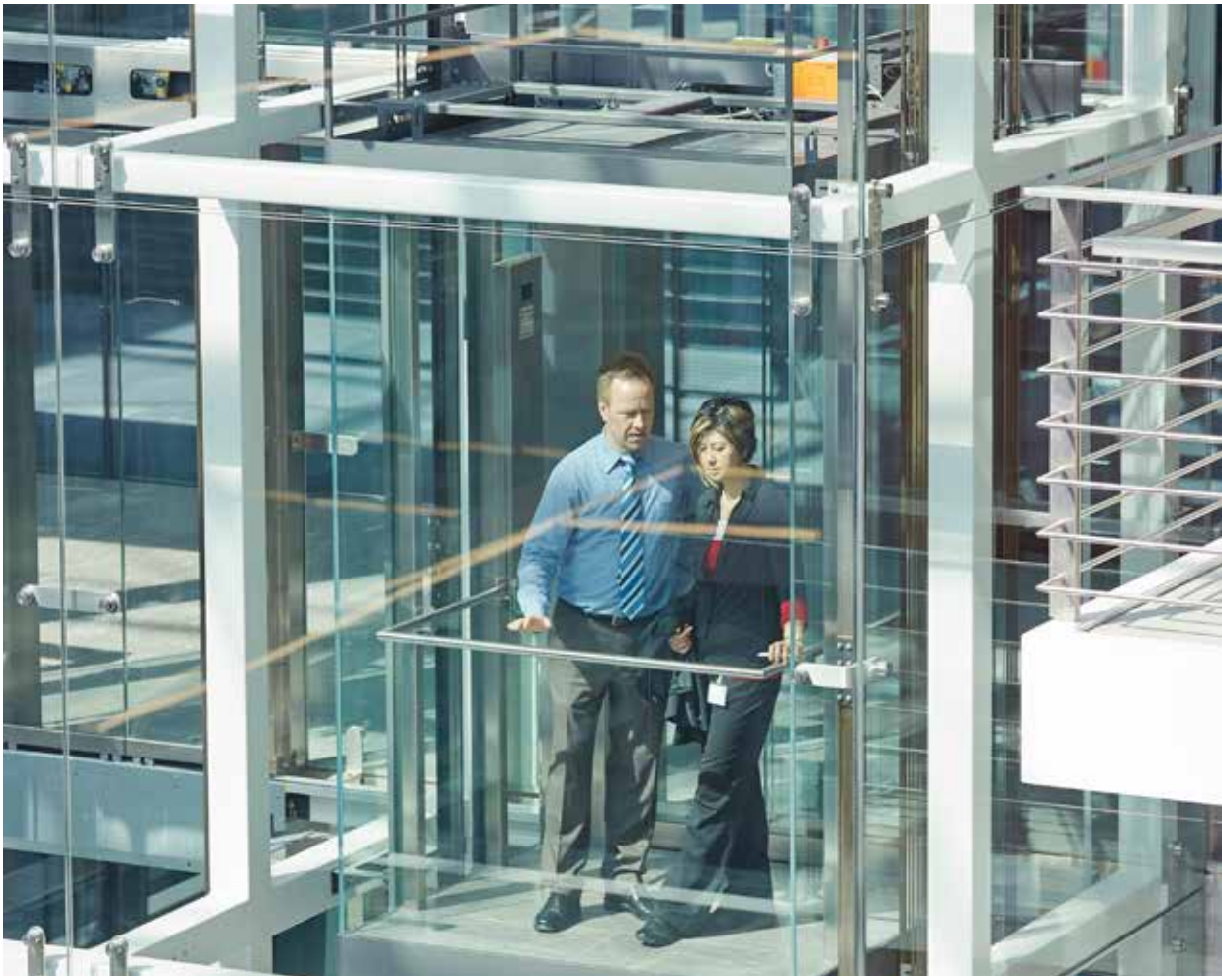
Tirando a fraude das sombras

Pesquisa Global sobre Fraudes e Crimes Econômicos 2018



pwc

www.pwc.com.br

Apresentação

Fernando Alves
Sócio-presidente
PwC Brasil

Leonardo Lopes
Sócio - Forensic Services
PwC Brasil

A edição deste ano da Pesquisa Global sobre Fraudes e Crimes Econômicos revela que metade das empresas no Brasil e no mundo sofreu algum tipo de crime ou fraude nos últimos dois anos. É o maior índice registrado desde a primeira edição da pesquisa, em 2001. Os resultados revelam também que os investimentos na prevenção e mitigação cresceram, praticamente, na mesma proporção.

