

# Importante:

**As informações compartilhadas durante o evento são sigilosas e todo o material divulgado pela KPMG é de sua propriedade, estando proibido fotografar, gravar, armazenar, reproduzir ou compartilhar todo o conteúdo divulgado no evento, salvo prévio e expresso consentimento por escrito da KPMG.**



**Websérie**

# KPMG Risk Journey 2023

**Uma tripla ameaça nas Américas**



# Moderadores

Uma tripla ameaça nas Américas



**André Coutinho**

Sócio-líder de Advisory da KPMG no Brasil e na América do Sul



**Lucio Anacleto**

Sócio-líder de Financial Risk Management da KPMG no Brasil



**Diogo Dias**

Sócio-líder de Risk Advisory Solutions da KPMG no Brasil

Webserie

# KPMG Risk Journey 2023

## Programação



Uma tripla ameaça nas Américas



Auditoria interna, compliance e riscos ESG



Riscos de tecnologias emergentes e inovação



Maturidade das funções de GRC e Strategic Risk Management



Criptoativos, desafios na regulamentação e impactos ESG



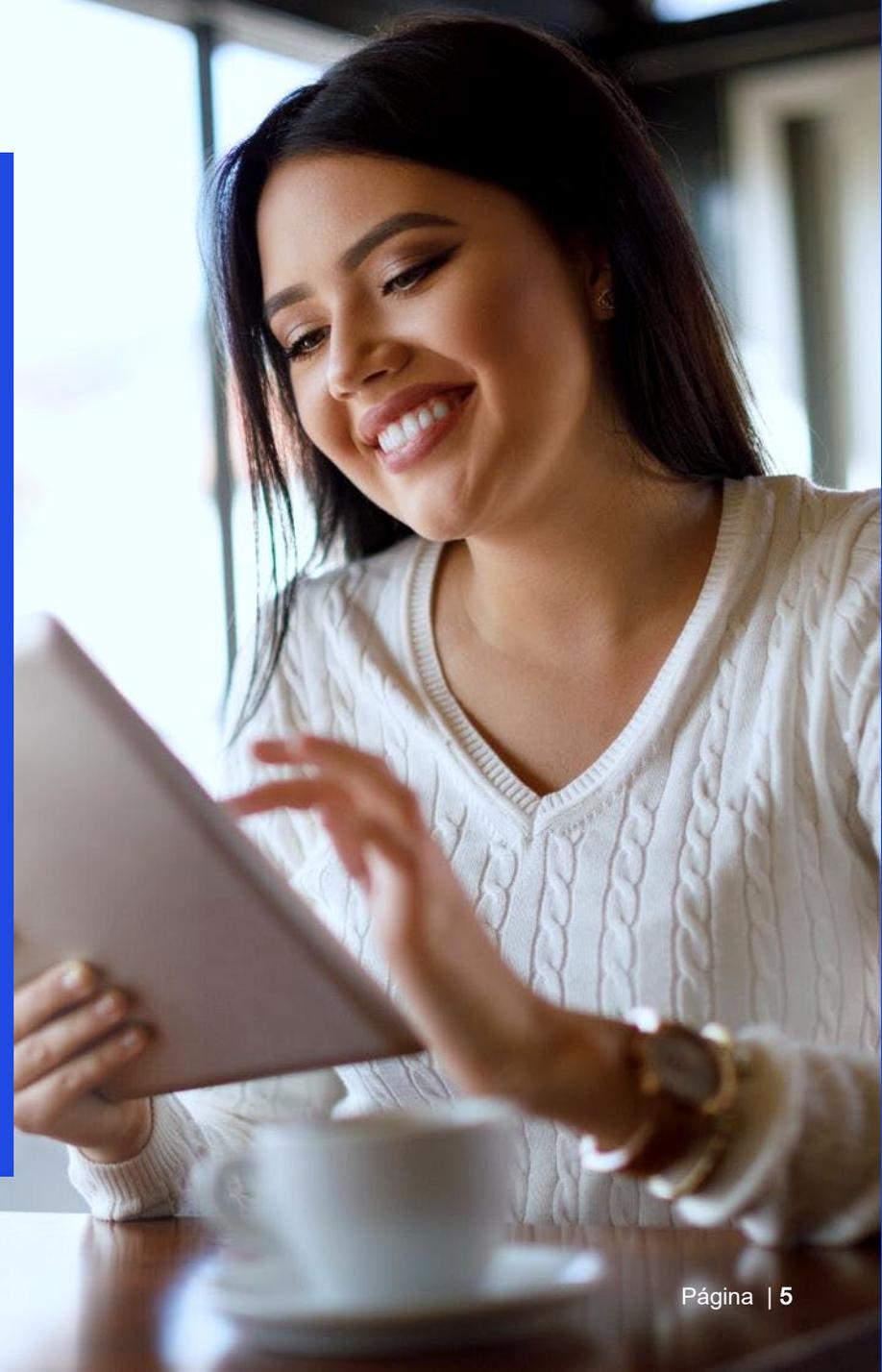
Tendências nas práticas de governança corporativa e de gerenciamento de riscos das empresas brasileiras em 2023



# Reveja os webcasts realizados pela KPMG:



Escaneie o QR code  
ou clique aqui



# Apresentação

Uma tripla ameaça nas Américas



**Emerson Melo**

Sócio-líder da prática de Forensic & Litigation da KPMG no Brasil e colíder na América do Sul



