organização e às necessidades da força de trabalho.
- Programas de atração e retenção de talentos e planejamento sucessório.
- Compreensão dos impactos trazidos pelo desligamento de funcionários, pela vacância de cargos e pelos congelamentos de contratações no ambiente de controle interno.
- Preparação e avaliação de riscos psicossociais.

# Confiança organizacional

A confiabilidade de uma organização e a cultura de confiança que a sustenta são fundamentais para o seu sucesso. Obter e manter a confiança de seus principais stakeholders, ou seja, de funcionários, clientes, investidores e reguladores, é crucial, mas não o suficiente. As vozes daqueles que compõem sua cadeia de suprimentos e dos membros da comunidade em que você opera também são essenciais. Por isso, é fundamental que as organizações compreendam e respondam aos anseios de seus stakeholders diretos e indiretos.

Nos últimos anos, mudou bastante a mentalidade das pessoas quando estas escolhem seus empregadores preferidos. A remuneração não é mais o principal motivador para que alguém escolha um local para trabalhar. Fatores como flexibilidade, cultura corporativa e abertura para a realização de um trabalho significativo favorecem as organizações que cultivam valores sociais mais fortes.

Da mesma forma, os clientes fazem escolhas cada vez mais conscientes em relação à integridade e à credibilidade dos produtos e serviços que adquirem; eles também valorizam a experiência de compra. Reguladores e investidores, por sua vez, estão em busca de evidências de confiabilidade organizacional por meio de transparência, integridade e responsabilidade no que concerne ao compliance e às divulgações relacionadas.

Organizações que não conseguem articular e incorporar uma proposta de valor convincente para os funcionários, que não estão cientes das preferências dos consumidores e/ou que não atendem às expectativas de compliance e desempenho encontrarão dificuldades em reter talentos e manter a integridade da marca e a relevância no mercado.

## Resposta da auditoria interna

A auditoria interna deve avaliar os controles de privacidade e proteção de dados relacionados à forma como, por que e quais dados são coletados, armazenados, protegidos, retidos e descartados, em conformidade com as expectativas regulatórias e sociais. Com o aumento da previsão algorítmica e da inteligência artificial, a Auditoria Interna deve questionar como e por quais motivos as informações estão sendo utilizadas.

Também deve compreender quais provedores terceirizados têm acesso aos dados de uma organização ou hospedam esses dados, bem como os controles que protegem seu uso.

# Privacidade e dados

Enquanto os avanços tecnológicos continuam sendo fundamentais para o crescimento e a eficiência das organizações, os clientes, funcionários e reguladores estão cada vez mais preocupados com a proteção e o uso de suas informações pessoais. Em 2022, ocorreram violações de dados significativas e de alto perfil, resultando em impactos generalizados na comunidade e maior conscientização sobre vulnerabilidades a ataques maliciosos. As organizações enfrentam penalidades financeiras mais altas por violações graves ou repetidas de privacidade, bem como ramificações reputacionais, caso as práticas de privacidade, segurança e dados não sejam eficazes.

Assim, as organizações devem determinar, tanto legal quanto eticamente, quais dados coletar, quais dados reter e por quanto tempo; quais controles devem ser usados para proteger esses dados; e quais decisões tomar com base nesses dados e de que maneiras fazer isso.

## Resposta da auditoria interna

A auditoria interna deve avaliar controles de privacidade e proteção de dados, abrangendo aspectos como a coleta, armazenamento, proteção, retenção e descarte de informações. É essencial que essa avaliação esteja em conformidade com as expectativas regulatórias e sociais. Com o avanço das previsões algorítmicas e da inteligência artificial, a Auditoria Interna deve se atualizar e abordar questões relevantes sobre o uso e a finalidade das informações coletadas.

Também deve compreender quais provedores terceirizados têm acesso aos dados ou hospedam as informações da organização. É crucial conhecer os controles implementados por esses provedores para proteger o uso adequado dos dados.





## Resiliência

No atual cenário econômico, geopolítico e ambiental enfrentado pelas organizações, destaca-se a importância de sistemas robustos e resilientes, sustentados por uma força de trabalho crítica. Eventos como a pandemia e o conflito na Ucrânia demonstram a interconexão de diferentes fatores e a concentração de risco quando esses eventos ocorrem. Estar preparado para lidar com disrupções é crucial, não apenas para sobreviver a elas, mas para prosperar.

Por exemplo: os efeitos das mudanças climáticas estão pressionando as organizações a se adaptarem e a prosperarem. A força e a frequência de eventos climáticos extremos, tais como as enchentes significativas ao longo da costa leste, em 2022, e no norte da Austrália Ocidental, no início de 2023, geraram pressões significativas sobre os sistemas das organizações, causando interrupções nas cadeias de suprimentos e danos à infraestrutura vital. As organizações devem garantir que suas operações tenham planejamento e sejam resilientes a esses impactos climáticos.

