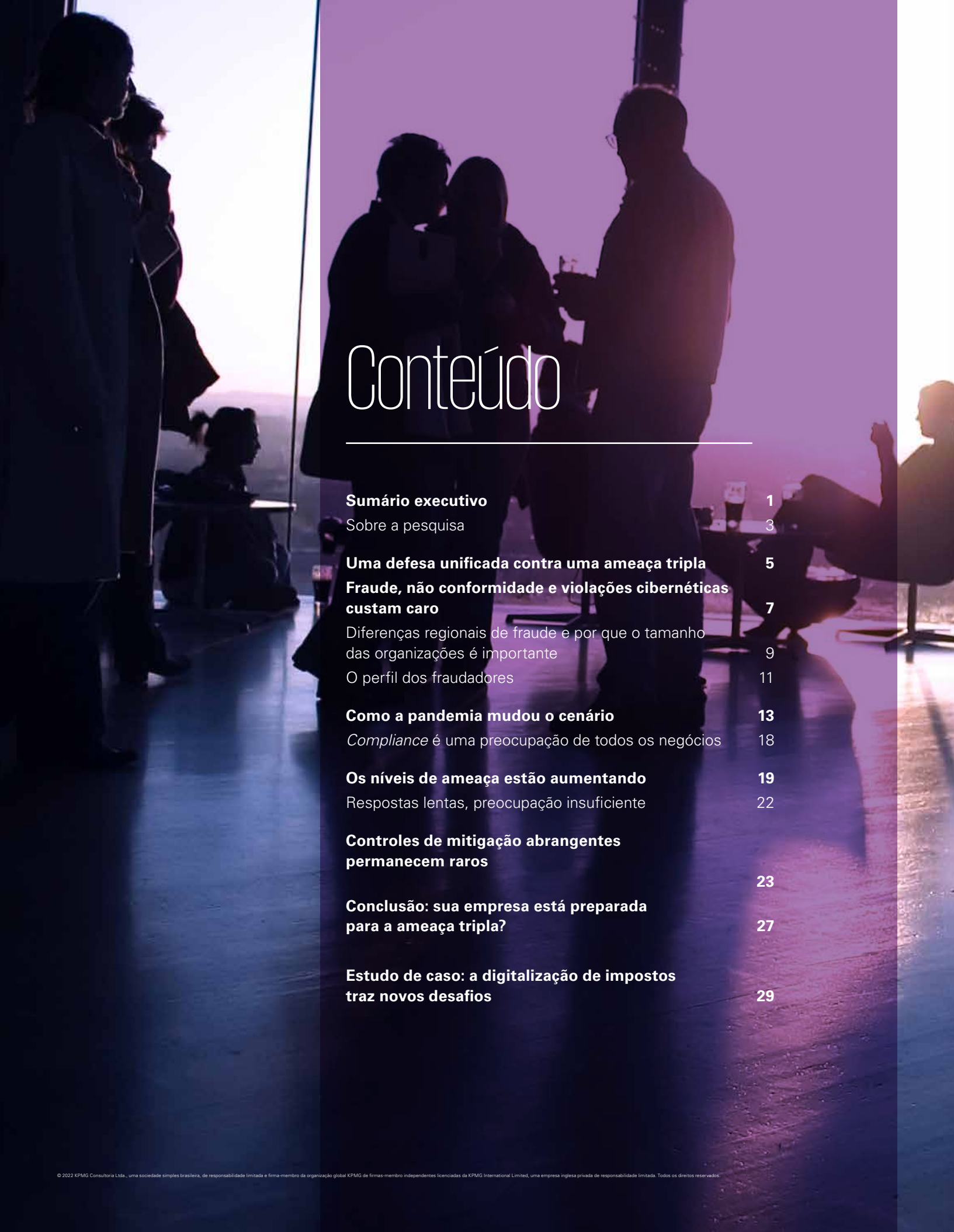
KPMG

Uma Ameaça Tripla nas Américas

KPMG 2022 Fraud Outlook

Janeiro de 2022

kpmg.com.br



Conteúdo

Sumário executivo

A KPMG tem a satisfação de apresentar suas perspectivas para 2022 sobre fraudes, ataques cibernéticos e questões de conformidade na região das Américas.

A pesquisa, realizada com mais de 600 executivos de diferentes setores, evidencia os efeitos provocados pela pandemia de covid-19 nessas três ameaças interconectadas. A análise aponta que a fraude, as questões de conformidade e os ataques cibernéticos tornaram-se mais graves e estão cada vez mais frequentes.

Neste relatório, a referência à KPMG significa uma colaboração entre as firmas-membro da KPMG na América Latina, nos Estados Unidos e no Canadá, para produzir as percepções do estudo.

As empresas nas Américas estão conseguindo se defender dessa tripla ameaça? Esta pesquisa sugere que muitas têm defesas locais limitadas e que a mudança para o trabalho híbrido ou remoto está tornando os controles existentes menos eficazes.

A maioria das empresas na América do Norte e na América Latina relatou ter sofrido perdas com fraudes, violações de conformidade e/ou ataques cibernéticos

Um percentual de 83% dos entrevistados afirmou que suas organizações tiveram pelo menos um ataque cibernético nos últimos 12 meses; 71% salientaram que suas empresas sofreram fraude; e mais de 50% disseram que suas organizações pagaram multas regulatórias ou tiveram impactos financeiros devido a riscos de conformidade não mitigados.

Tudo isso resulta em custos significativos. Os entrevistados relataram ainda uma perda média de 1% dos lucros com fraudes e multas relacionadas à conformidade em 2020.

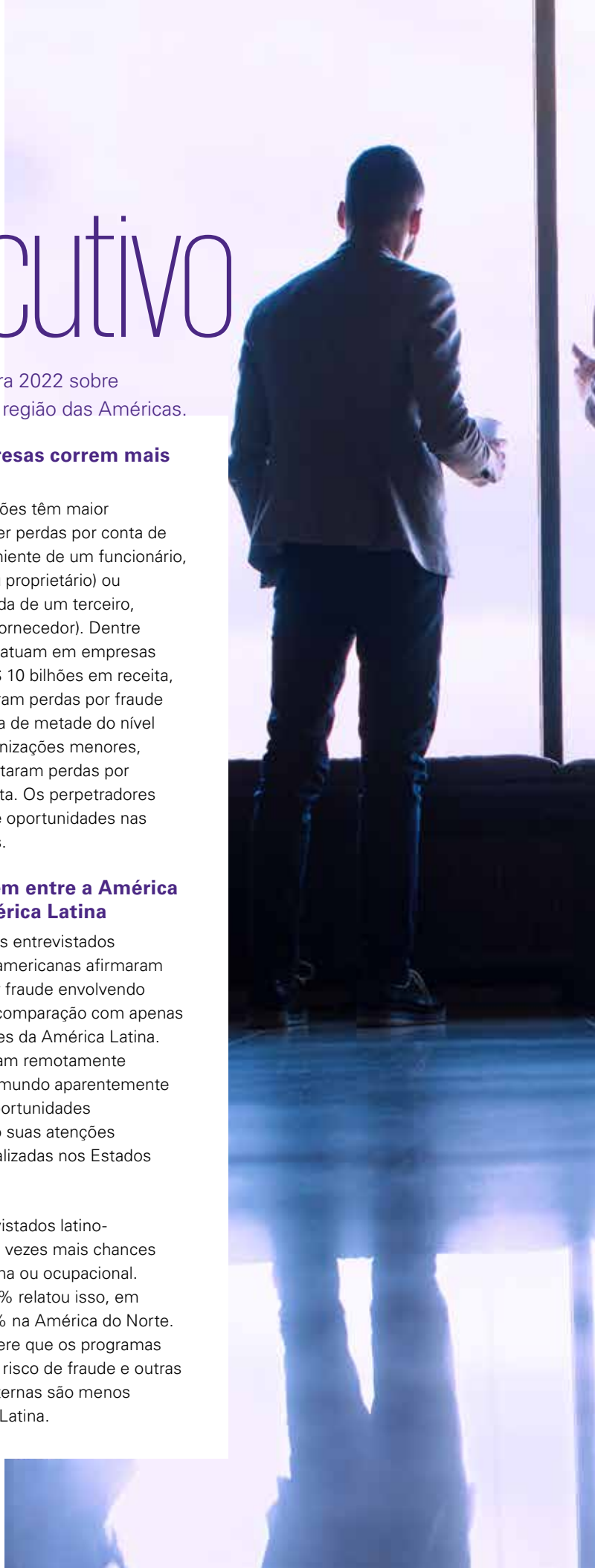
As grandes empresas correm mais risco de fraude

As grandes organizações têm maior probabilidade de sofrer perdas por conta de fraude interna (proveniente de um funcionário, gerente, executivo ou proprietário) ou fraude externa (advinda de um terceiro, como um cliente ou fornecedor). Dentre os entrevistados que atuam em empresas com pelo menos US$ 10 bilhões em receita, apenas 15% não tiveram perdas por fraude em 2020. Isso é cerca de metade do nível observado entre organizações menores, em que 29% não relataram perdas por esse tipo de ação ilícita. Os perpetradores enxergam claramente oportunidades nas maiores organizações.

As fraudes diferem entre a América do Norte e a América Latina

Na pesquisa, 76% dos entrevistados das empresas norte-americanas afirmaram ter sofrido perdas por fraude envolvendo partes externas, em comparação com apenas 42% dos respondentes da América Latina. Criminosos que operam remotamente de qualquer lugar do mundo aparentemente veem as melhores oportunidades e estão concentrando suas atenções nas organizações localizadas nos Estados Unidos e no Canadá.

No entanto, os entrevistados latino-americanos têm duas vezes mais chances de sofrer fraude interna ou ocupacional. Um percentual de 49% relatou isso, em comparação com 17% na América do Norte. Essa descoberta sugere que os programas de gerenciamento de risco de fraude e outras defesas antifraude internas são menos robustos na América Latina.



A pandemia de covid-19 piorou as coisas

Aproximadamente nove em cada dez entrevistados disseram que trabalhar em casa afetou negativamente a eficácia das medidas de prevenção de fraude, mitigação de risco de conformidade ou segurança cibernética de suas empresas. Para alguns, atrapalhou os três.

O trabalho remoto reduziu a capacidade das empresas de monitorar o comportamento, o que aumenta o risco de fraude, e também criou grandes fragilidades de segurança cibernética por conta de um acesso mais aberto aos sistemas. O aumento do trabalho híbrido e o crescimento expressivo do crime cibernético – ambos reflexos da crise – indicam que grande parte dos entrevistados precisará aprimorar seus processos operacionais mesmo após o controle da covid-19.

A fraude, o risco de conformidade e os ataques cibernéticos devem aumentar

A maioria dos entrevistados espera que a fraude, o risco de conformidade e/ou as ameaças cibernéticas se intensifiquem em 2022. Dois terços esperam que as fraudes externas ou internas aumentem. Já 77% dizem que os riscos cibernéticos devem crescer.

Seis em cada dez esperam que o risco de conformidade cresça, em parte graças à expectativa de maior regulamentação. Quase todos os respondentes esperam por mais requisitos regulatórios ou de conformidade relativos à privacidade de dados, às relações de trabalho e ao meio ambiente nos próximos cinco anos. Já um percentual de 41% também aguarda uma fiscalização regulatória mais eficaz.

Poucas empresas estão totalmente no topo do controle de fraude, conformidade e segurança cibernética

Poucos entrevistados disseram que suas empresas refletem as melhores práticas internacionais de conformidade anticorrupção (18%), conformidade ambiental (21%), conformidade contra lavagem de dinheiro (22%), controles antifraude (23%) e controles de privacidade de dados (27%).

