

# Pesquisa Global sobre Fraudes e Crimes Econômicos 2024



# Conteúdo

	Apresentação	03
01	Fraudes	09
02	Corrupção	20
03	Cadeias de suprimento	38
04	Sanções e controles de exportação	53
05	O próximo salto	74
	Contatos	77



# Apresentação

**Riscos são inevitáveis. É a forma como uma empresa os assume e mitiga, para crescer e prosperar, que diferencia os líderes.**

Neste cenário global e interconectado, o risco de fraudes e crimes econômicos é um desafio persistente. As pressões geopolíticas estão aumentando os riscos relacionados a sanções e controles de exportação. A exposição a suborno e corrupção tem aumentado à medida que multinacionais entram em novos mercados em busca de crescimento.

Há um escrutínio público e regulatório cada vez maior em relação ao uso de trabalho análogo ao escravo e outras responsabilidades ESG (*Environmental, Social and Governance*, na sigla em inglês) – não apenas nas empresas em si, mas em toda a cadeia de suprimentos que as sustenta.

Além disso, à medida que o mercado de fusões e aquisições se fortalece, quem compra pode estar exposto a eventuais passivos associados a atos ilegais encobertos nos novos ativos. Em resumo, o risco de fraudes e crimes econômicos está mais complexo do que nunca – e proteger e criar valor são uma tarefa ainda mais desafiadora.

Em paralelo, em todo o mundo, governos estão sinalizando expectativas crescentes de que as empresas façam a sua parte para prevenir fraudes e crimes econômicos e sejam totalmente transparentes sobre suas consequências. O *enforcement* regulatório e a cooperação transnacional entre as agências de aplicação da lei estão aumentando em um esforço de combater criminosos e o impacto devastador de suas ações sobre indivíduos, empresas e economias.

Neste contexto, a PwC lança a **Pesquisa Global sobre Fraudes e Crimes Econômicos**, a mais recente de uma série de mais de 20 anos. Para este estudo, realizado entre janeiro e março de 2024, a PwC entrevistou quase 2.500 empresas em 63 países. Dois terços dos respondentes eram executivos *C-Level* – incluindo 450 diretores de Auditoria, *Chief Compliance Officers* e diretores jurídicos – e 40% atuavam em companhias com receitas superiores a US\$ 1 bilhão.

Foram conduzidas ainda mais de 45 entrevistas com executivos sêniores de grandes corporações sobre suas melhores práticas. Essa ampla investigação nos proporcionou um olhar único sobre como os conselhos de administração e as lideranças empresariais estão lidando com os riscos de crimes econômicos que as empresas enfrentam diariamente.

Analizamos profundamente alguns dos riscos mais desafiadores, como fraudes em *procurement*, corrupção, trabalho análogo ao escravo, controles de exportação e sanções. Nossas descobertas incluem:



### **Fraudes em *procurement*:**

55% dos entrevistados afirmam que as fraudes em *procurement* são uma preocupação em seus países, mas apenas uma minoria adota as ferramentas disponíveis no mercado para identificá-las ou combatê-las.

Por exemplo, quase 20% não utilizam qualquer análise de dados (*analytics*) para identificar fraudes em *procurement* e apenas 26% aproveitam essa ferramenta para identificar padrões incomuns nas concorrências.



### **Corrupção:**

81% acreditam que os esforços governamentais para aplicar leis anticorrupção estão se tornando mais robustos ou minimamente estáveis nos países onde operam.

Embora 77% digam estar confiantes de que seus programas de *compliance* possam mitigar riscos emergentes, é preocupante notar que 42% das empresas não têm programas de gestão de riscos de terceiros ou não realizam nenhuma forma de pontuação de risco (*risk scoring*) como parte deles.



### **Trabalho análogo ao escravo:**

33% dos entrevistados relatam que a mensuração do risco de trabalho análogo ao escravo em suas cadeias de suprimento é prioridade em suas empresas e já o avaliaram ou pretendem fazê-lo no curto prazo.

Um terço disse ter mapeado suas cadeias para fornecedores Tier 1 e Tier 2. Em empresas com receita acima de US\$ 5 bilhões, 65% declararam ter feito isso em diferentes graus.



### **Controles de exportação:**

59% dos participantes concordam que os controles de exportação se tornaram mais complexos e mais da metade acredita que esses procedimentos estão sendo aplicados com maior rigor hoje do que há dois anos.

Se, por um lado, não é surpresa que as maiores empresas estejam mais bem preparadas. Por outro, apenas metade das corporações afirma ter um processo robusto de avaliação de riscos associados a controles de exportação.



## Sanções:

44% apontam que o *compliance* com regulamentações sobre sanções é uma prioridade, mas somente 30% adotam medidas para testar a robustez desse tipo de programa.

Dois terços consideram a possibilidade de que terceiros se envolvam em atividades proibidas como um dos dois maiores riscos relacionados a sanções, o que implica uma diferença de mais de 20 pontos em relação a outras ameaças analisadas.

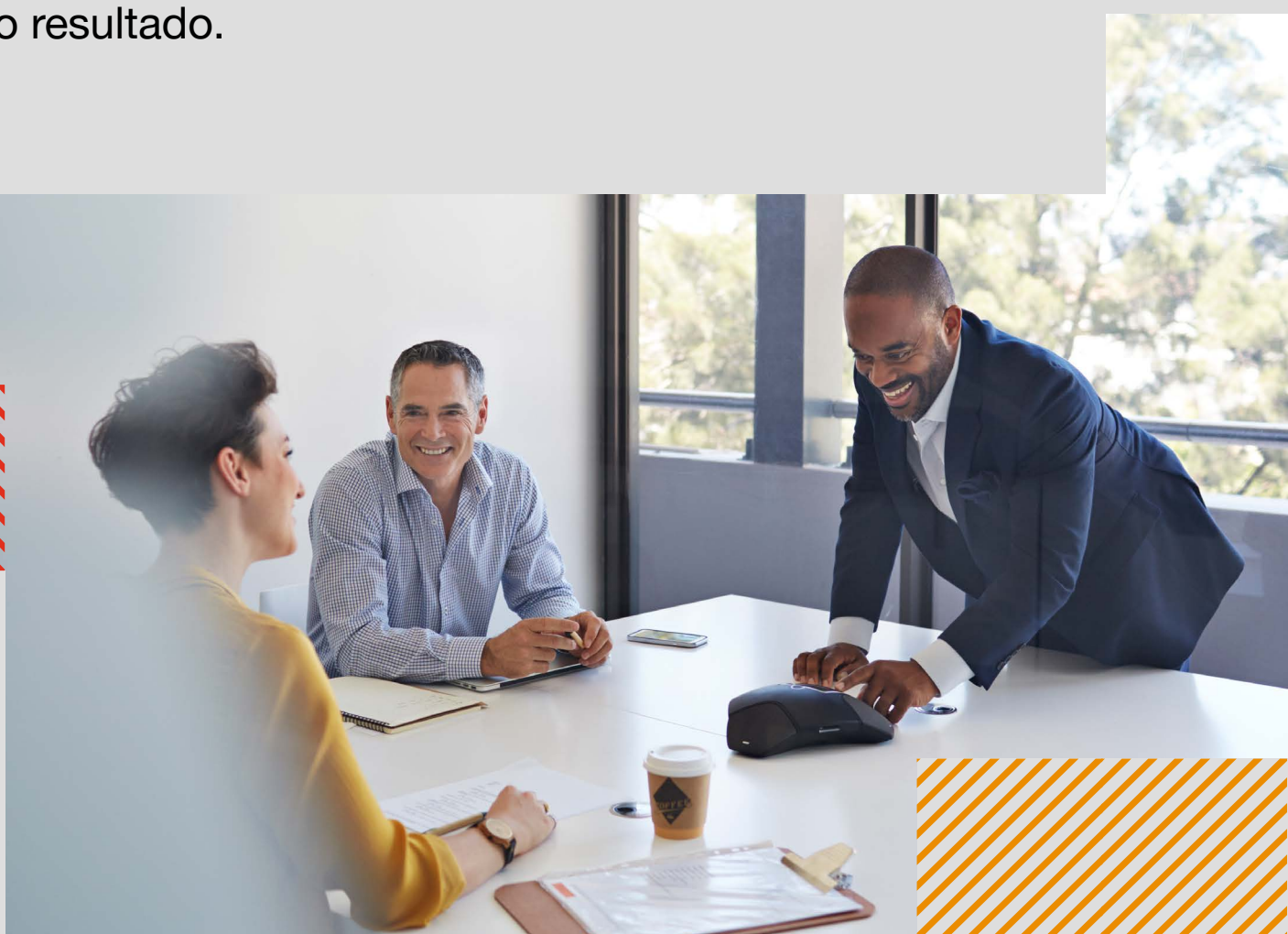
Em todos os tipos de riscos pesquisados, três questões comuns emergiram como ações que poderiam aperfeiçoar a gestão de riscos e o *compliance*: o fortalecimento das análises de risco, o aprimoramento das práticas de gestão de riscos de terceiros e um melhor aproveitamento dos dados e do *analytics* em benefício do *compliance* e das investigações.

Se a alta administração e os conselhos de administração ainda não têm um senso de urgência quanto à importância da análise de dados, seria bom considerar as palavras do Departamento de Justiça dos Estados Unidos sobre esse assunto.

Em um [discurso recente](#), a Procuradora-Geral Adjunta Interina dos EUA, Nicole M. Argentieri, afirmou: “Assim como estamos aprimorando nossa atuação em análise de dados, nossa expectativa é que as empresas façam o mesmo. Daqui para frente, vamos redobrar os esforços para nos ajudar a identificar condutas inadequadas que, de outra forma, poderiam passar despercebidas e utilizar ainda mais dados com ferramentas capazes de interpretar e sintetizar essas informações”.

Para os líderes à frente da gestão de riscos, incluindo os das áreas jurídica e de *compliance*, é fundamental garantir alinhamento com o CEO e o conselho de administração em relação à interseção entre crescimento e risco. Tanto a [Pesquisa Global de Riscos](#) quanto a [Pesquisa Global de Auditoria Interna](#) da PwC abordam justamente a desconexão de liderança no apetite ao risco e na oportunidade para que esses profissionais forneçam insights estratégicos ao alto escalão, possibilitando uma tomada de decisão mais eficaz.

Com os insights e os dados corretos para assumir riscos com confiança, as empresas podem se tornar mais ágeis – seja para entrar em novos mercados ou lançar novos produtos e serviços. Desse modo, *stakeholders* e clientes confiam mais, investidores se sentem seguros, e o crescimento e a criação de valor são o resultado.



Neste relatório, compartilhamos os destaques do cenário regulatório e de aplicação da lei no mundo, além de detalhes de onde as empresas estão posicionando seus esforços para aprimorar a gestão de riscos. Apresentamos ainda as perspectivas de líderes do setor sobre as etapas críticas para estruturação de programas de *compliance* que apoiem os negócios na preservação da confiança e construção da resiliência, contribuindo para a segurança necessária que levará à transformação, ao investimento e ao crescimento.



“

“Estamos vivendo em uma era de múltiplos riscos impulsionados pela disrupção tecnológica, pelos conflitos geopolíticos, pela instabilidade econômica e pelas demandas ESG. São desafios que podem se tornar oportunidades, dependendo do seu apetite ao risco. O que está em questão aqui é a saúde da sua gestão de riscos e do seu *compliance*. Por outro lado, a formação de equipes com as competências corretas pode garantir as bases de dados e os recursos tecnológicos necessários para gerar insights mais precisos e tomadas de decisão mais assertivas.”

**Marcos Panassol,**  
sócio e líder de Risk Services –  
Forensics da PwC Brasil





# Fraudes

**Um novo olhar sobre um problema persistente – fraudes em *procurement*.**

**Em todas as suas formas, as fraudes continuam a ser um desafio constante.**

Uma de suas formas mais antigas, aquela que acontece em contratos de compra, é ainda muito comum. Ela preocupa tanto pequenas empresas quanto multinacionais, independentemente da região ou setor da indústria.

**Nossa pesquisa revela que a fraude em *procurement*, em particular, está entre os três crimes econômicos mais disruptivos enfrentados pelas organizações em todo o mundo nos últimos 24 meses, atrás do crime cibernético e da corrupção.** Mais da metade das empresas considera que esse tipo de fraude é uma preocupação disseminada em seus países.

Embora haja dados em abundância para apoiar esforços de diligência em relação a terceiros e, ainda que os sistemas de planejamento de recursos empresariais reforcem boas práticas nos processos de compra, a tecnologia não é uma força que vem apenas para o bem. Nas mãos de criminosos, ela também possibilita esforços sofisticados para perpetrar fraudes em *procurement*.

Os riscos se acentuam à medida que as empresas entram em novos mercados ou começam a fazer aquisições em novos países. Em alguns casos, quando operações se estabelecem em locais mais distantes dos centros, garantir profissionais qualificados, especialmente em funções de controle, pode ser um desafio. Uma adoção eficaz de treinamentos sobre políticas de conflito de interesses, processos de aquisição e controles antifraude pode demorar a começar ou ser intermitente.

Para enfrentar esses desafios, os gestores devem revisar os processos de avaliação de riscos, intensificar os treinamentos e implementar controles mais avançados com base na análise de dados e automação.



## Uma análise mais profunda

A boa notícia é que 59% das empresas realizaram uma avaliação abrangente de riscos de fraude nos últimos 12 meses. Além disso, 12% planejam fazer isso dentro de um ano. 72% disseram que o conselho de administração está regularmente bem informado sobre os esforços para investigar acusações e mitigar riscos de fraude.

Contudo, é também verdade que existe um espaço significativo para melhorias. 10% das empresas brasileiras admitem que não utilizam nenhum tipo de análise de dados para identificar fraudes em *procurement*.

Mundialmente, esse dado é ainda mais desafiador: 18%. A produção industrial fica atrás de todos os outros setores nesse aspecto, o que sinaliza uma importante oportunidade para que sejam empregadas técnicas mais avançadas de detecção de fraudes.

No extremo oposto, o setor de tecnologia, mídia e telecomunicações (TMT) lidera o uso do analytics. 90% das companhias usam alguma modalidade desse tipo de solução para identificar fraudes em *procurement*, como análises de transações antes de serem concluídas e monitoramento em tempo real dos pagamentos.

Aliás, o uso difundido do *analytics* pelo TMT provavelmente contribuiu para que uma parcela menor dos profissionais desse setor relatasse que as fraudes em *procurement* tiveram impacto sério em suas organizações.

## Data analytics – uma questão essencial, mas muitas vezes ignorada

**Pergunta:** como sua empresa usa a análise de dados para identificar fraudes, desperdícios ou abuso em *procurement*?

**Base:** todos os entrevistados = 2446, Brasil = 52.



Análise de transações/negócios potenciais antes de serem fechados



Análise de transações/negócios depois de fechados



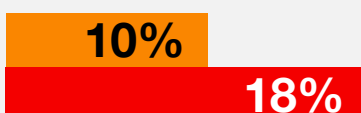
Monitoramento de pagamentos em tempo real com capacidade de bloquear pagamentos efetuados



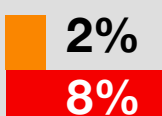
Análise retrospectiva periódica dos pagamentos efetuados



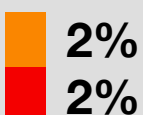
Não usa a análise de dados para esses fins



Não tem certeza/não sabe



Nenhuma das opções acima



**24%**

Governo e  
Serviços Públicos

**22%**

Produção  
Industrial

**20%**

Serviços  
Financeiros

**18%**

Mercados  
de Consumo

**15%**

Energia, Serviços de  
Utilidade Pública e  
Recursos Naturais

**15%**

Saúde

**18%**

Tecnologia, Mídia  
e Telecomunicações

Além disso, muitas empresas ainda não estão totalmente conscientes da dimensão de suas perdas com fraudes em *procurement*. 32% não procuram quantificar esses prejuízos e 31% fazem isso somente apenas de forma esporádica ou *ad hoc*.

Assim como na adoção do *analytics*, o setor de TMT lidera esse tipo de esforço de apuração de perdas, lado a lado com a área de serviços financeiros. Já a produção industrial fica bem atrás – somente 17% quantificam as perdas com essas fraudes ao menos anualmente.

No que diz respeito à mitigação dos riscos com fraudes nas aquisições, a grande maioria das companhias diz que está fortalecendo processos referentes à documentação e autorização e revisando os de seleção de fornecedores.

Um número muito menor está usando o *analytics*. Mundialmente, o uso dessa solução mostra que essa prática se verifica em apenas 26% das empresas. Esse percentual é um pouco melhor no Brasil, com 38% sinalizando afirmativamente para essa questão.

TMT, uma vez mais, lidera o uso da análise de dados para identificar padrões de licitação incomuns. Energia, serviços de utilidade pública e recursos naturais (EU&R) surge em segundo lugar entre os setores que mais usam *analytics*. O que não é surpreendente já que esse setor é o que mais se preocupa com fraudes em *procurement*. As empresas desse segmento gerenciam grandes projetos de capital e frequentemente operam em jurisdições desafiadoras. Elas têm bons motivos para gerenciar os riscos de forma mais agressiva.