Da mesma forma, a pandemia testou a resiliência, a flexibilidade e as habilidades das forças de trabalho para que estas mantivessem as operações de forma segura. As organizações devem entender a composição de sua força de trabalho crítica: quais funções e profundidade de recursos são necessárias? Que habilidades são exigidas agora e quais serão cruciais para atender às futuras necessidades organizacionais – por exemplo, operadores digitais e profissionais com habilidades energéticas contemporâneas? E quais opções existem, seja por meio da automação, seja aproveitando arranjos de contratação?

### Resposta da auditoria interna

A auditoria interna deve estar atenta às forças exteriores que podem impactar a organização e ter uma compreensão a respeito de como um evento imprevisto se manifestaria. Ao avaliar ameaças à resiliência, é importante que a Auditoria Interna entenda o que é mais importante para os clientes e principais *stakeholders*, reunindo esses diversos pontos de vista – tais como cadeias de suprimentos, segurança cibernética, tecnologia, riscos de terceiros, gerenciamento de instalações, saúde e segurança, regulatórios e especialistas em continuidade de negócios etc. – para garantir que todos os aspectos, as estratégias e os impactos resultantes sejam considerados.

Também deve garantir que a organização compreenda o impacto de possíveis interrupções, defina que tipos de disrupção seriam intoleráveis e o custo/benefício associado às medidas de resiliência.

## Regulação

A complexidade e a velocidade das mudanças regulatórias continuam à medida que a tecnologia, a disrupção e as questões ambientais, sociais e de governança (ESG) e a proteção dos indivíduos (privacidade, finanças do consumidor, segurança psicossocial) levam os órgãos reguladores a responder rapidamente com novos requisitos de *compliance*. As reformas regulatórias (propostas e promulgadas) refletem esforços crescentes para aprimorar a resiliência organizacional e responder às tecnologias emergentes que não se enquadram nas regulamentações atuais.

Além de se adaptar às mudanças regulatórias, as organizações devem desenvolver proativamente – e, o mais importante, manter – uma abordagem ágil e padronizada para *compliance*, que considere as tecnologias emergentes e seja aplicada em várias jurisdições, à medida que sua presença e suas expectativas regulatórias crescem. Da mesma forma, as organizações líderes estão investindo em automação para transformar operações, processos e até mesmo modelos de negócios, de modo a impulsionar a resiliência e a agilidade diante das mudanças regulatórias.

As abordagens regulatórias futuras provavelmente passarão da conformidade com regras detalhadas para uma abordagem baseada em resultados, priorizando a segurança das atividades e seu potencial em gerar benefícios para o cliente.

### Resposta da auditoria interna

As organizações precisam manter seus esforços de conformidade em constante evolução, para garantir que o ambiente de controle permaneça sólido diante das mudanças nas expectativas e nos requisitos regulatórios, das tendências de risco e dos riscos emergentes. A evolução na conformidade é imprescindível, mesmo que o perfil de risco de uma organização permaneça praticamente inalterado.

A auditoria interna deve garantir que o modelo operacional de conformidade e os sistemas de gestão atendam efetivamente às obrigações de conformidade da organização; mitiguem os riscos de não conformidade; e possam prever e responder rapidamente às mudanças nas expectativas regulatórias e dos *stakeholders*. A auditoria interna deve apoiar a gestão na identificação de oportunidades, para aprimorar as atividades de controle por meio da automação.

## Segurança cibernética

Os riscos cibernéticos continuam sendo uma área de foco primordial para as organizações. O ambiente empresarial permite que o risco cibernético seja alimentado por um volume cada vez maior de dados sensíveis, que circulam por redes interconectadas e integradas. Nos últimos anos, incidentes cibernéticos de alto perfil destacaram a necessidade de sistemas seguros e resilientes para proteger esses dados sensíveis.

O Centro Australiano de Segurança Cibernética (ACSC, na sigla em inglês) observa, em seu Relatório Anual de Ameaças Cibernéticas de 2021-2022, que os australianos relatam um novo incidente cibernético a cada sete minutos, apresentando riscos cibernéticos que podem resultar em graves violações regulatórias, impactos financeiros e perda da confiança do consumidor. As organizações devem compreender quais são esses riscos e tomar medidas para mitigá-los. As ameaças mais prevalentes são *phishing*, engenharia social e *ransomware*, deixando os dados e sistemas vulneráveis.

### Resposta da auditoria interna

A auditoria interna deve continuar avaliando a veracidade dos controles para mitigar os riscos de segurança cibernética. A auditoria interna deve garantir que a primeira e a segunda linhas avaliem e comuniquem continuamente a eficácia dos controles de segurança cibernética.