Sobre como as empresas atuam em uma série de medidas relacionadas ao controle de fraude, conformidade e segurança cibernética, a pesquisa aponta que apenas uma pequena proporção dos executivos relata fortes controles em pelo menos metade das medidas relevantes (intituladas de "meio ou mais padrão". Apenas 24% dos participantes disseram que suas organizações são fortes na metade ou mais das proteções de segurança cibernética relevantes, 17% em controles para prevenir e detectar fraudes e 13% no tratamento de riscos de conformidade. Apenas 4% dizem que suas empresas se destacam em todas as três áreas.

As prioridades das empresas

Fraude:

Nunca descarte a possibilidade de um trabalho interno. Um número significativo de 31% dos entrevistados disse que suas empresas sofreram com fraudes perpetradas por um *insider* em 2020.

Conformidade:

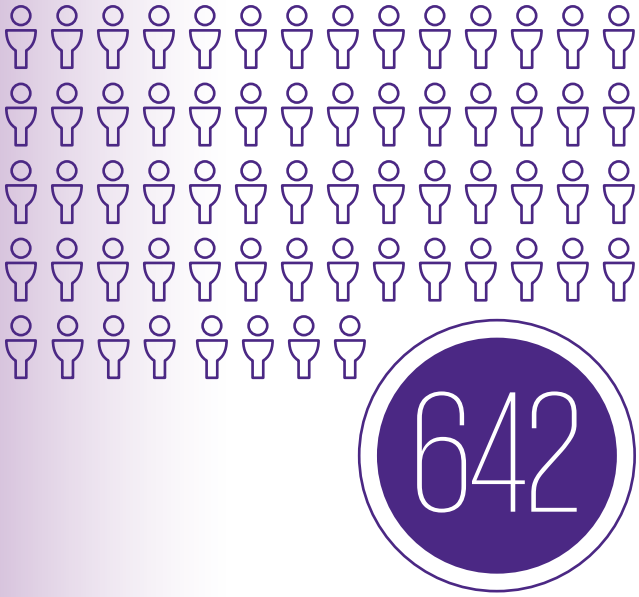
É um problema de reputação. Mais entrevistados dizem que as considerações de reputação fazem com que seus líderes prestem atenção à conformidade do que dizem o mesmo em relação às multas e à fiscalização.

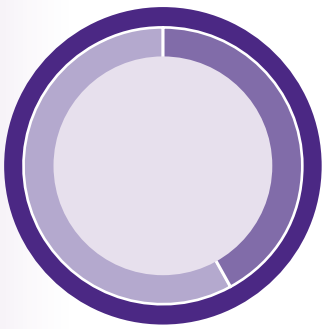
Segurança cibernética:

devagar e sempre não vencerá a corrida pela segurança cibernética. Os respondentes disseram que leva cerca de um mês, em média, para um ataque cibernético ser totalmente contido, e a maioria parece satisfeita com tal desempenho nessa área. Isso indica que há uma falta de urgência acerca de como as empresas estão respondendo à ameaça de ataques cibernéticos.

Sobre a pesquisa

Este estudo é baseado em uma pesquisa com 642 executivos:





Eles estão divididos de maneira quase uniforme em sete setores:

A pesquisa é predominantemente composta por lideranças seniores: **mais da metade dos entrevistados são membros de conselhos, do alto escalão ou líderes de departamentos.**

Sobre a pesquisa

As empresas possuem receitas de:

têm receitas anuais de **menos de US$ 1 bilhão**

têm receitas anuais entre **US$ 1 bilhão e US$ 10 bilhões**

têm receitas anuais de **mais de US$ 10 bilhões**

Também foram entrevistados seis líderes corporativos seniores e especialistas de toda a região:

José Calderón
Diretor de auditoria global do Grupo Bimbo

Larissa Galimberti
Sócia da Pinheiro Neto Advogados

Carlos García Jiménez
Diretor regional de ética e *Compliance* LATAM da Uber

Ariel Nowersztern
Especialista em cibersegurança do Banco Interamericano de Desenvolvimento (BID)

Beth Rose
Diretora de *Compliance*, ética e integridade da Ford Motor Company

Pascal Saint-Amans
Diretor do Centro de Política e Administração Tributária da Organização para a Cooperação e Desenvolvimento Econômico (OCDE)

Gostaríamos de agradecê-los por compartilhar suas ideias.

Alguns gráficos podem não somar 100% devido ao arredondamento.

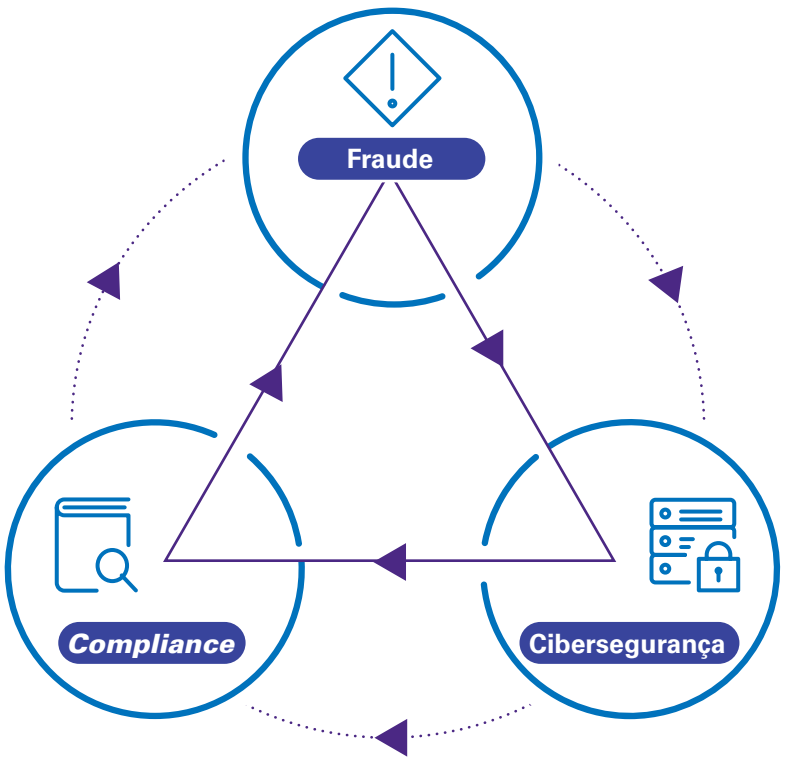
Uma defesa unificada contra uma ameaça tripla

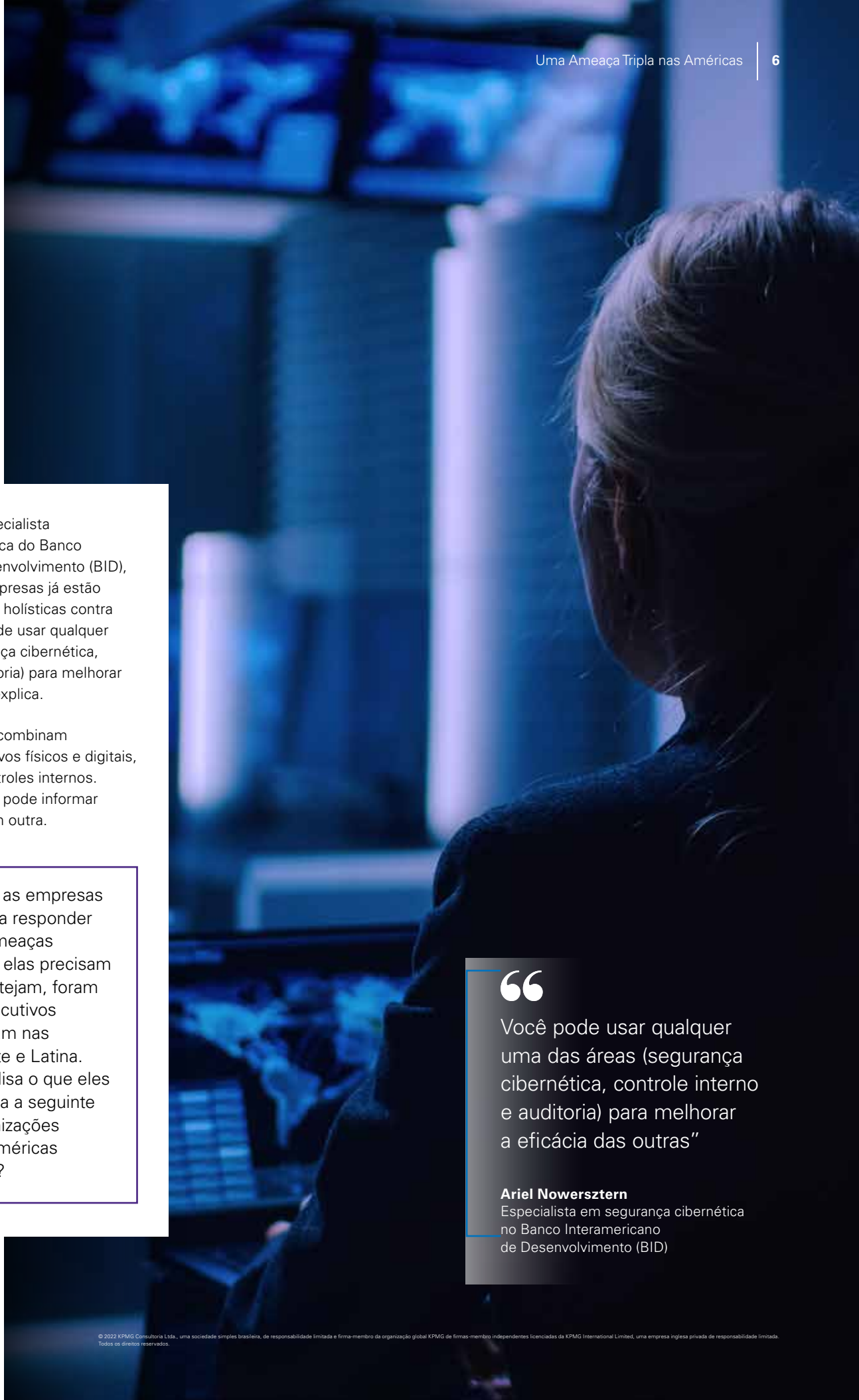
Fraude, riscos de conformidade e ataques cibernéticos são ameaças generalizadas e crescentes para empresas na América do Norte e América Latina.

E esses riscos estão interligados. Considere, por exemplo, o caso de um profissional que rouba dados de clientes enquanto trabalha em casa – isso levanta todas as três ameaças simultaneamente e as empresas precisam tratá-las como uma só.

As organizações também precisam reduzir o que a KPMG chama de "ciclo de ameaças", que compreende a tripla ameaça de fraude, o risco de conformidade e uma gama crescente de riscos à segurança cibernética. A defesa contra esse ciclo exige esforço coletivo e interconectado. As empresas precisam examinar o impacto criado por esses aspectos em conjunto – e não apenas os riscos isolados.

O ciclo da ameaça KPMG





Ariel Nowersztern, especialista em segurança cibernética do Banco Interamericano de Desenvolvimento (BID), afirma que algumas empresas já estão desenvolvendo defesas holísticas contra esses riscos. "Você pode usar qualquer uma das áreas (segurança cibernética, controle interno e auditoria) para melhorar a eficácia das outras", explica.

Algumas organizações combinam o monitoramento de ativos físicos e digitais, antifraude e outros controles internos. Um alerta em uma área pode informar que algo está errado em outra.

Para descobrir se as empresas estão prontas para responder a esse ciclo de ameaças e quanto trabalho elas precisam fazer caso não estejam, foram entrevistados executivos seniores que atuam nas Américas do Norte e Latina. Este relatório analisa o que eles disseram e levanta a seguinte questão: as organizações localizadas nas Américas estão preparadas?