## Desvendando manipulações de licitações – uma oportunidade perdida

**Pergunta:** quais medidas, se houver, sua empresa está tomando para mitigar o risco de fraude em *procurement*?

**Base:** todos os entrevistados = 2446, Brasil = 52.



Fortalecimento dos processos para confirmar documentação adequada e autorizações corretas



Aprimoramento dos treinamentos antifraude para os times de compras



Revisão dos processos de seleção de fornecedores



Adoção de uma equipe especializada (ex. um Centro de Excelência de *Compliance*) para resolver a escala de discrepâncias de preços, sinais de fraude ou pagamentos impróprios



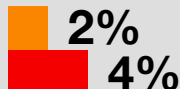
Adoção de uma política robusta de conflito de interesses



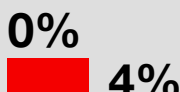
Uso do *analytics* para identificar padrões de licitação incomuns



Não tem certeza/não sabe



Nenhuma das opções



**21%**

Governo e Serviços Públicos

**22%**

Produção Industrial

**22%**

Serviços Financeiros

**27%**

Mercados de Consumo

**32%**

Energia, Serviços de Utilidade Pública e Recursos Naturais

**28%**

Saúde

**37%**

Tecnologia, Mídia e Telecomunicações

Os setores de TMT, EU&R e de saúde também têm, com mais frequência, um departamento especializado para resolver discrepâncias de preços, sinais de fraude ou pagamentos indevidos. Em termos regionais, a América do Norte se destaca na adoção dessa prática avançada – 53% das empresas têm uma divisão especializada de investigação. As empresas brasileiras, em particular, destacam-se na adoção dessa boa prática. Nada menos que 60% das companhias fazem uso dessas equipes especializadas.

## Fortalecendo esforços contra fraudes — Centros de Excelência podem ajudar

**Pergunta:** quais medidas, se houver, sua empresa está tomando para reduzir os riscos de fraudes em *procurement*? Resposta escolhida: utilizando uma equipe de *compliance* centralizada (por exemplo, um Centro de Excelência de *Compliance*) para resolver escaladas de discrepâncias de preços, sinais de fraude ou pagamentos impróprios.

**Base:** todos os entrevistados = 2446, Brasil = 52.

As porcentagens não somam 100% devido ao arredondamento.

60%

das empresas brasileiras têm uma equipe de *compliance* centralizada (por exemplo, um Centro de Excelência de *Compliance*) para resolver discrepâncias de preços, sinais de fraude ou pagamentos impróprios

31% América Latina

38% Ásia-Pacífico

34% África

43% Europa Ocidental

35% Europa Central

53% América do Norte



### Análises de riscos não necessariamente melhoram com o tempo

As fraudes em *procurement* prejudicam a lucratividade, destroem valor e minam a cultura corporativa. Agentes mal-intencionados existem dentro e fora da empresa. As ameaças internas não se limitam a crimes cibernéticos ou ao roubo de propriedade intelectual. As fraudes também precisam ser entendidas como uma ameaça dessa natureza e devem fazer parte de programas de combate.

As organizações devem atualizar regularmente suas avaliações de riscos para os segmentos de negócios e mercados geográficos de maior risco. Precisam ainda aprimorar seus esforços para ranquear os riscos de seus fornecedores a partir de fontes de dados mais diversas. Por fim, devem considerar descontinuar fornecedores sem atividade nos últimos doze meses e atualizar seu *risk scoring* com mais frequência.

Redobrar esforços na gestão de riscos de fraudes frequentemente requer o envolvimento de profissionais em níveis de gerência média, não apenas das áreas de *procurement* e de *supply chain*, mas também de recursos humanos, *compliance*, auditoria interna e de investigações. Essa combinação ajuda a tornar o risco de fraude algo mais visível dentro da organização, além de alinhar os objetivos e os esforços em toda a empresa.

Companhias de qualquer setor também podem se beneficiar de um modelo de consórcio, estabelecendo parceria tanto com organizações privadas quanto públicas para compartilhar inteligência, quando for possível, sobre tendências, riscos conhecidos e estratégias antifraude.

A indústria de seguros dos Estados Unidos, por exemplo, adotou essa abordagem de forma bem-sucedida, alavancando grandes conjuntos de dados para treinar plataformas de *analytics* antifraude. Aliás, esse é um modelo que está ganhando cada vez mais força no mundo.





## Insights de líderes

Confira algumas recomendações dos nossos entrevistados:



### **Incentive uma cultura de denúncia**

Sempre que os contratos de uma empresa com seus fornecedores são tecnicamente complexos, é maior a possibilidade de manipulação de propostas e manipulações em licitações. Delatores desempenham frequentemente um papel crítico para a descoberta de más condutas.



### **Mantenha uma política robusta para conflitos de interesse**

Uma política bem definida de conflito de interesses é essencial, assim como um treinamento regular sobre ela. Alguns dos nossos entrevistados pedem a seus profissionais que preencham um questionário antes da contratação e obtenham uma certificação quando já estão empregados. Essas ações ampliam a conscientização sobre esse risco e podem aumentar o número de questões reportadas.



## Elimine o isolamento entre os departamentos

Evitar que áreas internas se isolem é importante. A equipe de *compliance* precisa assegurar a adesão de uma abordagem baseada em riscos de terceiros pela área de *procurement*, inclusive com *due diligence* anterior à integração de novos funcionários (*onboarding*), auditorias *in loco* quando apropriado e reavaliação de fornecedores antigos. A auditoria interna é outro parceiro-chave e, ainda que suas métricas de riscos possam diferir das do *compliance*, ambas as funções precisam trabalhar em estreita colaboração e ter acesso às análises de dados e aos *dashboards* uma da outra.



## Explore as experiências com IA e IA generativa

A inteligência artificial (IA) e a inteligência artificial generativa, aliadas ao *analytics* avançado e à automação, podem contribuir para uma melhor gestão dos ciclos de vida dos contratos e a identificação de riscos relacionados a *procurement* por meio de um monitoramento aprimorado.



## Fortaleça as suas defesas

Tecnologias também podem ser parte do problema. Alguns de nossos entrevistados explicaram que organizações criminosas estão usando IA para emitir faturas falsas e se passar por executivos sêniores em ataques de *spearfishing*. Outros enfatizaram o papel dos funcionários ao facilitarem fraudes em *procurement* e defenderam que esses riscos precisam ser tratados como parte dos programas de ameaças internas. Um contínuo monitoramento dos e-mails das equipes, quando isso for legal e viável, também foi mencionado por diversos executivos.



## Monitoramento avançado de transações contra fraudes em *procurement*

Soluções de monitoramento de transações contra fraudes em *procurement* empregam algoritmos sofisticados e técnicas de aprendizagem de máquina para detectar atividades e padrões suspeitos. Ao analisar grandes volumes de dados, essas soluções podem identificar possíveis casos de fraude, como superfaturamento, propinas e manipulações.

A combinação dessas soluções com análises gráficas pode ampliar ainda mais a sua eficácia. Essas análises permitem às empresas visualizar e avaliar relações complexas entre agentes, como fornecedores, funcionários e terceiros.

Um *due diligence* que use dados corporativos públicos pode ajudar as organizações a mapear essas relações e conexões, permitindo uma compreensão mais holística dos beneficiários finais de terceiros e a identificação de potenciais conflitos de interesse ou relações ocultas. Essa combinação pode reduzir significativamente o risco de fraudes em *procurement* e outros pagamentos indevidos.





# Corrupção

**Expectativas crescentes e oportunidades perdidas – os desafios atuais da gestão de riscos de terceiros.**

**Em todo o mundo, governos sinalizam expectativas crescentes de que os programas de *compliance* corporativos precisam se tornar mais sofisticados.**

Autoridades judiciais e reguladores têm elevado as exigências para a gestão de riscos de terceiros, assim como para o uso de análises de dados para apoiar os esforços de *compliance* e investigação.

Incentivos ou proteções novas ou revisadas recentemente para lidar com *whistleblowers* em diversos países têm aumentado a pressão para que as empresas descubram e reajam rapidamente a alegações de má conduta, tanto faz se o caso acontece dentro da companhia ou em um fornecedor. Decidir se a denúncia deve ser feita, e para quem, continua sendo um desafio.

O Departamento de Justiça dos Estados Unidos estabeleceu, por exemplo, uma série de programas para encorajar a prática de *whistleblower*. Um programa piloto<sup>1</sup> visa preencher as lacunas de denúncia existentes da *Securities and Exchange Commission* (SEC) e da *Commodity Futures Trading Commission*, focando em crimes financeiros, suborno estrangeiro fora da jurisdição da SEC, suborno doméstico e o recém-adotado *Foreign Extortion Prevention Act* (FEPA).<sup>2</sup>

Outro programa piloto oferece a possibilidade de acordos de não-persecução a indivíduos que voluntariamente divulguem informações novas e acionáveis sobre condutas criminosas.<sup>3</sup> Esses programas ainda serão avaliados em relação ao seu sucesso. Contudo, somente no ano fiscal de 2023, a SEC recebeu mais de 18.000 denúncias e pagou quase US\$ 600 milhões em recompensas a 68 delatores, uma média de US\$ 9 milhões para cada um.<sup>4</sup>

O Departamento de Justiça americano esclareceu que, em casos de corrupção em fusões e aquisições, espera-se que as empresas se auto-denunciem em até seis meses, corrijam seus problemas em até um ano e devolvam os ganhos ilícitos.<sup>5</sup> Na maioria dos casos, empresas que seguirem essas orientações provavelmente não serão processadas. Enquanto isso, as investigações setoriais permanecem, e as monitorias tradicionais parecem dar lugar ao “auto-monitoramento”.



<sup>1</sup> <https://www.justice.gov/opa/speech/deputy-attorney-general-lisa-monaco-delivers-keynote-remarks-american-bar-associations>

<sup>2</sup> [https://www.justice.gov/jm/jm-9-47000-foreign-corrupt-practices-act-1977#:~:text=The%20Foreign%20Extortion%20Prevention%20Act%20\(FEPA\)%2C%20which%20criminalizes%20the,from%20certain%20individuals%20and%20entities](https://www.justice.gov/jm/jm-9-47000-foreign-corrupt-practices-act-1977#:~:text=The%20Foreign%20Extortion%20Prevention%20Act%20(FEPA)%2C%20which%20criminalizes%20the,from%20certain%20individuals%20and%20entities)

<sup>3</sup> <https://www.justice.gov/opa/blog/criminal-divisions-voluntary-self-disclosures-pilot-program-individuals>

<sup>4</sup> Relatório Anual de *Whistleblower* da *Securities and Exchange Commission Office* para o Congresso no ano fiscal de 2023, <https://www.sec.gov/files/fy23-annual-report.pdf>

<sup>5</sup> <https://www.justice.gov/opa/speech/deputy-attorney-general-lisa-o-monaco-announces-new-safe-harbor-policy-voluntary-self>

“A aplicação da *Foreign Corrupt Practices Act* (FCPA, ou a Lei de Práticas de Corrupção no Exterior) tem sido forte e ativa nos últimos 15 anos e continuará a ser um pilar dos programas de *enforcement* corporativo do Departamento de Justiça dos Estados Unidos e da SEC.

As unidades da FCPA em cada agência continuam muito bem equipadas financeiramente. Em termos políticos, o apoio a ações anticorrupção permanece forte, como evidenciado pelo *Foreign Extortion Prevention Act* (FEPA, ou a Lei de Prevenção a Extorsão no Estrangeiro), que fornecerá ao Departamento de Justiça mais uma ferramenta para combater a corrupção como parte de um kit integrado de aplicação da Lei, incluindo a FCPA, a FEPA, leis de combate à lavagem de dinheiro, estatutos de fraude e outros estatutos criminais federais.”

**Steven Fagell**, Covington & Burling

Revelar novas alegações de irregularidades é claramente a prioridade. “Além da denúncia voluntária e dos programas de *whistleblower*, o Departamento de Justiça dos Estados Unidos e a SEC continuarão a fazer uso de fontes de notícias, rastreadores da internet, colaboração com parceiros estrangeiros, informações obtidas em investigações em andamento e avanços em IA, análises de dados e outras tecnologias para buscar novos casos”, observou Adam Studner, do escritório de advocacia Covington & Burling. “Em resumo: um ambiente robusto de *enforcement* anticorrupção veio para ficar.”

Fora dos Estados Unidos, há muitos desenvolvimentos notáveis. O Reino Unido tem um novo diretor do *Serious Fraud Office* que provavelmente liderará uma organização maior, com novos poderes de investigação prévia sob o recentemente adotado *Economic Crime and Corporate Transparency Act* de 2023.<sup>6</sup>

<sup>6</sup> <https://www.legislation.gov.uk/ukpga/2023/56/enacted>

A França revisou suas diretrizes para acordos de suspensão condicional de processos, oferecendo incentivos significativos a auto-denúncias oportunas e investigações robustas internas.<sup>7</sup> Na Alemanha, embora não tenha havido progresso na reforma da responsabilidade criminal corporativa, uma nova Lei de Proteção ao *Whistleblower* foi adotada para implementar a Diretiva de *Whistleblower* da União Europeia (UE).<sup>8</sup>

A partir de janeiro de 2024, a Lei sobre *Supply Chain* da Alemanha vai estabelecer obrigações adicionais de diligência em direitos humanos e ambientais para empresas que tenham, pelo menos, 1.000 funcionários.

Na região Ásia-Pacífico, o Parlamento da Austrália aprovou o *Combating Foreign Bribery Bill*, uma mudança legislativa histórica e muito aguardada, que introduz um novo tipo de crime de responsabilidade por falhas ao não prevenir o suborno de um funcionário público estrangeiro. Grandes escândalos de corrupção no Japão, na Coreia do Sul e Malásia ganharam manchetes e podem sinalizar uma disposição para processar de forma mais agressiva a prática de suborno doméstico e estrangeiro.

No entanto, mundialmente, a percepção geral é que os riscos de corrupção estão avançando ou, ao menos, seguem estáveis. Quase 7 em cada 10 entrevistados compartilham essa visão. 43% entendem que esses riscos estão no mesmo patamar, mas 26% são pessimistas e acreditam que o cenário piorou. Somente 13% disseram que esses riscos estão diminuindo e existe um patamar considerável de executivos que não têm certeza ou não sabem responder (19%).

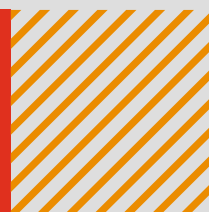
No Brasil, o quadro é semelhante. 42% acreditam que o risco de corrupção está estabilizado. No entanto, é maior o número de brasileiros que estão vislumbrando um crescimento desses riscos (31%). A percepção de que isso está diminuindo é de 21% e apenas 6% declararam não ter certeza ou não souberam responder.

<sup>7</sup> [https://www.tribunal-de-paris.justice.fr/sites/default/files/2023-03/Guidelines%20on%20the%20implementation%20of%20the%20CJIP\\_PNF\\_January%2016%202023%20VD.pdf](https://www.tribunal-de-paris.justice.fr/sites/default/files/2023-03/Guidelines%20on%20the%20implementation%20of%20the%20CJIP_PNF_January%2016%202023%20VD.pdf)

<sup>8</sup> <https://www.gesetze-im-internet.de/hinschg/BJNR08C0B0023.html>

<sup>9</sup> [https://www.aph.gov.au/Parliamentary\\_Business/Bills\\_Legislation/Bills\\_Search\\_Results/Result?bld=r7055](https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bld=r7055)

## Os riscos de corrupção não estão diminuindo, mas os esforços de fiscalização estão ganhando força

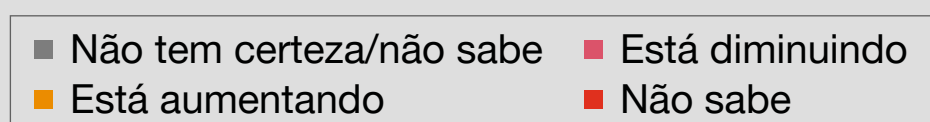


### Opinião dos entrevistados sobre o risco de corrupção

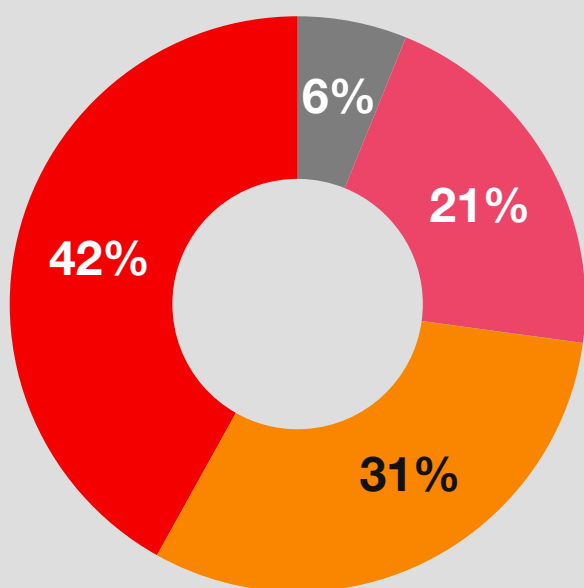
**Pergunta:** na sua opinião, os riscos associados a pagamentos corruptos ou indevidos a funcionários públicos e/ou clientes comerciais aumentaram, diminuíram ou permaneceram os mesmos nos últimos 12 meses no país onde você mora?

**Base:** todos os entrevistados = 2446, Brasil = 52.

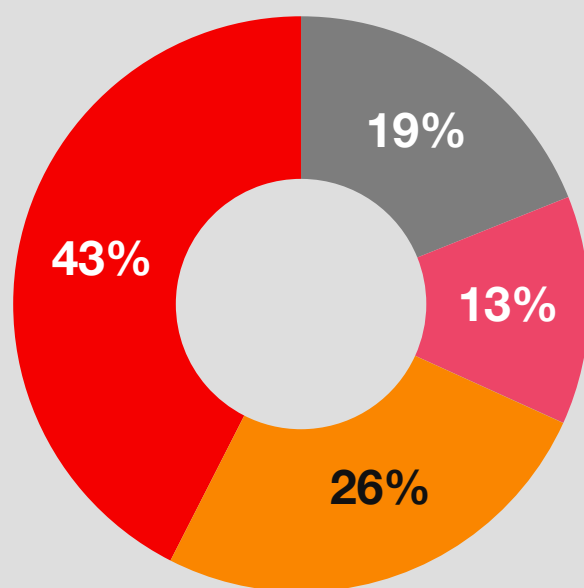
As porcentagens não somam 100% devido ao arredondamento.