**Carolina Paulino**

Sócia de Forensic da KPMG no Brasil

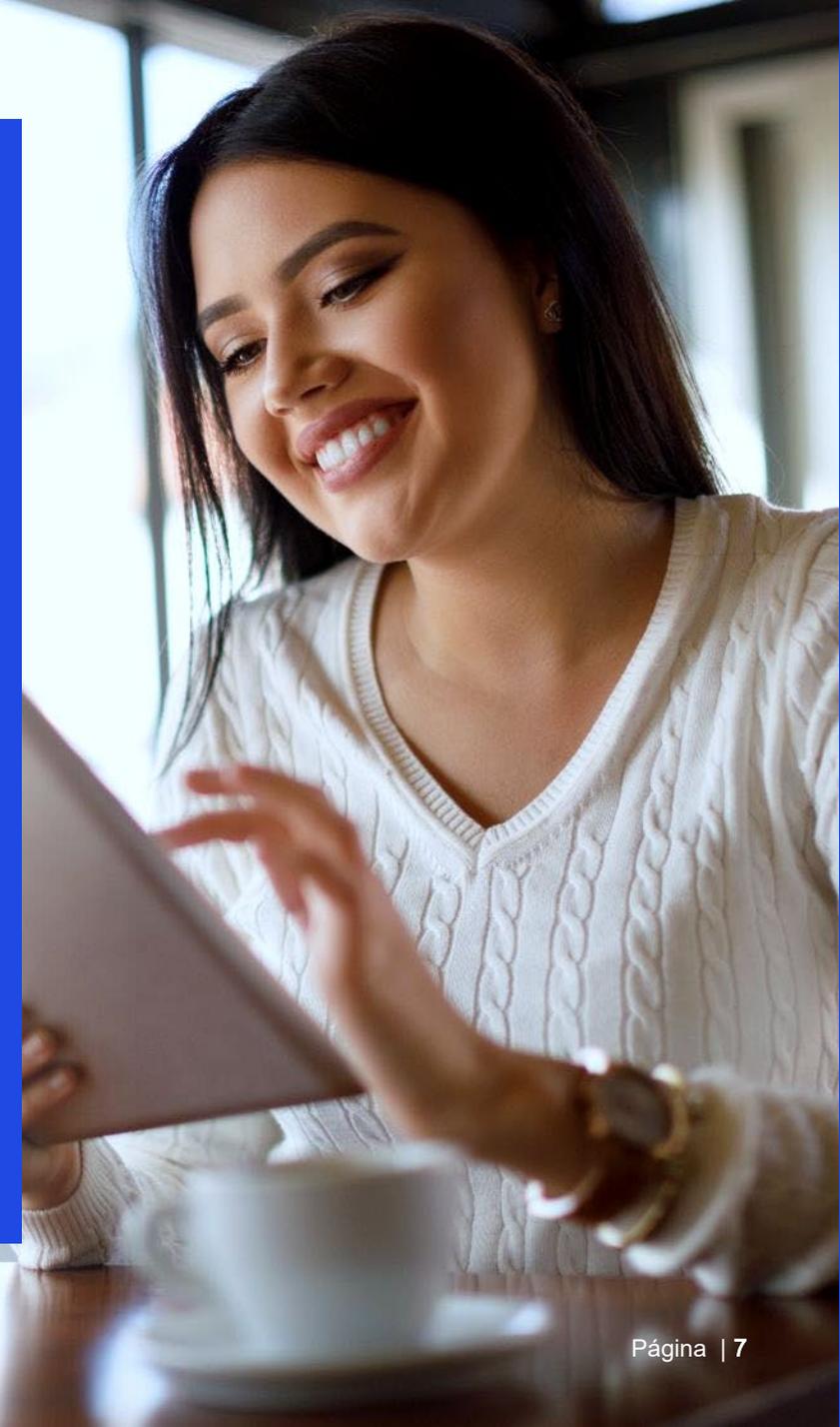


**Leandro Augusto**

Sócio-líder de Cyber Security da KPMG no Brasil

# Conteúdo

<b>Sobre a pesquisa</b>	<b>3</b>
<b>Sumário executivo</b>	<b>4</b>
<b>Os dados revelaram</b>	<b>5</b>
• Uma defesa unida contra a tripla ameaça	5
• Fraude, não conformidade e violações cibernéticas são a norma dispendiosa	6
• Diferenças de fraude regionais e por que o tamanho importa	7
– Visualização Rápida de Dados I: Um bando de fraudadores	11
• Como a pandemia mudou o quadro	15
– Visualização Rápida de Dados II: A conformidade é uma preocupação de todos os negócios	17
• Os níveis de ameaça estão crescendo	18
– Visualização Rápida de Dados III: Respostas lentas, preocupação insuficiente	20
• Controles mitigadores abrangentes permanecem raros	23
<b>Sua empresa está preparada para a tripla ameaça?</b>	<b>25</b>

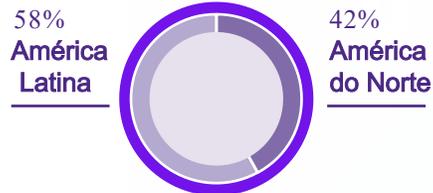
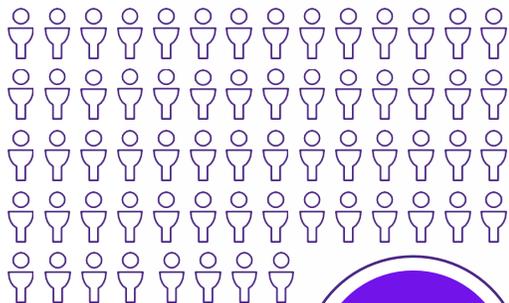


# Sobre a pesquisa



# Sobre a pesquisa

Este estudo baseia-se em uma pesquisa com 642 executivos:



Eles estão divididos uniformemente por sete setores:



A amostra é predominantemente composta de liderança sênior: **mais da metade dos entrevistados são membros do conselho, membros da administração ou chefes de departamentos.**

As suas empresas variam de tamanho:



# Sumário Executivo

A nossa pesquisa revela que as fraudes, as preocupações com conformidade e os ataques cibernéticos são comuns, aumentaram em gravidade e devem se tornar mais frequentes.