Os líderes empresariais estão mais conscientes dos riscos e a tecnologia tem sido um aliado importante para geri-los. Adicionalmente, as mudanças nas legislações e nos cenários geopolíticos estão dando mais visibilidade às motivações e às formas de atuação dos fraudadores.

A pesquisa ainda indica outro fator importante por trás dos resultados: os gestores estão, cada vez mais, sendo responsabilizadas e penalizadas pelas fraudes e crimes econômicos ocorridos em suas respectivas organizações.

Mesmo com a maior conscientização, ainda há muitos pontos cegos que impedem identificar claramente a ocorrência de fraudes. Neste relatório, apresentamos os resultados da nossa pesquisa e as medidas que vêm sendo adotadas para combater fraudes e crimes econômicos de maneira mais eficaz.

Esperamos que a leitura seja útil, reveladora e ofereça ideias para serem consideradas e implementadas.

Introdução

Metade das organizações globais diz ter sido vítima de fraudes e de crimes econômicos ao longo dos últimos dois anos, segundo a nossa Pesquisa Global sobre Fraudes e Crimes Econômicos 2018. Nossa experiência de assessoria a empresas sobre esse assunto indica, no entanto, que esses índices podem ser muito maiores. *O que estaria acontecendo com a outra metade dos participantes deste estudo?*

A realidade é que poucas empresas estão totalmente conscientes dos riscos de fraude que enfrentam. Por isso, a nossa Pesquisa Global sobre Fraudes e Crimes Econômicos deste ano, com base em dados valiosos fornecidos por mais de 7.200 participantes de 123 países, pretende tirar a fraude das sombras - e lançar luz sobre alguns dos desafios estratégicos mais importantes que toda organização enfrenta.

O principal concorrente que você não sabia ter

O combate à fraude ganhou destaque e hoje é uma questão de negócios essencial. Vai longe o tempo em que o problema era visto como um incidente isolado de mau comportamento, um incômodo caro ou uma mera questão de *compliance*. Isso se deu porque a escala e o impacto da fraude cresceram de forma muito significativa em um mundo movido pela tecnologia digital. Na verdade, ela pode ser encarada por si só como um grande negócio – uma iniciativa facilitada pela tecnologia, inovadora, oportunista e muito difundida. Encare-a como o seu maior concorrente, que você nem sabia que existia.

Não é difícil ver como chegamos a esse ponto. Por um lado, a tecnologia avançou a passos largos, ajudando os fraudadores a mirar objetivos mais estratégicos e a sofisticar seus métodos. Por outro lado, os regimes regulatórios em grande parte do mundo tornaram-se muito mais fortes, com uma aplicação da lei muito mais rigorosa, e contando frequentemente com a cooperação transnacional. Além disso, diante de casos de corrupção e outros escândalos de grande repercussão, as expectativas do público em todo o mundo estão convergindo para um padrão comum de transparência e responsabilidade.

Cada vez mais empresas, organizações e Estados nacionais reconhecem que a corrupção e a fraude representam um obstáculo à capacidade de competir no cenário mundial e que esses problemas simplesmente se tornaram muito onerosos para serem ignorados.

Uma tempestade perfeita de riscos

Em uma época de vigilância incomparável do público, as organizações enfrentam hoje uma "tempestade perfeita" de riscos de fraude – internos e externos – com impactos regulatórios e para sua reputação. É o momento certo, portanto, para as organizações adotarem uma visão nova e mais holística da fraude. Uma visão que reconheça o problema como uma ameaça real: não apenas um "custo de fazer negócios", mas uma indústria subterrânea com tentáculos em todos os países, setores de atuação e funções corporativas. Como o problema se esconde nas sombras, a falta de consciência a respeito da fraude em uma organização é uma atitude altamente perigosa.

A questão central, portanto, não é: a sua organização é vítima da fraude? Mas sim: você está ciente de como a fraude afeta a sua organização? Você está lutando às cegas ou de olhos bem abertos?