> "Você pode usar qualquer uma das áreas (segurança cibernética, controle interno e auditoria) para melhorar a eficácia das outras"
>
> **Ariel Nowersztern**
> Especialista em segurança cibernética no Banco Interamericano de Desenvolvimento (BID)

Fraude, não conformidade e violações cibernéticas custam caro

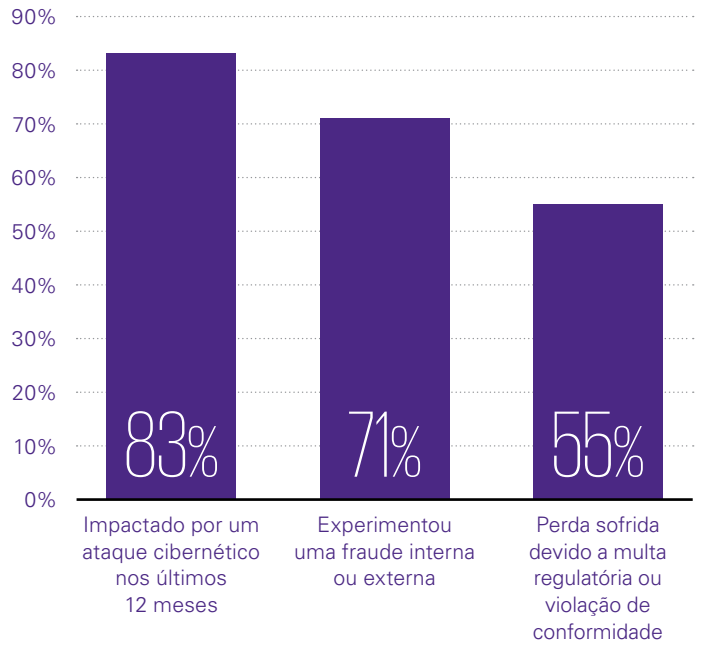
> Agora é o caso de *quando*, e não *se*, um ataque cibernético acontacerá."
>
> **Larissa Galimberti**
> Sócia do Pinheiro Neto Advogados

"Agora é o caso de *quando*, e não *se*, um ataque cibernético acontecerá." Explica Larissa Galimberti, sócia especializada em Tecnologia do escritório de advocacia Pinheiro Neto Advogados. Os participantes da pesquisa concordam que, para as empresas nas Américas, fraude e não conformidade são inevitáveis.

Dos riscos analisados, os entrevistados indicaram que suas empresas têm maior probabilidade de sofrer ataques cibernéticos. No geral, 83% dos entrevistados nas Américas salientaram que suas empresas sofreram pelo menos um ataque cibernético nos últimos 12 meses. A pesquisa pediu aos entrevistados que comentassem apenas sobre os incidentes que tiveram um impacto comercial perceptível, portanto, o número geral de ataques cibernéticos provavelmente será maior do que o relatado.

A fraude também é citada com frequência preocupante: 71% dos entrevistados relataram que suas empresas descobriram fraudes nos últimos 12 meses. Isso sobe para 85% das empresas com mais de US$ 10 bilhões em receitas anuais. Enquanto isso, 55% dos executivos reconhecem que pagaram multas regulatórias ou sofreram financeiramente devido a violações de conformidade em 2020. Casos não descobertos de fraude e não conformidade significam que esses números provavelmente não são representativos e o problema subjacente pode ser ainda maior.

A realidade de uma ameaça tripla



Entre as empresas participantes, a perda média combinada entre fraude, questões de conformidade e multas regulatórias representaram 1% de seus lucros. Além disso, 58% dos entrevistados disseram que suas organizações sofreram perdas econômicas diretas com um ataque cibernético. Enquanto isso, 20% relataram danos à reputação e 32% ressaltaram que suas empresas tiveram que lidar com uma investigação de conformidade. Esses ataques podem representar uma séria ameaça, alerta Nowersztern, especialmente para negócios menores. Uma perda substancial de capital, uma reputação gravemente danificada ou mesmo a exposição de informações operacionais importantes (como contatos de clientes) podem prejudicar profundamente a organização.

Os custos nessas áreas crescem de acordo com o tamanho do negócio. Entrevistados de grandes empresas (definidas aqui como aquelas com receitas anuais de mais de US$ 10 bilhões) dizem que, em média, suas empresas perderam 0,7% do lucro líquido com fraudes em 2020 e pagaram 0,8% do lucro líquido em multas por não conformidade, reunindo um prejuízo total de 1,5%.

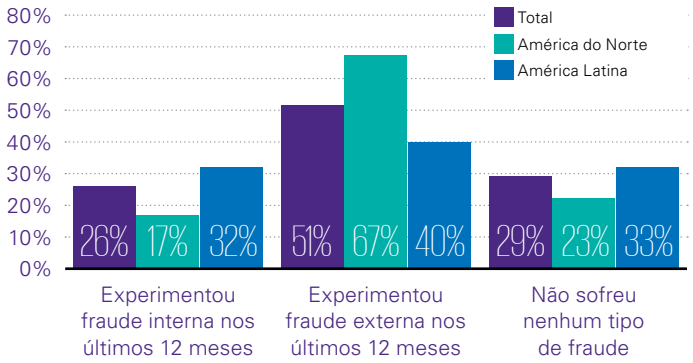
Beth Rose, diretora de *compliance*, ética e integridade da Ford Motor Company, enfatiza que esses números não são a única razão pela qual conformidade, prevenção de fraudes e segurança cibernética são importantes para os negócios. Em boas empresas, reputação e integridade são considerações cruciais. Da mesma forma, porém, custos dessa magnitude serão importantes para as organizações e seus *stakeholders*. "Os executivos são naturalmente inclinados a olhar para o impacto econômico", completa Rose.

Carlos García Jiménez, diretor regional de ética e *compliance* LATAM da Uber, concorda e destaca que a proteção eficaz contra esses riscos "custa uma fração" da média de perdas avaliada para todas as empresas.

Diferenças regionais de fraude e por que o tamanho das organizações é importante

De forma geral, os entrevistados da América do Norte e da América Latina relatam incidências de fraude marcadamente diferentes, conforme exemplo abaixo.

Comparação das fraudes na América do Norte e América Latina

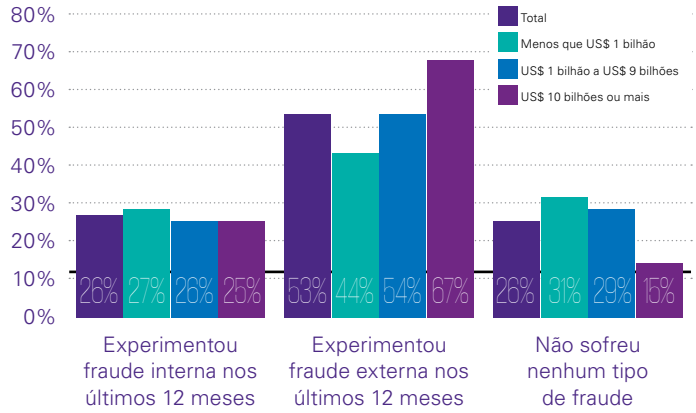


Duas observações são essenciais. Em primeiro lugar, os entrevistados indicam que a fraude é um problema mais comum para as empresas norte-americanas. Em segundo lugar, o ambiente de risco difere entre as regiões. As empresas latino-americanas têm quase duas vezes mais probabilidade do que as organizações norte-americanas de relatar envolvimento interno em fraudes. Na América do Norte, a fraude externa é um problema muito maior.

1,5%: percentual dos lucros que as grandes empresas estão perdendo por conta da fraude e da não conformidade

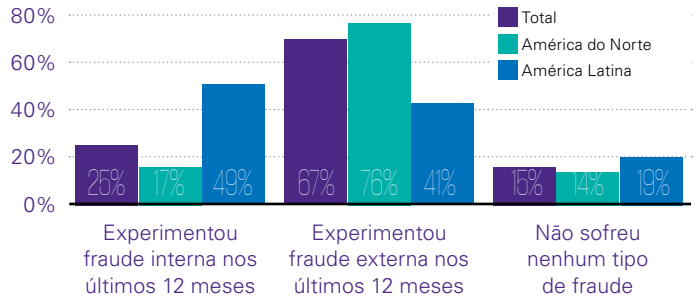
Esses resultados, no entanto, são provavelmente afetados pela forte variação no tamanho médio das empresas entre as duas regiões. A maioria das organizações norte-americanas que pesquisamos são consideravelmente maiores, com receita média anual de US$ 2,9 bilhões, em comparação com US$ 846 milhões na América Latina. A pesquisa também mostra que negócios maiores e mais ricos são mais frequentemente alvo de fraudes externas.

Comparação das fraudes de acordo com o tamanho da companhia



Mas quanto das aparentes diferenças regionais se devem ao tamanho da empresa? A resposta vem da comparação apenas das maiores organizações – aquelas com receitas de US$ 10 bilhões ou mais – em cada parte das Américas.

Comparação das fraudes: companhias com pelo menos US$ 10 bilhões de receita anual



Ao comparar os respondentes de grandes empresas por região, os números dos afetados por alguma fraude convergem. A diferença entre a proporção das organizações norte-americanas e latino-americanas é de 10 pontos percentuais, 77% e 67%, respectivamente. No entanto, entre os entrevistados de negócios maiores, 86% na América do Norte relataram alguma fraude nos últimos 12 meses, em comparação com 80% na América Latina – uma diferença visivelmente menor.

Os resultados para diferentes tipos de fraude, no entanto, divergem acentuadamente. Entre os respondentes de grandes empresas latino-americanas, 49% dizem que pelo menos uma fraude interna ocorreu em 2020, quase três vezes a taxa na América do Norte. Isso sugere que, embora as empresas norte-americanas não estejam imunes à fraude interna, as organizações latino-americanas devem priorizar ainda mais a implementação de controles internos para lidar com tal tipo de risco.

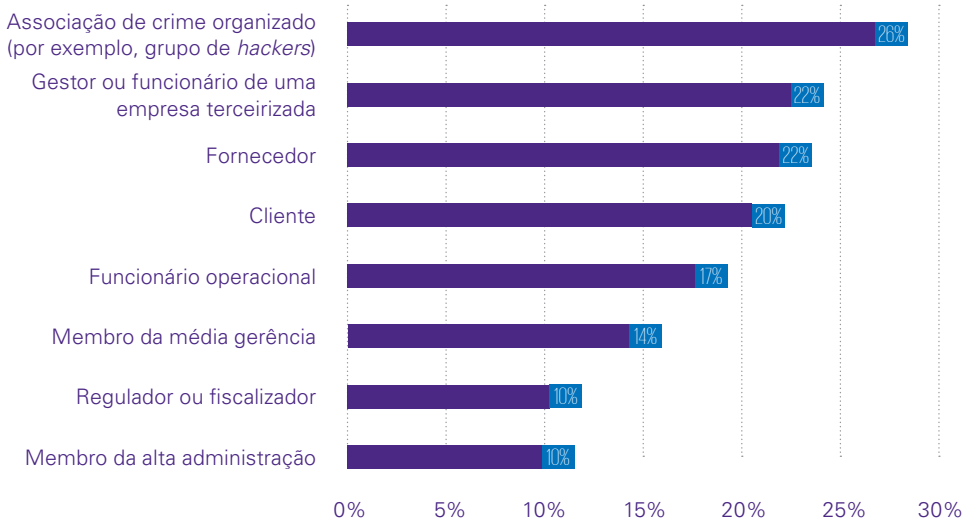
O que fazer, porém, com o percentual muito maior de empresas norte-americanas que sofreram fraude externa (76% em comparação com 42% na América Latina)? Uma explicação plausível reside na experiência divergente do crime cibernético. De todos os entrevistados das grandes empresas latino-americanas, apenas 7% relataram um ataque cibernético em 2020. Na América do Norte, impressionantes 43% dos respondentes sofreram um ataque cibernético no mesmo ano.