Também cabe à auditoria interna ir além das avaliações tradicionais de estrutura para avaliar comportamentos pessoais que afetam a capacidade da organização de se proteger contra ataques cibernéticos.

### O Relatório de Insights de Segurança Cibernética, da KPMG, destaca:

48%

estavam menos confiantes na capacidade de sua organização de avaliar subjetivamente os riscos cibernéticos.

80%

sentiram que a adoção de Inteligência Artificial e Aprendizado de Máquina (IA/ML) levanta desafios únicos de segurança cibernética, os quais devem ser priorizados.

75%

acreditam que colaborar com partes interessadas ampliadas, como fornecedores e clientes, é vital para garantir a segurança cibernética de uma organização.

Os brasileiros têm uma das atitudes mais positivas em relação à IA (Inteligência Artificial) no cenário global. Na comparação com os respondentes dos 16 países pesquisados eles frequentemente são superados apenas pelos indianos e chineses na abordagem de questões-chave, e frequentemente estão lado a lado com os sul-africanos.

Fonte: KPMG. Trust in Artificial Intelligence. 2023.

## Disrupção

Muitas organizações estão lidando com os riscos e as oportunidades da disrupção digital de alguma forma. Avanços tecnológicos, como inteligência artificial (IA), *blockchain*, computação em nuvem e Internet das Coisas (IoT), continuam impulsionando a digitalização. No atendimento ao cliente, o uso de *chatbots* propicia suporte instantâneo e personalizado aos clientes, por meio de plataformas de mensagens, sites e aplicativos móveis. O rápido crescimento de aplicações de IA generativa, como o ChatGPT, representa uma aplicação de negócios significativa por meio da automação de tarefas humanas e do processamento de dados complexos. Nas cadeias de suprimentos, o aprendizado de máquina transformou a forma como as atividades de previsão de demanda são realizadas, identificando padrões para prever a demanda futura.

Atitudes sociais em mudança impulsionaram e demandaram a digitalização. No ambiente de trabalho, muitas pessoas aderiram ao trabalho remoto e às interações virtuais. Em casa, as pessoas estão usando dispositivos digitais para realizar tarefas cotidianas, incluindo fazer pedidos de comida e interagir com fornecedores de serviços de saúde. As organizações também têm adotado novos modelos de negócios por meio do comércio eletrônico, pagamentos sem contato e implementação de *buy now, pay later* (compre agora, pague depois).

É essencial manter um foco contínuo na proteção de dados, na privacidade e no uso ético das tecnologias emergentes no âmbito das organizações; e deve-se fazer isso cada vez mais, por meio da cadeia de fornecimento estendida e das alianças de negócios.

### Resposta da auditoria interna

À medida que as organizações adotam tecnologias emergentes e novas formas de negócio, o plano de auditoria interna deve permanecer ágil e adaptar-se aos processos de negócio em constante mudança. A Auditoria Interna deve garantir que os riscos e aspectos éticos associados a essas mudanças tenham sido avaliados e que os controles e a governança apropriados tenham sido implementados.

Os auditores internos precisam constantemente aprimorar seus conhecimentos técnicos para acompanhar as últimas tendências em tecnologia.

# ESG

Cada vez mais países estão adotando as melhores práticas globais; além disso, a sociedade está exigindo divulgações de maior qualidade com evidências de progresso em relação às metas ESG. Requisitos obrigatórios de ESG entrarão em vigor à medida que o Conselho Internacional de Normas de Sustentabilidade (ISSB) finalizar sua base global abrangente de Normas de Divulgação de Sustentabilidade e Clima.

Esse impulso exigirá o desenvolvimento de métricas comparáveis, acesso a dados de qualidade e estratégias de gerenciamento de dados para auxiliar no monitoramento e medição do cumprimento e desempenho das metas ESG. A COP27 deu grande ênfase à priorização de uma transição para uma economia descarbonizada, com a transição energética no centro desse processo. As organizações devem compreender os riscos de transição para alcançar seus objetivos ESG.

## Resposta da auditoria interna

Combinando a mudança em direção a requisitos de relatórios obrigatórios e a quantidade de capital comprometido com a transição ESG, a auditoria interna desempenha um papel fundamental no apoio às organizações para que estas gerenciem adequadamente os riscos ESG.

### Considerações em toda a organização

Definição de ESG:

- Missão, visão, valores e estratégia.
- Revisão periódica pela alta administração.
- Análise do contexto e dos *stakeholders*.
- Tempo, recursos e orçamento.

### Relatórios

- Relatórios regulatórios prováveis.
- Relatórios periódicos para a administração e o conselho.
- Relatório externo para os *stakeholders*.
- Manutenção de registros.

### Gestão de problemas e investigação

- Gestão e remediação de problemas/reclamações.
- Resposta a exames/inspeções regulatórias.
- Plano de resposta e processo para investigar alegadas não conformidades.
- Melhoria contínua.