A maioria das empresas por toda a América do Norte e a América Latina relatou que sofreu perdas com fraudes, com violações de conformidade e/ou com ataques cibernéticos



Grandes empresas estão correndo mais riscos de fraude



Ameaças de fraude se diferenciam entre a América do Norte e a América Latina



A pandemia da COVID-19 piorou as coisas



As empresas têm a expectativa de que a fraude, o risco de conformidade e os ataques cibernéticos aumentem



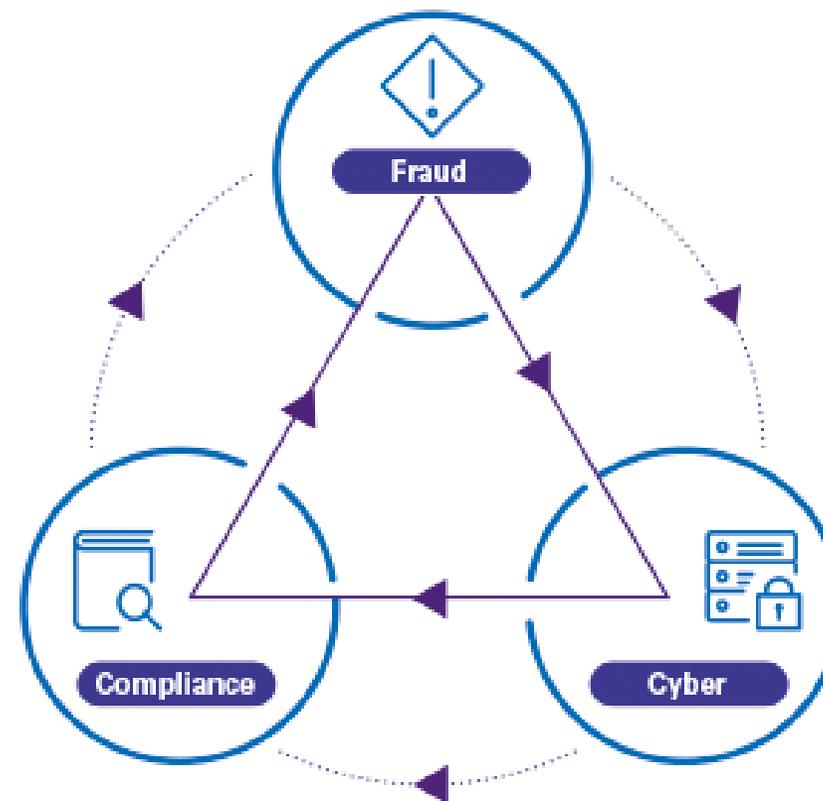
Não há muitas empresas lidando completamente bem com controles de fraude, com conformidade e com segurança cibernética

# Uma defesa unida contra uma tripla ameaça

As fraudes, os riscos de conformidade e os ataques cibernéticos estão disseminados, aumentando assim o perigo para as empresas localizadas em toda a América do Norte e a América Latina.

As empresas precisam mitigar o que a KPMG chama de "circuito fechado de ameaças", que compreende a tripla ameaça de fraude, de risco de conformidade e de uma série crescente de ameaças à segurança cibernética.

## Circuito fechado de ameaças da KPMG

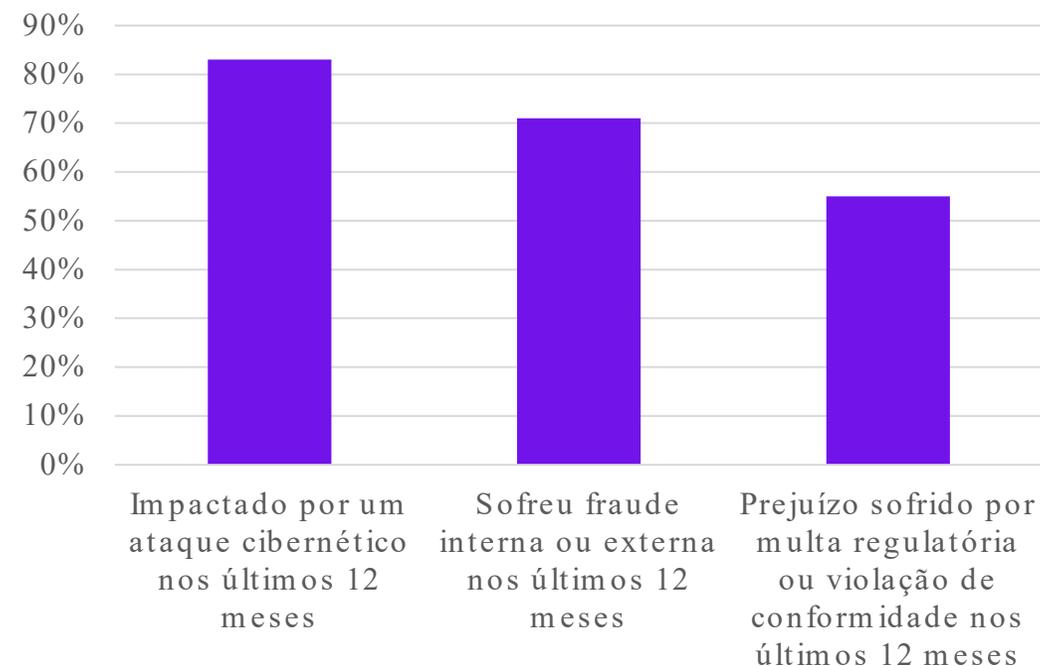


# A fraude, a não-conformidade e as violações cibernéticas são a norma dispendiosa

Dos riscos que examinamos, os respondentes indicaram que suas empresas são mais propensas a terem sofrido ataques cibernéticos.

- 83% dizem que as suas empresas sofreram pelo menos um ataque cibernético nos últimos 12 meses.
- 71% dos respondentes relatam que as suas empresas descobriram fraudes nos últimos 12 meses.
- 55% dos respondentes reconhecem que as suas empresas pagaram multas regulatórias ou sofreram financeiramente devido a violações de conformidade no último ano.