A fraude que você não vê é a mais importante

A Pesquisa Global sobre Fraudes e Crimes Econômicos deste ano mostra que, embora haja uma crescente conscientização sobre os perigos desse tipo de crime, poucas empresas estão plenamente cientes do cenário de riscos que elas enfrentam individualmente. Essa lacuna de consciência é o que queremos abordar neste relatório. Exploramos nas próximas páginas não só o que é visível, mas os pontos cegos que impedem as empresas de ver a fraude em seu ambiente, e o que elas podem e devem fazer a respeito.

O que a nossa pesquisa nos diz então sobre as medidas que a sua organização pode tomar hoje para combater a fraude de forma mais eficaz?

Quatro passos para combater a fraude

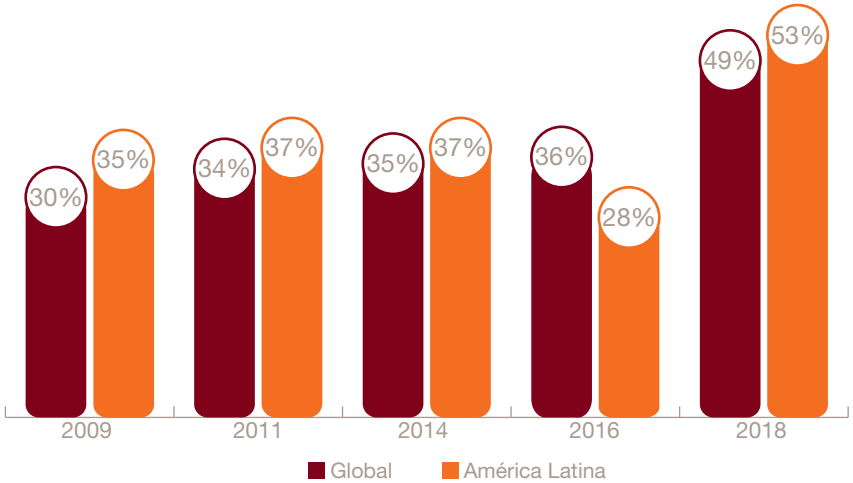
Reconheça a fraude ao deparar-se com ela

A fraude está mesmo aumentando ou apenas a nossa consciência dela?

Este ano, 49% dos participantes da pesquisa global disseram que suas empresas foram vítimas de fraudes e crimes econômicos, um aumento em relação aos 36% de 2016. Na América Latina, a alta também foi acentuada, de 28% para 53%. No Brasil, o percentual passou de 12% para 50%. Acreditamos que esse aumento se deva a uma combinação de fatores: maior consciência global a respeito da fraude, maior número de respostas à pesquisa e maior clareza sobre o que a fraude realmente significa (uso intencional de meios fraudulentos ou de outra conduta criminosa para obter dinheiro, propriedades ou direitos de um indivíduo ou para causar um prejuízo econômico).

As empresas hoje enfrentam uma 'tempestade perfeita' de riscos de fraude – internos e externos – com impactos regulatórios e para sua reputação.

