

**Deloitte.**



# Cinco Pilares de Riscos Empresariais 2022

7ª edição da pesquisa

# Índice

01

Estrutura de riscos, governança e compliance 5

02

Os riscos no mapa 15

03

ESG: importante, mas desafiador 22

04

A tecnologia como aliada 24

05

Perfil da amostra 28

# A função de riscos entre oportunidades e inflexões

A cada dois anos, a Deloitte apresenta ao mercado os resultados da pesquisa “**Cinco Pilares de Riscos Empresariais**”. Em sete edições de nossa pesquisa bianual sobre as tendências e práticas da gestão de riscos, pudemos acompanhar a evolução do mercado e como as organizações respondem, em cada momento, aos temas mais relevantes para a função.

Neste biênio, observamos a emergência do ESG, sigla em inglês para governança ambiental, social e corporativa. A função de gestão de riscos tem uma visão privilegiada sobre como esses aspectos influenciam as operações e os resultados de negócios. Indo além, é um agente fundamental para incutir esse tema na prática, por meio de ações estruturadas e sinérgicas.

Assim, neste relatório você poderá observar como as 130 organizações pesquisadas compreendem e lidam com a pauta ESG – e como esse tema tende a se tornar tão tangível e discutido nas altas instâncias quanto os resultados financeiros.

A tecnologia é uma alavanca para o aperfeiçoamento da função de riscos nas organizações, como mostra o apetite apresentado pelas empresas participantes em incorporar sistemas e metodologias.

Mais uma vez, compartilhamos um retrato do cenário atual, em meio a um ciclo repleto de oportunidades e inflexões. Espero que as informações aqui trazidas tragam luz ao debate e contribuam o amadurecimento da função de gestão de riscos no ambiente de negócios do Brasil.

Tenha uma ótima leitura!



**Anselmo Bonservizzi**  
Sócio-líder de Risk Advisory da Deloitte

“A função de gestão de riscos é um agente fundamental para incutir o tema de ESG na prática, por meio de ações estruturadas e sinérgicas.”



01

02

03

04

05

# Sumário executivo



## A conclusão

Frente a um contexto de negócios global e interinfluyente, a função de gestão de riscos deve transformar-se para endereçar não apenas os aspectos financeiros e operacionais, mas privilegiar também os grandes temas de impacto sobre os negócios, tais como mudanças climáticas, ESG e cadeia de fornecimento.



## O cenário

Empresas avançam na estruturação de áreas e funções para a gestão de riscos, mas enfrentam desafios em formalização, integração e acompanhamento tempestivo e contínuo dos processos.



## A resposta

A tecnologia, ainda explorada de forma superficial pelas empresas em seus processos de gestão de riscos, é uma forte aliada para habilitar a integração, o caráter preditivo e a automatização dos reportes relacionados à função.

## Metodologia e amostra

Os dados foram coletados por meio de questionário eletrônico, entre agosto e outubro de 2021. Participaram do estudo 130 empresas, entre as quais 39% têm receita líquida anual maior que R\$ 1 bilhão. Entre os respondentes, 73% ocupam cargos executivos ou em conselho em suas respectivas empresas.



01

02

03

04

05

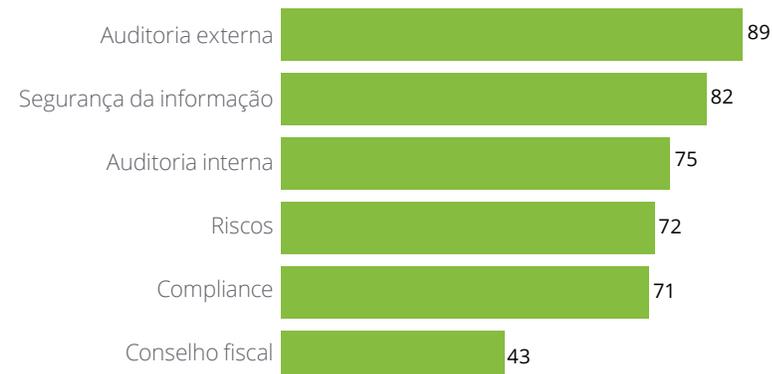
# 01 | Estrutura de riscos, governança e compliance



Muitas empresas avançaram na estruturação de áreas e funções para a gestão de riscos – tais como auditoria contábil, segurança da informação, auditoria interna, riscos e compliance, mas ainda enfrentam desafios na formalização e no acompanhamento tempestivo e contínuo de apetite a riscos, planejamento estratégico e política de gestão de riscos.

A integração das práticas de identificação e classificação de riscos é importante para fortalecer as iniciativas de monitoramento e respostas a ameaças. Nesse sentido, 57% das organizações pesquisadas adotam metodologia Enterprise Risk Management integrada, que identifica e aborda metodicamente os eventos potenciais que representam riscos para a realização de objetivos estratégicos ou para oportunidades de obtenção de vantagem competitiva. Além disso, 54% têm critério unificado na classificação de impacto de riscos e 53% adotam um dicionário unificado de riscos.

**Têm áreas de... (em %; respostas múltiplas)**



**Têm formalizados... (em %; respostas múltiplas)**



“Com a evolução do mercado e o aumento da complexidade da função de riscos empresariais, as organizações deverão aprimorar de forma contínua a sua estrutura de governança, por meio da adoção de modelos mais preventivos e da integração de suas práticas de acordo com o modelo das três linhas para auxiliar na consecução de suas estratégias de negócios.”

**Alex Borges**, sócio e líder de Regulatory Support & Strategic Risk da Deloitte

#### Grau de maturidade da função de riscos

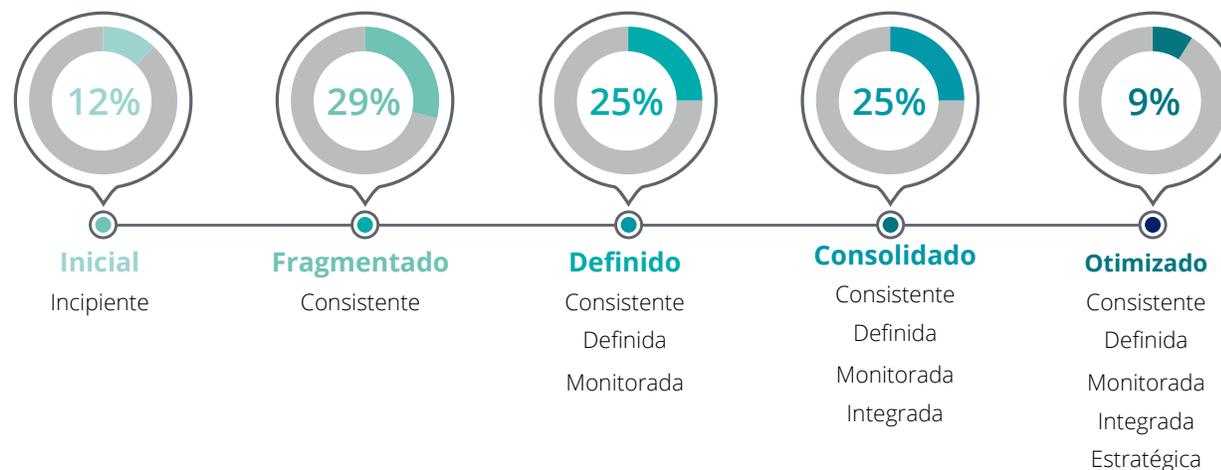
Em termos gerais, a maior parcela das empresas pesquisadas posicionou-se como tendo uma gestão de riscos em estágio fragmentado; ou seja, consistente em pelo menos um de seus processos. Nove por cento afirmaram ter todos os seus processos consistentes, definidos, monitorados de forma centralizada, integrados e alinhados à estratégia. Entre essas organizações com gestão de riscos em estágio otimizado, metade teve receita anual superior a R\$ 1 bilhão em 2020 e apenas 8% faturaram menos de R\$ 100 milhões por ano.