## A realidade da tripla ameaça



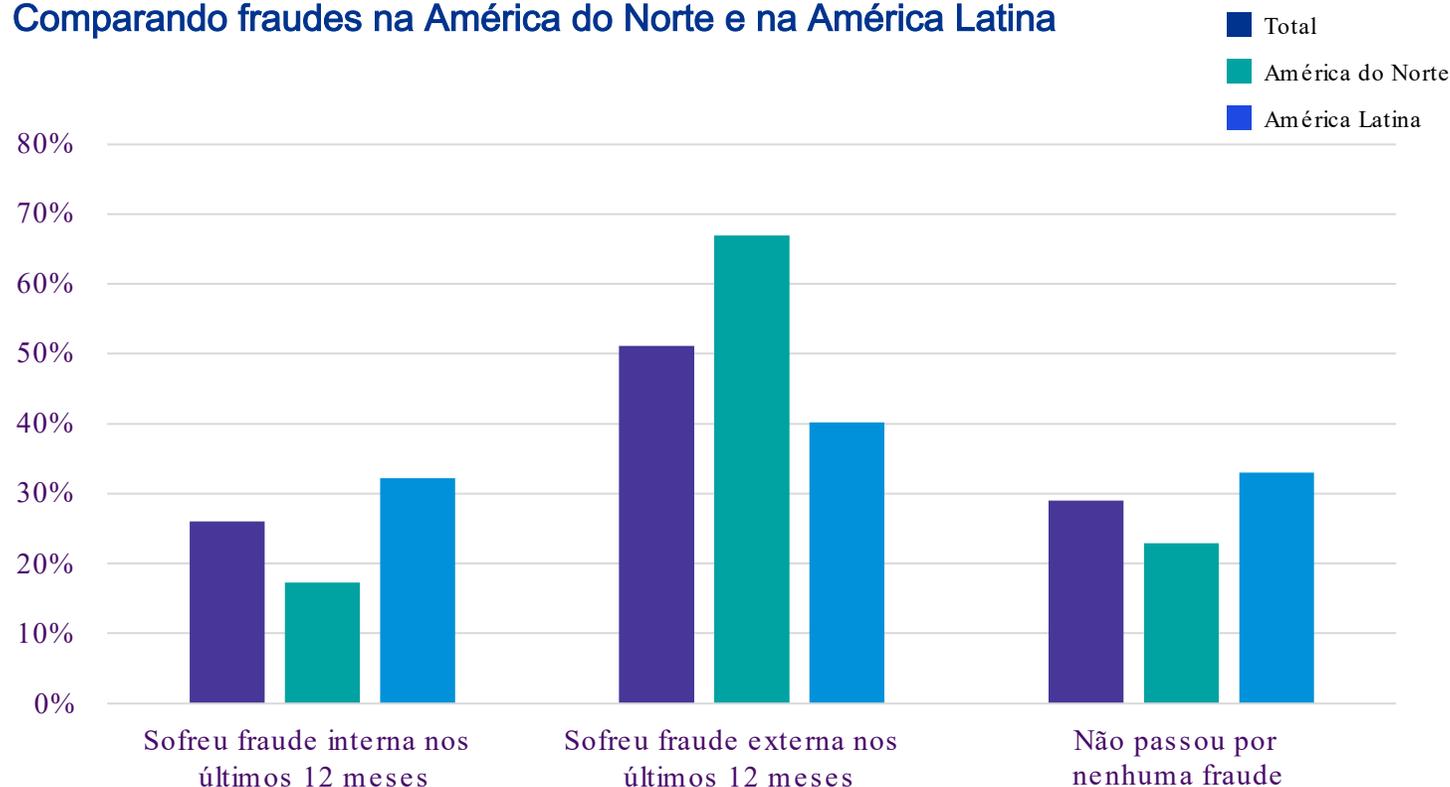
Os respondentes nos disseram que, a perda combinada média de fraudes, questões de conformidade e multas regulatórias foi de 1% de seus lucros.

# Diferenças de fraude regionais e porque o tamanho importa

A sua empresa já sofreu algum dos seguintes tipos de fraude nos últimos 12 meses?

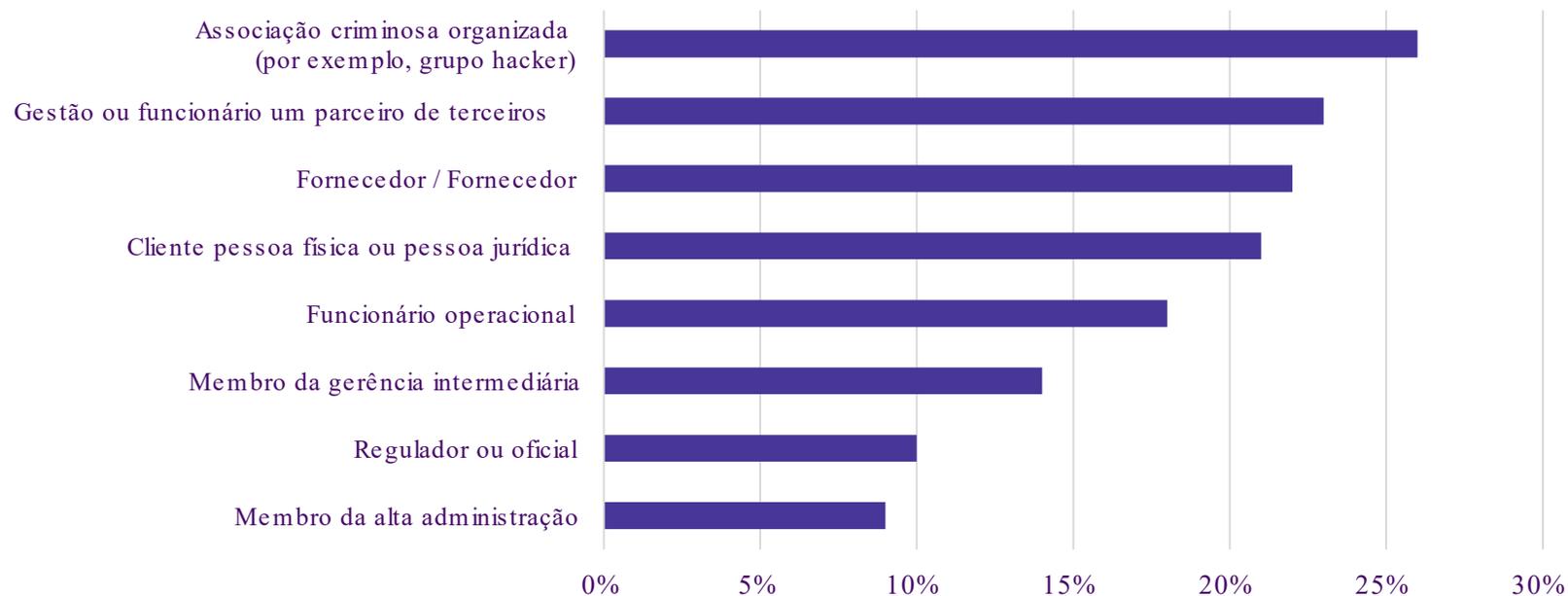
- Os respondentes indicam que a fraude é um problema mais disseminado para as empresas norte-americanas.
- O ambiente de risco difere entre as regiões.
  - As empresas latino-americanas têm quase o dobro de chances de suas pares norte-americanas de denunciarem envolvimento interno em fraudes.
- Na América do Norte, a fraude externa é um problema muito maior.