Além de ter receitas mais altas, Nowersztern sugere que esses alvos norte-americanos são mais digitalizados e, portanto, têm maior exposição. Como alternativa, eles podem ser melhores em detectar quando ocorre um ataque cibernético, de modo que as taxas reais de tentativas de incursão em empresas norte-americanas e latino-americanas podem ser mais próximas do que refletidas nas respostas.

É claro que as empresas da América do Norte precisam de melhores defesas cibernéticas, mas as empresas da América Latina não podem ser complacentes: à medida que crescem, elas se tornam alvos maiores para ataques cibernéticos.

O perfil dos fraudadores

Quais dos seguintes indivíduos estiveram envolvidos em fraude ou má conduta (sozinhos ou em conluio) em sua empresa nos últimos 12 meses?

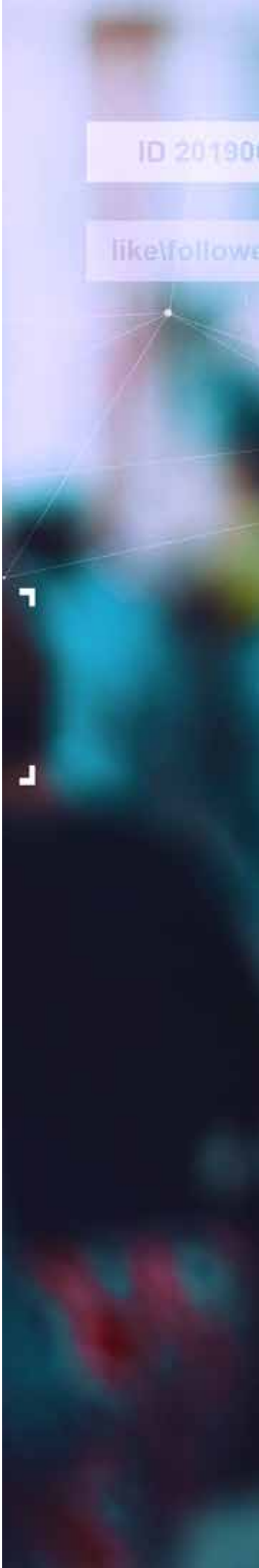


As organizações são vulneráveis a uma ampla gama de fraudadores. José Calderón, do Grupo Bimbo, explica que sua empresa lançou uma estrutura global para reduzir uma variedade de riscos de fraude. "Todas as coisas que podem afetar os processos, desde a obtenção de matéria-prima de fornecedores, passando pela produção, pelas vendas e pela execução", pode, sugere ele, criar um risco de fraude. "Então, você também tem desafios de conformidade e fraude, com associados internos e externos, regulamentações ambientais e trabalhistas, privacidade de dados – o risco é muito amplo."

De acordo com nossa pesquisa, o tipo de criminoso que mais se infiltra nas empresas – ou, pelo menos, é mais frequentemente descoberto – é o fraudador de empresas terceiras, muitas vezes habilitado digitalmente. Logo atrás estão aliados, vendedores e fornecedores. Nos países onde as operações locais da empresa têm poucos controles em vigor e usam um grande número de terceirizados, o potencial para fraude ou conluio de fornecedor era correspondentemente grande.

Existe ainda a ameaça interna: 31% dos entrevistados relataram que, em 2020, a fraude interna (conduzida por um funcionário, gerente, executivo ou proprietário) foi cometida em suas empresas.

Os perfis também variam por região. Entre os entrevistados norte-americanos, 43% citam ocorrências de fraude perpetrada por uma organização criminosa externa (como um grupo de *hackers*), em comparação com apenas 14% na América Latina – consistente com os níveis mais altos de crimes cibernéticos na América do Norte. Por outro lado, 36% dos entrevistados latino-americanos disseram que suas empresas sofreram fraude interna, em comparação com apenas 23% dos respondentes norte-americanos.



Como a pandemia mudou o cenário

A pandemia de covid-19 e os bloqueios resultantes complicaram o ambiente de ameaças.

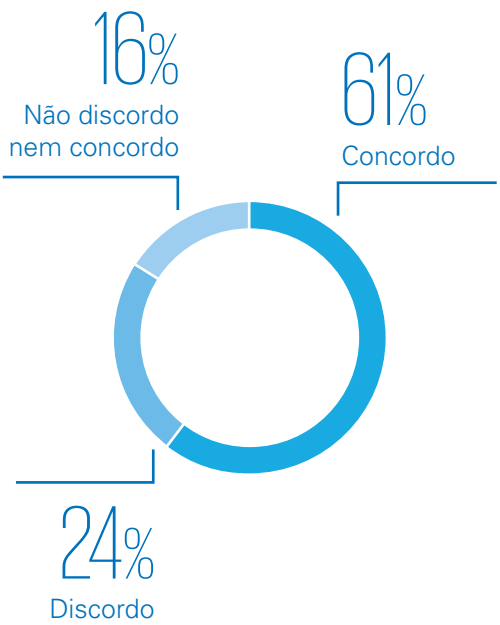
Em todas as áreas, o cenário de risco piorou, enquanto o aumento do trabalho remoto minou as defesas existentes. No geral, 86% dos entrevistados disseram que o trabalho remoto afetou negativamente pelo menos um elemento dos programas de prevenção de fraude, conformidade e segurança cibernética em suas empresas.

86%: proporção de entrevistados que disseram que trabalhar remotamente afetou negativamente pelo menos um elemento dos programas de prevenção de fraude, conformidade ou segurança cibernética de sua empresa

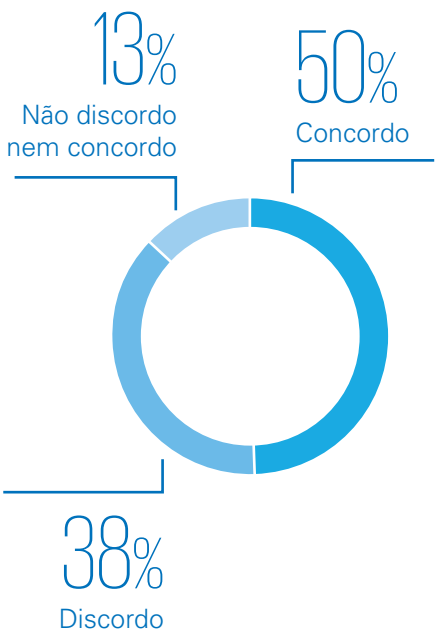
Prevenção de fraude

Oportunidades de fraude dentro de uma empresa são o produto de suas operações. Segundo José Calderón, do Grupo Bimbo, a necessidade de obter matérias-primas e peças sobressalentes com rapidez cria riscos substanciais. Isso ocorre porque, se a empresa precisa solucionar rapidamente a aquisição de um produto, os responsáveis por aquela operação ficam mais inclinados a contornar os controles existentes (por exemplo, *due diligence* em terceiros) para resolver sua demanda imediata.
Esse tipo de risco fez-se presente em muitas empresas, desde o advento da pandemia até a subsequente crise nas cadeias de suprimentos que afetou boa parte do mundo no final de 2021.

A mudança para o trabalho remoto aumentou o risco de fraude na medida em que reduziu a capacidade de monitorar e controlar comportamentos fraudulentos



Trabalhar em casa tem impactado negativamente a nossa habilidade de responder apropriadamente às fraudes em nossos negócios



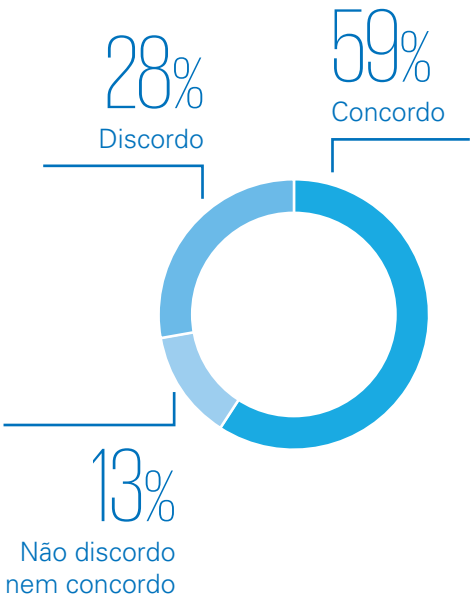
O rápido aumento do trabalho remoto também impôs desafios à prevenção de fraudes, especialmente para supervisão e investigação: 61% dos entrevistados indicaram maior risco de fraude devido à capacidade reduzida de monitorar o comportamento dos funcionários. Isso não está relacionado apenas aos funcionários operacionais: 28% dos entrevistados relataram que o trabalho remoto impediu os controles de gerenciamento e supervisão. E a questão transcende o fato de os profissionais terem um local de trabalho novo e remoto.

Garcia Jiménez explica, por exemplo, que muitos funcionários são da geração Y. Ou seja, compartilham apartamentos com outras pessoas, que não são associadas à empresa. Por isso, garantir que não-funcionários não tenham acesso aos sistemas da empresa tornou-se ainda mais desafiador.

Metade dos entrevistados disse que trabalhar em casa afetou negativamente a capacidade de suas empresas de responder a fraudes. Garcia Jiménez observa que até os controles básicos de fraude tiveram que mudar. Fora de um ambiente normal de escritório, os investigadores não têm mais o mesmo nível de controle físico sobre determinadas situações: "É um grande desafio coletar informações ou recuperar arquivos e *e-mails*. Até a condução de uma entrevista ficou mais difícil. De uma perspectiva logística, você precisa desenvolver arranjos diferentes dos anteriores. Alguns funcionários podem até estar trabalhando remotamente de outro estado ou país", explicou Jiménez.

É improvável que esses desafios diminuam. Hoje, a expectativa é a de que o trabalho híbrido será cada vez mais comum. A maioria das empresas nas Américas permanece despreparada para responder a esses riscos.

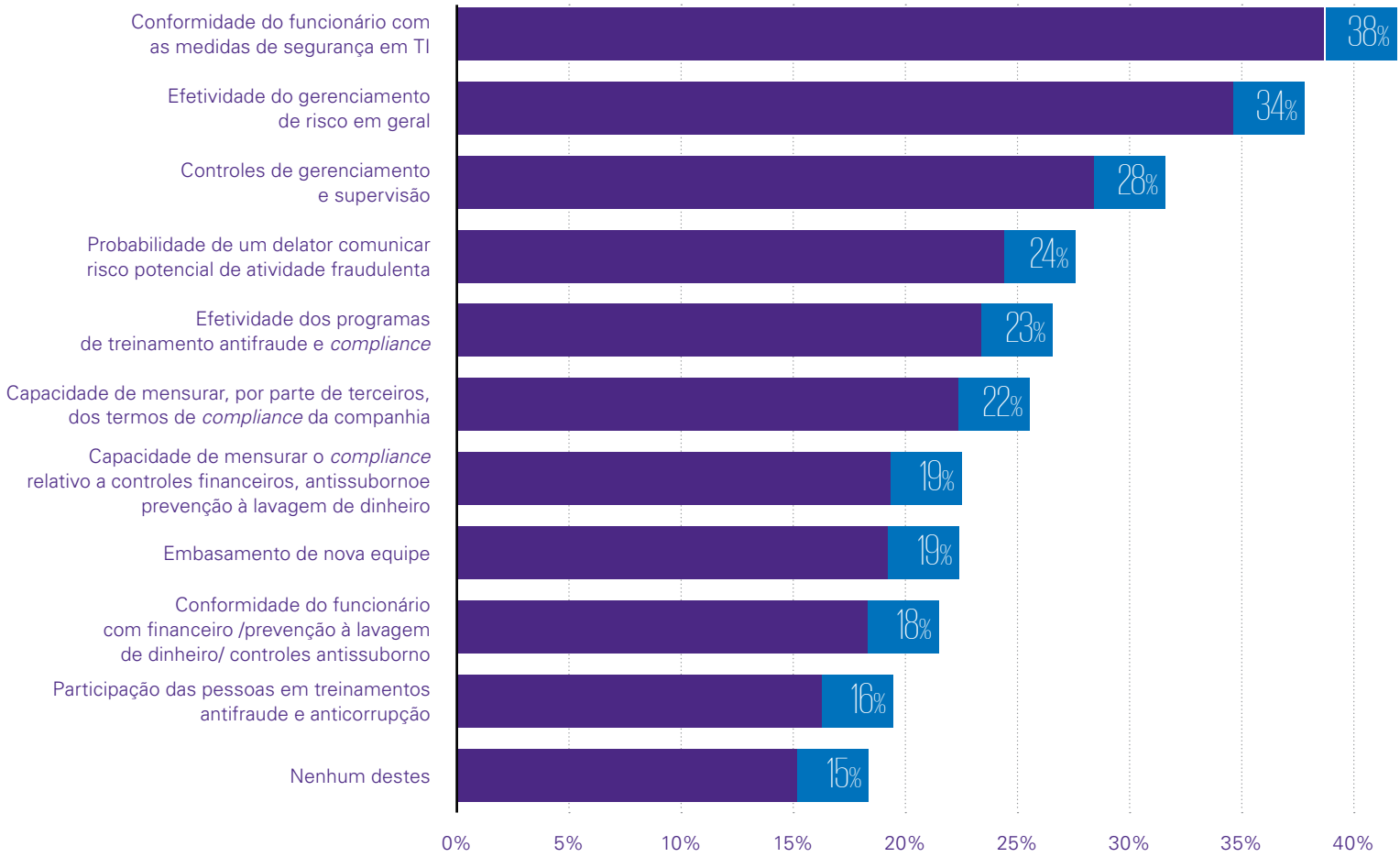
Os controles antifraude que tínhamos antes da pandemia não foram efetivamente atualizados para refletir a nova realidade profissional