**57%** contam com metodologia ERM integrada

**54%** têm critério unificado na classificação de impacto de riscos

**53%** adotam dicionário unificado de riscos

#### Estágio da gestão de riscos da organização

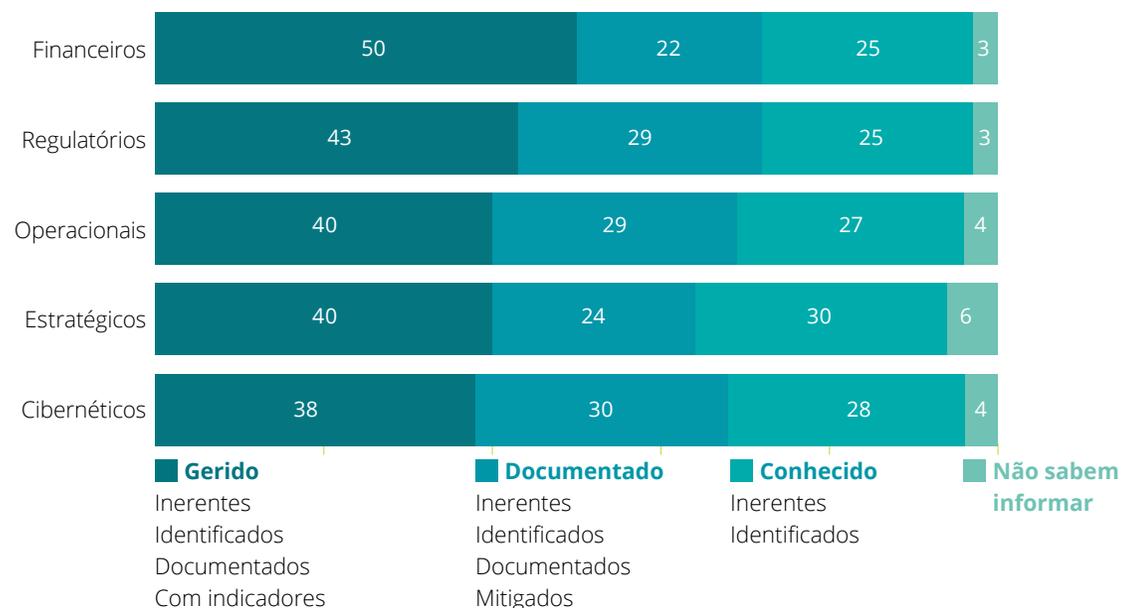


## Cinco Pilares de Riscos Empresariais | Estrutura de riscos, governança e compliance

Para cada um dos pilares de riscos mapeados, a maior parte das empresas indicou ter um grau de ciência avançado, com riscos inerentes, identificados, documentados e com indicadores estabelecidos para gerenciamento tempestivo pela administração. Frente aos demais, os riscos financeiros são os acompanhados mais de perto, enquanto os cibernéticos têm a menor adesão ao grau "gerido" de ciência.

Os riscos financeiros também são os que mais contam com indicadores entre as organizações respondentes, enquanto os riscos cibernéticos são os menos acompanhados por métricas.

### Grau de ciência sobre os riscos (em %)



### Têm indicadores....



**Atividades com espaço para melhorar**

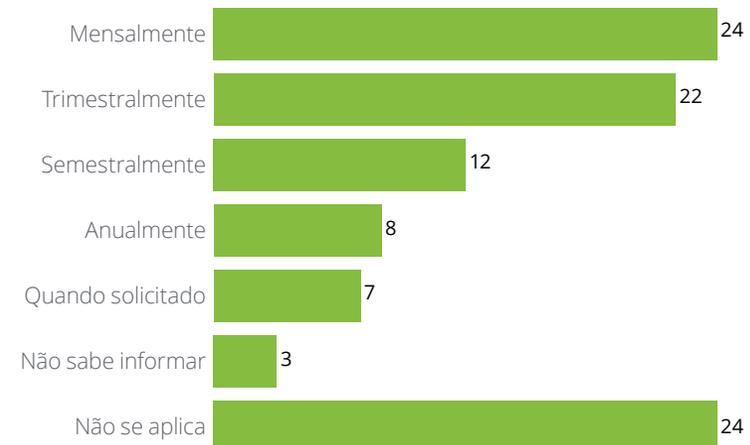
Entre as atividades de gestão de riscos de demandam atenção, a implementação de softwares e plataformas é a que se encontra em nível mais incipiente, segundo os participantes da pesquisa.

O reporte tempestivo de fatores de riscos é uma atividade elementar e que conformará a base para a tomada de decisão das mais altas instâncias da organização, sejam elas executivas ou de governança. Dois terços das empresas pesquisadas destacaram reportar riscos com alguma regularidade – anual, semestral, trimestral ou mensalmente – para o conselho de administração estatutário. Ou seja, ainda há espaço que as empresas se engajem mais na tempestividade e na integração do reporte de riscos às demais funções da gestão de riscos como um todo.

**Nível insuficiente de implementação (em %; respostas múltiplas)**



**Periodicidade com que reportam riscos para conselho de administração estatutário (em %; respostas múltiplas)**



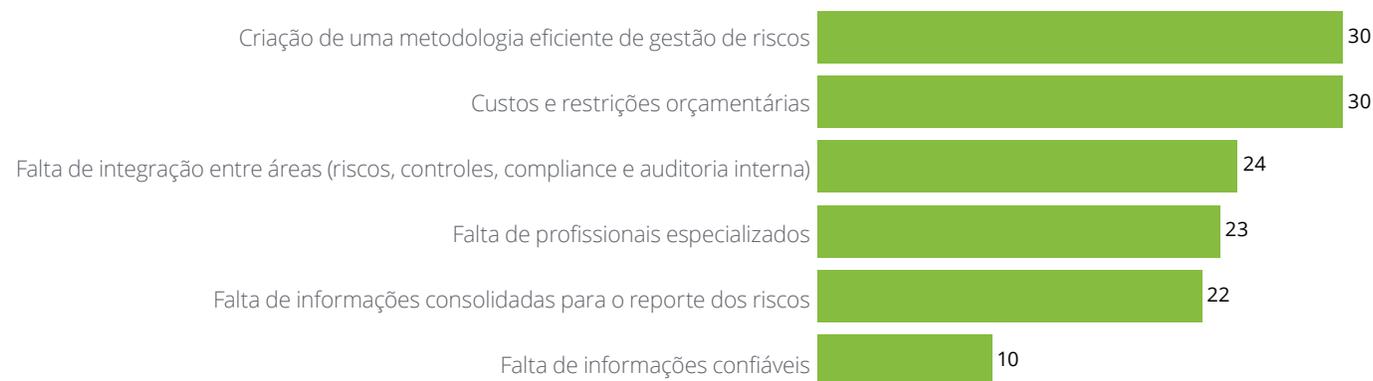
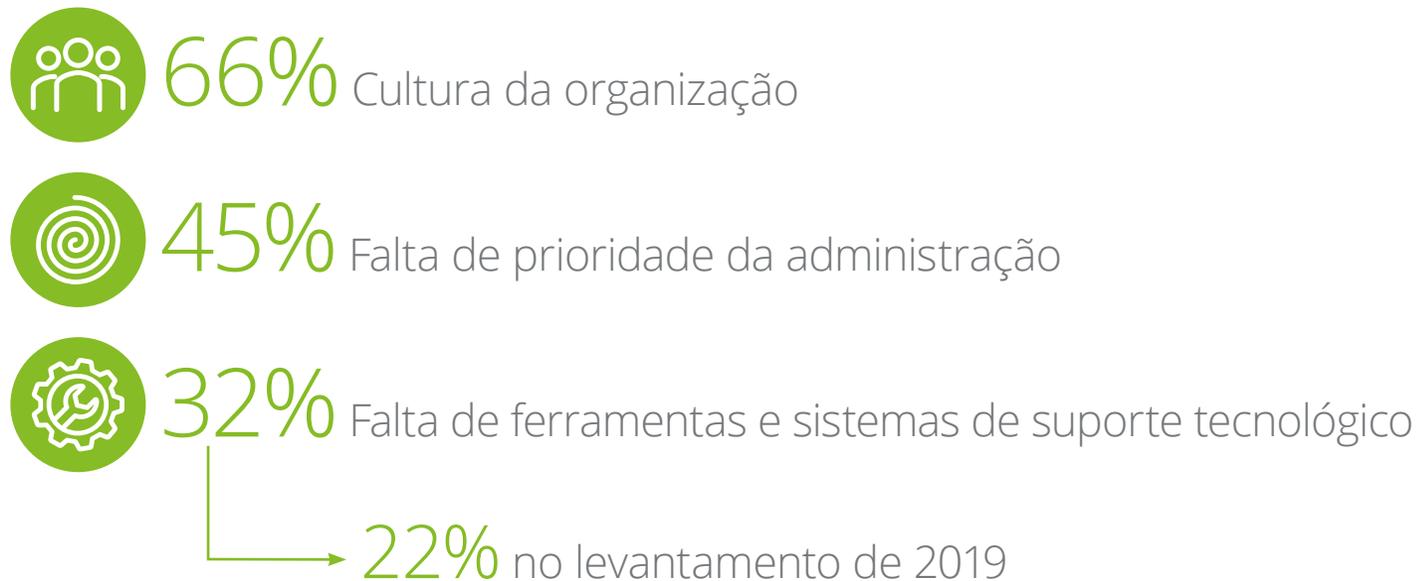
### Cultura e tecnologia como desafios

A cultura organizacional e o engajamento da liderança são os maiores desafios apontados pelas empresas participantes em relação à implantação de um processo eficaz de gestão de riscos, tendência que reproduz algumas das prioridades identificadas na edição de 2019 desta pesquisa. Em 2021, o levantamento registra também a emergência dos aspectos tecnológicos agora ganhando mais relevância entre os desafios identificados: se, em 2019, a falta de ferramentas e de sistemas de suporte tecnológico foi o sexto desafio enfrentado, em 2021 essa alternativa ficou em terceiro lugar.