Comparando fraudes na América do Norte e na América Latina



# Perfil do fraudador

Qual dos seguintes tipos de indivíduos é conhecido por estar envolvido em fraude ou conduta ilícita (seja só em conluio) em sua empresa durante os últimos 12 meses?



- Entre os respondentes norte-americanos, 43% citam ocorrências de fraudes cometidas por uma organização criminosa externa (como um grupo *hacker*), em comparação com apenas 14% na América Latina – dados consistentes com os níveis mais altos de crimes cibernéticos na América do Norte.
- Por outro lado, 36% dos respondentes latino-americanos dizem que suas empresas sofreram fraudes internas, em comparação com apenas 23 % dos respondentes norte-americanos.

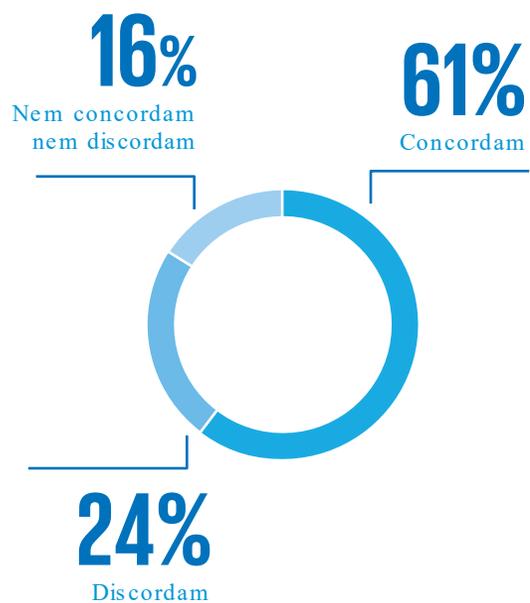


# Trabalho remoto e o seu impacto no ambiente de risco

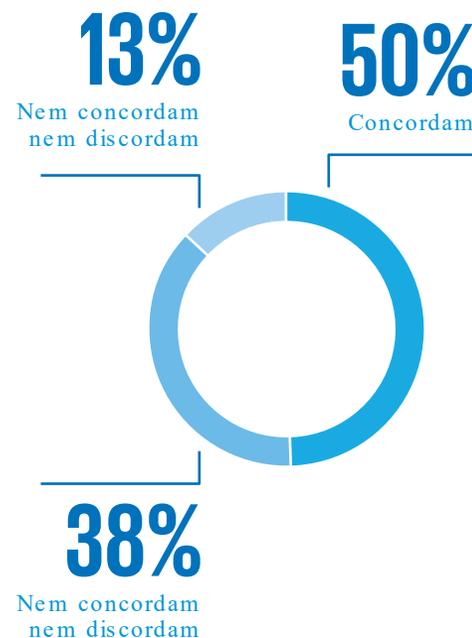
No geral, **86%** dos respondentes dizem que o trabalho remoto afetou negativamente pelo menos um elemento de programas de conformidade, de segurança cibernética e de prevenção de fraude em suas empresas.

Metade dos respondentes nos diz que o trabalho em regime de home office impactou negativamente a capacidade de suas empresas de responder às fraudes

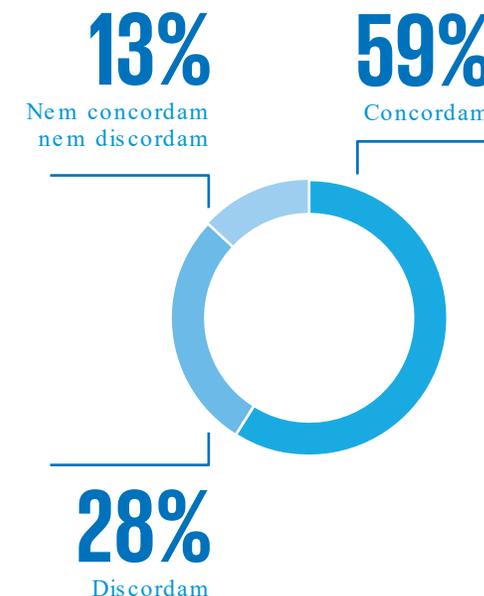
A mudança para o trabalho remoto aumentou o nosso risco de fraude, devido a uma capacidade reduzida de monitorar e controlar comportamentos fraudulentos



Trabalhar em regime de *home office* impactou negativamente a nossa capacidade de responder adequadamente à fraude em nossos negócios



Os controles antifraude que tínhamos em vigor pré - pandemia não foram efetivamente atualizados para refletir a nova realidade de trabalho



# Trabalho remoto e o seu impacto no ambiente de risco (cont.)

7% dos entrevistados afirmam que suas empresas tiveram que desenvolver novas estratégias durante a pandemia para acompanhar as demandas de conformidade em evolução

19% relatam que o trabalho remoto tornou mais difícil medir o cumprimento dos controles financeiros, antilavagem de dinheiro e anti-suborno.