Compliance

Até 77% dos entrevistados disseram que suas empresas tiveram que desenvolver novas estratégias durante a pandemia para acompanhar a evolução das demandas de conformidade. Em alguns casos, isso refletiu os novos desafios da situação. Diante da pergunta "como você cumpre com a saúde e segurança?", Beth Rose, da Ford, lembrou que "a covid-19 exigiu uma grande mudança em todos os departamentos de *compliance*". Ela também relatou que, quando a Ford começou a fabricar ventiladores e respiradores, ela teve que entender e implementar os requisitos de conformidade relacionados a esses produtos.

Quais aspectos sofreram mais impacto negativo com o aumento do número de funcionários trabalhando em casa no último ano?



As considerações de trabalho remoto também desempenharam um papel significativo no que se refere a *compliance*. Garcia Jiménez sugere que o treinamento de conformidade sofreu o maior impacto, com os cursos presenciais mudando para *on-line*. Isso foi mais do que uma mudança no meio de interação: em muitas empresas, foi preciso fazer uma revisão substancial dos materiais de treinamento e investir no desenvolvimento de diferentes habilidades de comunicação tanto por parte daqueles que lideram quanto daqueles que aprendem. O tempo gasto com essas adequações pode ter deixado lacunas no treinamento de muitos.

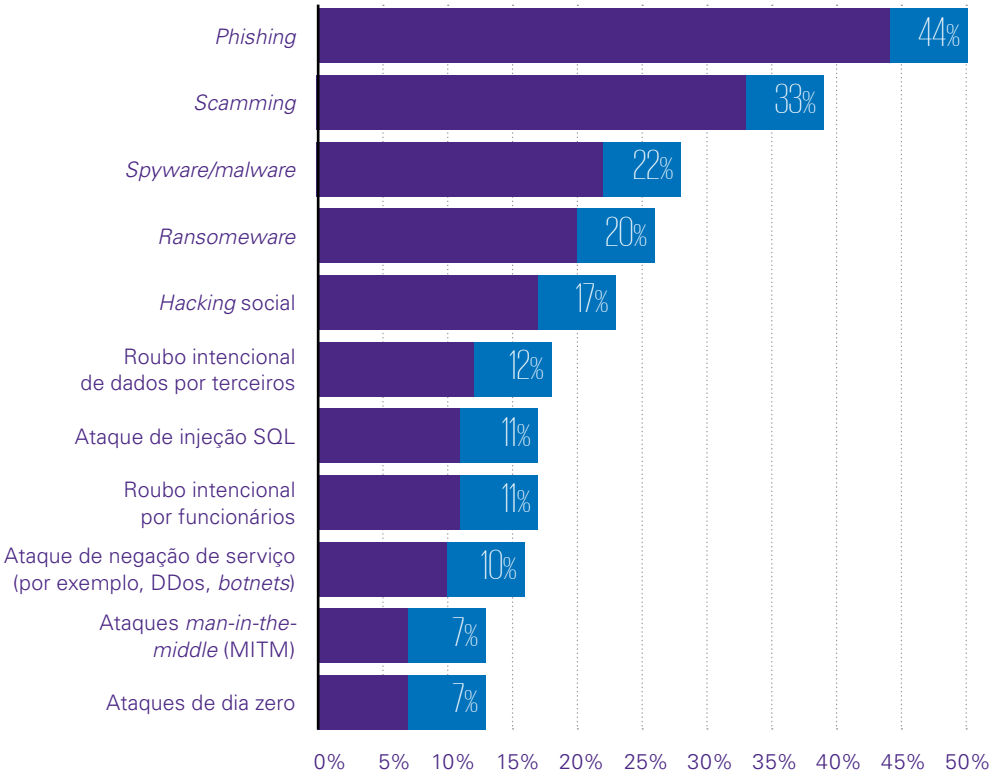
O aumento do trabalho remoto também exigiu uma mudança cultural significativa. "Parte da conformidade é ver o que está acontecendo para ter uma noção dos pontos em que pode haver algum risco", explica Rose. "Quando nos tornamos virtuais, isso virou um problema." Muitos entrevistados concordam: 19% relataram que o trabalho remoto tornou mais difícil medir a conformidade com os controles financeiros, antilavagem de dinheiro e antissuborno.

O ajuste ao novo ambiente de conformidade continua sendo um trabalho em andamento. Rose relata que a Ford está planejando continuar com seu modelo de trabalho híbrido atual. Descobrir as implicações para a conformidade é, em suas palavras, "a questão de um milhão de dólares. Temos que pensar diferente sobre treinamento, conscientização, equipes e avaliação de riscos. Indústrias diferentes terão necessidades distintas."

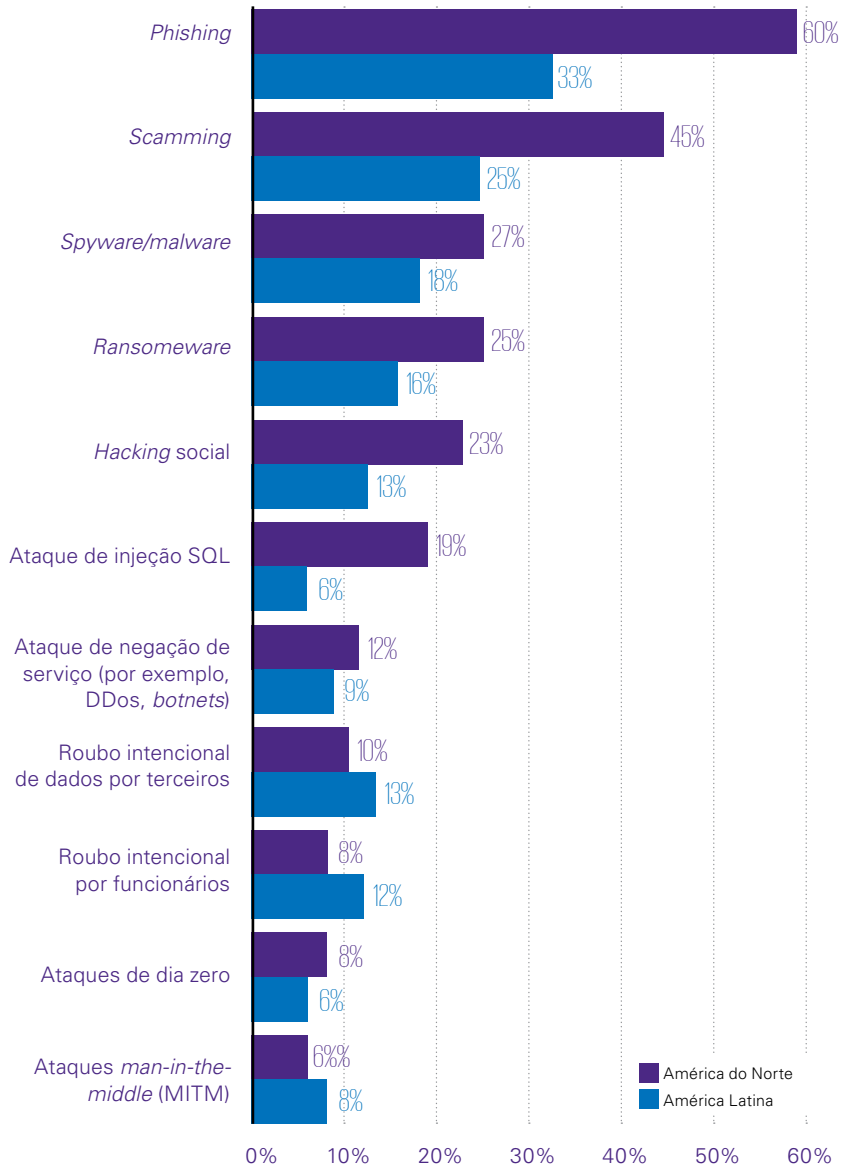
Segurança cibernética

A ocorrência de crimes cibernéticos aumentou durante a pandemia e não diminuiu até agora. Como mostra o gráfico, as empresas pesquisadas para este relatório estão relatando aumentos na frequência de vários tipos de ataque, como *phishing* (citado por 44%), golpes (33%), *malware* (22%) e desafios crescentes de *ransomware*. No geral, 79% dos entrevistados viram crescimento em pelo menos um dos tipos de ataque abordados pela pesquisa.

Em quais dos seguintes tipos de ataques cibernéticos houve aumento de ocorrência na sua empresa nos últimos 12 meses (se houver)?



Em qual dos itens abaixo você observou crescimento?



Mesmo incidentes isolados podem ter um grande impacto. Por exemplo: o ataque de *ransomware* a um oleoduto em maio de 2021 levou à escassez de petróleo em vários estados do sul dos Estados Unidos. Como outro exemplo com efeito substancial, Galimberti cita um grande roubo de dados ocorrido no Brasil no início de 2021: "Arquivos de 220 milhões de brasileiros foram colocados na *dark web* com todo tipo de informação", relembra.

Nowersztern destaca que várias tendências anteriores à pandemia – e por ela intensificadas e/ou aceleradas – impulsionaram as atividades criminosas em abientes virtuais. Por exemplo, mensagens de *phishing* adotaram o tema covid-19 para atrair consumidores ansiosos por informações acerca do novo coronavírus. E, à medida que as empresas e a sociedade dependem cada vez mais de ativos e equipamentos digitais, nos tornamos mais vulneráveis.