“Cada nível na organização tem o seu papel, e a cultura de riscos nos ajuda a dar clareza tanto dos benefícios a serem perseguidos quanto dos eventos que podem nos impedir de atingir os principais objetivos como organização.”

**Eduardo Farias**, diretor executivo de Governança e Gestão Integrada da B3

### Principais desafios na implantação de um processo eficaz de gestão de riscos (em %; respostas múltiplas)



### Riscos emergentes

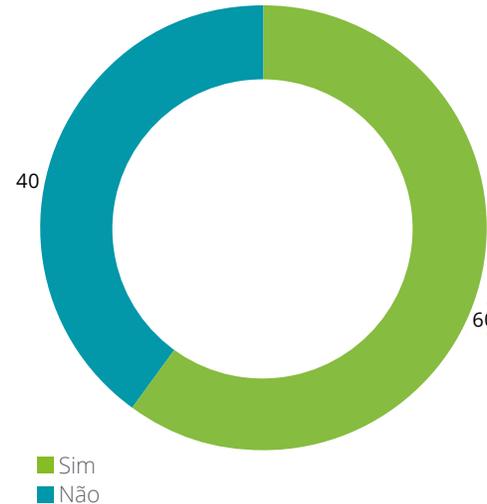
Embora estejam engajadas em identificar riscos emergentes, uma parcela expressiva das organizações pesquisadas ainda não monitora ou responde propriamente e esses riscos.

#### Em relação a riscos emergentes, têm mecanismos para...



Seis em cada dez empresas pesquisadas têm mecanismos para antecipar riscos emergentes. Entre essas organizações, um terço conta com modelagem para esta função.

Têm mecanismos para riscos emergentes (em %)



32% têm modelagem para antecipação de riscos

“A segurança cibernética acelera a transformação digital, na medida em que permite às empresas explorar novas estratégias e novas tecnologias para alavancarem ainda mais os seus negócios.”

**André Gargaro**, sócio e líder da Deloitte Cyber



01

02

03

04

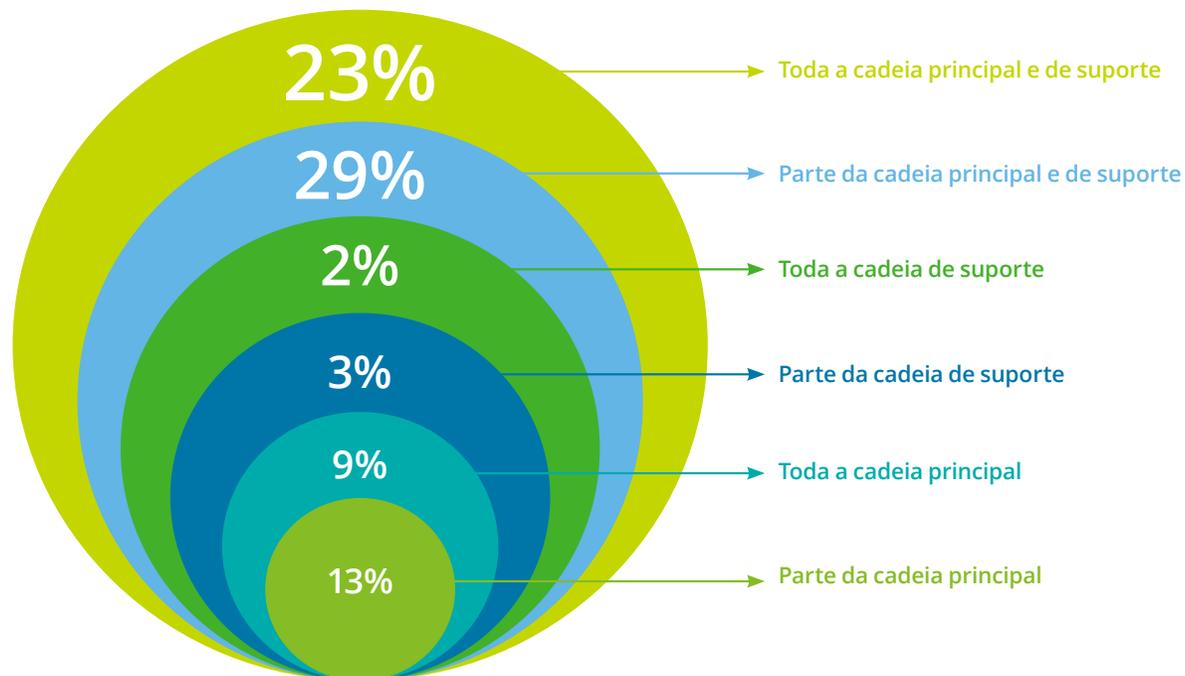
05

### Cadeias principal e de suporte

Ter uma matriz de riscos que mapeie tanto os riscos tanto da cadeia principal quanto de suporte é fundamental para uma gestão de riscos eficaz e adequada aos desafios um ecossistema de negócios cada vez mais integrado e dinâmico. Quase 30% das organizações pesquisadas afirmaram ter uma matriz de riscos e controles mapeados e atualizados para parte das cadeias principal e de suporte. E praticamente um quarto sinalizou contar com essa matriz para todas as etapas de ambas as cadeias.

As organizações de maior porte prevalecem entre as empresas com matriz de riscos definidas parcial ou totalmente para as cadeias principal e de suporte. Entre essas empresas, 58% registraram receita maior do que R\$ 1 bilhão em 2021. Os setores de atividades financeiras, bens de consumo e serviços são os mais avançados na definição dessas matrizes.

Têm matriz de riscos e controles mapeados para...



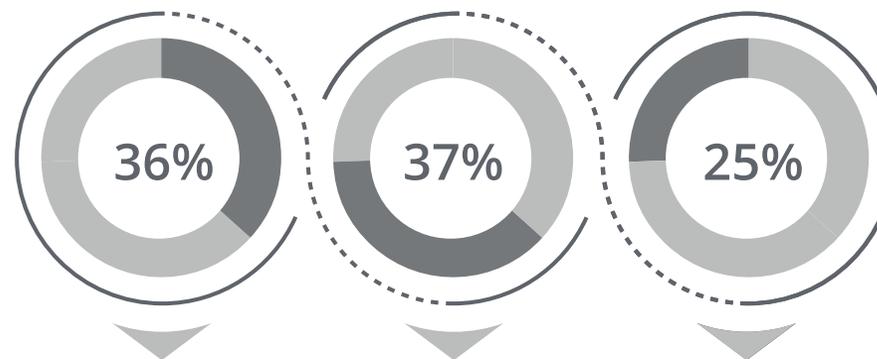
**20%** não têm matriz de riscos definida



O modelo das três linhas visa observar como as lideranças de negócios e as diferentes funções de controles e gestão de riscos interagem para promover a identificação e o endereçamento das ameaças. Em etapas de menor maturidade, há uma carga maior sobre a média e a alta lideranças operacionais e administrativas, em detrimento de atividades robustas de supervisão de riscos e asseguuração. Conforme esta estrutura ganha maturidade, todos os elos dessa cadeia se fortalecem e ganham papéis e reponsabilidade definidos. Mais do que isso: suas funções são vistas não em silos, mas de forma integrada.

Em nossa pesquisa, grande parte das empresas pesquisadas posicionou-se em uma etapa de implementação do modelo das três linhas, ou como tendo a esse processo estabelecido. Um quarto indicou ter maturidade na implementação desse modelo.