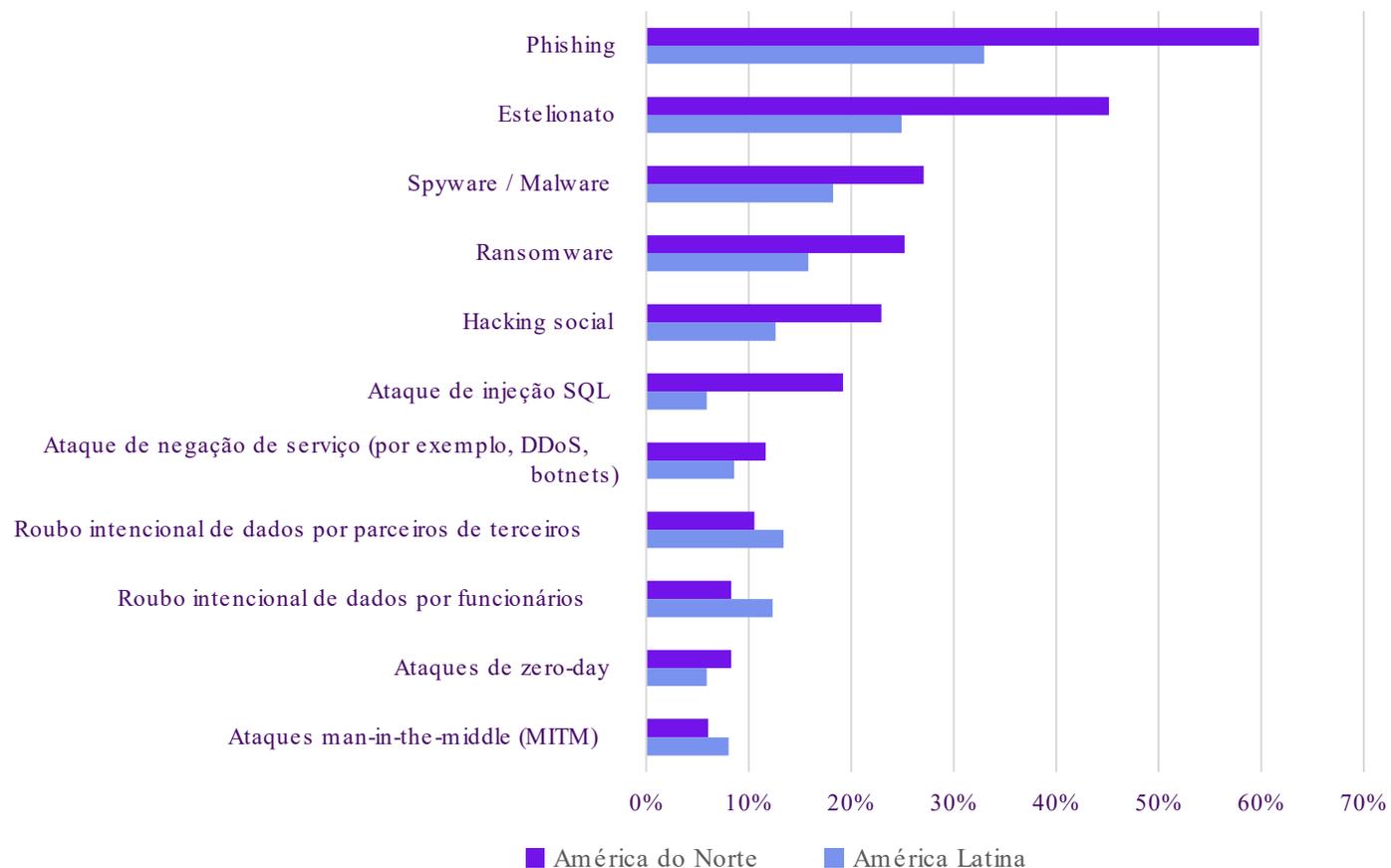
Quais foram impactados negativamente pelo aumento de funcionários trabalhando em regime de *home office* no último ano?



# Trabalho remoto e o seu impacto no ambiente de risco (cont.)

- O crime cibernético aumentou em volume durante a pandemia e não diminuiu.
- Como mostra o gráfico, as empresas pesquisadas para este relatório estão relatando aumentos na frequência de vários tipos de ataque.
- No geral, **79%** dos respondentes observaram crescimento em pelo menos um dos tipos de ataque cobertos pela pesquisa.
- **69%** dos respondentes dizem que o trabalho remoto tem sido um grande desafio de segurança cibernética para seus negócios

Em relação a qual dos seguintes itens você viu um aumento no último ano?



# Os níveis de risco estão subindo...

**69%** dos respondentes esperam um aumento do risco em pelo menos uma fraude externa ou interna no próximo ano.

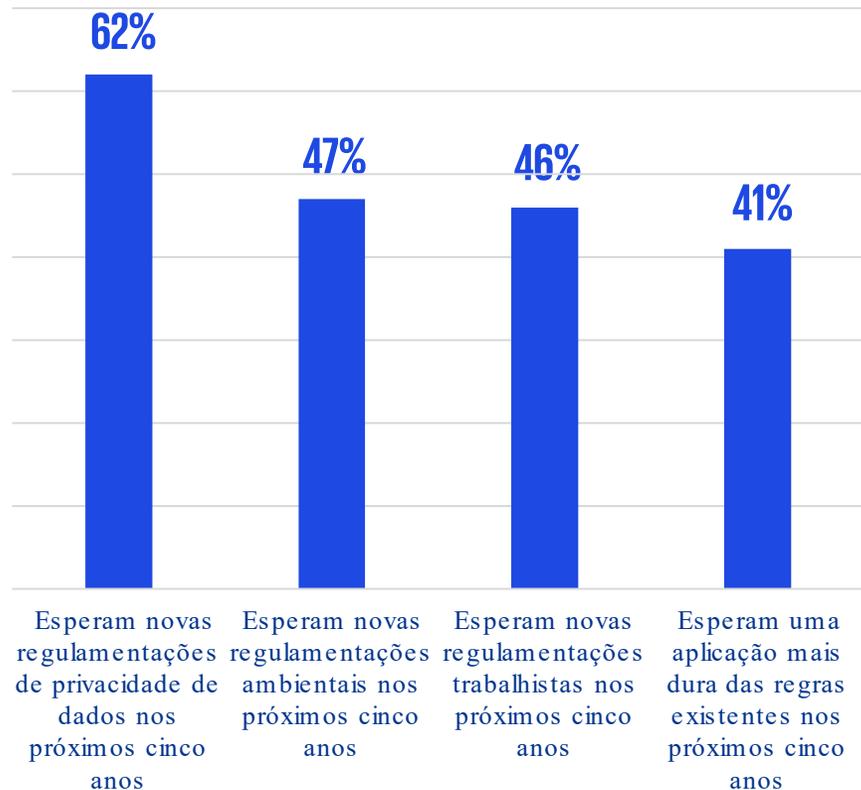
**29%** projetam um aumento em ambas.