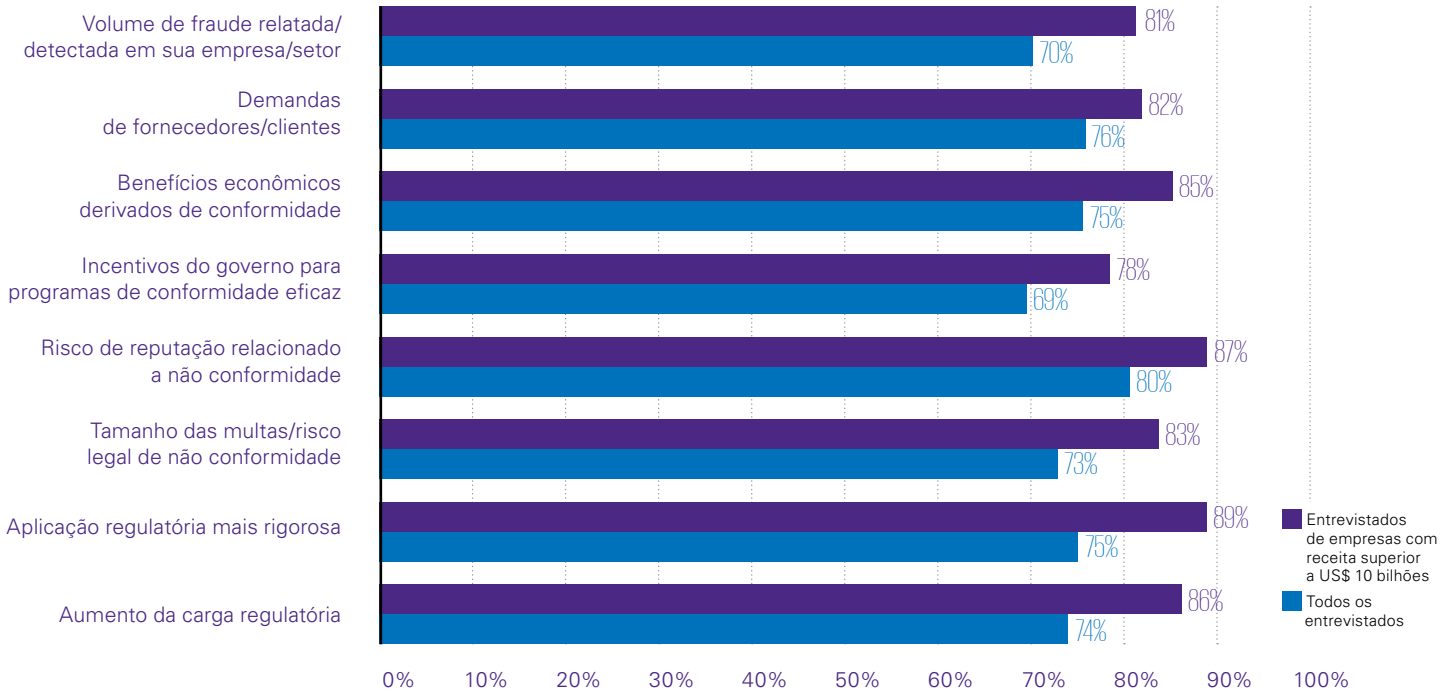
Quase todos os entrevistados relataram que suas empresas tomaram medidas para lidar com os riscos de segurança cibernética, incluindo: implementação de autenticação dupla (55%), melhorias na segurança da rede (5%) e melhor treinamento (47%). O investimento resultante necessário para atender a esses desafios de segurança cibernética pode ser substancial. Calderón relata que, no Grupo Bimbo, "o conselho aumentou o orçamento de segurança cibernética em mais de cinco vezes". Esse aumento foi necessário, embora menos de um em cada cinco funcionários do Grupo Bimbo trabalhe de forma remota.

69% dos entrevistados disseram que o trabalho remoto tem sido um grande desafio de segurança cibernética para seus negócios

O surto de covid-19 e a mudança relacionada ao trabalho remoto tornaram mais difícil para as empresas lidar com sua segurança cibernética: 67% dos entrevistados continuam preocupados com os riscos cibernéticos inerentes ao trabalho híbrido. Mesmo que a pandemia chegue ao fim, os modelos de trabalho nas Américas parecem ter mudado para sempre – e isso vai requerer atenção redobrada aos quesitos de segurança cibernética.

Compliance é uma preocupação de todos os negócios

Até que ponto os itens abaixo estão exigindo mais tempo e atenção da liderança com questões ligadas a conformidade? (O gráfico mostra a proporção de entrevistados que selecionaram a opção 4 ou a opção 5 em uma escala de 1 a 5, em que 1 é definido como "Nem um pouco", 3 é definido como "Um pouco" e 5 é definido como "Muito")



Compliance não é mais (se é que alguma vez foi) apenas uma questão de cumprir diretrizes legais. Como mostra o gráfico, mais de 70% dos entrevistados relatam que a aplicação rigorosa das regras de *compliance*, o aumento dos encargos regulatórios e as penalidades potenciais aumentam o tempo e a atenção que seus líderes corporativos dedicam às questões de conformidade – nas grandes empresas, essa é a visão de cerca de 80% dos entrevistados.

No entanto, as demandas dos *stakeholders*, os benefícios econômicos e a reputação têm a mesma probabilidade de concentrar a atenção da liderança na conformidade: 64% dos entrevistados relataram que fornecedores e clientes estão exigindo cada vez mais prova de conformidade com os regulamentos de privacidade de dados e 52% dizem o mesmo sobre corrupção e legislação contra lavagem de dinheiro.

Beth Rose, da Ford, não se surpreende: "Com a evolução das mídias sociais e a proliferação de pessoas opinando sobre a reputação e a marca, você precisa se preocupar em fazer o *compliance* certo." A aplicação estrita e a importância de evitar conexões inadvertidas em suas alianças e fusões com terceiros também são demandas imperativas.

Esse conjunto mais amplo de considerações torna o papel do *compliance* ainda mais relevante. Garcia Jiménez comenta que, embora o *compliance* ainda seja uma questão de mitigação de riscos, agora também se trata de "construção de narrativas, interna e externamente". Parte do trabalho é mostrar aos reguladores, aos *stakeholders* e à sociedade em geral os benefícios econômicos, sociais e ambientais que a empresa oferece à comunidade.

Essa construção de narrativa mais ampla traz outros benefícios indiretos para as empresas. Mais notavelmente, a boa conformidade ajuda a comunicar a confiabilidade de uma empresa a outras partes interessadas, sejam reguladores, investidores, aliados ou clientes.

Os níveis de ameaça estão aumentando

Os desafios de trabalhar remotamente são apenas parte de um padrão mais amplo de dificuldades crescentes relacionadas à fraude, conformidade e segurança cibernética: 69% dos entrevistados esperam um aumento no risco em fraude externa ou interna no próximo ano, e 29% projetam um aumento em ambos os riscos, ou seja: receiam sofrer fraudes internas e externas. As preocupações com o aumento do crime cibernético são generalizadas: 77% dizem que o risco de segurança cibernética aumentará nos próximos 12 meses; apenas 7% preveem um declínio. Galimberti concorda, dizendo que "as empresas estão enfrentando cada vez mais *hackers*, ataques de r*ansomware*, *phishing* e outros".

O aumento das ocorrências de fraudes e ataques cibernéticos nem sempre está conectado. Calderón observa que qualquer pressão sobre os modelos operacionais pode criar um aumento no risco de fraude. Na indústria de alimentos e bebidas, por exemplo, o interesse do consumidor por produtos mais saudáveis a preços mais baixos está remodelando a demanda. Uma mudança em direção ao uso de fornecedores de custo mais baixo para atender a essa nova demanda requer a devida diligência relacionada à forma como esses parceiros fazem negócios, incluindo considerações sobre o modo como negociam contratos e a asseguração de que os preços baixos não resultam, por exemplo, do uso de processos altamente poluentes.

No entanto, a fraude e a insegurança cibernética se sobrepõem – e isso acontece com cada vez mais frequência. Os tipos de ataque cibernético para os quais o maior número de entrevistados viu aumentos no ano passado incluem *phishing* (44%), *scamming* (33%), *spyware* (22%) e *ransomware* (20%).

69% dos entrevistados esperam um aumento no risco de fraude externa ou interna no próximo ano

As tendências atuais dos negócios aumentam inadvertidamente essa convergência de fraude e risco cibernético, proporcionando aos fraudadores uma nova oportunidade. Calderón observa, por exemplo, que a digitalização de processos, a migração para nuvem e o aumento no uso de dispositivos móveis acarretam riscos. Rose acrescenta: "Como todos estão remotos e usando computadores, os malfeitores encontraram maneiras mais criativas de operar". Ela comenta que esses esforços não são todos *on-line*. Os dados corroboram a análise da executiva da Ford: 17 dos entrevistados relataram um aumento no *hackeamento* social, pelo qual os criminosos virtuais usam engenharia social e manipulação de comportamentos humanos para obter acesso aos sistemas.

62%
Esperam por novos regulamentos de privacidade de dados nos próximos cinco anos

47%
Esperam por novas regulamentações ambientais nos próximos cinco anos

46%
Esperam por novas regulamentações trabalhistas nos próximos cinco anos

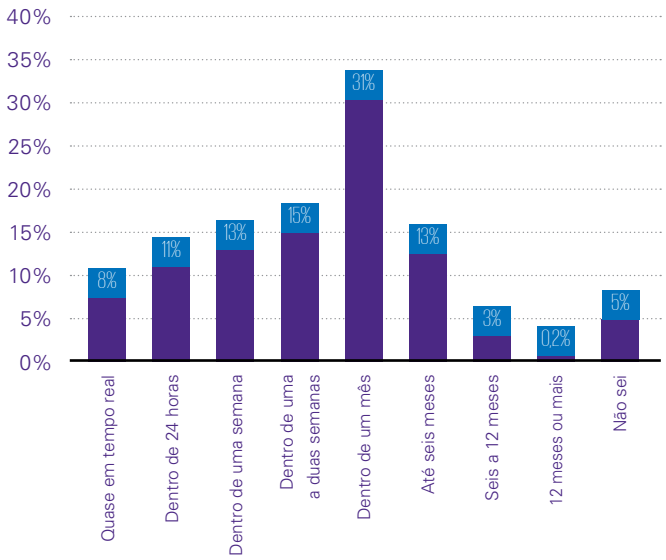
41%
Esperam por uma aplicação mais rígida das regras existentes nos próximos cinco anos

O risco geral de *compliance* também deve crescer no próximo ano, de acordo com 60% dos entrevistados, apenas 17% esperam uma redução nesse tipo.
Este desafio, como explica Rose, da Ford, é multifacetado, que exige mais requisitos de *compliance* em campos com substancial regulamentação existente. Também pode requerer a introdução de regras em novas áreas e uma fiscalização mais ativa por parte dos responsáveis pela conformidade. Como mostra o gráfico, um número significativo de entrevistados espera novas regulamentações relacionadas à privacidade de dados, regulamentação ambiental e relações trabalhistas pelos próximos cinco anos.
No geral, 89% dos respondentes acreditam que haverá novos requisitos de conformidade em pelo menos uma dessas áreas no próximo ano. Rose confirma que "o atual governo dos Estados Unidos não escondeu que está aumentando a fiscalização e a regulamentação em todas as áreas. Isso inclui regulamentações ambientais, sociais e de governança (ESG). A questão da segurança cibernética deve seguir junto", afirma.

Na América Latina, aumentos regulatórios semelhantes estão em curso. Galimberti relata que a Lei Geral de Proteção de Dados (LGPD) do Brasil, que entrou em vigor em setembro de 2020, tem impulsionado a atividade de *compliance* por empresas de grande e pequeno portes. A lei concede direitos substanciais aos titulares dos dados e exige que todas as empresas que processam dados designem um responsável para cuidar desse "bem". Calderón acrescenta que as exigências ambientais em áreas como consumo de água e gestão de resíduos estão crescendo.
"Há desafios e, ao mesmo tempo, oportunidades para respondermos às necessidades do consumidor", diz ele.