 Brasil



 Mundo



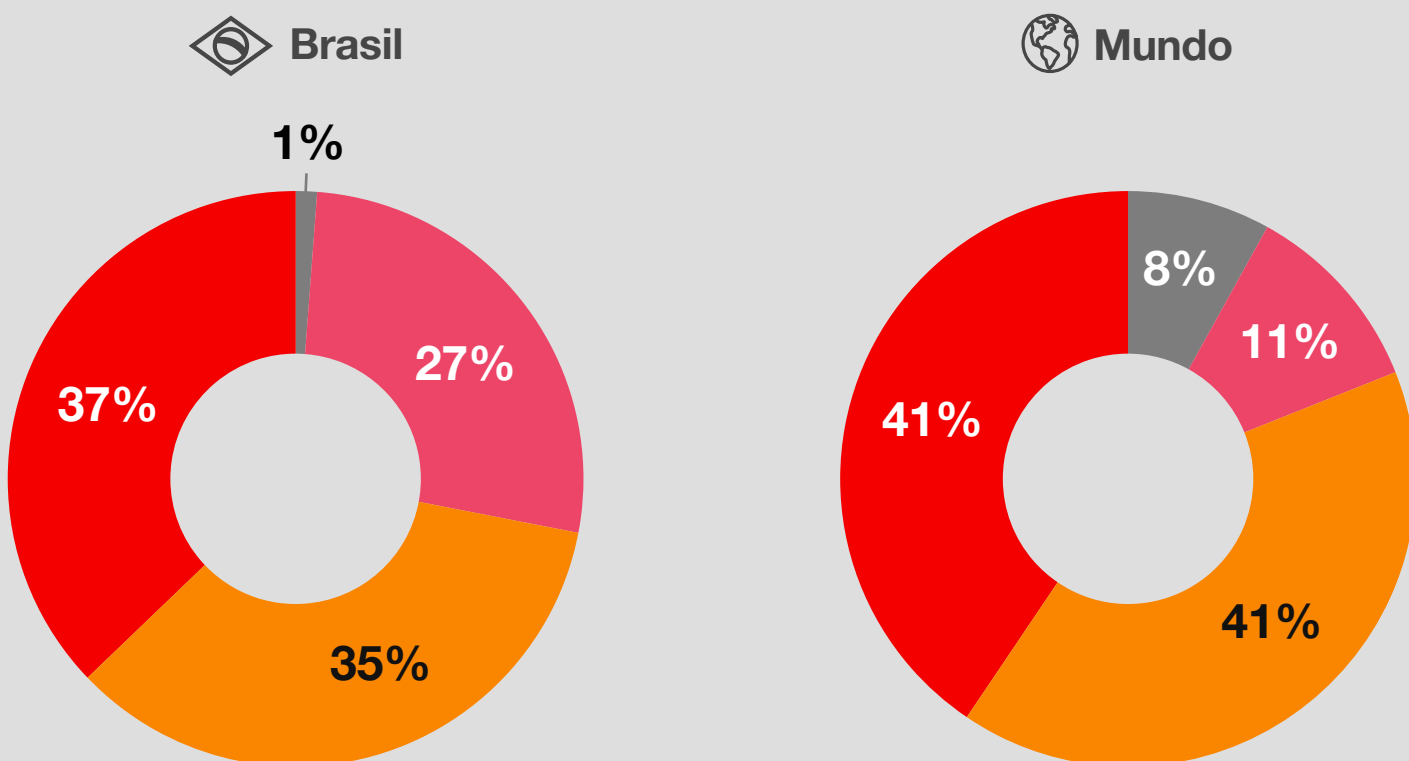


## Opinião dos entrevistados sobre a aplicação de leis anticorrupção

**Pergunta:** como os esforços do governo para fazer cumprir as leis anticorrupção estão mudando no país/países em que você opera?

**Base:** todos os entrevistados = 2446, Brasil = 52.

As porcentagens não somam 100% devido ao arredondamento.



Nossa pesquisa aponta ainda que 81% dos executivos entrevistados acreditam que os esforços governamentais para aplicar leis anticorrupção estão se tornando mais robustos ou ao menos permanecendo estáveis nos países onde operam – e esse percentual chega a 92% para companhias sediadas na América do Norte.

No Brasil, são mais de 70%. No total, 37% acreditam que esses esforços estão se tornando mais robustos e 35% entendem que está tudo igual. Chama a atenção, entretanto, a expressiva parcela (27%) que avalia que as ações de combate à corrupção, por parte do governo, estão perdendo força. O que pode ser um alerta para os negócios.

De qualquer forma, mundialmente, é forte a pressão para que empresas implementem e mantenham programas de *compliance* anticorrupção efetivos, utilizando análises de dados para informar e acelerar a tomada de decisões.

Uma gestão de riscos de terceiros robusta permanece como uma questão central, dado que eles estão envolvidos na maioria dos grandes casos de suborno ou corrupção. De fato, todas as [resoluções corporativas da FCPA em 2023](#) envolveram pagamentos a funcionários de governos estrangeiros que foram contratados por meio de terceiros.<sup>10</sup>

## Uma análise mais profunda

À primeira vista, os executivos demonstram confiança de que seus programas de *compliance* conseguem mitigar os riscos emergentes de corrupção. 77% acreditam ter isso sob controle. A maioria (70%) está confiante que sua empresa tem uma compreensão completa e precisa de todas as partes interessadas (fornecedores, distribuidores e outros intermediários).

No entanto, essa pode muito bem ser uma falsa confiança, já que uma análise mais profunda mostra que a maioria das organizações não está empregando amplamente as práticas necessárias para reduzir de forma efetiva o risco de terceiros e combater a corrupção.

Percebemos que, na prática, é muito comum que as empresas tenham informações incompletas sobre seus fornecedores, distribuidores e outros prestadores de serviços terceirizados, mesmo as organizações de capital aberto com bilhões de dólares em receitas. Isso pode ocorrer devido a sistemas díspares oriundos de aquisições anteriores ou por haver divisões, regiões ou países que desfrutam de uma autonomia operacional significativa.

<sup>10</sup> Carta de Acordo de Não-Persecução do Departamento de Justiça dos EUA, Divisão Criminal, para Courtney Trombly e William Barry, Re: Albemarle (28 de setembro de 2023), <https://www.justice.gov/opa/file/1316796/dl?inline>. Acordo de Persecução Diferida, Estados Unidos contra Corporacion Financiera Colombiana S.A., No. 8:23-cr-00262-PJM (D. Md. 10 de agosto de 2023), <https://www.justice.gov/media/1311296/dl?inline>. Anexo A-2 do Acordo de Confissão de Culpa, Estados Unidos v. Telefonaktiebolaget LM Ericsson, No. 1:19-cr-0084-LTS (S.D.N.Y. 20 de março de 2023), <https://www.justice.gov/media/1283591/dl?inline>.



Sem um sistema contábil integrado e sem um sistema de gestão de fornecedores/contas a pagar, pode ser muito difícil ter uma visão completa. A importância do monitoramento contínuo de terceiros – e da devida diligência em novos fornecedores de alto risco – não pode ser subestimada.

Entre os componentes de um programa eficaz de *compliance* e anticorrupção de terceiros, o *risk scoring*, o monitoramento e as auditorias são elementos críticos. Veja como as empresas estão se posicionando nessas frentes.

Mundialmente, quase metade (48%) realiza o *risk scoring* como parte da sua gestão de riscos de terceiros, ao passo que quase dois terços das que fazem isso consideram o risco de corrupção nesse processo. O dado alarmante é que 42% das organizações apontam que não têm um programa de gestão de riscos de terceiros ou, se têm, o *risk scoring* não é feito.

No Brasil, é maior o número dos que afirmam que o *risk scoring* integra seus programas de gestão de riscos de terceiros (50%). 35% destacam que o risco de corrupção faz parte desse processo e 15% afirmam que ele não entra em seu programa. É importante destacar também que 45% relatam não ter esse tipo de programa ou, se têm, não há *risk scoring*.

Ordem, In re Koninklijke Philips N.V., Securities Exchange Act Release No. 97479 (11 de maio de 2023), <https://www.sec.gov/litigation/admin/2023/34-97479.pdf>.

Ordem, In re 3M Co., Securities Exchange Act Release No. 98222 (25 de agosto de 2023), <https://www.sec.gov/litigation/admin/2023/34-98222.pdf> [“Ordem 3M de agosto de 2023”].

## Há espaço para melhoria do *risk scoring*

**Pergunta:** sua empresa atribui uma *risk scoring* para cada um de seus fornecedores como parte de seu programa de gestão de riscos de terceiros?

**Base:** todos os entrevistados = 2446, Brasil = 52.



Não, não se avalia o *risk score* de cada um dos terceiros




Sim, e o risco de corrupção é a parte desse processo



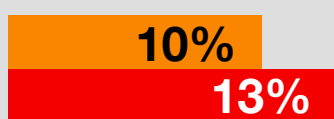
 **Brasil**  
**50%**

Sim, mas o risco de corrupção não é parte desse processo

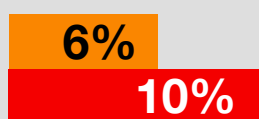


 **Mundo**  
**48%**

Não, não existe um programa de gestão de riscos de terceiros



Não tem certeza/não sabe



Os programas de gestão de riscos de terceiros deveriam refletir o perfil de riscos da organização. Contudo, é importante reconhecer que, sob a perspectiva de combate à corrupção, a integração padrão de terceiros não é a mesma coisa que *due diligence*.

Toda empresa se beneficiaria de alguma forma de *risk scoring*. Sem ela, não haveria como escalonar o nível de *due diligence* e o monitoramento contínuo que determinada parte mereceria em relação à outra. As regiões onde o *risk scoring* é menos feito incluem a Ásia-Pacífico e a América Latina. Mesmo na América do Norte, 29% das empresas respondentes não adotam essa prática.

Em relação às auditorias antissuborno/anticorrupção de terceiros, apenas 37% das empresas as conduzem regular ou ocasionalmente. No Brasil, esse número é um pouco maior, de 44%. Um número próximo de companhias brasileiras diz não se recordar desse tipo de auditoria nos últimos dois anos ou em nenhum momento (48%).

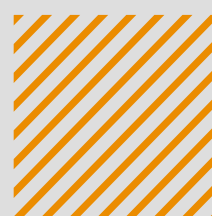
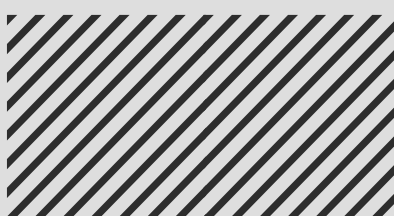
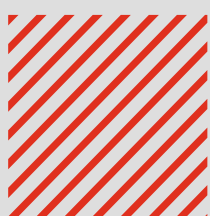
Essa porcentagem é maior nos setores de TMT e saúde, e bem menor em EU&R. De qualquer forma, todos os setores têm ampla margem para melhorias. É importante destacar ainda que companhias com sede na América do Norte conduzem auditorias antissuborno/anticorrupção regularmente (quase o dobro de vezes em relação a outras regiões).

O uso de análises de dados (*analytics*), processos robustos de investigação interna e análises de causa raiz são elementos importantes em um programa de *compliance* anticorrupção eficaz. Por exemplo, algumas organizações, particularmente nas áreas de *financial services*, TMT e saúde, estão adotando *analytics* para monitorar constantemente certas formas de transação.

No entanto, 23% não estão usando de nenhuma maneira esse tipo de solução para apoiar o *compliance* anticorrupção. No Brasil, o número é um pouco menor (13%), o que é preocupante, uma vez que implementar o *analytics* não é necessariamente caro. Essa é, então, uma oportunidade perdida para essas empresas.

“Por mais que as empresas busquem inovar e utilizar *analytics* em seus programas de ética e *compliance*, elas ainda tendem a confiar em ferramentas e métodos tradicionais, como canais de denúncias, políticas e treinamentos”, observou Ben Morgan, do escritório de advocacia Freshfields Bruckhaus Deringer.

“Acreditamos que essa é uma área que se tornará mais importante e relevante no futuro, especialmente à luz das expectativas do Departamento de Justiça dos Estados Unidos e do *Serious Fraud Office* do Reino Unido em relação a procedimentos razoáveis e *compliance* corporativo.”



## Compliance anticorrupção sem *analytics*? Isso é preocupante

**Pergunta:** como sua empresa emprega o *analytics* em apoio a seus objetivos de *compliance* anticorrupção?

**Base:** todos os entrevistados = 2446, Brasil = 52.



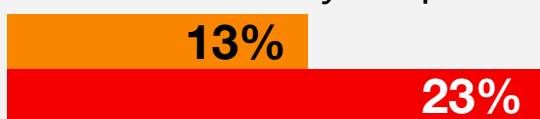
Monitoramento contínuo de certos tipos de transação



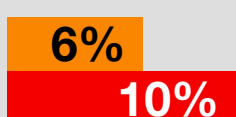
Análises retrospectivas *ad hoc* das transações



Não utiliza o *analytics* para apoiar a equipe de *compliance*



Não tem certeza/não sabe



**26%**

Governo e  
Serviços Públicos

**29%**

Produção  
Industrial

**19%**

Serviços  
Financeiros

**25%**

Mercados  
de Consumo

**26%**

Energia, Serviços de  
Utilidade Pública e  
Recursos Naturais

**19%**

Saúde

**15%**

Tecnologia, Mídia  
e Telecomunicações



## Auditorias locais – subutilizadas e subvalorizadas

**Pergunta:** sua empresa realizou uma auditoria de anticorrupção/antissuborno em um ou mais de seus terceiros nos últimos dois anos?

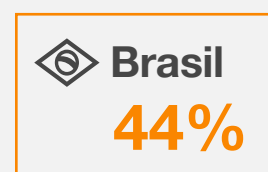
**Base:** todos os entrevistados = 2446, Brasil = 52.



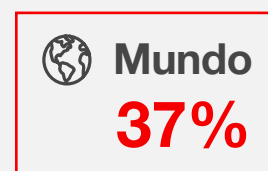
Não me recordo de nossa organização ter conduzido essas auditorias nos últimos dois anos



Sim, realizamos regularmente auditorias de prevenção à corrupção/suborno em terceiros



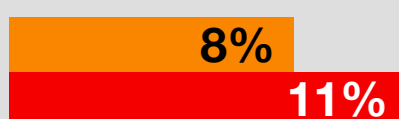
Sim, mas essas auditorias de prevenção à corrupção/suborno em terceiros são raras



Não me recordo de nossa organização ter conduzido qualquer auditoria desse tipo



Não tem certeza/não sabe



Processos bem-desenhados de investigação interna podem ajudar a acelerar o tempo de resposta frente a alegações de conduta inapropriada – o que é particularmente importante considerando os incentivos notáveis para que *whistleblowers* denunciem entidades governamentais – e podem fundamentar melhor a tomada de decisões das empresas em relação a autodenúncias.

Com o estabelecimento desses processos, é importante revisá-los de forma regular, especialmente à medida que as expectativas de reguladores e autoridades judiciais evoluem, e as leis de privacidade de dados mudam.

Segundo a nossa pesquisa, quase 40% das empresas estão atingindo esse objetivo, revisando seus processos nos últimos 12 meses. Por outro lado, 30% não os revisaram no último ano e outros 16% não têm uma função de investigação.

Uma vez que parte substancial dos fatos é conhecida em uma investigação, a análise da causa raiz, para entender “o porquê” e “como” aconteceu uma fraude, é um elemento essencial para a melhoria contínua dos processos. Essa análise pode incluir, por exemplo, a identificação de lacunas de controles internos, limitações de sistemas ou casos de sobreposição de gestão, assim como fatores externos à empresa.



Essa pode ser uma oportunidade para quase metade das companhias que não estão fazendo análise de causa raiz, não a fazem frequentemente ou sem aplicar as lições aprendidas. As empresas estariam em melhor situação se não focassem tanto e de forma limitada em questões específicas que surgiram em uma investigação, mas sim se ampliassem o escopo de suas análises para compreender como essas causas raízes poderiam se materializar em outras áreas do negócio.



### Conduzindo auditorias anticorrupção efetivas em terceiros

Não é apenas bom para os negócios, mas também prudente do ponto de vista do *compliance*, que as empresas regularmente revisem sua abordagem na avaliação, no monitoramento de terceiros e na realização de auditorias anticorrupção. Em outras palavras, as empresas devem avaliar a frequência e o tipo de auditoria que fazem.

As organizações fazem isso, muitas vezes, de forma reativa em vez de proativa. Além disso, as avaliações de menor risco de terceiros são frequentemente feitas remotamente, usando processos de “escritório” focados em informações já disponíveis internamente e, muitas vezes, sem o envolvimento ou conhecimento dos terceiros.

O foco está em apenas analisar a documentação interna da empresa para descobrir se ela está em conformidade com os procedimentos de *due diligence* aplicáveis e testar transações de dados internos de contas a pagar e/ou despesas em busca de sinais de alerta.

No caso de terceiros com maior risco, as empresas devem considerar a importância das visitas presenciais às suas instalações. Essas visitas precisam ser adicionais ao trabalho realizado no escritório e podem incluir, por exemplo, entrevistas com funcionários de terceiros, avaliações de seu programa de *compliance* e testes de transações a partir de seus balanços e registros.

Essas auditorias, especialmente as que incluem testes de transações, requerem mais recursos para serem realizadas e envolvem muito mais socialização e alinhamento, seja dentro da organização ou externamente. No entanto, os insights encontrados podem ser consideravelmente mais valiosos do que aqueles desenvolvidos apenas por meio de procedimentos corporativos à distância.

Diante disso, a metodologia de seleção da auditoria voltada a terceiros deve ser baseada em riscos e incorporar contribuições não apenas do *compliance*, mas também das unidades de negócios e outras áreas. O que as empresas devem evitar é cair na rotina de seguir práticas informais e não documentadas que são inconsistentes e não podem ser justificadas objetivamente.