As preocupações com o aumento do crime cibernético são generalizadas

**77%** dizem que o risco de segurança cibernética aumentará nos próximos 12 meses

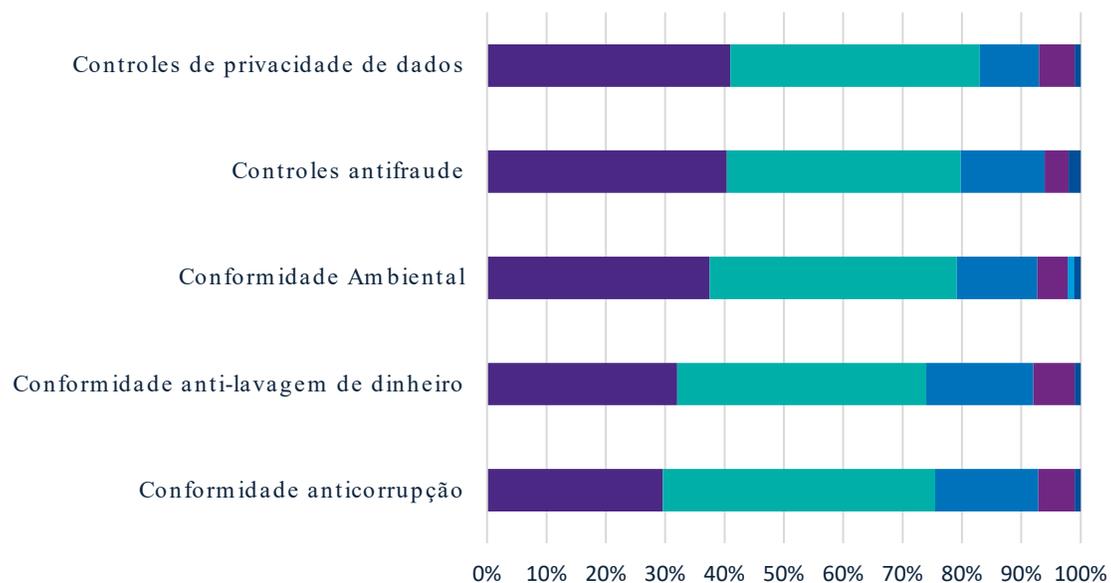
**7%** Apenas 7% vislumbram um declínio.

## Novos requisitos e aplicação mais dura da regulamentação no futuro

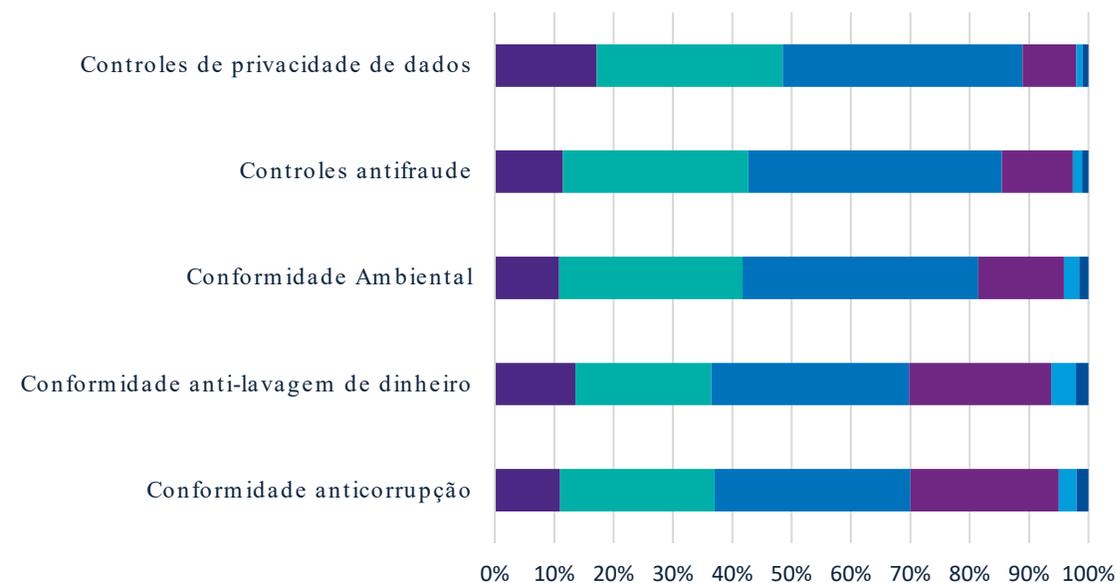


# Tratando o Circuito Fechado de Ameaças

Quão maduros são os programas da sua empresa nas seguintes áreas? Respostas norte-americanas



Quão maduros são os programas da sua empresa nas seguintes áreas? Respostas latino-americanas



Modelo de melhores práticas internacionais

Compara-se bem com os pares domésticos/fica aquém das melhores práticas internacionais