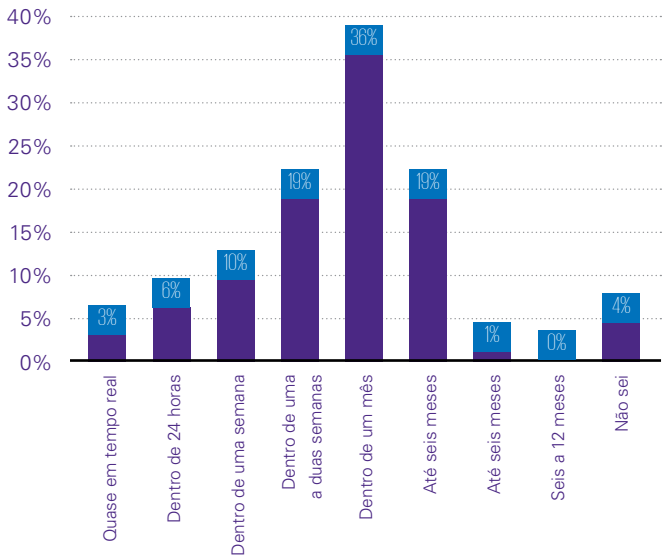
Respostas lentas, preocupação insuficiente

Normalmente, em quanto tempo é identificado um ataque cibernético ou violação em sua empresa?



Média: aproximadamente duas semanas

Normalmente, em quanto tempo é contido um ataque cibernético ou violação em sua empresa, uma vez identificado?



Média: aproximadamente duas semanas e meia

"Após um incidente cibernético, seus dados podem desaparecer em minutos ou segundos. Nesse sentido, nenhuma velocidade de resposta é rápida o suficiente", observa Ariel Nowersztern, do BID. Da mesma forma, os malfeitores podem causar danos às empresas de várias maneiras ao obter acesso às redes.

Parece preocupante que apenas uma pequena proporção dos entrevistados tenha dito que suas empresas são capazes de identificar e conter um ataque cibernético em tempo real, ou mesmo em 24 horas. O tempo médio de identificação é muito mais longo – cerca de duas semanas – e a contenção requer mais duas semanas e meia. No geral, de acordo com nossa pesquisa, normalmente leva cerca de um mês o período entre o início de um ataque cibernético a uma empresa e sua contenção.

Os entrevistados parecem surpreendentemente despreocupados: 81% estão bastante ou completamente satisfeitos com o tempo que suas empresas levam para reconhecer um ataque de TI e 76% estão satisfeitos com a velocidade de resposta.

Nowersztern explica que existem inúmeras barreiras para melhorar a segurança cibernética, incluindo a falta de profissionais treinados e a percepção comum de que cuidar desse aspecto é um gasto extra e não um investimento fundamental. "Basicamente", acrescenta Nowersztern, "a solução começa com ter um foco maior na segurança cibernética. Isso é o que você deve fazer. Existem ferramentas e, mesmo que às vezes sejam difíceis ou caras de implantar, devem ser adotadas".

Controles de mitigação abrangentes permanecem raros

Que tipo de proteção as empresas possuem contra a complexidade crescente de fraude, *compliance* e ameaças cibernéticas?

Há muito espaço para melhorar todos esses quesitos, especialmente na América Latina – convém ressaltar, porém, que as respostas norte-americanas não despertam otimismo.

No geral, apenas uma minoria dos entrevistados afirma que suas empresas adotam as melhores práticas internacionais em conformidade anticorrupção (18%); conformidade ambiental (21%); combate à lavagem de dinheiro (22%); controles antifraude (23%); ou controles voltados à segurança de dados (27%). As empresas norte-americanas se comparam com padrões mais altos. Como mostram os gráficos, a maioria dos entrevistados de empresas norte-americanas acha que está atendendo aos padrões internacionais ou indo bem para os padrões locais. Mas a resposta mais frequente dos entrevistados latino-americanos a essas perguntas é que, embora suas empresas cumpram suas obrigações legais, elas não se alinham plenamente aos padrões nacionais ou internacionais.

No que se refere às regulamentações anticorrupção e antilavagem de dinheiro, mais de 25% dos entrevistados latino-americanos não têm certeza sequer de estarem cumprindo integralmente as regras locais.

Para obter um retrato mais detalhado, a pesquisa investigou como os entrevistados classificaram suas empresas em aspectos individuais de controle de fraude (11 áreas), conformidade (sete áreas) e segurança cibernética (seis áreas)[2]. Uma empresa pode não precisar necessariamente se destacar em cada uma dessas 26 áreas do ciclo de ameaças. Segundo Rose, "a conformidade deve ser baseada em riscos". Muito esforço direcionado para áreas de baixo risco seria um dreno inadequado de recursos. No entanto, os assuntos cobertos pela pesquisa (como controles financeiros e administrativos e prevenção de furto de dados) são suficientemente importantes para que a maioria das empresas se esforce para melhorar sua gestão.

Do lado positivo, para cada controle de fraude, consideração de conformidade e controle de segurança cibernética, entre 85% e 95% dos entrevistados classificaram seus negócios como excelentes em pelo menos uma das áreas cobertas pela pesquisa. Poucos, no entanto, classificaram suas empresas como tendo um desempenho

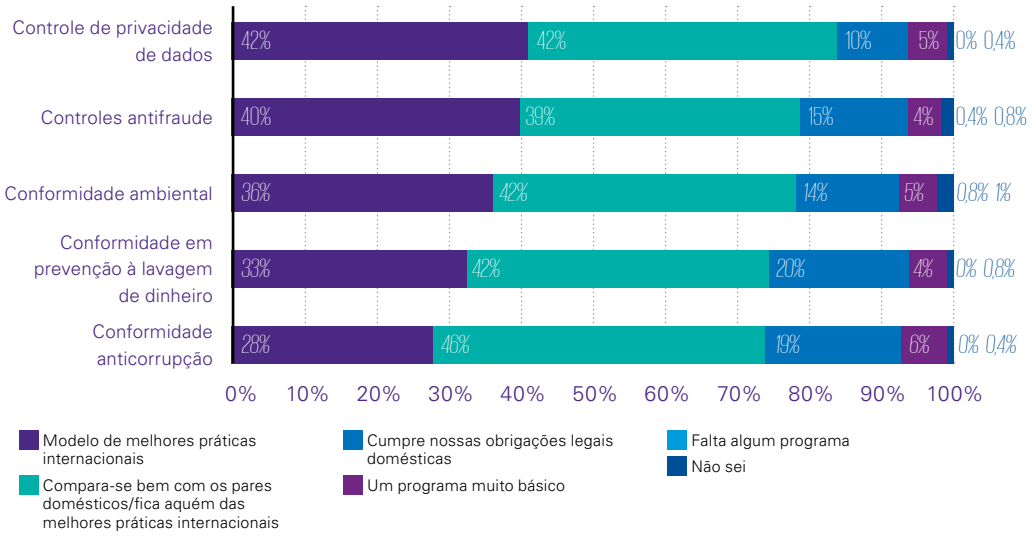
[2]As áreas específicas cobertas são:
Para controle de fraude - controles financeiros; segurança de ativos físicos; segurança de TI; controles de gestão e supervisão; triagens de plano de fundo da equipe; denunciante ou outros mecanismos de denúncia; processos de *due diligence* relacionados a fornecedores, aliados e/ou; políticas antifraude/matrizes de fraude; avaliações de risco; treinamento de equipe; planos de resposta à fraude.
Para conformidade - prevenção de não conformidade; encontrar e investigar casos de não conformidade; tomar medidas para mitigar os casos de não conformidade; reportar irregularidades às autoridades de forma a minimizar o risco corporativo, multas e penalidades; ajustar e cumprir os novos requisitos regulamentares em tempo hábil; identificar risco de conformidade e fraude entre terceiros potenciais; adotar novas tecnologias para melhorar o desempenho nas áreas acima.
Para segurança cibernética - prevenção de roubo de dados por hackers externos; prevenção de furto de dados por funcionários; prevenção de perda/roubo de dados decorrente de erros de funcionários; prevenção de roubo de dados por vendedores/fornecedores/aliados; prevenção de ataques de *ransomware*; prevenção de outros ataques a redes ou ativos.

de alta qualidade em todos os setores. Calculamos então quantos entrevistados avaliaram suas empresas como excelentes para pelo menos metade das áreas cobertas em cada parte (chamamos isso de padrão "metade ou mais").

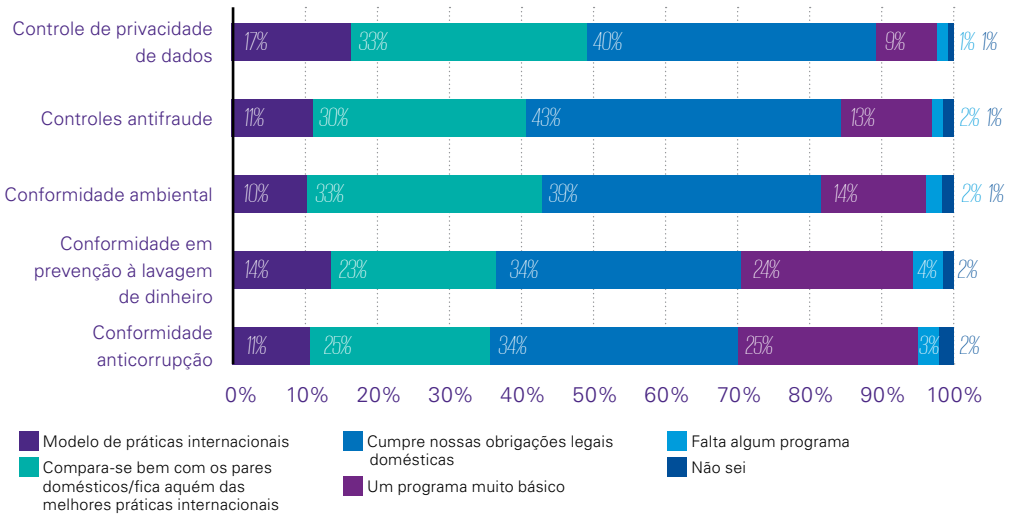
No geral, apenas 24% dos entrevistados disseram que suas empresas alcançaram o padrão "pela metade ou mais" no que se refere à segurança cibernética; 17% no que diz respeito aos controles de fraude; e apenas 13% no que se refere à conformidade. Apenas 4% dos entrevistados disseram que suas empresas alcançaram o padrão "pela metade ou mais" em todas as três áreas. Resumindo: a maioria das empresas precisa melhorar a qualidade de seus esforços no combate à fraude, na implementação de medidas de *compliance* e na mitigação dos riscos cibernéticos.

O problema é mais disseminado na América Latina: apenas 20% dos entrevistados disseram que suas empresas atendiam ao padrão "pela metade ou mais" para segurança cibernética; 11% no que se refere aos controles de fraude; e 9% no que diz respeito à conformidade. O impacto dessa carência em medidas adequadas evidencia-se em outros resultados da pesquisa. Por exemplo: os entrevistados observaram que as auditorias internas eram responsáveis por revelar casos de fraude ou violação de conformidade ou segurança cibernética em 43% das empresas norte-americanas, mas o mesmo ocorre em apenas 27% das empresas latino-americanas.

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



Da mesma forma, outros controles internos trouxeram esses problemas à luz em 41% das empresas da América do Norte, mas em apenas 31% na América Latina. Seus níveis mais baixos de excelência em controles internos também podem ajudar a explicar os níveis mais elevados de fraude interna que as empresas latino-americanas dizem enfrentar.

Os líderes de muitas empresas entrevistadas parecem compreender que as defesas precisam ser reforçadas. Cerca de 65% dos respondentes esperam que os gastos com segurança cibernética aumentem no próximo ano; 53% esperam um aumento nos gastos com prevenção de fraude; e 44% acreditam que haverá um aumento nos gastos com conformidade. Menos de 7% dos respondentes, em cada caso, estimam que os gastos nessas áreas diminuirão no próximo ano.