Figura 1: O índice informado de crimes econômicos está aumentando

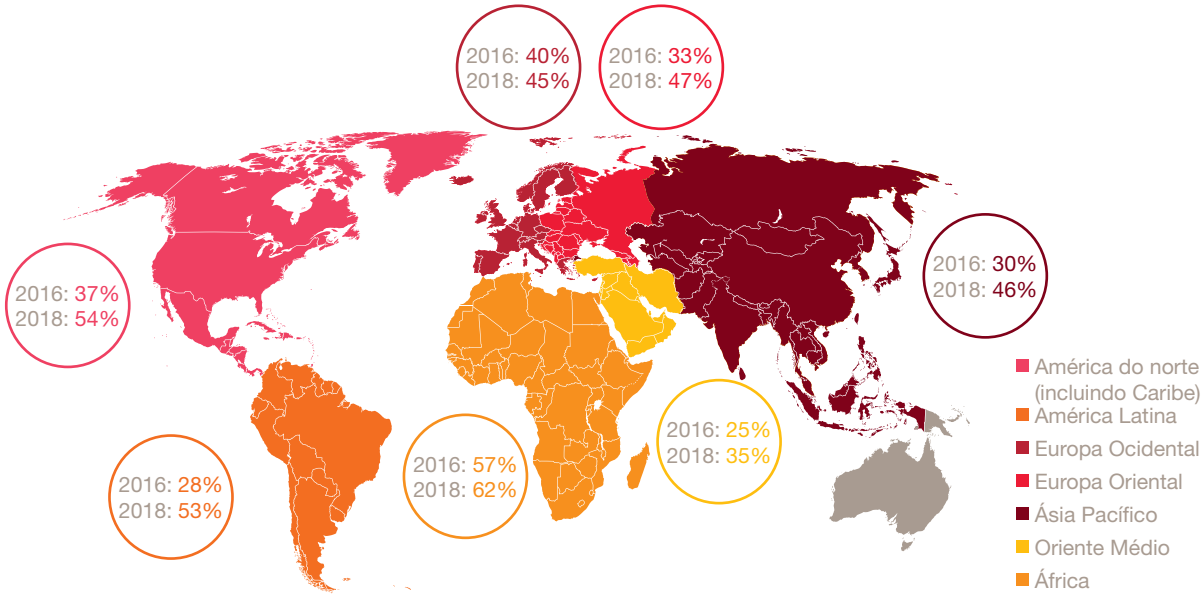


Q. Sua organização foi vítima de alguma fraude e/ou crime econômico nos últimos 24 meses?

Fonte: *Pesquisa Global sobre Fraudes e Crimes Econômicos 2018* da PwC

Obs.: os percentuais dos gráficos deste relatório nem sempre somam 100% por questões de arredondamento.

Figura 2: O índice informado de crimes econômicos aumentou em todas as regiões



Q. Sua organização foi vítima de alguma fraude e/ou crime econômico nos últimos 24 meses?

Fonte: *Pesquisa Global sobre Fraudes e Crimes Econômicos 2018* da PwC

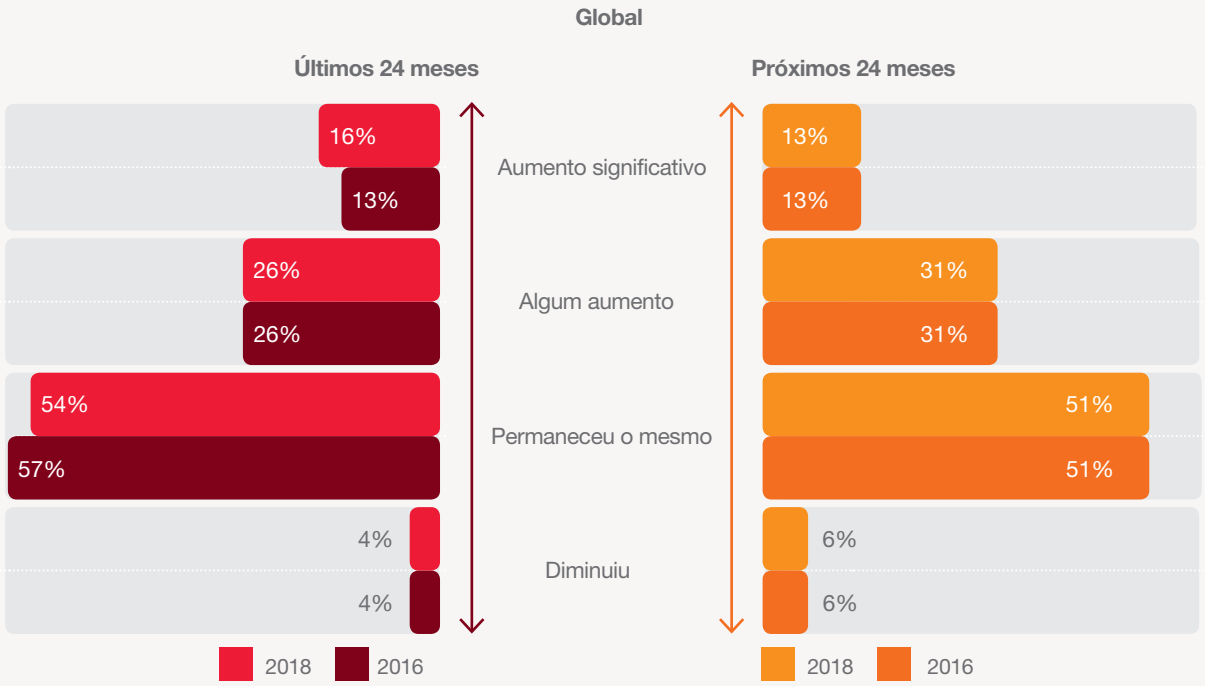
Acompanhando a alta no índice de crimes econômicos relatados, nossa pesquisa revela também que as empresas estão gastando mais para combater o problema.