Atende às nossas obrigações legais domésticas

Um programa muito básico

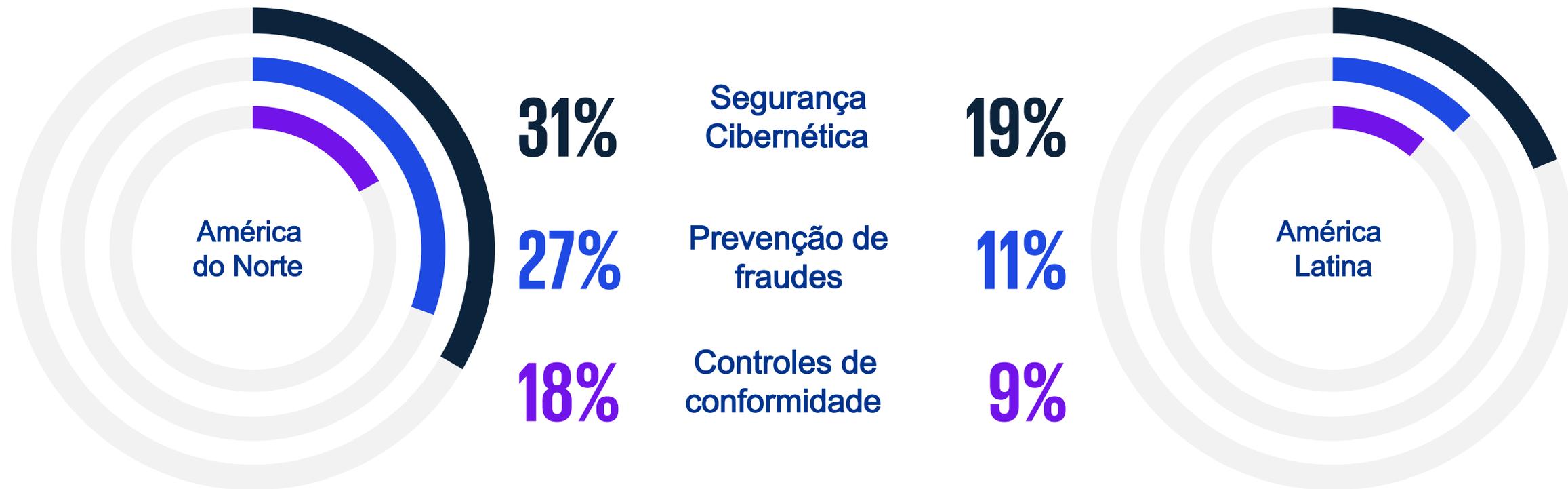
Falta qualquer programa

Não sei

Apenas 18% dos respondentes disseram que suas empresas modelam as melhores práticas internacionais em conformidade com medidas anticorrupção

# Tratando o Circuito Fechado de Ameaças (cont.)

Empresas que atendem ao padrão de mais da metade<sup>1</sup>



<sup>1</sup> A proporção de **respondentes que** classifica os esforços de suas empresas como **sendo** excelentes para pelo menos metade dos controles ou medidas listados em cada parte do **circuito fechado** de ameaças – seis ou mais de 11 áreas para prevenção de fraudes, quatro ou mais para conformidade e três ou mais para segurança cibernética.

# A sua empresa está preparada para a tripla ameaça?

Fraudes, não-conformidade e ataques cibernéticos representam uma ameaça cara para as empresas em todas as Américas, situação essa que foi exacerbada pela pandemia.

A maioria das empresas tem algumas defesas em vigor, mas a excelência abrangente é algo raro.

## As cinco coisas mais importantes a considerar



Definir o tom certo da alta direção



Realizar uma revisão de risco



Comunicar-se efetivamente



Fortalecer a detecção



Criar uma cultura de aplicação de regras e de responsabilização



# Q&A



# Próximos webcasts



Acesse a agenda completa e inscreva-se!

**31/01**

Das 17:30 às 19:00

**Uma tripla ameaça nas Américas**

*(Emerson Melo | Carolina Paulino | Leandro Augusto )*

**02/02**

Das 17:30 às 19:00

**Auditoria interna, compliance e riscos ESG**

*(Nelmara Arbex | Fernando Lage)*

**07/02**

Das 17:30 às 19:00

**Riscos de tecnologias emergentes e inovação**

*(Leandro Augusto | Thammy Marcato)*

**09/02**

Das 17:30 às 19:00

**Maturidade das funções de GRC e Strategic Risk Management**

*(Thais Mendonça | Julio Carvalho)*

**14/02**

Das 17:30 às 19:00

**Criptoativos , desafios na regulamentação e impactos ESG**

*(KPMG: Fabio Lacerda | Maria Eugenia Buosi | CVM: Antônio Carlos Berwanger )*

**16/02**

Das 17:30 às 19:00

**Tendências nas práticas de governança corporativa e de gerenciamento de riscos das empresas brasileiras em 2023**

*(Sidney Ito | Fernanda Santanna)*



# Descubra a KBS



Acesse o site



# Accounting *Journey'23*

O seu treinamento de contabilidade.



Acesse o site



# Fale com nosso time



## André Coutinho

Sócio-líder de Advisory da KPMG no Brasil e na América do Sul  
[acoutinho@kpmg.com.br](mailto:acoutinho@kpmg.com.br)



## Lucio Anacleto

Sócio-líder de Financial Risk Management da KPMG no Brasil  
[lanacleto@kpmg.com.br](mailto:lanacleto@kpmg.com.br)



## Diogo Dias

Sócio-líder de Risk Advisory Solutions da KPMG no Brasil  
[dsdias@kpmg.com.br](mailto:dsdias@kpmg.com.br)



## Emerson Melo

Sócio-líder da prática de Forensic & Litigation da KPMG no Brasil e colíder na América do Sul  
[emersonmelo@kpmg.com.br](mailto:emersonmelo@kpmg.com.br)



## Carolina Paulino

Sócia de Forensic da KPMG no Brasil  
[cpaulino@kpmg.com.br](mailto:cpaulino@kpmg.com.br)



## Leandro Augusto

Sócio-líder de Cyber Security da KPMG no Brasil  
[lantonio@kpmg.com.br](mailto:lantonio@kpmg.com.br)