**Maturidade do modelo das três linhas**



	<b>Em implementação</b>	<b>Estabelecido</b>	<b>Amadurecido</b>
<b>1ª linha</b> Média e alta gestão das áreas de apoio e de negócios	Excesso de confiança nas gerências	Gerências carecem de propriedade para riscos e controles	Tem responsabilidade ativa na gestão de riscos e inicia o monitoramento de controles
<b>2ª linha</b> Gestão de riscos, canal de denúncias, controles internos e conformidade	Imaturidade em atividades de supervisão	Não possuem um monitoramento de conformidade eficaz	Visão holística e expandida na identificação de riscos emergentes
<b>3ª linha</b> Auditoria interna	Independente e objetiva, mas com asseguuração insuficiente	Esta é a principal fonte de asseguuração	Esforços de asseguuração duplicados



### Gestão de crises

Entre os itens relacionados à gestão de crises, a definição de papéis e responsabilidades é o mais implementado, com larga vantagem sobre o segundo mais adotado – o monitoramento contínuo de potenciais cenários de crises. Os itens menos implementados nesse sentido são comunicações mensais sobre continuidade de negócios e gestão de crises, treinamento de alta gestão para responder a cenários de crises e processos para minimizar cenários de crises. A baixa implementação desses itens é um fator de atenção para as organizações, pois são fundamentais para reação rápida e imediata a fim de evitar ou minimizar possíveis consequências negativas de um evento de crise.

#### Itens de gestão de crises implementados (em %; respostas múltiplas)



**29%** realizaram um simulado de crise nos últimos 24 meses



02

## Os riscos no mapa



01

02

03

04

05

Segundo os respondentes da pesquisa, os riscos que as organizações mais têm gerenciado atualmente são os financeiros e os operacionais, tais como os relacionados a demonstrações financeiras, aderência a regras, endividamento e fluxo de caixa.

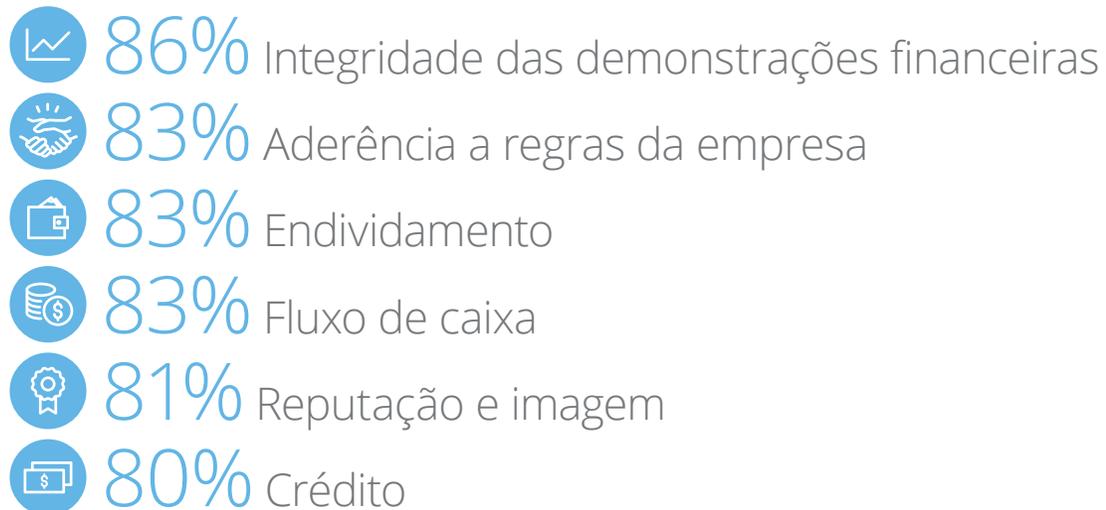
Contudo, quando vemos o horizonte para o médio e o longo prazos, os riscos que mais se mostram desafiadores para as empresas são os estratégicos, que envolvem temas complexos e abrangentes como mudanças climáticas, ESG, comportamento populacional, cadeias de fornecimento e disruptura tecnológica.

Frente a um contexto de negócios global e interinfluyente, a função de gestão de riscos deve, na visão de seus próprios líderes, transformar-se para endereçar não apenas os aspectos financeiros e operacionais do cotidiano da organização, mas privilegiar também os grandes temas de impacto sobre os negócios, como a crise ambiental e a responsabilidade corporativa e social.

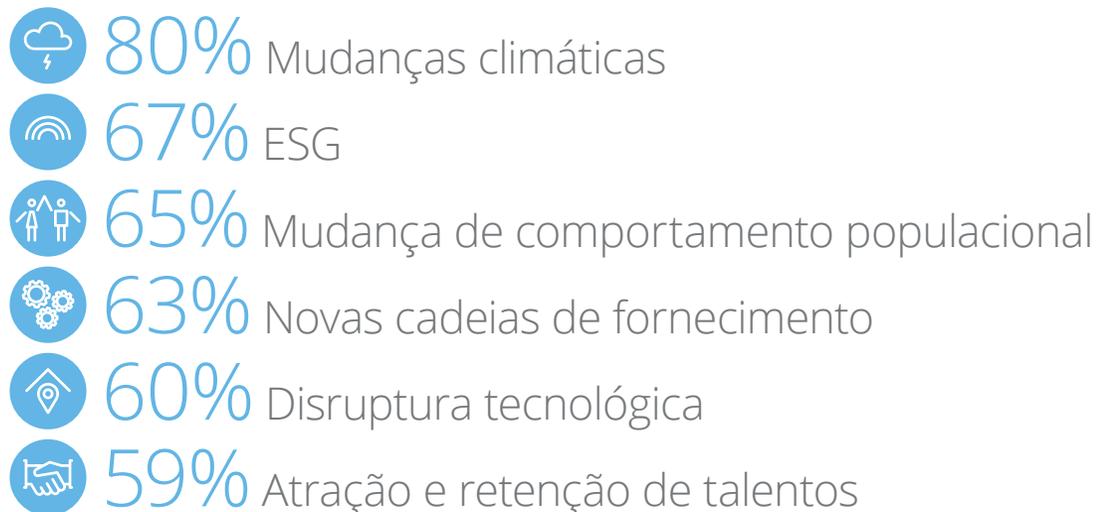
“Ao estruturar de forma robusta e estratégia a sua gestão de riscos, a organização poderá ir além do cumprimento das normas para promover uma cultura de integridade e gerar valor para o negócio e para todas as partes interessadas.”