- No Brasil, 52% dos participantes aumentaram as despesas com o combate à fraude nos últimos dois anos, contra 42% no mundo. A pesquisa anterior já havia registrado um aumento de 34% no país e de 39% no mundo.
- 38% dos brasileiros (44% no mundo) planejam continuar aumentando esses gastos nos próximos dois anos.

Mas onde esse dinheiro está sendo gasto? As organizações estão usando ferramentas de tecnologia e análise de dados cada vez mais poderosas. Além de fortalecer os controles baseados em tecnologia, muitas também expandiram seus programas de denúncias, e a maioria mantém a liderança da empresa informada: entre os crimes econômicos considerados mais graves para o negócio, 97% foram levados ao conhecimento da diretoria ou de líderes encarregados pela governança no Brasil (contra 91% no mundo).

Algumas dúvidas, porém, permanecem: essas medidas refletem uma mudança real para abordagens mais proativas contra a fraude e o crime econômico? Ou são apenas uma ação de retaguarda, motivada por um claro fortalecimento da legislação anticorrupção/antissuborno e sua aplicação cada vez mais globalizada? Em outras palavras, estamos deixando de perceber algo vital na luta contra a fraude? Os resultados da nossa pesquisa sugerem fortemente que sim.

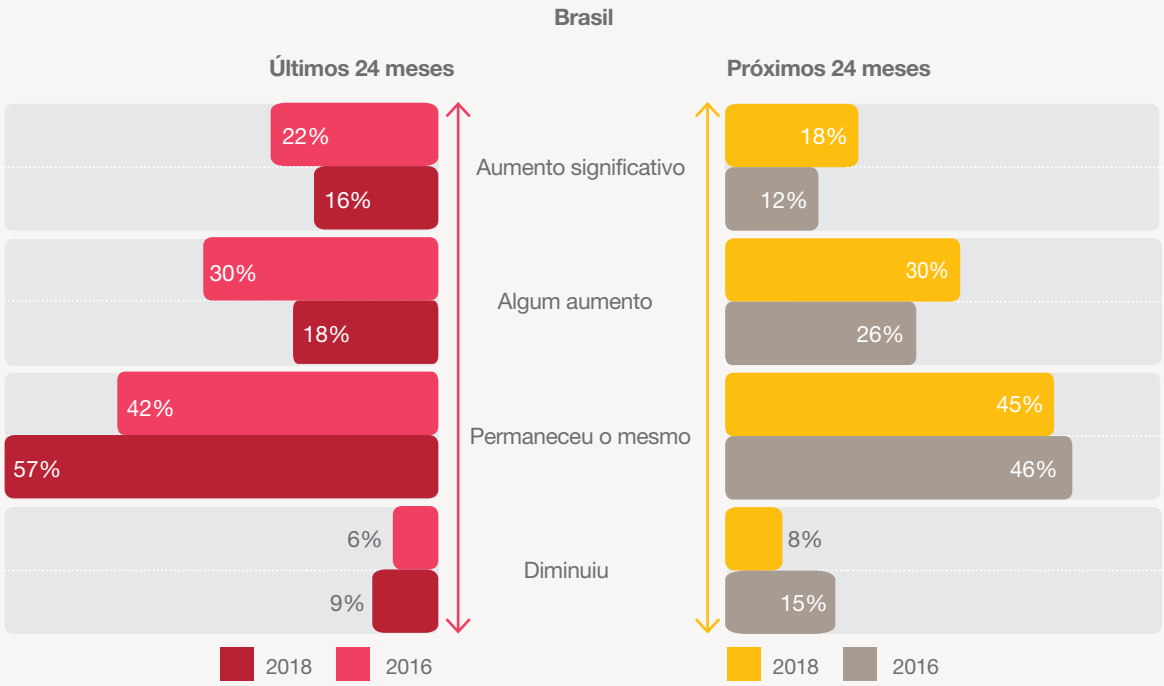
Figura 3: Os gastos com o combate à fraude continuam a crescer



As avaliações de risco são o primeiro passo na prevenção da fraude antes que ela crie raízes