Isso pode resultar em uma aversão à seleção de terceiros que podem ser particularmente sensíveis ou difíceis de avaliar. A frequência das auditorias presenciais em terceiros pode ser ajustada com base no risco presente, e os fornecedores que passam por essas auditorias com um score elevado podem não precisar ser revisitados por três ou quatro anos, exceto em situações extraordinárias.

## O processo investigativo e o papel do conselho de administração

Um departamento de investigação efetivo contribui tanto para a mitigação de risco quanto para o *compliance*. Muitas agências de fiscalização consideram especificamente a forma como uma empresa investiga desvios de conduta quando estão avaliando programas de *compliance* corporativos.

Portanto, os conselhos de administração devem pressionar regularmente seus executivos a reverem o modo como gerenciam seus departamentos internos de investigação, focando em como os dados são coletados e revisados, as análises de causa raiz são efetuadas e as lições aprendidas são retroalimentadas para proporcionar uma melhoria contínua.

Os principais indicadores de desempenho (KPIs) para acompanhamento da eficácia e eficiência do processo investigativo, assim como o monitoramento de tendências, incluem métricas como o volume de relatórios de incidentes (100 funcionários), a taxa de confirmação de denúncias ou incidentes relatados, o tempo médio para cada decisão de confirmar ou não a veracidade de uma denúncia ou incidente reportado, os casos por tipo de incidente e por localização e a média de dias para encerrar casos, entre outros.



## Insights de líderes

Confira algumas recomendações dos nossos entrevistados:



### Faça uso do *analytics* preditivo

Tome medidas para explorar a IA na produção de análises preditivas de próxima geração, utilizando diferentes fontes de dados tanto de dentro da empresa (gastos com presentes e entretenimento, atividades do canal de denúncias, avaliações da área de recursos humanos) quanto de fora (mudanças na contratação de fornecedores ou distribuidores) que possam identificar unidades de negócios ou mercados geográficos de maior risco.



### Considere o uso da IA no monitoramento de mudanças regulatórias

Se sua empresa opera em dezenas de países, considere usar as ferramentas de IA generativa para ler, interpretar e monitorar regulamentações em vários mercados em busca de mudanças, por exemplo, na definição legal de funcionários públicos, responsabilidade criminal corporativa ou em regras de licitação pública. Com isso, os departamentos jurídicos e de *compliance* internos podem ser liberados para envolver consultores externos em casos mais complexos.



### **Faça pesquisas com seus funcionários**

Breves pesquisas anuais com funcionários focadas em ética e *compliance* podem proporcionar dados adicionais úteis para manter informadas outras atividades de gestão de riscos. Incorporar essas pesquisas no treinamento anual de *compliance* pode ampliar as taxas de participação.



### **Adote programas de ouvidoria**

Criar uma rede de ouvidores – ou “campeões de *compliance*” nas unidades de negócio/localizações que não são membros em tempo integral da empresa – pode ser altamente efetivo já que isso pode ajudar a disseminar mensagens-chave e melhores práticas ao mesmo tempo que contribui para a disposição dos funcionários de questionar. Esses papéis podem ser limitados em termos de dedicação de tempo para aumentar o número de executivos que tenham interações mais intensas com o *compliance*.



### **Fortaleça as classificações de risco por país**

As classificações de risco por país devem ir além do simples uso do Índice de Percepção de Corrupção da Transparência Internacional e revisões superficiais de pontos de contato com governos. O *compliance* e a auditoria interna devem se unir para decidir sobre o uso de uma variedade de fontes externas e internas de dados que possam proporcionar uma visão mais holística do risco em cada um dos países onde a empresa opera, como aquisições ou desinvestimentos recentes, preocupações de *compliance*, resultados de investigações internas, achados anteriores dessas auditorias, resultados de pesquisas com funcionários etc.



### **Faça um *benchmarking* do seu programa de *compliance***

Periodicamente, avalie seus programas de *compliance* para compará-los com os já existentes, as expectativas dos reguladores e as melhores práticas do mercado.

## **Data warehouses empresariais também impulsionam a eficácia dos programas de *compliance***

*Data warehouses* empresariais, que já existem em muitas grandes corporações para fins comerciais, podem utilizar *analytics* avançado e mineração de dados para extrair insights valiosos para o departamento de *compliance*. *Analytics* avançados direcionados podem ajudar as companhias a identificar áreas de alto risco, como regiões ou departamentos com maior probabilidade de corrupção, e tomar medidas proativas para reduzir esses riscos.

A integração das bases de dados diferentes – por exemplo, sistemas de *Enterprise Resource Planning* (ERP) regionais, de tesouraria, de gestão do conhecimento, de despesas e investigações, além de canais de denúncia e *due diligence* de terceiros – permite um monitoramento mais eficiente e preciso das transações financeiras e dos dados de eventos relacionados.

Além disso, esses *data warehouses* permitem às empresas monitorar e acompanhar holisticamente os KPIs relacionados à detecção de corrupção, prevenção e *compliance*. São exemplos de KPIs as taxas de relato de incidentes, indicadores de conclusão de treinamento de *compliance*, resultados de auditorias dessa área e treinamentos de terceiros sobre a temática da conformidade. Ao analisar esses índices, as organizações podem avaliar a eficácia de seus processos de linha de frente, assim como dos controles e programas de *compliance* em geral.

As *warehouses* empresariais aumentam a eficácia dos programas ao garantir relatórios consistentes e padronizados, o que tende a facilitar a demonstração de conformidade com a regulação e as políticas internas. Além disso, elas possibilitam às corporações acelerar as investigações de violações em potencial e responder rapidamente a alegações de *whistleblowers*, exames de auditoria e questionamentos de órgãos reguladores.

Ao acessar e analisar dados relevantes de sistemas de origem diferentes, já consolidados nos *data warehouses*, as empresas conseguem reunir evidências de forma rápida, identificar responsáveis e tomar medidas disciplinares e legais em menos tempo e usando menos recursos internos e externos.



# Cadeias de suprimento

**Protegendo direitos humanos por meio de uma profunda visibilidade das cadeias de suprimento**

Um escrutínio público cada vez maior e um ambiente regulatório em rápida evolução estão impondo uma pressão crescente para que as empresas identifiquem e reduzam os riscos associados ao trabalho análogo ao escravo e a outros abusos em relação aos direitos humanos em suas cadeias de suprimento.

Tom Plotkin, do escritório de advocacia Covington & Burling, notou que as mudanças fundamentais incluem avanços recentes e significativos na UE e a intensificação da fiscalização por parte das autoridades americanas. Para ele, esses desafios de *compliance* não se limitam mais a um conjunto restrito de setores industriais, operando em um punhado de jurisdições de maior risco, mas impactam todas as empresas que fazem negócios globalmente.

Muitas das mais recentes regulações da UE, como a *Corporate Sustainability Due Diligence Directive* (a nova Diretiva de *Due Diligence* de Sustentabilidade Corporativa)<sup>11</sup>, estão exigindo o mapeamento das cadeias de suprimento e avaliações de risco de direitos humanos.

Um exemplo disso são as exigências de relatórios demandadas pela *Corporate Sustainability Reporting Directive* (a nova Diretiva de Reporte de Sustentabilidade Corporativa, ou CSRD) da UE, que passou a vigorar em janeiro de 2024, e que exige, em certas circunstâncias, que as empresas divulguem informações sobre questões referentes a direitos humanos e ao trabalho análogo ao escravo em suas cadeias de valor.<sup>12</sup>

Nossa pesquisa mostra que quase três quartos das empresas para as quais a CSRD pode ser relevante determinaram sua aplicabilidade. No entanto, 27% não ouviram falar da CSRD ou ainda não a estudaram a fundo para saber se seus negócios serão impactados. Além disso, em março de 2024, o Conselho e o Parlamento Europeu anunciaram um acordo provisório para proibir produtos feitos com trabalho análogo ao escravo.

Nos EUA, a intensificação da fiscalização tem focado principalmente nos riscos de trabalho análogo ao escravo nas cadeias de suprimentos e, em particular, em possíveis violações da *Uyghur Forced Labor Prevention Act* (a Lei de Prevenção ao Trabalho Forçado Uigur, ou UFLPA).<sup>13</sup>

Somente em 2023, o departamento de Alfândega e Proteção das Fronteiras dos EUA deteve US\$ 1,42 bilhão em remessas como parte da fiscalização da UFLPA, impactando setores como automotivo, vestuário, eletrônicos, produtos farmacêuticos e outros.<sup>14</sup> Não há dúvida, portanto, de que a *due diligence* de direitos humanos está se tornando uma prioridade.



<sup>11</sup> [https://www.europarl.europa.eu/doceo/document/TA-9-2024-0329\\_EN.html](https://www.europarl.europa.eu/doceo/document/TA-9-2024-0329_EN.html)

<sup>12</sup> <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2464>

<sup>13</sup> <https://www.govinfo.gov/app/details/PLAW-117publ78>

<sup>14</sup> <https://www.cbp.gov/newsroom/stats/trade/uyghur-forced-labor-prevention-act-statistics>

## Uma análise mais profunda

A boa notícia para as empresas e seus conselhos de administração é que existem excelentes fontes de informação disponíveis que podem guiar os esforços corporativos.

“As empresas que estão começando sua jornada de *compliance* com direitos humanos e trabalho análogo ao escravo deveriam consultar dois documentos fundamentais: os Princípios Orientadores das Nações Unidas para Empresas e Direitos Humanos e o Guia de *Due Diligence* da OCDE para Conduta Empresarial Responsável”, explicou Tom Plotkin, da Covington & Burling.

Esses documentos estabelecem muitos elementos essenciais que um programa de *compliance* efetivo deveria ter e são referências úteis para avaliar tanto programas existentes quanto os que estão surgindo.

Já que mais de um em cada três executivos (34%), no mundo, acredita que a avaliação dos riscos do trabalho análogo ao escravo em suas cadeias de suprimentos é uma prioridade – e quase 50% das empresas que estão na Europa Ocidental já fizeram esse tipo de avaliação ou planejam fazer no próximo ano –, a expectativa é que as organizações possam aproveitar bem esses guias das Nações Unidas e da OCDE.

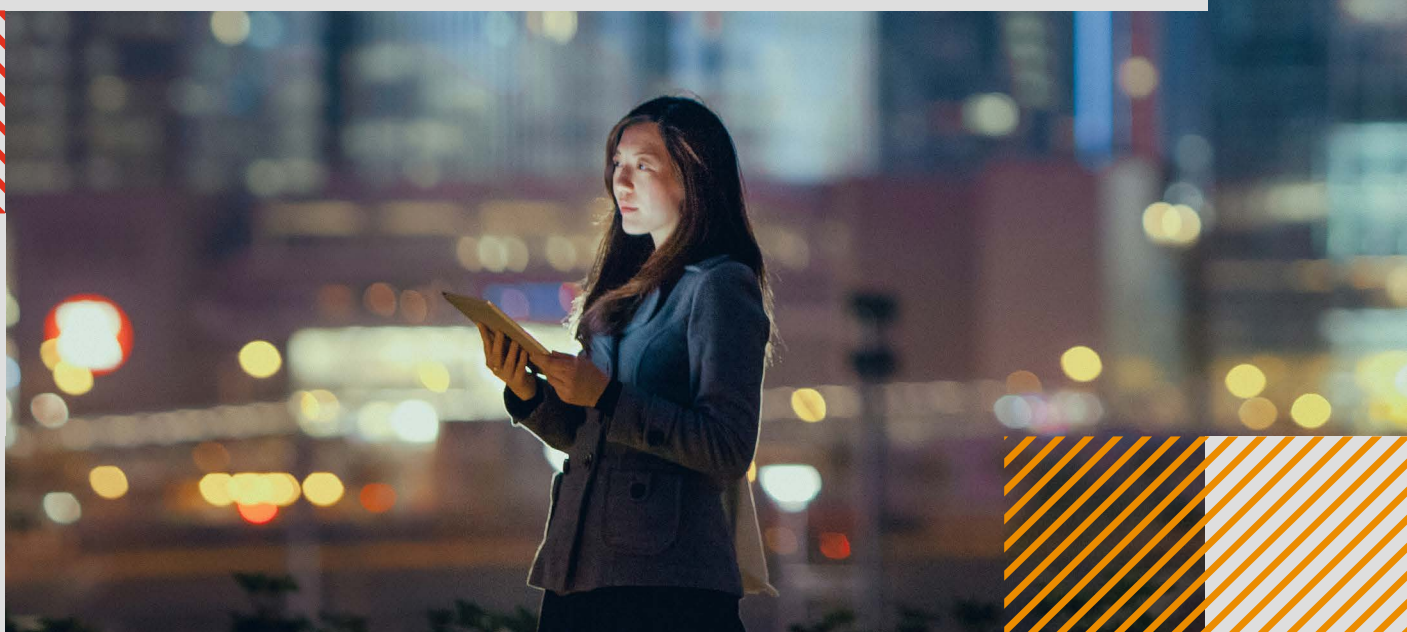
No entanto, a preocupação das empresas brasileiras em relação a esse tema é menor. Somente 27% apontaram que uma avaliação dos riscos do trabalho análogo ao escravo já teria sido concluída, estaria em andamento ou poderia ocorrer dentro de um ano. Por outro lado, 35% declararam que essa não é uma prioridade para a empresa. Globalmente, 26% pensam da mesma forma.



Nossa pesquisa sugere que essa despreocupação se verifica, mundialmente, mesmo naqueles setores com expressivo risco de trabalho análogo ao escravo. Enquanto 40% das empresas de EU&R e 38% de TMT já fizeram ou planejam fazer uma avaliação desse tipo de risco, as de produção industrial estão atrasadas. Metade dessas companhias diz que isso não é prioridade ou que, ainda que seja um assunto importante, não planeja avaliar esse tipo de risco.

Para entender bem onde estão situados os maiores riscos de direitos humanos em suas cadeias de suprimentos, muitas empresas começaram a mapeá-las. Mais de um terço (36%) mapeou suas cadeias, segundo nossa pesquisa, até os fornecedores Tier 1 (T1) ou Tier 2 (T2).

No caso dos respondentes da Europa Ocidental e América do Norte, esse número é maior, de quase 50%. Entre os setores, o de varejo e consumo é o que está mais avançado, já que 42% das empresas mapearam até T1 ou T2.



No Brasil, o mapeamento dos fornecedores se volta somente ao primeiro nível (T1) para quase 40% das empresas, ao passo que, globalmente, esse número é de 26%. O outro lado deste quadro é que o número daqueles que vão além, isto é, mapeiam T2, T3 e adiante, é de 29%, no mundo, mas um número menor foi verificado no Brasil (22%).

Como o esforço para atingir o Tier N – os níveis inferiores das cadeias – pode envolver o gasto de muitos recursos, são essenciais o desenvolvimento de uma estratégia sofisticada de engajamento dos fornecedores e a compreensão das complexidades técnicas associadas.

## A avaliação dos riscos do trabalho análogo ao escravo é prioridade ou não para a sua empresa? Talvez o foco seja insuficiente

**Pergunta:** independentemente de estar ou não sob a vigência da *Corporate Sustainability Reporting Directive*, você acredita que avaliar o risco de trabalho análogo ao escravo na cadeia de suprimentos é uma prioridade para sua empresa?