**Camila Boretti**, sócia e líder de Accounting & Internal Controls da Deloitte

#### Riscos gerenciados hoje

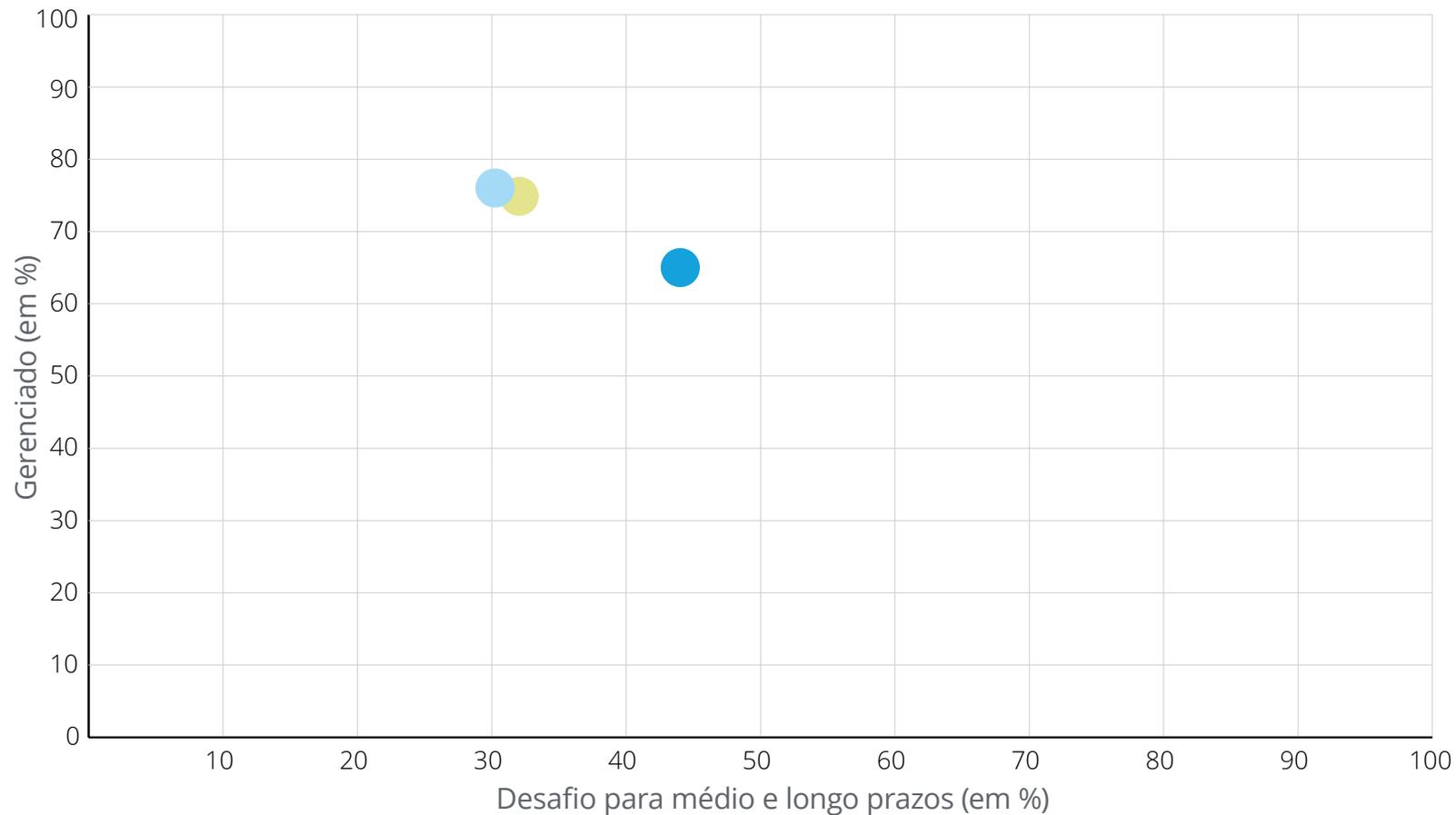


#### Desafios para médio e longo prazos (1 a 3 anos)



## Riscos cibernéticos

### Gerenciamento de riscos cibernéticos



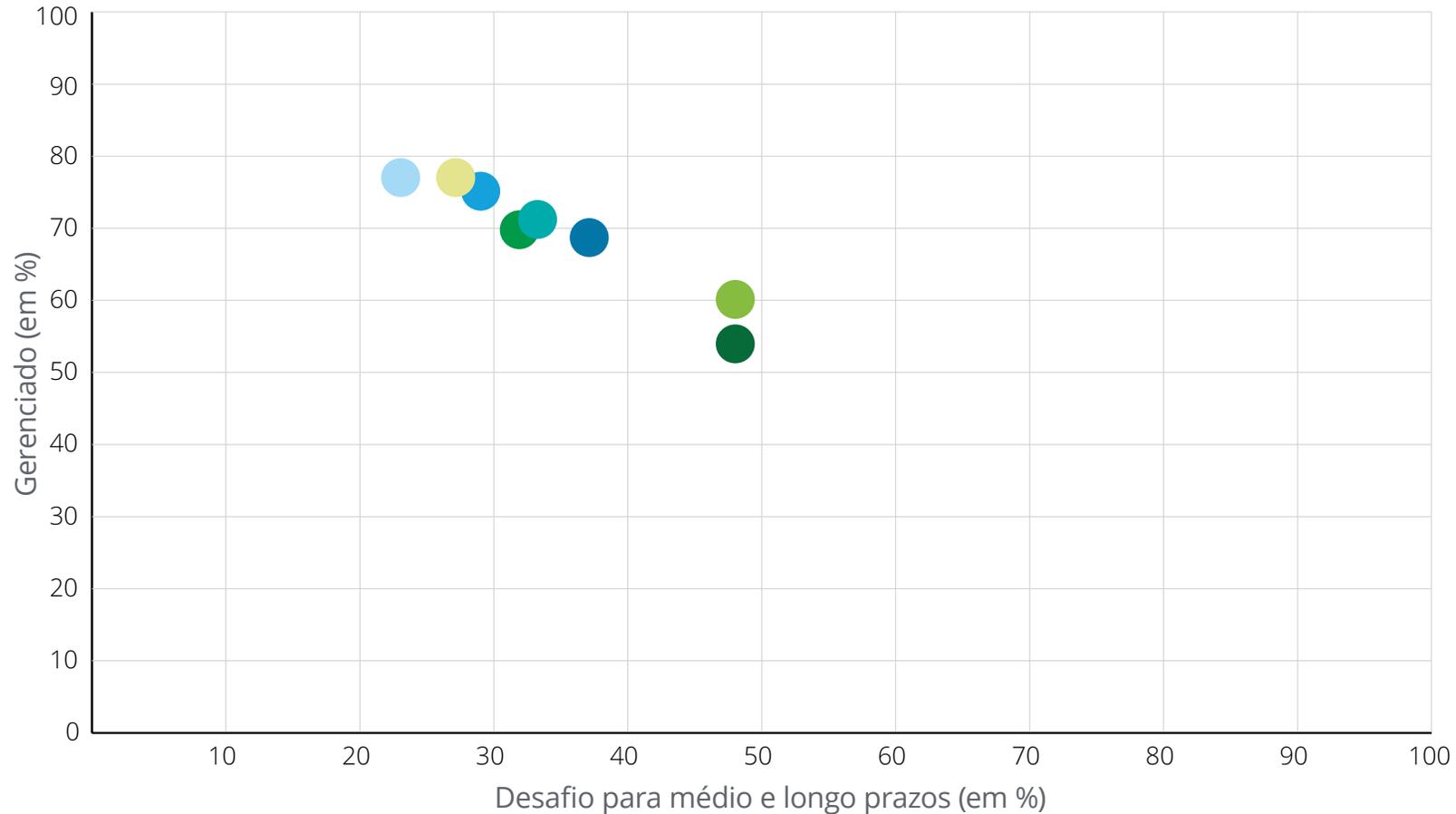
- Identidade e acesso
- Confidencialidade e privacidade
- Ataques de phishing/Engenharia social

A pesquisa **“Cyber – Estratégias para um futuro cibernético”**, de 2021, indica que empresas respondentes que sofreram ataques cibernéticos, 89% realizam investimentos em segurança cibernética. Já entre os 49% dos participantes que não sofreram ataques, o percentual que investe em segurança cibernética é menor: 69%. Esse resultado revela que as empresas tendem a adotar práticas mais robustas de segurança cibernética como respostas a ataques, mais do que preventivamente.



## Riscos regulatórios

### Gerenciamento de riscos regulatórios



- Tributário/fiscal
- Trabalhistas
- Corrupção
- Lei Geral da Proteção de Dados
- Lavagem de dinheiro
- Regulamentações setoriais
- Meio ambiente
- Anticoncorrencial

A pesquisa [“Riscos de conduta – Pessoas e organizações na construção de uma cultura de integridade”](#), de 2020, revela que apropriação indevida e fraude, assédio moral, violação de normas e leis e corrupção foram os tipos de denúncias de maior procedência entre as organizações pesquisadas que sofreram autuação.