### Riscos de sustentabilidade

- Avaliação de riscos (e oportunidades).
- Requisitos regulatórios.
- Revisão de novos produtos.
- *Due diligence* de terceiros.

### Avaliação de controles

- Monitoramento e rastreamento de mudanças regulatórias.
- Testes de processos e controles.
- Avaliação periódica do programa de riscos ESG.
- Coordenação com outros provedores de garantia (por exemplo, 2ª linha).

### Cultura organizacional e conscientização

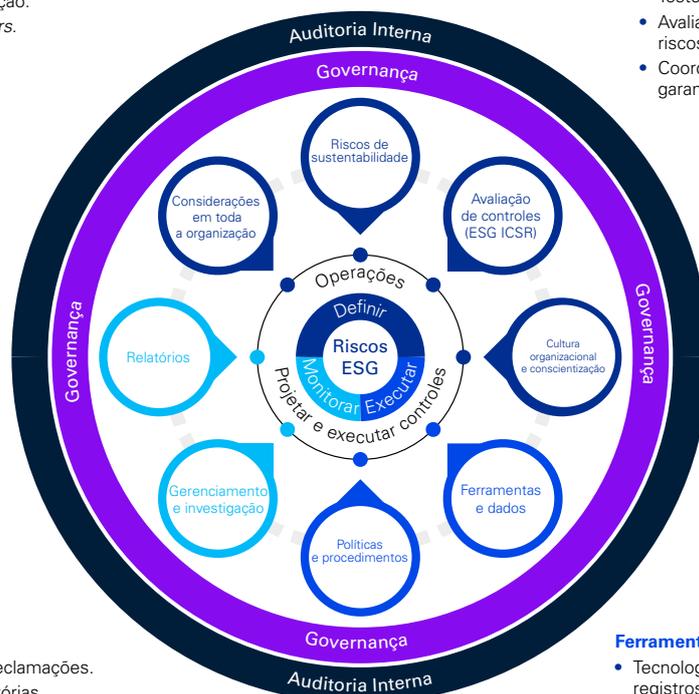
- Engajamento e diálogo com todos os *stakeholders*.
- Cultura/ambiente de ESG/sustentabilidade e mudança comportamental.
- Treinamento regular e frequente e comunicação.

### Ferramentas e dados

- Tecnologia para apoiar o programa ESG (testes, registros de treinamento etc.).
- Medidas preditivas: indicadores-chave de risco e de desempenho.
- Análise e tendências de causa raiz.
- Governança/gerenciamento de dados.

### Políticas e procedimentos

- Existência e gestão de políticas de ESG.
- Políticas e procedimentos em toda a entidade (capital humano, saúde e segurança, segurança cibernética, práticas de empréstimos e crédito, investimentos etc.).
- Coerência entre o arcabouço de políticas e a estratégia.





# Auditoria Interna em Foco: Ano Fiscal 2024

Uma perspectiva de auditoria interna sobre os principais riscos enfrentados pelas organizações

Agosto de 2023

[kpmg.com.br](https://kpmg.com.br)

# Fale com o nosso time

## **Fernando Lage**

**Sócio-líder de Governance, Risk & Compliance Services da KPMG no Brasil**

Tel: +55 19 3198-6745

flage@kpmg.com.br

## **Julio Carvalho**

**Sócio-líder de Auditoria Interna da KPMG no Brasil**

Tel: +55 85 99175-6611

julio-carvalho@kpmg.com.br

## **Érica Oliveira**

**Gerente de Auditoria Interna da KPMG no Brasil**

Tel: +55 11 94156-8332

ecoliveira@kpmg.com.br

[kpmg.com.br](https://kpmg.com.br)



Os serviços descritos neste material, no todo ou em parte, podem não ser permitidos a ser prestados a clientes de auditoria da KPMG e suas afiliadas ou entidades relacionadas.

© 2023 KPMG Consultoria Ltda., uma sociedade simples brasileira, de responsabilidade limitada e firma-membro da organização global KPMG de firmas-membro independentes licenciadas da KPMG International Limited, uma empresa inglesa privada de responsabilidade limitada. Todos os direitos reservados. MAT230806

O nome KPMG e o seu logotipo são marcas utilizadas sob licença pelas firmas-membro independentes da organização global KPMG.

Todas as informações apresentadas neste documento são de natureza genérica e não têm por finalidade abordar as circunstâncias de um indivíduo ou entidade específicos. Embora tenhamos nos empenhado em prestar informações precisas e atualizadas, não há nenhuma garantia sobre a exatidão das informações na data em que forem recebidas ou em tempo futuro. Essas informações não devem servir de base para se empreender ação alguma sem orientação profissional qualificada e adequada, precedida de um exame minucioso da situação concreta.