**Base:** todos os entrevistados = 2446, Brasil = 52.



Brasil



Mundo

Não, essa não é uma prioridade hoje



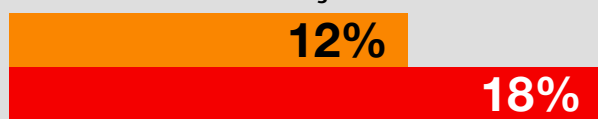
Sim, mas não há planos para uma avaliação ainda



Sim, uma avaliação está planejada para os próximos 12 meses



Sim, uma avaliação está em andamento ou já terminou



Não tem certeza/não sabe



**33%**

Governo e  
Serviços Públicos

**27%**

Produção  
Industrial

**30%**

Serviços  
Financeiros

**20%**

Mercados  
de Consumo

**28%**

Energia, Serviços de  
Utilidade Pública e  
Recursos Naturais

**22%**

Saúde

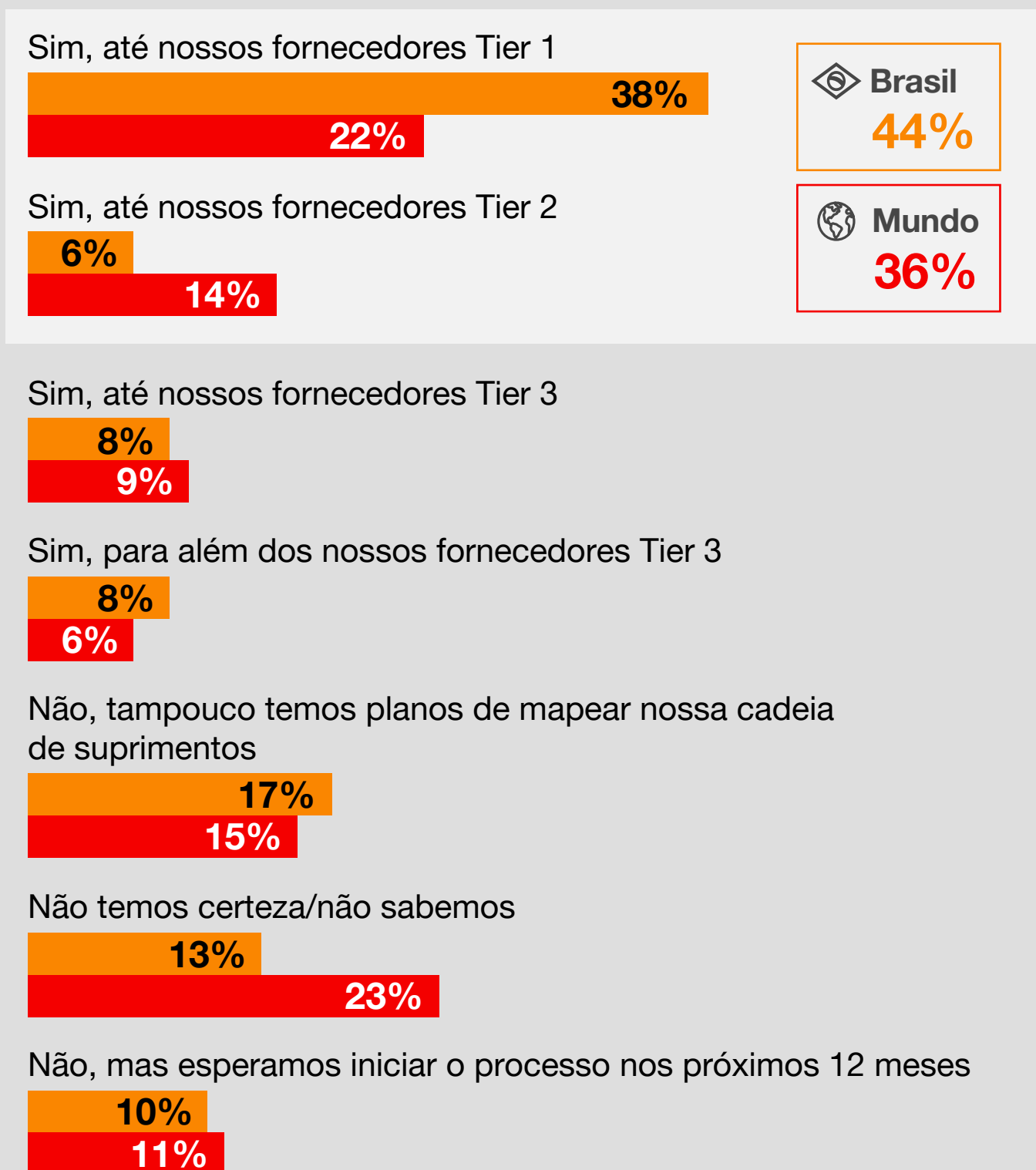
**24%**

Tecnologia, Mídia  
e Telecomunicações

## Mapeamento das cadeias de suprimentos – o início da jornada

**Pergunta:** sua empresa já mapeou sua cadeia de suprimentos?

**Base:** todos os entrevistados = 2446, Brasil = 52.

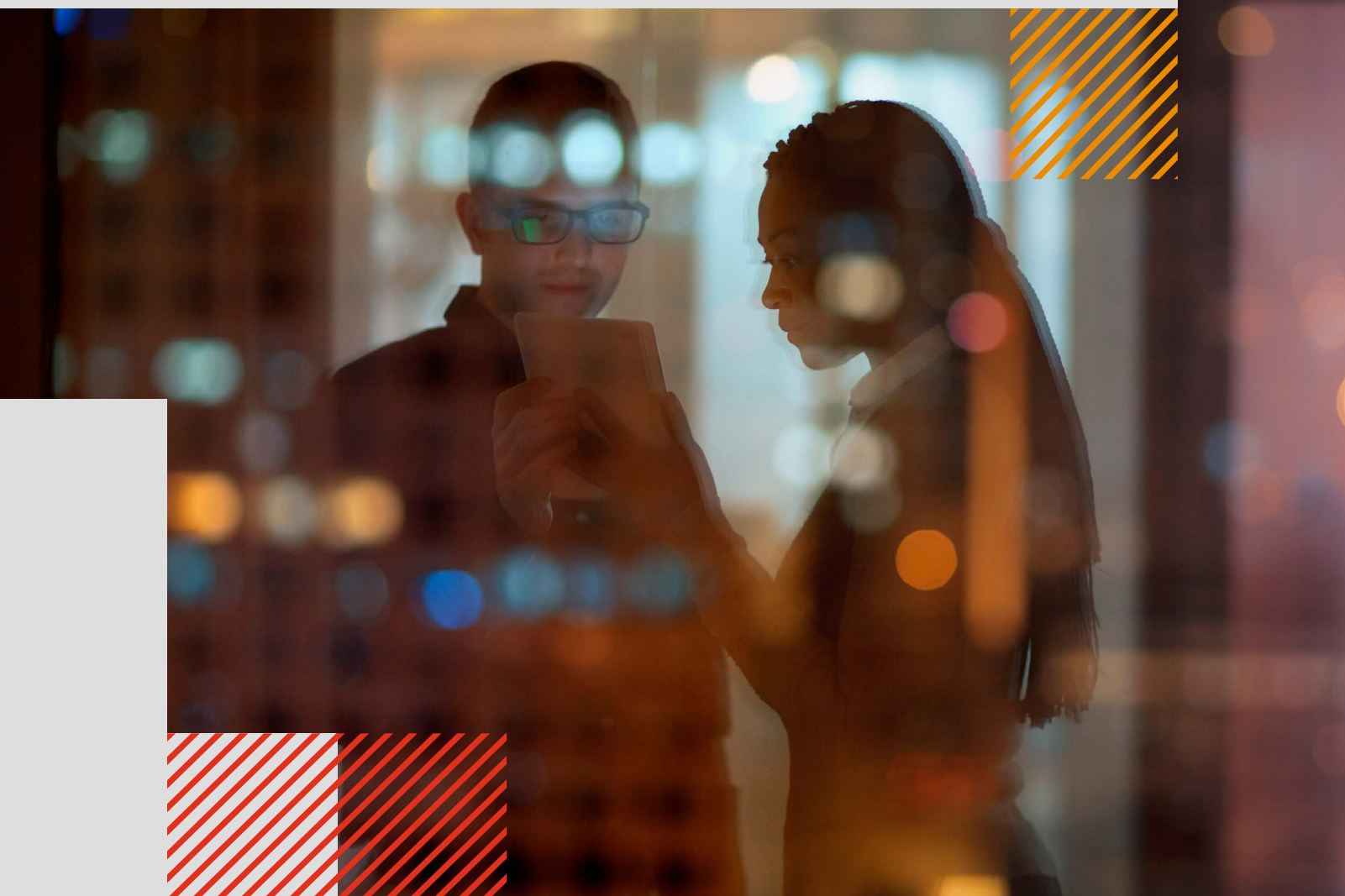


Auditorias *in loco* são outra ferramenta que pode auxiliar a compreender as condições e práticas de trabalho em um fornecedor de alto risco. Ao contrário do impulso que ganhou o mapeamento das cadeias de suprimento, uma minoria está realizando auditorias de terceiros para avaliar a conformidade dos fornecedores com regulamentações de trabalho análogo ao escravo.

Na verdade, somente 15% das empresas conduzem essas auditorias regularmente, sobretudo na América do Norte e na Europa Ocidental. Empresas com receitas superiores a US\$ 5 bilhões lideram o caminho. Uma parcela maior de companhias do varejo e consumo (20%) realizam de forma regular auditorias para prevenir o trabalho análogo ao escravo e outras 20% fazem isso, mas menos frequentemente.

Enfim, o que motivaria uma organização a implementar um programa robusto de auditoria de terceiros em relação ao trabalho análogo ao escravo? Mundialmente, nossa pesquisa mostra que os principais motivos seriam o peso da lei, uma investigação regulatória ou o entendimento de que é a coisa certa a se fazer. Publicidade negativa sobre as práticas da sua cadeia de suprimentos também está entre os três motivos principais.

No Brasil, há uma peculiaridade, mais que a questão da publicidade negativa (10%) surge a pressão dos acionistas (12%) que ocupa o terceiro principal motivo para uma implementação desse tipo de programa de auditoria. De qualquer modo, duas das três principais inspirações relatadas em nosso estudo são de natureza reativa. No final da lista, está a pressão de organizações não-governamentais.



## Risco de investigação judicial e outros fatores que impulsionam uma nova abordagem para auditorias de terceiros na prevenção do trabalho análogo ao escravo

**Pergunta:** quais dos seguintes fatores levariam sua empresa a implementar um programa robusto de auditoria de terceiros para prevenção do trabalho análogo escravo?

**Base:** todos os entrevistados = 2446, Brasil = 52.



Investigação judicial ou regulatória da sua empresa



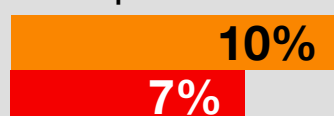
Porque é a coisa certa a fazer



Pressão dos acionistas



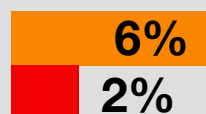
Publicidade negativa sobre as práticas das cadeias de suprimento de seu setor



Publicidade negativa sobre as práticas das cadeias de suprimento de sua empresa



Pressão de organizações não governamentais



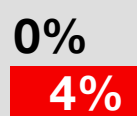
Pressão do conselho sobre a diretoria



Não tem certeza/não sabe



Nenhuma das opções acima





### Envolvimento proativo do conselho de administração

Diante da crescente atenção à questão do trabalho análogo ao escravo nas cadeias de suprimentos, os conselhos de administração precisam priorizar esse tema antes que ele se transforme em uma crise por causa da pressão externa. Na prática, isso significa começar a requerer atualizações anuais dos executivos, inclusive descobrir como anda o mapeamento das cadeias de suprimentos.

Ao exigir esses updates, os conselhos podem demonstrar sua vontade de lidar com o risco de trabalho análogo ao escravo e fazer com que seus diretores sejam passíveis de responsabilização. Esse esforço de atualização deve abarcar uma avaliação abrangente dos riscos nas cadeias de suprimentos da empresa, preparada por um grupo de trabalho multifuncional, que identifique quaisquer ameaças ou sinais de alerta (*red flags*) que possam indicar a existência de trabalho análogo ao escravo.

Devem ocorrer também, ao menos anualmente, reavaliações dos mapas das cadeias de suprimento existentes. As empresas deveriam incluir cláusulas contratuais junto a fornecedores-chave para que eles os atualizem sobre mudanças em seus fornecedores T1 pelo menos. Todos esses esforços contribuirão para que o primeiro, o segundo e o terceiro níveis da cadeia (T1, T2 e T3) trabalhem juntos para tratar desse risco a partir de uma abordagem de garantia integrada.

Por meio de relacionamentos existentes com fornecedores ou processos de onboarding, as empresas podem coletar informações relevantes – como, por exemplo, o local da manufatura ou processamento, e o tipo de força de trabalho envolvido – e identificar riscos potenciais ou prejuízos reais aos direitos humanos.

Elas podem ainda tomar medidas proativas, como a realização de *due diligences* minuciosas em entidades que apresentem sinais que possam indicar a presença de trabalho análogo ao escravo ou outros abusos. Isso deve ser acompanhado por ações apropriadas de mitigação e remediação, como se engajar com fornecedores para melhorar suas condições de trabalho ou buscar fornecedores alternativos que sigam padrões éticos.

## Auditorias robustas *in loco*

Conforme mencionamos, auditorias *in loco* podem ser uma ferramenta valiosa para identificar possíveis violações. Definir exatamente que equipe da empresa as conduz geralmente depende do modelo operacional. O *compliance* ou a equipe responsável pela seleção de fornecedores são duas das escolhas comuns.

O executivo responsável pela gestão de riscos também pode variar, embora, em organizações mais maduras, o risco seja de responsabilidade da empresa como um todo (primeira linha de defesa). De qualquer modo, a recomendação é que os relatórios produzidos pós-auditoria devem ser amplamente compartilhados, inclusive com o time de auditoria interna.

Vale notar ainda que essa prática deve estar incorporada a um arcabouço de gestão de riscos de fornecedores mais amplo. Por si só, a prática de auditorias como avaliação de padrões sociais e éticos representa apenas uma “fotografia” do local de trabalho em questão em determinado momento e lugar.

Não raro, elas não trazem um retrato genuíno das condições diárias de trabalho. As auditorias têm severas limitações – por exemplo, entrevistas insuficientes com trabalhadores, barreiras linguísticas, falta de revisões profundas, práticas de subcontratação, entre outras –, e as empresas não devem confiar exclusiva ou excessivamente nelas para detectar e remediar o trabalho análogo ao escravo.

Em vez disso, recomenda-se uma abordagem mais ampla que envolva ativamente os fornecedores por meio de treinamentos, capacitação, envolvimento dos trabalhadores, fortalecimento da gestão e maior transparência.

“Estamos assistindo a um aumento dos riscos de trabalho análogo ao escravo nas cadeias de suprimento globais dos nossos clientes. O risco reputacional é alto, requer gestão proativa e *due diligence*.”

**Matthew Bruce,**  
Freshfields Bruckhaus Deringer



## Insights dos profissionais líderes

Confira algumas recomendações dos nossos entrevistados:



### **Adote KPIs de sustentabilidade para terceiros**

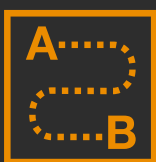
As empresas devem considerar a adoção de uma categoria adicional de *risk scoring* de terceiros: o *score* de sustentabilidade. Um dos nossos entrevistados explicou, por exemplo, que sua empresa desenvolveu mais de 20 indicadores-chave de desempenho relacionados à sustentabilidade de terceiros.



### **Audite regularmente terceiros de maior risco**

Faça auditorias regulares em seus *stakeholders* externos de maior risco. Auditorias presenciais devem ser realizadas em aproximadamente 75% do grupo de terceiros de maior risco ao menos uma vez a cada dois anos.





## **Não deixe de avançar no mapeamento da sua cadeia de suprimentos**

Os conselhos de administração precisam insistir no mapeamento como parte integrante do programa de gestão de riscos de terceiros. Por sua vez, os executivos da empresa devem fornecer atualizações regulares sobre o cronograma para concluir o mapeamento do próximo nível de fornecedores até que se tenha analisado com sucesso toda a cadeia.



## **Pondere a oportunidade de receita e as unidades de produção em comparação com riscos operacionais**

As empresas deveriam avaliar os grandes mercados estrangeiros para julgar se a oportunidade de receita e os riscos operacionais justificam uma estratégia de cadeia de suprimentos que possa ser inteiramente autossuficiente em determinado país (por exemplo, uma estratégia “na China para a China”). Em outras situações, uma unidade de produção em um mercado de menor receita pode não valer o risco operacional associado.

## **Oito complexidades que desafiam o mapeamento da cadeia de suprimentos**

O mapeamento efetivo da cadeia de suprimentos de uma empresa implica um complexo conjunto de desafios que abrangem áreas técnicas, organizacionais e de dados. Confira algumas complexidades:

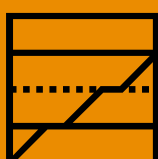


**Integração e harmonização de dados:** combinar dados de várias fontes muitas vezes significa ter de lidar com diferentes formatos, padrões e níveis de detalhe. Essas fontes incluem tanto as de origem interna, como listas detalhadas de materiais por produto, quanto externas, como bancos de dados agregados de bases de carregamento. Garantir que dados tão diferentes possam ser integrados de forma coerente requer processos robustos de harmonização.



### **Qualidade e precisão dos dados:**

coletar dados de qualidade pode ser desafiador. Por isso, é essencial criar um mapa confiável da cadeia de suprimentos. Uma estratégia de engajamento com fornecedores bem fundamentada ajuda a garantir que os dados coletados sejam precisos, completos e oportunos. Já os desafios comuns incluem problemas de gestão de dados mestres com fornecedores e a identificação completa das relações comerciais mais importantes e estratégicas da cadeia de suprimentos.



### **Escalável e replicável:**

uma cadeia de suprimentos pode ser vasta e complexa. Logo, a solução técnica para mapeá-la deve ser escalável o suficiente para lidar com uma grande quantidade de dados de várias fontes sem comprometer o desempenho, com capacidade de detectar mudanças significativas e se atualizar conforme necessário.



### **Segurança e privacidade dos dados:**

as cadeias de suprimentos frequentemente trazem consigo informações sensíveis e com alcance global. É vital, portanto, entender as regulamentações regionais de privacidade de dados – como a *General Data Protection Regulation* (GDPR) da UE, por exemplo – e manter níveis elevados de segurança para protegê-los contra ameaças cibernéticas, além de garantir o *compliance* com diferentes leis e marcos regulatórios de privacidade.



### **Visualização e análise de dados:**

analisar dados integrados para extrair *insights* relevantes é uma tarefa complexa que frequentemente requer técnicas de visualização e *analytics* avançado, que podem se beneficiar do uso de *machine learning* ou outras ferramentas potencializadas pela IA.



**Questões legais e de *compliance*:** diferentes regiões podem ter leis diferentes sobre armazenagem e transferência de dados, o que pode complicar a infraestrutura técnica necessária para um mapa robusto da cadeia de suprimentos global.



**Processamento de eventos complexos:** reconhecer padrões e correlações entre diferentes bases de dados e compreender suas implicações na cadeia de suprimentos requer capacidades para processamento de eventos complexos.



**Ferramentas de colaboração:** um mapeamento eficaz da cadeia de suprimentos exige a colaboração entre diversas áreas dentro da empresa e a participação de parceiros externos. A solução técnica deve apoiar, portanto, uma colaboração eficiente e segura. Enfrentar esses desafios geralmente exige uma abordagem multidisciplinar que reúne expertise em ciência de dados, TI, gestão da cadeia de suprimentos e cibersegurança, entre outras áreas.



## Você conhece indicadores de que o trabalho análogo ao escravo pode estar presente?

A Organização Internacional do Trabalho (OIT) compilou 11 indicadores que correspondem aos sinais ou às “pistas” mais comuns da possível existência de trabalho análogo ao escravo.

Como enfatizou Tom Plotkin, da Covington, “esses indicadores não necessariamente são uma confirmação do trabalho análogo ao escravo, mas refletem possíveis estruturas ou vulnerabilidades em que essa situação pode existir. Esses índices se tornaram alertas críticos não apenas para as empresas, mas também para os reguladores que os utilizam para orientar as atividades de fiscalização.”