01

02

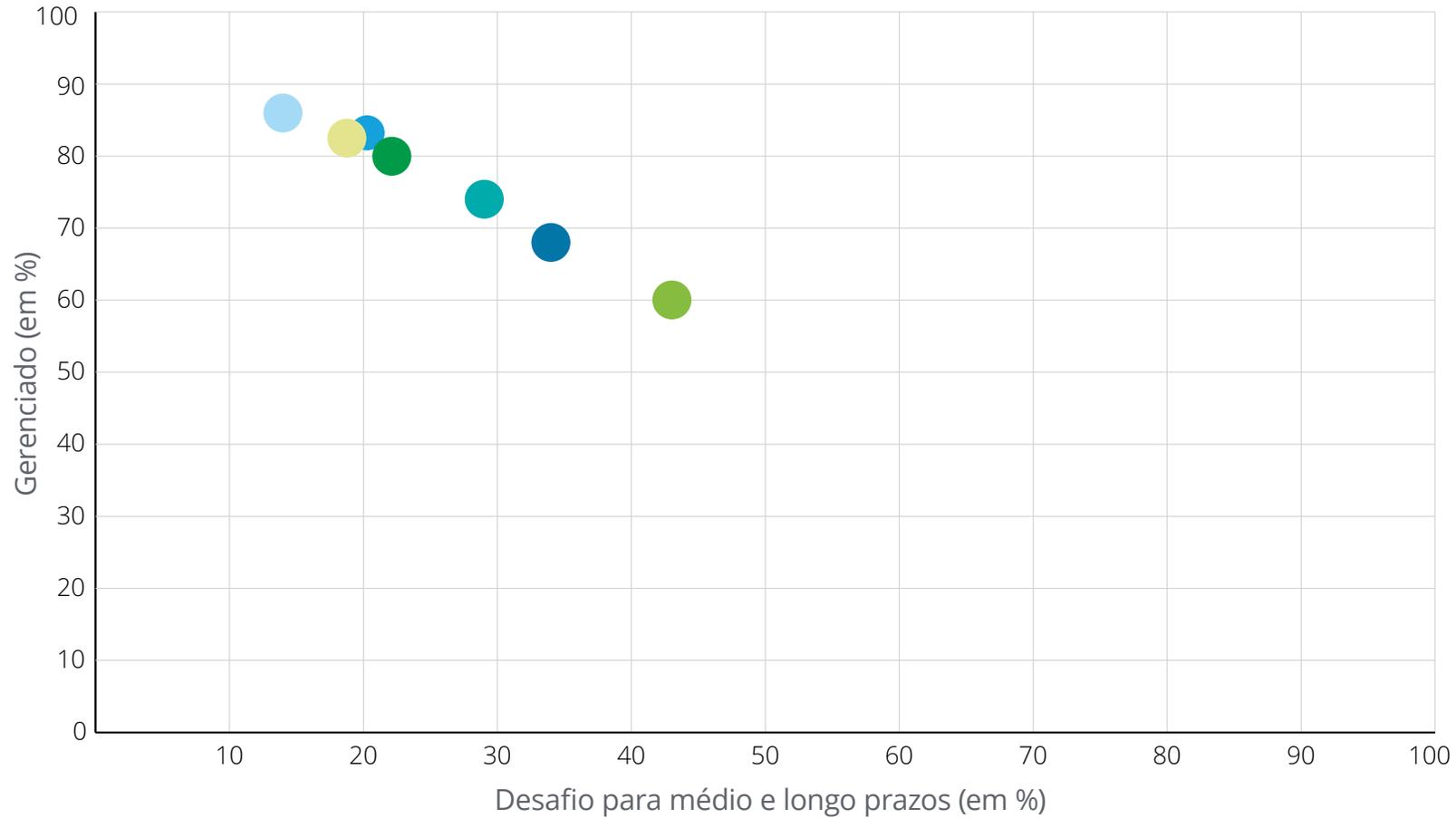
03

04

05

## Riscos financeiros

### Gerenciamento de riscos financeiros



De acordo com a [“CFO Survey 2021”](#), as incertezas do cenário econômico, da política tributária e do ambiente político no Brasil foram apontados pelos líderes de finanças entrevistados como os principais riscos para as empresas.



01

02

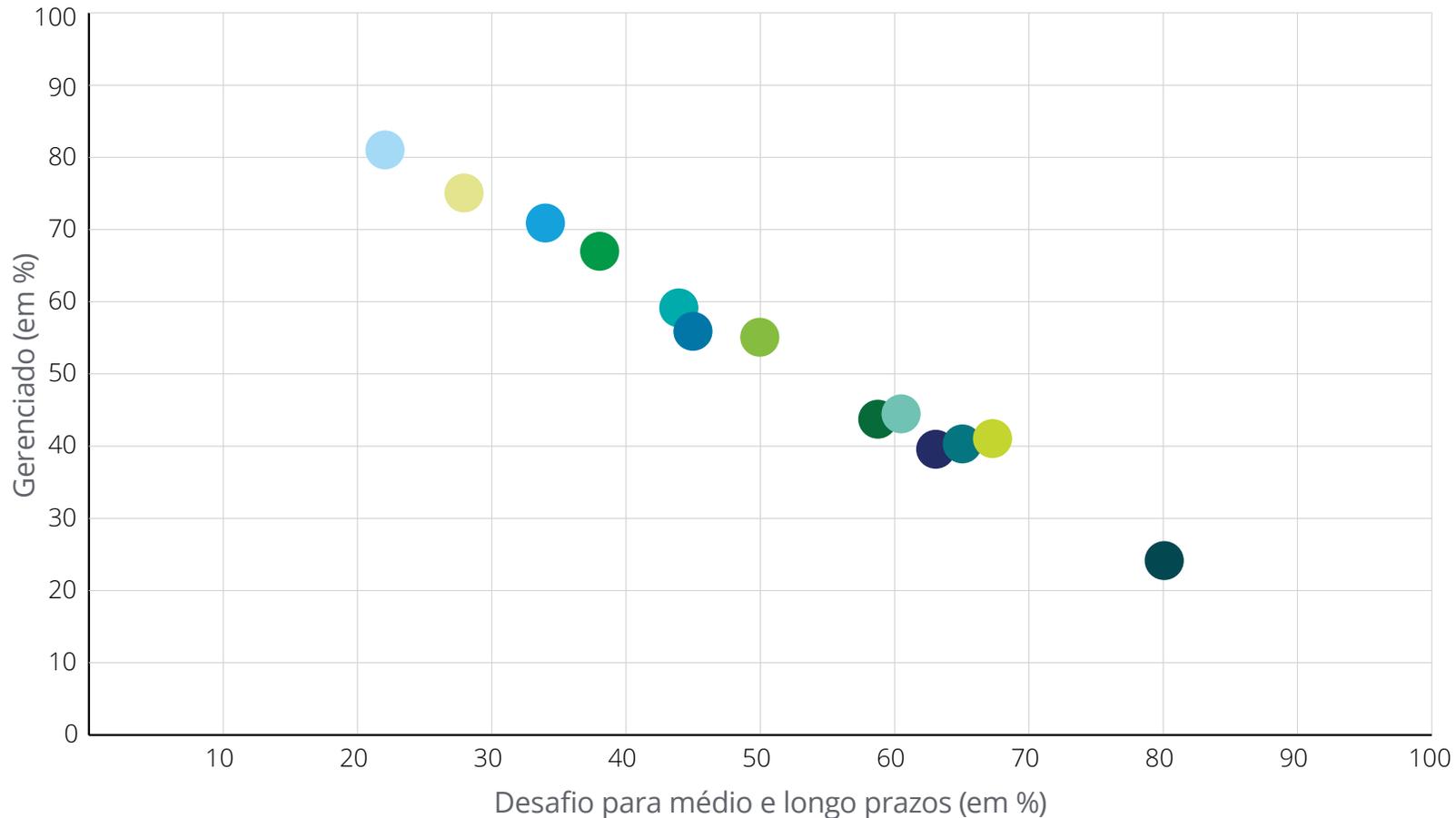
03

04

05

### Riscos estratégicos

#### Gerenciamento de riscos estratégicos



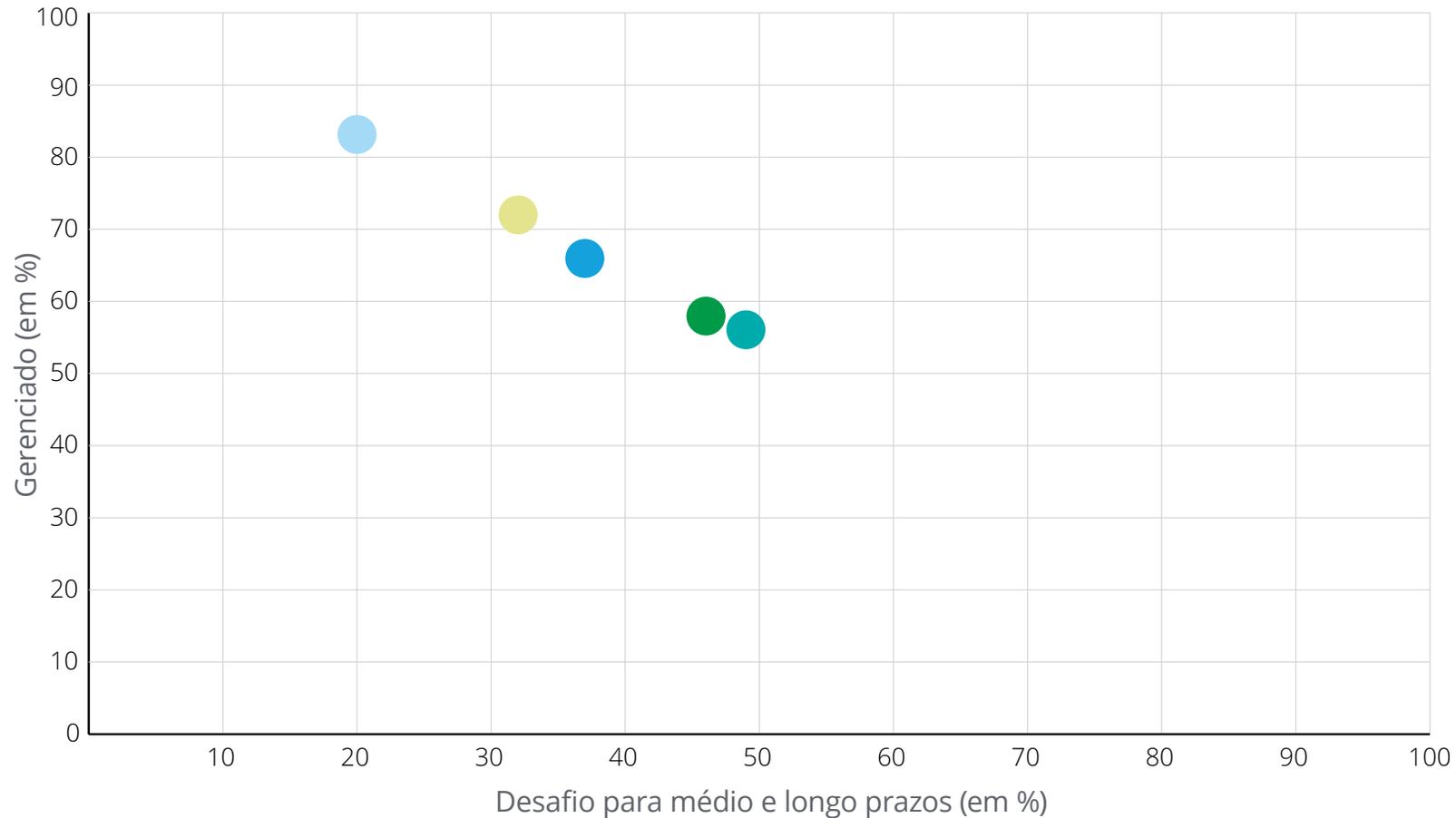
- Reputação e imagem
- Relacionamento com acionistas
- Pandemias
- Concorrência e mercado
- Modelo de trabalho virtual
- Mídias sociais (fake news/reclamações/plágio)
- Dependência de fornecedores
- Disruptura tecnológica
- Atração e retenção de talentos
- ESG
- Mudança de comportamento populacional
- Novas cadeias de fornecimento
- Mudanças climáticas