À medida que as empresas tomam essas decisões relativas a gastos – ou, melhor ainda, a investimentos –, o conselho mais importante que nossos profissionais oferecem é não esquecer as pessoas. Segundo Calderón, "o treinamento e a retenção de bons funcionários é uma das coisas mais importantes para prevenir a fraude. Isso espalha a cultura certa". Rose concorda que "o maior problema é a cultura". Ela acrescenta que não basta oferecer treinamento: é preciso cuidar dos funcionários, que estão exaustos por todos os desafios inerentes ao período de pandemia. "As pessoas podem estar atingindo seus limites, e isso pode levar a erros ou conduta imprópria. Como podemos ajudar a garantir que as pessoas estejam bem e com suporte? Esse é o grande problema", pondera.

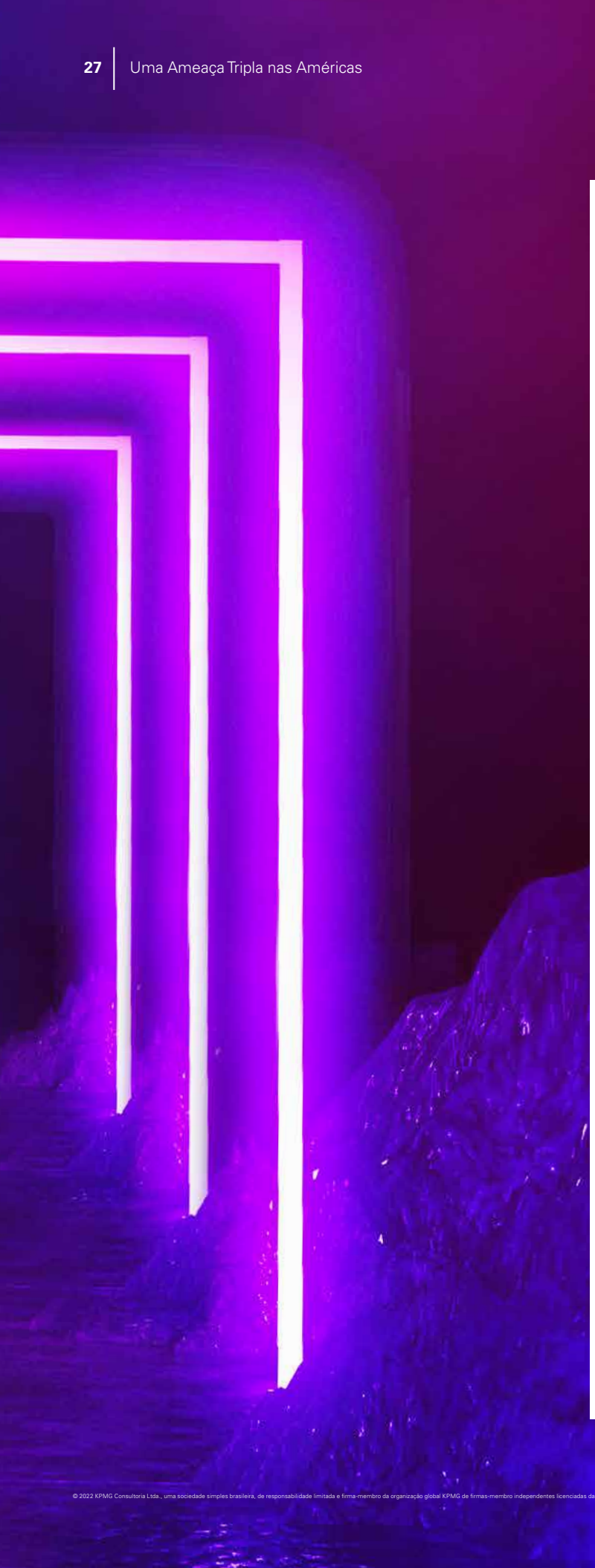
Empresas que atendem ao padrão "meio ou mais"

América do Norte

31%	27%	18%
Cibersegurança	Prevenção de fraude	Controles de conformidade

América Latina

19%	11%	9%
Cibersegurança	Prevenção de fraude	Controles de conformidade



Conclusão: sua empresa está preparada para a ameaça tripla?

Antes da pandemia, questões como fraude, não observância às regras de *compliance* e ataques cibernéticos já representavam uma ameaça e tanto para as empresas nas Américas. Agora, eles se tornaram mais extensos e complexos. Olhando para o futuro, os executivos esperam outro aumento generalizado nos riscos oferecidos por esse "tripé de fragilidades". A maioria das empresas possui algumas defesas, mas a excelência abrangente é rara. Isso é especialmente claro na América Latina, onde, conforme a pesquisa mostra, a falta de controles eficazes é responsável por níveis mais elevados de fraude interna. As organizações norte-americanas estão se saindo melhor, mas a maioria ainda fica aquém do que seria ideal.

Grande parte das empresas pretende gastar mais dinheiro e aumentar o foco da liderança nessas áreas. A KPMG recomenda que elas sigam estas cinco etapas para mitigar a ameaça tripla:

01

Defina o tom certo com a alta administração e o Conselho

É importante que, desde as mais altas instâncias, seja promovida uma cultura de incentivo à conduta ética e o compromisso com a conformidade. Para tanto, é preciso estabelecer padrões e procedimentos para prevenir e detectar fraudes, mitigar os riscos de *compliance* e segurança cibernética e monitorar a conformidade com esses padrões. Para apoiar isso, as empresas devem implementar protocolos que garantam que o conselho tenha conhecimento e possa exercer supervisão razoável sobre conformidade e ética.

02

Realize uma revisão de riscos

As empresas devem implementar um processo abrangente de avaliação de riscos corporativos, incluindo os riscos de fraude e má conduta, conformidade e riscos de segurança cibernética. É importante colocar foco nos riscos reais. O ideal é que a administração, o conselho, a auditoria interna, os responsáveis por tudo o que se refere à conformidade, áreas operacionais e outras partes interessadas trabalhem conjuntamente para identificar as principais áreas de risco e projetar controles para sua mitigação.

03

Comunique-se com eficácia

As empresas devem avaliar os protocolos existentes de treinamento e comunicação para detalhar como as mensagens sobre riscos podem fluir com mais eficácia pela organização. Todas as pessoas relevantes devem receber comunicações claras da alta administração acerca das responsabilidades de controle – e é fundamental que estas sejam levadas a sério. Para dar suporte a isso, o treinamento direcionado ajudará os funcionários a compreender seu próprio papel na proteção dos ativos da empresa e no aprimoramento dos sistemas de controle interno e a entender de que maneira suas próprias atividades se relacionam com o trabalho dos outros.

04

Fortaleça a detecção

Os funcionários são aliados essenciais para identificar fraudes e condutas impróprias. Organizações nas quais os profissionais acreditam ter a responsabilidade de levantar as mãos e denunciar a má conduta são as que têm maior probabilidade de detectar a fraude e a má conduta precocemente. Nessas organizações, os funcionários se sentem confortáveis em dar o alarme e não temem retaliações. Eles esperam que a administração seja responsiva. As empresas precisam desenvolver e divulgar meios de os funcionários e terceiros relevantes relatarem suspeitas de irregularidades e buscarem aconselhamento e esclarecimento sobre as leis, regulamentos e padrões de conduta da empresa.

05

Crie uma cultura de disciplina e responsabilidade

As empresas devem considerar o aprimoramento de suas políticas e protocolos para incluir elementos de disciplina e responsabilidade que não sejam punitivos. Por exemplo: é possível incluir princípios éticos, de integridade e de comportamento em suas avaliações de desempenho e fornecer incentivos ou recompensas para atingir metas relacionadas a esses temas. Medidas dessa natureza transmitem a mensagem de que as medidas disciplinares em casos de fraude e não conformidade são aplicadas de forma consistente, independentemente do posto, mandato ou função no trabalho.

Estudo de caso:

A digitalização de impostos traz novos desafios

A digitalização de impostos representa uma evolução multifacetada, que abrange impostos indiretos. Desse processo, participam desde funcionários fiscais até empresas e contribuintes individuais. Ou seja, temos muitos atores em cena. Nas corporações, isso envolve uma interação quase em tempo real com as autoridades fiscais.

Vários países latino-americanos têm evoluído na digitalização tributária. A região foi uma das primeiras a adotar sistemas de fatura eletrônica para solucionar problemas com fraude de IVA (Imposto sobre o Valor Acrescentado), maior transparência e redução de encargos.

No geral, essa tendência de digitalização de impostos remodelou o ambiente de conformidade, fraude e segurança cibernética de várias maneiras, explica Pascal Saint-Amans, diretor do Centro de Política e Administração Tributária da Organização para a Cooperação e Desenvolvimento Econômico (OCDE).

Conformidade

O grande benefício da digitalização para as empresas, observa Saint-Amans, é que a integração dos relatórios fiscais com outros sistemas de negócios pode reduzir encargos, aumentar a precisão e a conformidade e tornar os impostos um processo contínuo. “Grande parte da conformidade de relatórios será automática”, ele diz. A automação, no entanto, não elimina totalmente a experiência em conformidade necessária às funções tributárias corporativas. “A interpretação dos casos mais complexos continua sendo um problema”, afirma Saint-Amans. “Nem sempre será possível reduzir a divergência ao decidir, por exemplo, se algo é dedutível ou não.”

Fraude

Da mesma forma, Saint-Amans explica que a digitalização não elimina o risco de fraude, embora possa reduzir a oportunidade para isso. “Se alguém ainda planeja trapacear”, diz Saint-Amans “o sistema de TI precisa ser mais perceptivo, para que a intenção do crime seja mais clara.”

Em outras palavras: é importante haver uma clara diferenciação entre um erro intencional e outro não intencional. Quanto maior a atenção das autoridades fiscais aos riscos que o aumento da quantidade de dados disponíveis pode gerar, menor a probabilidade de sucesso para quem pratica atividades criminosas. O Chile, por exemplo, agora implanta modelos analíticos e preditivos para descobrir fraudes de IVA; no Peru, foram adotadas ferramentas semelhantes para cortar seus custos de auditoria em 15%. Como? Simples: direcionando melhor os investimentos nesse aspecto específico.

Segurança cibernética

Embora a digitalização de impostos tenha diminuído os riscos sobre a conformidade e fraude, o tráfego intenso de informações confidenciais entre empresas e autoridades fiscais aumenta os riscos da segurança cibernética.

A fim de reduzir riscos específicos, a OCDE está incentivando as administrações fiscais digitais da próxima geração a incorporar regras fiscais aos sistemas das empresas. Estas poderiam remeter às autoridades fiscais algumas informações mínimas necessárias, como valores em dívida e principais dados de suporte, sendo o restante mantido em servidores da própria empresa. Essa abordagem exigiria credenciamento e auditoria remota, mas poderia reduzir significativamente os riscos cibernéticos.

Entre em contato conosco

Amanda Rigby
Líder de Forensic para
a região das Américas
KPMG nos Estados Unidos
amandarigby@kpmg.com

Ana Lopez Espinar
Sócia-líder de Forensic da KPMG
na Argentina e na América do Sul
KPMG na Argentina
ablopez@kpmg.com.ar

Emerson Melo
Sócio-líder de Forensic da KPMG
no Brasil e na América do Sul
KPMG no Brasil
emersonmelo@kpmg.com.br

Enzo Carlucci
Sócio de Forensic da KPMG no Canadá
KPMG no Canadá
ecarlucci@kpmg.ca

Luis Preciado
Sócio-líder de Risk Advisory Solutions da
KPMG no México e na América Central
KPMG no México
luispreciado@kpmg.com.mx

A prestação dos serviços descritos neste material, no todo ou em parte, pode não ser permitida a clientes de auditoria da KPMG e suas afiliadas ou entidades relacionadas.

Ser especialista transforma negócios.

#KPMGTransforma

Baixe o nosso APP

kpmg.com.br /kpmgbrasil