- Abuso de vulnerabilidades
- Fraude
- Restrição de movimento
- Isolamento
- Violência física e sexual
- Intimidação e ameaças
- Retenção de documentos de identidade
- Retenção de salários
- Servidão por dívida
- Condições abusivas de trabalho e de moradia
- Horas extras excessivas

Fonte, com mais informações: [Indicadores de Trabalho Forçado da OIT](#).



# Sanções e controles de exportação

**Tensões geopolíticas tornam os esforços de *compliance* corporativo mais complexos.**

**Questões geopolíticas – como o conflito entre Rússia e Ucrânia, as tensões entre China e Estados Unidos e as incertezas no Oriente Médio – dão origem ao ambiente regulatório de sanções e controles de exportação em que empresas de todo o mundo têm de operar.**

O governo americano, com seus departamentos de Justiça, Tesouro e Comércio, está impulsionando muitos desses desenvolvimentos, ao mesmo tempo que o alinhamento de outros países com essas políticas está aumentando. As multinacionais, por sua vez, independentemente de apoiarem ou não essas prioridades políticas, têm pouca escolha a não ser seguir as mudanças legislativas e regulatórias.

Como enfatizou Steven Fagell, do escritório de advocacia Covington & Burling, “o Procurador-Geral Adjunto e outros líderes seniores do Departamento de Justiça dos EUA observaram que os conselhos de administração das corporações deveriam ver o *compliance* com controles comerciais como uma prioridade absoluta e um fator-chave de risco legal. As empresas estão respondendo com investimentos em *compliance*, levando as investigações mais a sério e informando os riscos associados a controles de comércio nos níveis do conselho e da direção executiva.”

As declarações do *Bureau of Industry and Security* (o BIS, Gabinete da Indústria e Segurança) do Departamento de Comércio dos EUA e de seu Secretário Adjunto para Exportações, Matthew Axelrod, são leituras obrigatórias para executivos de *compliance* corporativo em todo o mundo. A estreita colaboração do BIS com a Justiça e o Tesouro é ilustrada por uma série de *Notas de Compliance Tri-Seal*, publicadas de forma conjunta pelos três departamentos, que fornecem orientações importantes sobre questões de controle e sanção de exportações.<sup>15</sup>

A intensificação dos esforços de fiscalização é também provável. “Em particular, os Departamentos de Comércio e Justiça estão seguindo teorias jurídicas criativas e expansivas e contratando dezenas de novos advogados e agentes dedicados a esses casos”, explicou Eric Sandberg-Zakian, da Covington & Burling. “Já as agências de fiscalização estão buscando penalidades maiores e impondo compromissos de *compliance* mais onerosos nos acordos.”

Para evidenciar o comprometimento americano de liderar esforços coordenados globalmente, seria recomendável que os conselhos de administração e executivos das empresas se debruçassem sobre as declarações do “*Export Enforcement Five*” – grupo formado por EUA, Canadá, Reino Unido, Austrália e Nova Zelândia, semelhante ao arranjo de cooperação de inteligência “*Five Eyes*”.

<sup>15</sup> Há vários outros anúncios de múltiplas agências sobre controles de exportação e questões relacionadas a sanções. Para alguns desses anúncios, confira os links a seguir:  
<https://www.justice.gov/nsd/compliance-notes>  
[https://www.fincen.gov/sites/default/files/shared/FinCEN\\_Joint\\_Note\\_US\\_Export\\_Controls\\_FINAL508.pdf](https://www.fincen.gov/sites/default/files/shared/FinCEN_Joint_Note_US_Export_Controls_FINAL508.pdf)

Outros esforços bilaterais e multilaterais incluem o movimento do BIS para envolver o Japão e a Coreia do Sul em uma Rede de Proteção de Tecnologia Disruptiva<sup>16</sup>, alinhada à Força-Tarefa de Tecnologia Disruptiva do BIS/Departamento de Justiça americano. De forma semelhante, outros países estão fortalecendo suas capacidades de aplicação da lei, como o estabelecimento do Escritório de Implementação de Sanções Comerciais pelo Reino Unido, que têm a responsabilidade de investigar atividades de empresas que possam estar tentando evitar sanções ao enviar produtos por meio de outros países.



Mundialmente, 59% dos executivos entrevistados concordam que os controles de exportação se tornaram mais complexos nos últimos dois anos. No Brasil, 61% fizeram a mesma avaliação. Esse percentual vai a 69% para empresas com mais de US\$ 5 bilhões em receitas anuais e em organizações norte-americanas. Por fim, uma parcela ainda maior de companhias nos setores de TMT e EU&R, de 66% em cada, acredita que recentemente aumentou a complexidade desses controles.

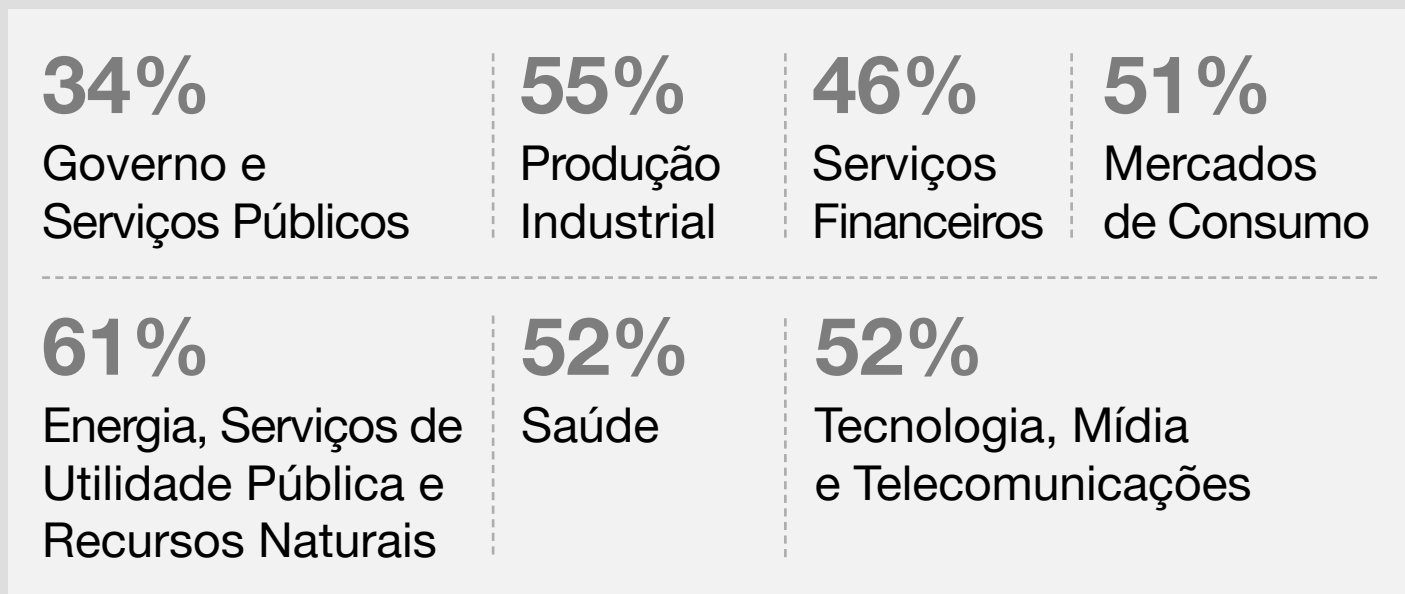
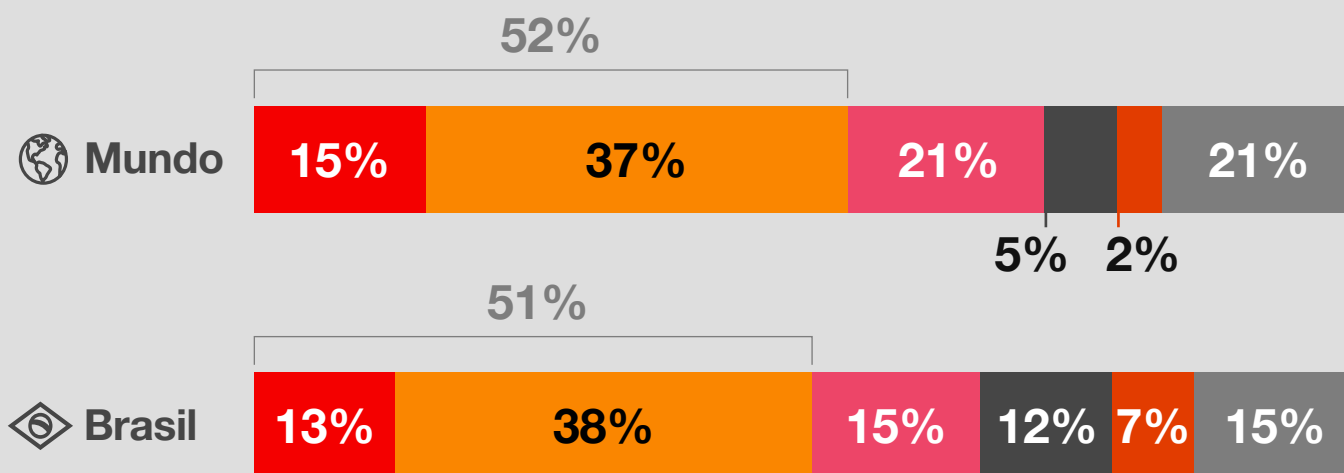
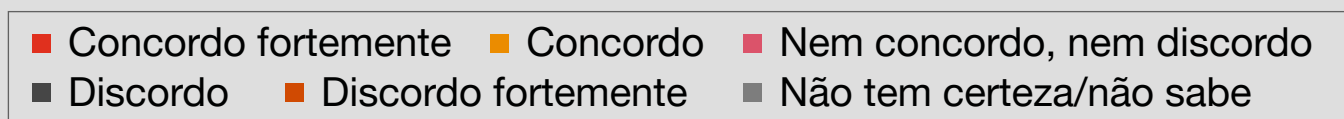
<sup>16</sup> <https://www.bis.gov/press-release/departments-justice-and-commerce-launch-disruptive-technology-protection-network>

## Um cumprimento das leis de controle de exportação mais rigoroso

**Pergunta:** até que ponto você concorda ou discorda das seguintes afirmações? Nos últimos dois anos, os controles de exportação por parte de governos de vários países estão sendo aplicados de forma mais rigorosa.

**Base:** todos os entrevistados = 2446, Brasil = 52.

Observe que as porcentagens não totalizam 100% devido ao arredondamento.



No que diz respeito aos esforços de fiscalização, os executivos também concordam que eles estão aumentando. Mais da metade (52%) dos executivos no mundo e no Brasil (51%) avaliam que os controles de exportação estão sendo aplicados de forma mais robusta do que há dois anos. 62% dos respondentes que trabalham em corporações com receita de US\$ 5 bilhões ou mais concordam com essa crença.



Embora a percepção comum seja de que esses controles se aplicam mais aos setores de tecnologia, produtos químicos, aeroespacial e de defesa, há uma ampla gama de produtos em outros que vão de bens de consumo a produção industrial, assim como farmacêuticos que também são controlados para não acabar em países com sanções.

Assim como na multiplicação de setores para os quais os controles de exportação têm relevância, a crença de que a fiscalização está se intensificando é generalizada. Mais da metade dos executivos de produção industrial, EU&R, varejo e consumo, saúde e TMT concordam.

Matthew Axelrod, do BIS, resumiu bem o ambiente de controle cada vez mais intenso das exportações ao compartilhar os objetivos de sua agência em um [discurso recente](#). Ele disse: “Nosso objetivo é encorajar e incentivar o investimento em *compliance* desde a fase inicial, ao mesmo tempo em que enfatizamos o custo financeiro e reputacional de enfrentar uma ação de fiscalização. Estamos igualmente comprometidos em adotar maneiras cada vez mais agressivas e eficazes de implicar as empresas que não cumprem a lei.”

## Uma análise mais profunda

Fazer a gestão dos controles de exportação não é uma questão restrita a poucos setores industriais. Na verdade, mais da metade dos respondentes (56%) concorda que essa é uma prioridade em seu segmento. Uma parcela ainda maior dos executivos nos setores de EU&R, saúde e produção industrial concordou com essa afirmação.

Em relação ao risco desse tipo de controle, mais da metade (56%) afirmou que sua gestão é importante para a empresa, com números ainda maiores na América do Norte (65%). Restrições relacionadas à China estão direcionando o foco das empresas na gestão de riscos associados a controles de exportação na Ásia-Pacífico (60% consideram isso uma prioridade).

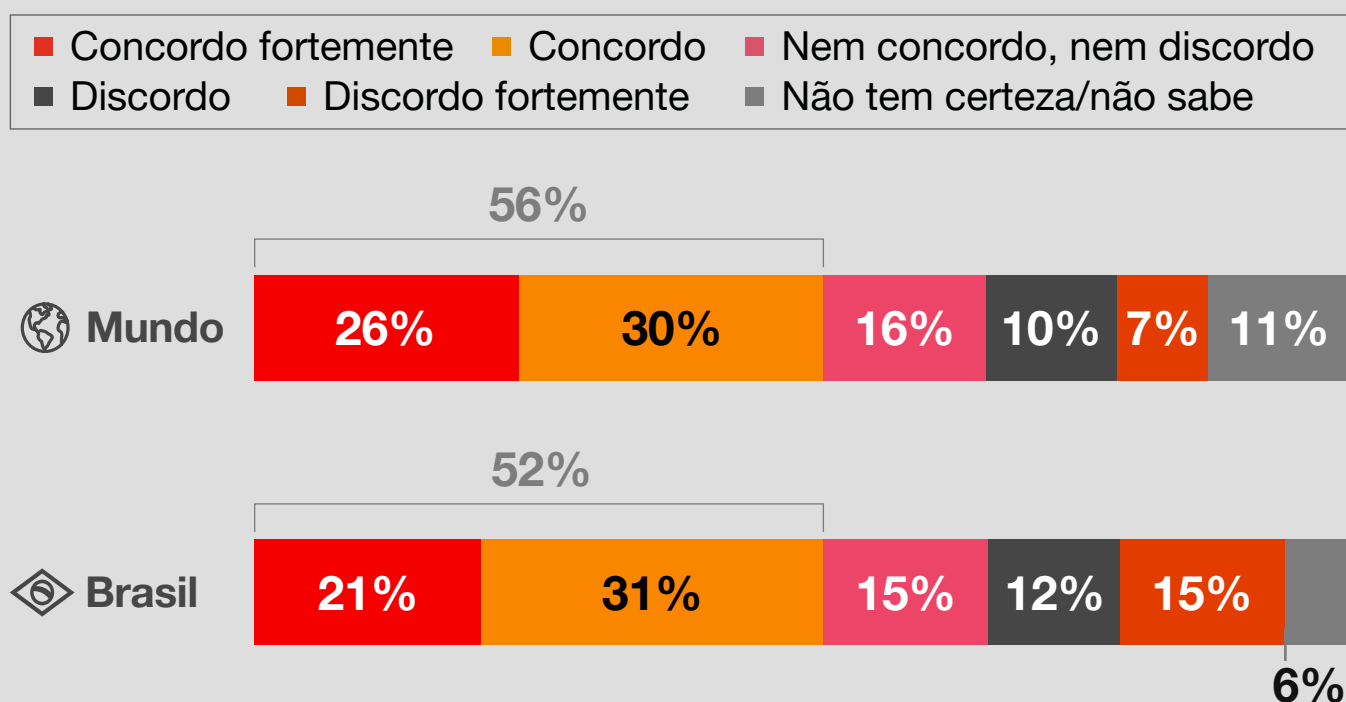
O número expressivo das companhias da Europa Central (55%) que consideram isso importante pode ser fruto das preocupações em torno do conflito Rússia-Ucrânia. Igualmente, as grandes empresas – com receitas superiores a US\$ 5 bilhões – estão mostrando que estão se sentindo pressionadas, uma vez que 72% afirmam que gerenciar os riscos associados a controles de exportação é uma prioridade. Dessa forma, elas parecem estar tomando medidas efetivas.

Quase três quartos relataram que têm processos robustos de avaliação de riscos de controle de exportação, que incluem a colaboração de equipes jurídicas, de *compliance* comercial e operacionais, tanto nas sedes das corporações quanto em jurisdições de maior risco.

## Naturalmente, a gestão de riscos está ganhando atenção

**Pergunta:** até que ponto você concorda ou discorda das seguintes afirmações? A gestão de riscos associados a controles de exportação é uma prioridade em nossa organização.