Conforme a pesquisa **“Novos desafios de comunicação e ESG nas Relações com Investidores”**, de 2021, apenas 12% das empresas pesquisadas listadas em bolsa integram as diferentes áreas da empresa por meio de softwares para responder questões de ESG. Na maior parte das companhias, essa ação é realizada manualmente, por meio de comitê ou pelas áreas de ESG ou RI. Esse resultado revela uma oportunidade de maior adoção de tecnologia para a realização dessas atividades.



## Riscos operacionais

### Gerenciamento de riscos operacionais



- Aderência às regras da empresa
- Capacidade operacional
- Gestão de contratos
- Metas e remuneração variável
- Gestão de terceiros

Segundo a [“Third-party Risk Management Global Survey 2021”](#), 50% das organizações entrevistadas identificaram, durante a pandemia de Covid-19, que necessitavam aumentar moderada ou significativamente seus investimentos na gestão de riscos de terceiros.



01

02

03

04

05

03

**ESG: importante,  
mas desafiador**



01

02

**03**

04

05

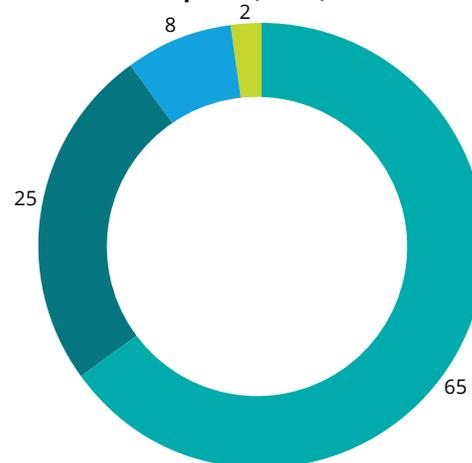
## Cinco Pilares de Riscos Empresariais | ESG: importante, mas desafiador

A governança ambiental, social e corporativa – em sua sigla ESG – já se tornou um verdadeiro mantra na gestão das empresas. E a relevância desse tema tem sido reconhecida pelas organizações: 65% das empresas pesquisadas consideram o ESG importante nas suas atividades cotidianas.

Apesar desse reconhecimento, 58% dos respondentes indicaram que o nível de maturidade de sua empresa em ESG é baixo, em especial entre as empresas de menor porte.

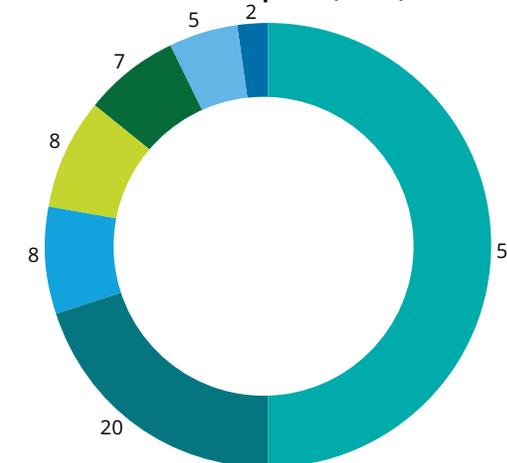
Os respondentes pontuam algumas barreiras a serem enfrentadas, especialmente a falta de compreensão sobre como mensurar e gerir esse tema e a falta de conhecimento sobre o assunto.

Importância do ESG nas atividades do dia a dia da empresa (em %)



- Já é importante
- Será importante em breve
- Não têm perspectiva
- Não sabem informar

Principal barreira para a integração de ESG com o dia a dia da empresa (em %)



- Falta de compreensão sobre como mensurar e gerir
- Falta de conhecimento sobre o assunto
- Crença de que consome muitos recursos financeiros
- Crença de que não cria valor
- Falta de interesse
- Percepção de que consome muito tempo
- Não há barreiras

 **58%** indicam que nível de maturidade de ESG na empresa é baixo

→ **36%** dessas empresas têm receita anual de até R\$ 100 milhões

“A maturidade da organização em ESG envolve a implantação de uma cultura efetiva e com ações concretas, indicando um real engajamento nas questões ambientais, sociais e de diversidade, focando na geração de valor a longo prazo e sem esquecer da governança, que deve refletir a deliberação ética.”

Ricardo Lemos, membro das comissões de Ética na Governança do Conselho do Futuro do IBGC



04 |

## A tecnologia como aliada



01

02

03

04

05

Com larga vantagem, a identificação preditiva de riscos é a principal contribuição de uma boa infraestrutura de dados para a gestão de riscos, conforme as empresas pesquisadas.

Vimos anteriormente que a implementação de softwares e plataformas se encontra em nível insuficiente para 42% das empresas pesquisadas, figurando como a atividade de gestão de riscos mais incipiente entre as organizações participantes. Confirmando esta percepção, pouco mais de um quarto dos respondentes considera avançada a adoção tecnológica de sua organização para a gestão de riscos.

“Tecnologias como a inteligência artificial têm o poder de transformar a gestão de riscos tradicional das empresas, promovendo agilidade e capacidade de análise de cenários futuros.”

**Ronaldo Fragoso**, sócio de Risk Advisory e líder de alianças e ecossistemas da Deloitte

**Principal benefício de uma boa infraestrutura de dados para a gestão de riscos (em %; respostas múltiplas)**



**26%** consideram avançada a adoção tecnológica de sua organização para a gestão de riscos



01

02

03

**04**

05

O mapeamento e o reporte de resultados são as ações mais incorporadas ao sistema de gerenciamento de controles das organizações pesquisadas.

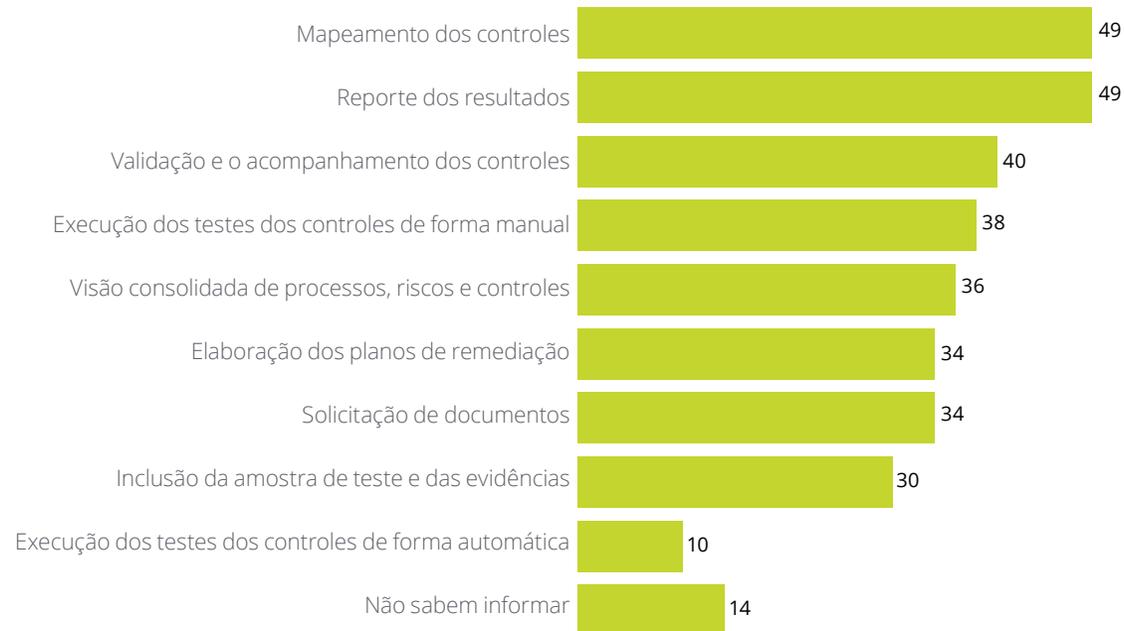
Em relação à estrutura tecnológica, pouco mais da metade das empresas pesquisadas têm uma área de desenvolvimento de novas tecnologias que atende a empresa como um todo.

Cloud é principal iniciativa de transformação digital a ser adotada nos próximos 12 meses pelas organizações. Na sequência estão data analytics e controles operacionais.

**Iniciativas de transformação digital a serem adotadas nos próximos 12 meses**

- 1 Cloud
- 2 Data analytics
- 3 Controles da operação
- 4 Inteligência artificial
- 5 Internet das coisas (IoT)
- 6 Blockchain/Criptomoeda

**O sistema de gerenciamento de controle da organização permite... (em %, respostas múltiplas)**



**54%** têm área de desenvolvimento de novas tecnologias que atende a empresa como um todo



## Cinco Pilares de Riscos Empresariais | **A tecnologia como aliada**

A área de controles internos pode ser envolvida em diferentes etapas do desenvolvimento de tecnologias e de implementação de sistemas. Contudo, a maior parcela das empresas pesquisadas apenas incorpora a função de controles na etapa final, de pós implementação, perdendo a oportunidade de ter uma avaliação criteriosa de riscos em etapas anteriores da adoção de tecnologias e sistemas, como planejamento, desenho e implementação.

### **Etapas de desenvolvimento de tecnologias ou implementação de sistemas com envolvimento de controles internos (respostas múltiplas)**



01

02

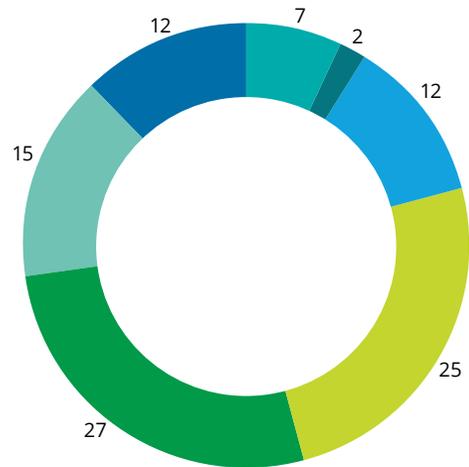
03

04

05

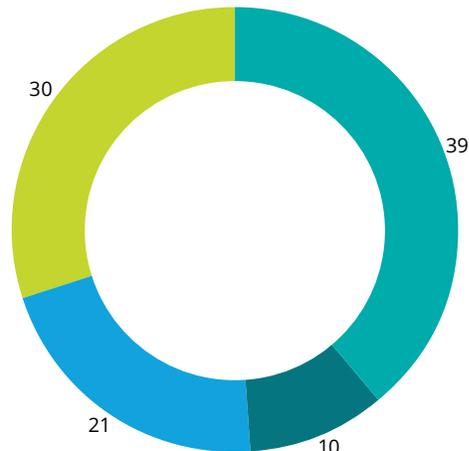
# Perfil da amostra

Cargo do respondente (em %)



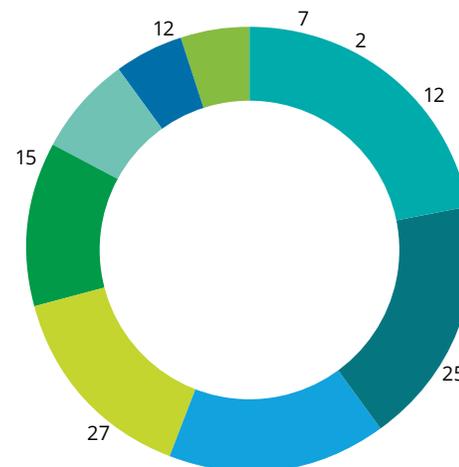
- Conselho
- Sociedade
- Presidência/CEO
- Diretoria/Superintendência
- Gerência
- Supervisão/Coordenação
- Analista

Receita líquida em 2021 (em %)



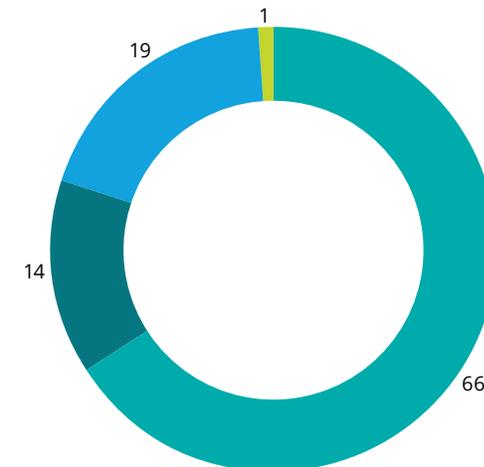
- Maior que R\$ 1 bilhão
- Entre R\$ 500 milhões e R\$ 1 bilhão
- Entre R\$ 100 milhões e R\$ 500 milhões
- Menor que R\$ 100 milhões

Sector de atuação (em %)



- Serviços
- Atividades financeiras, holdings e seguros
- Infraestrutura e construção
- Bens de consumo
- Agronegócio, alimentos e bebidas
- Saúde e farmacêutica
- TI e Telecomunicações
- Comércio

Modelo de governança (em %)



- Conselho estatutário
- Conselho consultivo
- Não têm conselho
- Não sabem informar

 39% familiares

 35% listadas em bolsa

 12% estatais



01

02

03

04

05

# Expediente

## Pesquisa “Cinco Pilares de Riscos Empresariais 2022”

### Liderança do projeto

#### **Anselmo Bonservizzi**

Sócio-líder de Risk Advisory da Deloitte

#### **Alex Borges**

Sócio e líder de Regulatory Support & Strategic Risk da Deloitte

#### **André Gargaro**

Sócio e líder da Deloitte Cyber

#### **Camila Boretti**

Sócia e líder de Accounting & Internal Controls da Deloitte

#### **Ronaldo Fragoso**

Sócio de Risk Advisory e líder de alianças e ecossistemas da Deloitte

### Realização da pesquisa

Equipe de Research & Market Intelligence da Deloitte

### Divulgação da pesquisa

Equipe de Marketing, Brand & Communications da Deloitte

### Contato

[pesquisa@deloitte.com](mailto:pesquisa@deloitte.com)



# Deloitte.

A Deloitte refere-se a uma ou mais empresas da Deloitte Touche Tohmatsu Limited (“DTTL”), sua rede global de firmas-membro e suas entidades relacionadas (coletivamente, a “organização Deloitte”). A DTTL (também chamada de “Deloitte Global”) e cada uma de suas firmas-membro e entidades relacionadas são legalmente separadas e independentes, que não podem se obrigar ou se vincular a terceiros. A DTTL, cada firma-membro da DTTL e cada entidade relacionada são responsáveis apenas por seus próprios atos e omissões, e não entre si. A DTTL não fornece serviços para clientes. Por favor, consulte [www.deloitte.com/about](http://www.deloitte.com/about) para saber mais.

A Deloitte é líder global de auditoria, consultoria empresarial, assessoria financeira, gestão de riscos, consultoria tributária e serviços correlatos. Nossa rede global de firmas-membro e entidades relacionadas, presente em mais de 150 países e territórios (coletivamente, a “organização Deloitte”), atende a quatro de cada cinco organizações listadas pela Fortune Global 500®. Saiba como os cerca de 345 mil profissionais da Deloitte impactam positivamente seus clientes em [www.deloitte.com](http://www.deloitte.com).

© 2022. Para mais informações, contate a Deloitte Global.