**Base:** todos os entrevistados = 2446, Brasil = 52.



45%

América Latina

53%

África

55%

Europa Central e do Leste

60%

Ásia-Pacífico

57%

Europa Ocidental

65%

América do Norte

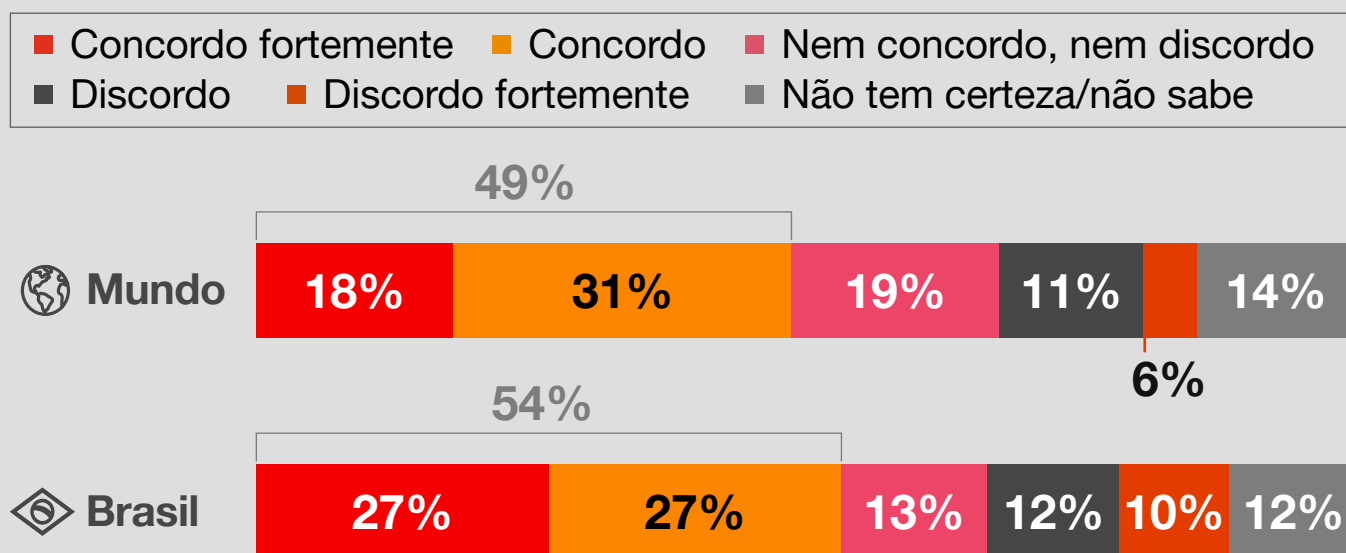
Por outro lado, de modo geral, o cenário é contrastante. Apenas metade indicou que tem um processo robusto de avaliação. Regionalmente, cerca de dois terços das companhias da América do Norte (62%) relataram ter um processo forte de avaliação de riscos de controle de exportação, ao passo que, no Brasil, 42% foram na mesma direção.

Por causa da conscientização em relação aos riscos associados a controles de exportação, incluindo o de um concorrente relatar sua conduta ao governo americano, e especialmente à luz das mudanças na política de *self-disclosure* voluntário<sup>17</sup> em abril de 2023, não é surpreendente que o BIS tenha observado um aumento anual de quase 80% nessas divulgações realizadas de forma voluntária e um terço a mais de denúncias setoriais sobre condutas de terceiros no mesmo período.

## Reúna todo mundo e estabeleça um processo robusto de avaliação de riscos de controle das exportações

**Pergunta:** até que ponto você concorda ou discorda das seguintes afirmações? Nossa empresa possui um processo robusto de avaliação de riscos associados a controles de exportação, inclusive com participação de equipes jurídicas, de *compliance* comercial e de operações - tanto na sede quanto em jurisdições de maior risco.

**Base:** todos os entrevistados = 2446, Brasil = 52.



41%

América Latina

42%

África

48%

Europa Central e do Leste

50%

Ásia-Pacífico

53%

Europa Ocidental

62%

América do Norte

<sup>17</sup> <https://www.bis.gov/speeches/remarks-prepared-delivery-assistant-secretary-export-enforcement-matthew-s-axelrod-biss>

Assim como demonstra uma especial atenção aos riscos de controle de exportação, metade das empresas brasileiras apontou que o *compliance* com o risco de sanções tem uma prioridade alta. Outros 33% atribuíram ao tema uma prioridade moderada. De modo geral, os resultados foram um pouco menores, respectivamente, 44% e 24%.

Embora as empresas de produção industrial tenham indicado uma alta conscientização sobre os riscos de controle de exportação, elas classificaram a prioridade de conformidade em relação aos riscos de sanções a uma taxa inferior à média global.

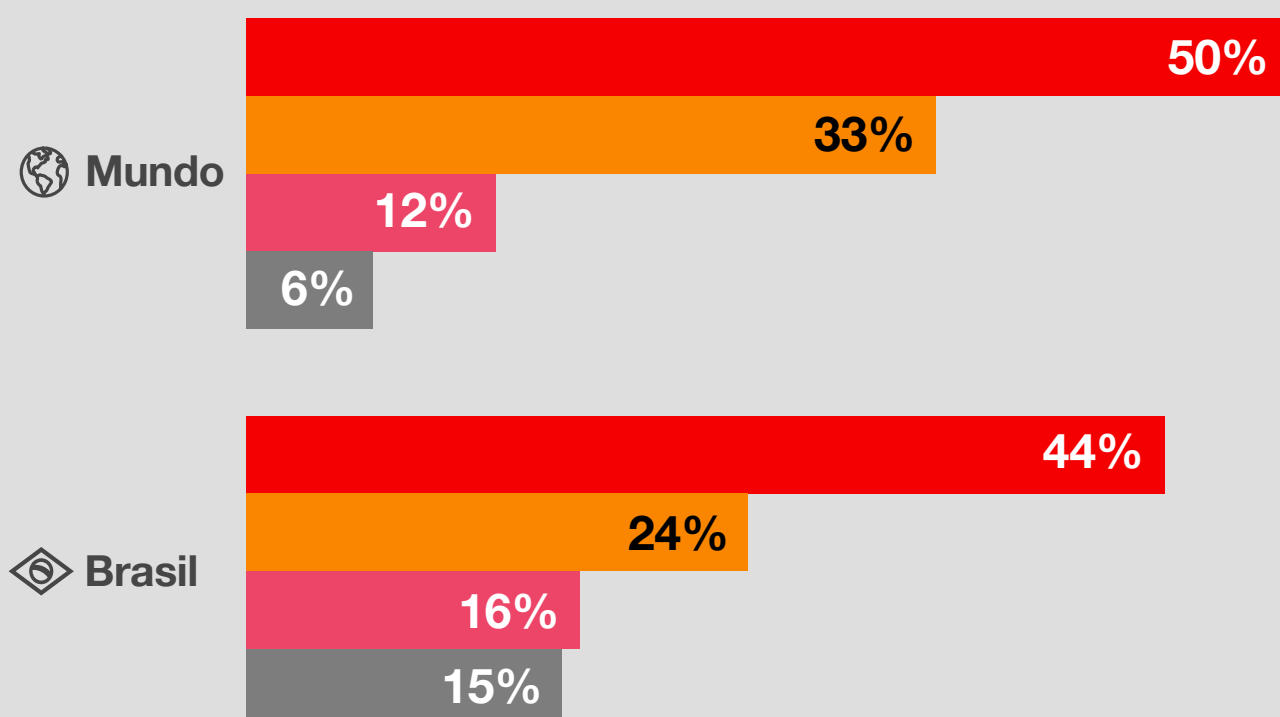
## O compliance em relação ao risco de sanções recebe grande atenção de várias empresas

**Pergunta:** em que medida o *compliance* com o risco de sanções é uma prioridade dentro da sua empresa?

**Base:** todos os entrevistados = 2446, Brasil = 52.

As porcentagens não somam 100% devido ao arredondamento.

- Alta prioridade – temos uma equipe dedicada para assegurar que nossa organização trata o *compliance* com riscos de sanções
- Prioridade moderada – temos uma equipe específica que se reúne regularmente para tratar o *compliance* com riscos de sanções
- Prioridade baixa – temos uma equipe informal que se reúne *ad hoc* para tratar dos riscos de sanções se e quando algum problema surge
- Não é uma prioridade hoje – não há um processo formal de *compliance* com risco de sanções dentro da empresa



Quando o assunto é o *compliance* em relação ao risco de sanções, terceiros são o foco. De fato, 65% dos respondentes consideram que a possibilidade de envolvimento de terceiros em atividades ilícitas representa um dos dois maiores riscos de sanções. No caso do Brasil, a percepção na liderança ainda é mais evidente, já que 71% enxergam riscos em terceiros como fornecedores, distribuidores e clientes.

Essa descoberta destaca a urgência da gestão desse risco. Sentem mais fortemente a influência de terceiros nos riscos de sanções os profissionais baseados na América do Norte (74%), América Latina (69%) e Europa Ocidental (67%). Os setores de EU&R (74%) e saúde (71%) são os que parecem estar mais conscientes desse risco, enquanto um número menor de produção industrial o classifica como um risco significativo.



## Terceiros no foco novamente - fontes de preocupação em relação ao *compliance* em sanções

**Pergunta:** qual dos seguintes riscos de *compliance* em sanções você acredita ser o maior para sua empresa? (Rankeado nos dois primeiros)

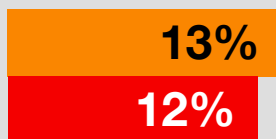
**Base:** todos os entrevistados = 2446, Brasil = 52.



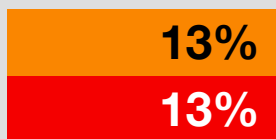
Terceiros (ex: fornecedores e distribuidores) realizando atividades que podem não ser permitidas, criando risco de sanção para a empresa



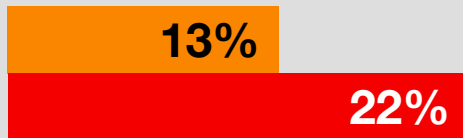
Processos ou tecnologias inadequadas que falham em identificar de forma adequada potencialmente proibidas



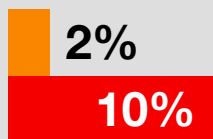
Operações comerciais em certas jurisdições de alto risco (ex: países conhecidos e identificados como pontos de transbordo)



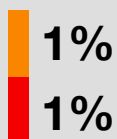
Clientes diretos envolvidos em atividades que possam violar sanções, utilizando os serviços comerciais da empresa



Não tem certeza/não sabe



Outros riscos



Ainda que as empresas reconheçam os riscos de sanções, ainda há muito espaço para aperfeiçoamento dos testes de robustez de seus programas de conformidade. Para se ter ideia, apenas 30% realizam uma variedade de testes, como revisar políticas e procedimentos, pôr à prova as equipes para saber se estão tratando os alertas e casos corretamente e avaliar o desempenho dos sistemas de sanções e a rastreabilidade dos dados.

Mesmo em empresas com receitas superiores a US\$ 5 bilhões, apenas 45% fazem isso de forma abrangente. Quando analisadas por setor, apenas cerca de um quarto das companhias nas áreas de produção industrial (22%), varejo e consumo (25%) e TMT (29%) têm testes robustos. 19% das empresas respondentes não testam regularmente seu programa de compliance em sanções.

Em relação à possibilidade de que as novas tecnologias, como a IA, possam ajudar na eficiência e eficácia do *compliance* em sanções, os brasileiros demonstram otimismo. Quase metade (49%) entende que elas aumentarão de forma drástica a eficiência dos programas de sanções da empresa, inclusive com redução dos custos.

Mundialmente, no entanto, essa ainda é uma questão em aberto. Quase um terço (31%) dos respondentes concorda que essas tecnologias podem ser promissoras em algum momento, mas não acredita que haverá impacto material no curto prazo.

Um quarto (25%) entende que é necessária mais orientação por parte dos reguladores sobre como as novas tecnologias podem se tornar parte integrante do *compliance* em sanções. EU&R, varejo e consumo e serviços financeiros, em particular, estão buscando orientação regulatória em relação a outros setores.

# Opiniões sobre o impacto das novas soluções tecnológicas são, de fato, divergentes

**Pergunta:** considerando as novas tecnologias e novos sistemas (por exemplo, a inteligência artificial com aprendizado de máquina ou a IA generativa), qual impacto você acredita que elas trarão para o seu programa de *compliance* em sanções nos próximos 12 meses?

**Base:** respondentes que indicaram ter um processo de *compliance* com o risco de sanções – Mundo = 2068, Brasil = 49.



Minha aposta é que essas novas tecnologias aumentarão drasticamente a eficiência do nosso programa de sanções, inclusive reduzindo custos



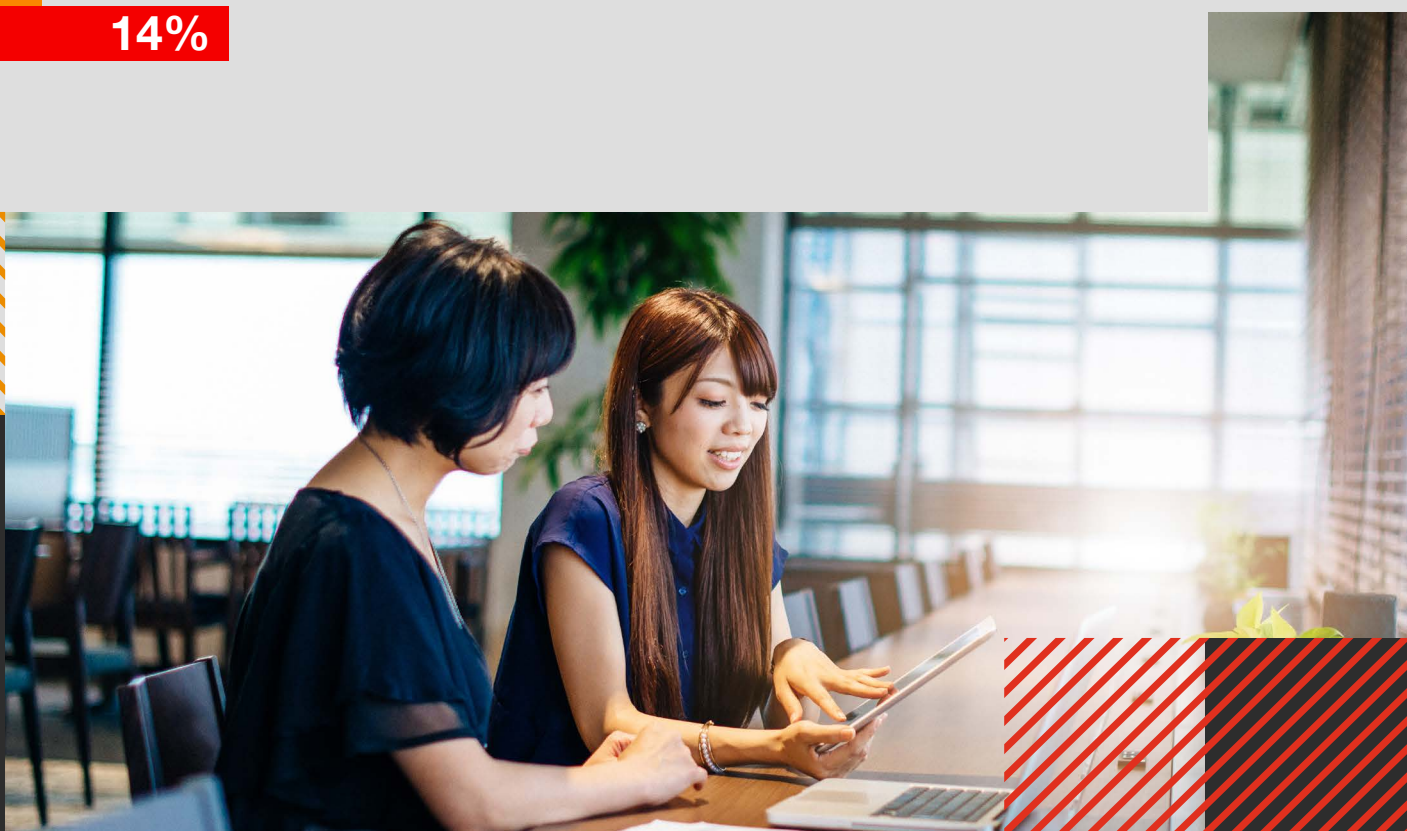
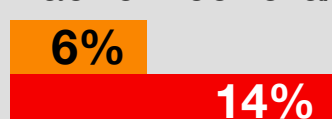
Minha previsão é que essas tecnologias trarão impacto, mas precisamos de mais orientação e aprovação regulatória sobre como e se vamos poder integrá-las a nosso programa de *compliance* com sanções



Embora promissoras, não acho que essas novas tecnologias terão um impacto material no nosso programa no próximo ano



Não tem certeza/não sabe





## Pontos importantes

### Engajando o conselho de administração nos controles de exportação e nas sanções

As prioridades dos conselhos e das lideranças das empresas são claras. Primeiramente, esforços maiores para antecipar tendências geopolíticas devem estar alinhados com a capacitação do negócio para reagir rápido a acontecimentos locais. Essas medidas, por sua vez, contribuirão para avaliações de riscos de maior qualidade e utilidade.

Em segundo lugar, os conselhos devem incentivar seus executivos a adotarem uma abordagem voltada a “toda a empresa” na gestão dos riscos identificados. Por fim, os sistemas tecnológicos que sustentam os esforços de controle de exportação e sanções devem ser avaliados regularmente para garantir que permaneçam “adequados ao propósito”.

“Nossos clientes estão atentos aos riscos geopolíticos e às possíveis restrições comerciais, especialmente em relação à China e ao Oriente Médio. Eles estão cientes da volatilidade e incerteza no cenário global e do impacto potencial em suas operações.”

**Ali Sallaway,**  
Freshfields Bruckhaus Deringer

Ao acompanhar e antecipar tendências diante das constantes mudanças das políticas e exigências dos EUA, assim como de outros países relevantes para as operações de sua empresa, é possível integrar com maior prontidão esses aprendizados ao design, à manutenção e ao aprimoramento de seus programas de *compliance*. Compartilhar esses novos desenvolvimentos com grupos relevantes de funcionários é um componente crítico para manter um programa robusto de *compliance* em as exportações.

## Expectativa de avaliação periódica dos riscos

Embora as autoridades americanas não exijam uma frequência específica para realização de análises de riscos, as empresas devem avaliar periodicamente as mudanças em suas operações comerciais, como fusões e aquisições, localizações, produtos e serviços, e interações com terceiros.

Para complementar essas avaliações internas, a equipe dedicada ao *Trade Compliance* deve realizar auditorias de conformidade em vendas ao exterior. O foco deve ser as áreas-chave – como a revisão dos programas de *compliance* em exportações para implementar salvaguardas ao longo de todo o ciclo de vida desse tipo de operação – e à adequação dos compromissos da liderança, ações de suporte, comunicação, alocação de recursos e fornecimento de financiamento aos times de *compliance* em exportações.

A área de *Trade Compliance* também deve fornecer treinamento contínuo para conscientizar toda a companhia. Isso pode envolver treinamento especializado para as unidades de negócios mais afetadas pelos controles de exportação (por exemplo, engenharia, desenvolvimento de produtos, *procurement*, jurídico, logística e recursos humanos), além de uma formação mais abrangente para a empresa como um todo sobre os fundamentos desses controles. As corporações precisam estar preparadas para mobilizar, realocar e treinar pessoas conforme as exigências do cenário regulatório.



## A conformidade em controles de exportação abrange o ciclo de vida do produto e a organização

Ao passar da avaliação de riscos para as ações de mitigação, é importante destacar que o esforço de uma empresa para gerenciar os riscos de controle de exportação frequentemente começa com as equipes de pesquisa e desenvolvimento (P&D). Devem trabalhar em estreita colaboração com elas os times dedicados ao *Trade Compliance*, especialmente por conta dos potenciais riscos relacionados ao acesso a tecnologias controladas.

É fundamental que o *Trade Compliance* lembre sua organização de que plantas, esquemas, fotografias, manuais de instrução e informações sobre produtos sensíveis podem estar sob o escopo das leis de controle de exportação. Por exemplo, segundo a legislação norte-americana, se um indivíduo não autorizado obtiver acesso a documentos, mesmo que tenham sido acessados no país de origem do produto, este pode ser “considerado exportado” ao último país de residência ou a países de cidadania estrangeira por essa pessoa sem autorização ter acessado as informações.

As autoridades dos Estados Unidos dão grande importância à questão do acesso a itens sensíveis tanto no pré-desenvolvimento quanto no pós. Para implementar controles internos que monitorem quem tem capacidade de trabalho e acesso a produtos sensíveis, a equipe de *Trade Compliance* pode se associar às áreas de TI, segurança da informação, recursos humanos, entre outras.

As implicações do controle de exportação acompanham o produto durante todo o seu ciclo de vida. Embora algumas empresas ainda prefiram seguir o caminho das categorizações baseadas em transações – ou seja, que o *Trade Compliance* classifique um produto no dia em que ele está sendo embarcado –, outras adotam abordagens mais holísticas de classificação.

Nesse último caso, as equipes de *Trade Compliance* têm visibilidade tanto dos produtos atuais quanto dos que devem surgir em um futuro previsível. Geralmente, as equipes de engenharia de produtos são as que estão mais bem posicionadas para lidar com essas questões, dada sua centralidade no ciclo de produção.

Por fim, as áreas de *procurement* também desempenham um papel crítico no *compliance* em controles de exportação. Isso porque alguns produtos de terceiros, como *hardware* e *software*, podem exigir salvaguardas adicionais e requisitos de licença de exportação antes de serem embarcados para plantas e escritórios de uma empresa, além da integração aos produtos preexistentes.



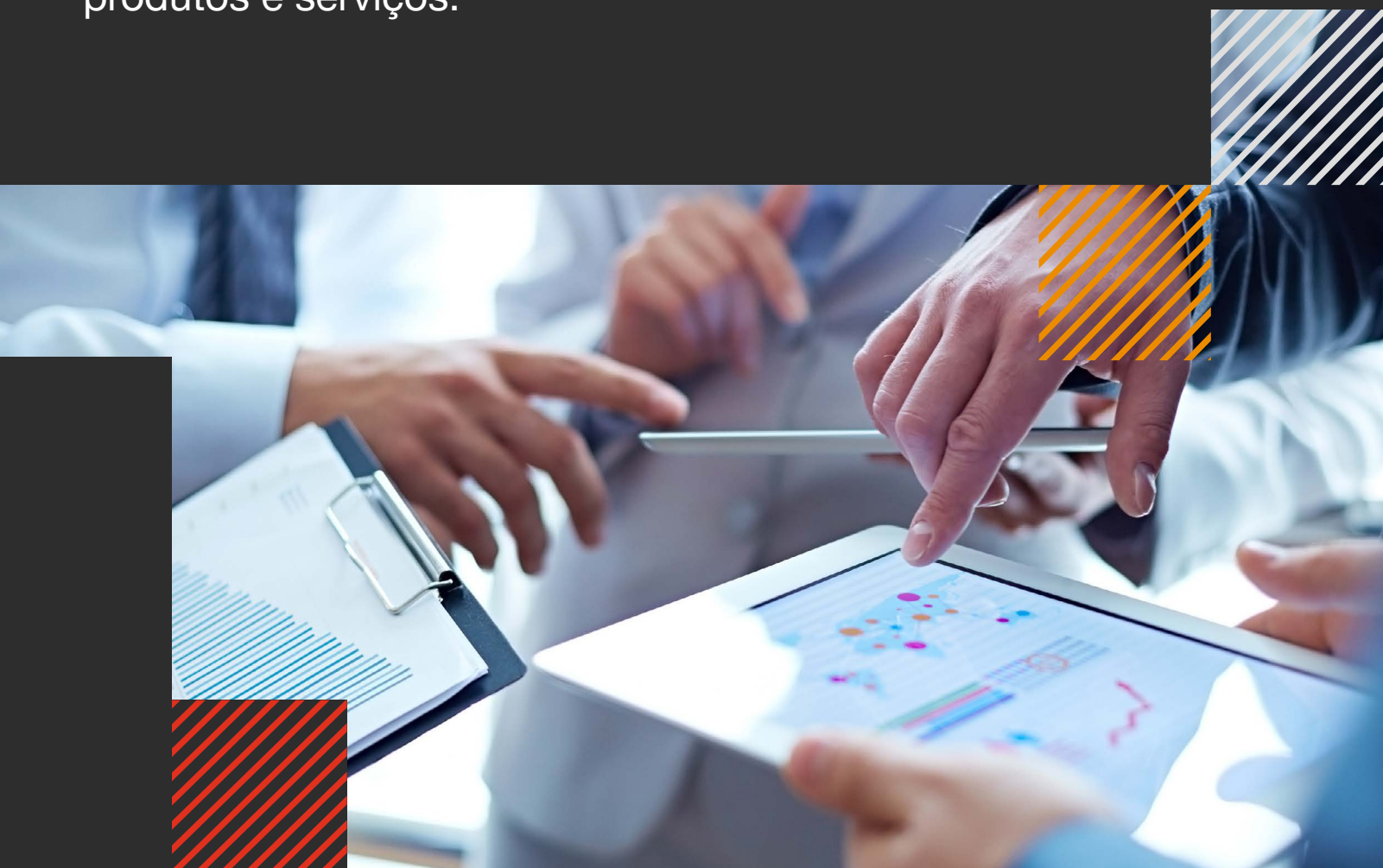
## O papel da tecnologia nos controles de exportação

É crucial que as ferramentas e plataformas tecnológicas que permitem esforços mais amplos de gestão de riscos – incluindo as que apoiam os processos de triagem de partes restritas e de classificação de controle de exportação, além da gestão do ciclo de vida da transação ponta-a-ponta – contribuam para eficiências operacionais e proporcionem uma conformidade sustentável.

Naturalmente, soluções ERP mais sofisticadas incorporam várias dessas capacidades. Módulos disponíveis nessas soluções dão suporte às empresas com a automação e a integração de várias cadeias de suprimentos globais e processos relacionados, incluindo a classificação, definição e redução das licenças de exportação; o embargo e a triagem de partes restritas para que sejam embarcadas ao exterior; e a determinação da elegibilidade de *minimis* (que, por ser muito pequena, não merece atenção jurídica).

É recomendável que os executivos de *Trade Compliance* considerem adotar recursos tecnológicos para a armazenagem segura dos dados controlados de exportação – usando, por exemplo, bancos de dados “offline” ou “nas instalações da empresa” em vez do armazenamento em nuvem.

Eles também precisam estar ativamente envolvidos nas discussões que abrangem o ciclo de vida das tecnologias, como as etapas anteriores à implementação, a implementação em si e os ajustes após. Assim como nas outras partes dos programas de *compliance* com controles de exportação, as plataformas tecnológicas e as soluções automatizadas devem ser frequentemente avaliadas para confirmar se estão “*fit for purpose*” de acordo com o perfil de riscos da empresa, a complexidade das operações comerciais e os tipos de produtos e serviços.



## O papel do conselho de administração na promoção da agenda de conformidade

Assim como a gestão de riscos dos controles de exportação, um *compliance* efetivo em sanções exige o envolvimento ativo do conselho e da alta administração da empresa. Esses executivos – incluindo conselheiros, conforme necessário e apropriado – devem receber *briefings* regulares para garantir que tenham visibilidade dos riscos referentes a sanções e sejam, em última instância, passíveis de responsabilização.

Esses relatórios devem incluir indicadores-chave de riscos – os KRIs, na sigla em inglês, que podem ser, por exemplo, questões não-resolvidas e aumentos significativos dos alertas de sanções ou níveis de exposição – e os de desempenho – os KPIs, por exemplo, o cumprimento dos prazos definidos no Acordo de Nível de Serviço para revisão e liberação de alertas de sanções.

Empresas que contratam terceiros, como revendedores ou distribuidores, para vender produtos e serviços, devem adotar mecanismos para avaliar e compreender os programas de *compliance* em sanções desses fornecedores. Destaca-se que as autoridades regulatórias americanas, em particular, adotaram medidas coercitivas nos últimos anos contra pessoas dos EUA que enviaram produtos a distribuidores que posteriormente os venderam a jurisdições ou pessoas sancionadas.

Diante disso, as empresas devem testar os programas de *compliance* nesses terceiros de forma regular ou amostral, incluindo a revisão de sua modelagem e a análise de transações específicas. Essa estratégia reduz o risco regulatório de sanções tanto ao limitar a probabilidade de que a empresa esteja trabalhando com uma entidade que fornece bens ou serviços a pessoas ou jurisdições sancionadas, quanto ao restringir a exposição legal se o revendedor/redistribuidor estiver envolvido em alguma atividade.



## Insights de líderes

Confira algumas recomendações dos nossos entrevistados:



### Fique atento aos conflitos de interesse

As empresas devem estar atentas ao fato de que violações de *compliance* em controles de exportação podem começar com conflitos de interesse. Por exemplo, por meio do recebimento de benefícios pessoais de partes e/ou indivíduos de países sancionados.



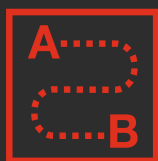
### Simule crises

Os conselhos de administração devem incentivar a liderança a simular crises focadas em cenários geopolíticos e, quando aplicável, no potencial de retaliação de outros países. É importante ainda aplicar as lições aprendidas aos programas corporativos de *compliance* em controles de exportação e sanções, assim como aos planos mais amplos para garantir a continuidade do negócio.



## Use os dados de vendas para identificar desvios

As corporações devem intensificar seus esforços para fazer uso dos dados de vendas e identificar possíveis casos de desvio de países sancionados por meio de terceiros em nações vizinhas. A identificação de produtos específicos que provavelmente têm maior valor para os países sancionados pode direcionar os esforços de análise de dados da empresa.



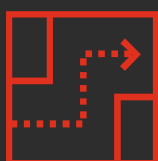
## Reconheça as limitações dos bloqueios geográficos

As companhias precisam estar cientes das limitações dos bloqueios geográficos – principalmente no que diz respeito a territórios sancionados, que existem dentro de países não sancionados, como a Crimeia, por exemplo – e dos esforços de indivíduos que usam redes privadas virtuais (VPNs) para burlar os sistemas de bloqueio geográfico de TI.



## Monitore as redes sociais

Empresas que fabricam produtos “físicos” e de marca devem monitorar as redes sociais em busca de imagens de seus produtos sendo usados em países sancionados.



## Não espere os governos para orientações corporativas específicas

As empresas não devem esperar que as autoridades governamentais forneçam orientações sobre as melhores práticas fora do contexto de uma investigação ou um inquérito regulatório. Assessoria jurídica externa e outros consultores, que frequentemente comparecem perante essas autoridades, devem estar familiarizados com as suas expectativas e podem ajudar.



## **O *compliance* em sanções depende de dados precisos em tempo hábil**

Testes de sistemas de triagem de sanções devem incluir a rastreabilidade e a qualidade dos dados, além da incorporação de listas e a performance geral do sistema. Se uma empresa não faz corretamente a triagem dos dados que tem de clientes e contrapartes – seja porque os dados não estão sendo alimentados corretamente no sistema ou porque ele não está utilizando listas de sanções atualizadas –, a probabilidade de fazer negócios com uma pessoa ou em uma jurisdição sancionada aumenta significativamente.

Na medida do possível, as companhias devem se certificar de que coletam todas as informações relevantes de clientes e contrapartes, os dados coletados são precisos e completos e que eles cheguem de maneira integral e rastreável aos sistemas de triagem de sanções. Além disso, elas devem assegurar que esses sistemas estejam atualizando corretamente, e em tempo hábil, as listas de sanções relevantes sempre que novas atualizações regulatórias aconteçam.



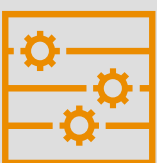


# O próximo salto

**Cadeias de suprimentos. Mercados.  
Concorrentes. Reguladores. Fiscalizações.  
Mudanças tecnológicas.**

**A complexidade não precisa ser sua adversária. Assuma riscos de forma inteligente e construa ainda mais confiança no *compliance*.**

Aborde estas questões com sua equipe antes de receber questionamentos do conselho de administração ou dos reguladores



**Seu conselho de administração está realmente comprometido com os desafios da empresa?**

Pode ser um desafio manter o conselho dedicado, especialmente após a conclusão de uma investigação relevante ou de uma questão regulatória. Também pode ser difícil agendar reuniões sobre questões novas, como a necessidade de mapear de forma abrangente a cadeia de suprimentos para lidar melhor com os riscos de trabalho análogo ao escravo, por exemplo. Diante desse quadro, vale a pena trabalhar com visualizações de dados atualizados sobre a gestão de riscos-chave.



## **Seu apetite ao risco está alinhado com o do CEO?**

Com um engajamento estratégico mais proativo e precoce com o seu CEO, as equipes dedicadas à gestão de riscos podem ajudar a solucionar eventuais desconexões com a alta liderança que, às vezes, podem existir. Confira as mais recentes [Pesquisa Global de Riscos](#) e [Pesquisa Global de Auditoria Interna](#) da PwC para mais informações.



## **Suas avaliações de riscos estão atrasadas?**

É hora de desenvolver um novo olhar sobre seus pressupostos de riscos geopolíticos, as novas obrigações regulatórias e as tendências de aplicação da lei entre fronteiras.



## **Será que uma visibilidade maior, dentro e fora da empresa, de casos passados de desvio de conduta de funcionários, e de seus esforços para responsabilizar pessoas e reduzir os riscos de problemas futuros, vai ajudar a frear comportamentos inadequados?**

Pesquisas breves e mais frequentes, junto com as equipes, sobre questões relativas à ética e ao *compliance* podem fornecer informações valiosas para a segunda e terceira linhas de defesa. Comparar sua estratégia de comunicação com a dos líderes de seu setor, mesmo de empresas de fora dele, é um exercício válido.



## **A capacidade de investigação à sua disposição vai esclarecer os fatos tão rápido quanto você precisa?**

O *upskilling* das competências de IA e *analytics* dos seus times, inclusive das ferramentas que eles utilizam, é um investimento sólido. Decisões críticas – seja sobre a veracidade das informações de um *whistleblower*, seja sobre os benefícios de uma autodenúncia – são feitas a partir da qualidade da análise de dados.



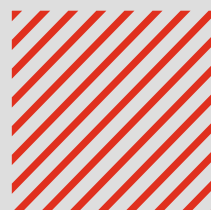
## Você está medindo suas perdas com fraudes de maneira adequada e chegando à raiz do problema?

Talvez seja necessária uma perspectiva mais ampla para ter mais confiança de que riscos semelhantes não estejam à espreita em outras áreas da empresa.



## Sua estratégia para gestão de riscos de terceiros está à altura do desafio?

Você pode ter acesso aos dados de que precisa atualmente, mas os dados **desejados** são outra história. A formação de equipes mais bem preparadas de *compliance*, auditoria interna e *procurement* poderia garantir as bases de dados e os recursos analíticos necessários para gerar insights de conformidade mais precisos.



# Contatos



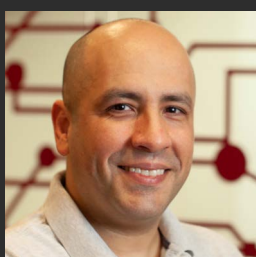
## Marcos Panassol

Sócio e líder de Risk Services – Forensics da PwC Brasil  
[marcos.panassol@pwc.com](mailto:marcos.panassol@pwc.com)



## Leonardo Lopes

Sócio de Risk Services – Forensics da PwC Brasil  
[leonardo.lopes@pwc.com](mailto:leonardo.lopes@pwc.com)



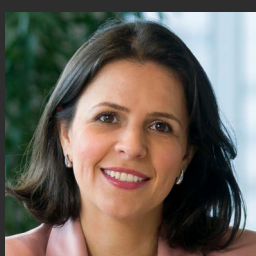
## Adriano Vargas

Sócio  
[adriano.s.vargas@pwc.com](mailto:adriano.s.vargas@pwc.com)



## João Castilho

Sócio  
[joao.castilho@pwc.com](mailto:joao.castilho@pwc.com)



## Elisa Mayor

Sócia  
[elisa.mayor@pwc.com](mailto:elisa.mayor@pwc.com)



Acesse o site:

[www.pwc.com.br](http://www.pwc.com.br)

Siga a PwC nas redes sociais



Neste documento, “PwC” refere-se à PricewaterhouseCoopers Brasil Ltda., firma membro do network da PricewaterhouseCoopers, ou conforme o contexto sugerir, ao próprio network. Cada firma membro da rede PwC constitui uma pessoa jurídica separada e independente. Para mais detalhes acerca do network PwC, acesse: [www.pwc.com/structure](http://www.pwc.com/structure)

© 2024 PricewaterhouseCoopers Brasil Ltda. Todos os direitos reservados.