Apesar do aumento dos gastos, muitas organizações ainda estão lidando com a prevenção à fraude de uma maneira reativa/defensiva

- **Apenas 58% das organizações brasileiras (54% das globais) disseram ter realizado algum tipo de avaliação de risco de fraude ou crime econômico nos últimos dois anos.**
- Apenas 41% avaliaram sua vulnerabilidade aos ataques cibernéticos (46% das globais).
- O Brasil aparece à frente da média global nas avaliações de risco realizadas nas áreas essenciais de prevenção ao suborno e à corrupção (42% x 33%) ou controles de exportação e sanções (21% x 19%), mas não de combate à lavagem de dinheiro (15% x 23%).
- **Do total, 7% dos participantes não realizaram nenhuma avaliação de risco nos últimos 24 meses (abaixo da média global de 10%).**



Q. Q. Como a sua organização ajustou/ajusta o volume de recursos usados para combater fraudes e/ou crimes econômicos?

Fonte: *Pesquisa Global sobre Fraudes e Crimes Econômicos 2018* da PwC

No entanto, as regras para as empresas estão mudando de forma profunda e irreversível. A tolerância por parte do público ao mau comportamento corporativo e/ou pessoal está terminando. Não só a sensibilidade à má conduta corporativa alcançou um recorde histórico como também algumas empresas e líderes estão sendo responsabilizados por comportamentos passados, quando as "regras não declaradas" dos negócios talvez fossem menos rígidas. Nossa 21ª Pesquisa Global com CEOs, de 2018, destaca esse tema: os líderes executivos entrevistados citam a falta de confiança e de responsabilidade da liderança como duas das maiores ameaças empresariais ao crescimento.

Isso aponta para o aumento dos riscos quando ocorrem incidentes de fraude ou crime econômico – e para uma necessidade maiorde as organizações assumirem a iniciativa da prevenção antes que esses riscos possam se enraizar. Avaliações de risco de fraude podem ajudar as organizações em relação a esse tema ao identificarem as fraudes específicas que elas precisam procurar. Além disso, essas avaliações são cada vez mais recomendadas pelos reguladores em ações de execução.

59%

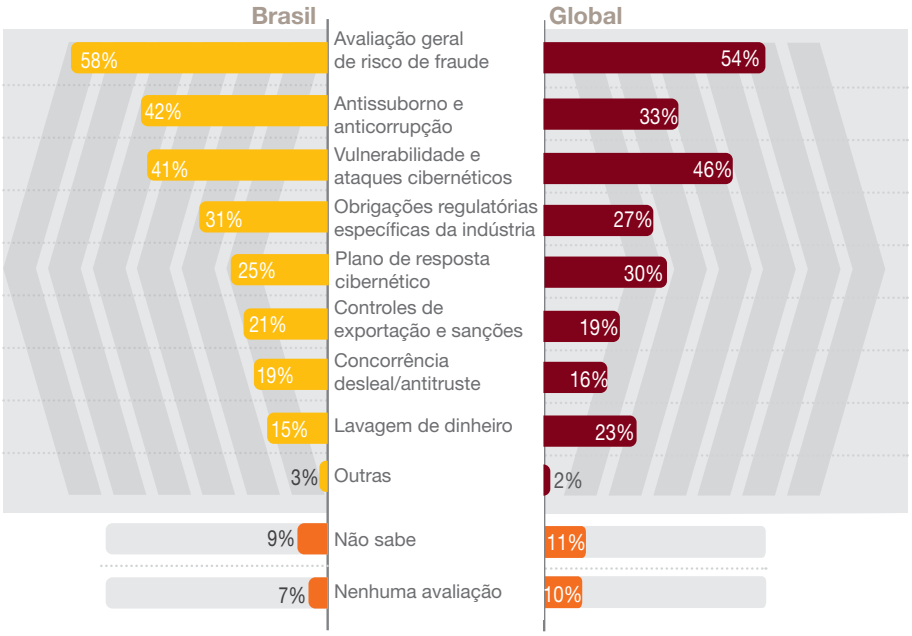
dos CEOs globais concordam ou concordam fortemente que as organizações estão enfrentando pressões crescentes para responsabilizar seus líderes por qualquer má conduta organizacional.

71%

dos CEOs globais medem a confiança entre a força de trabalho e a alta liderança da organização.

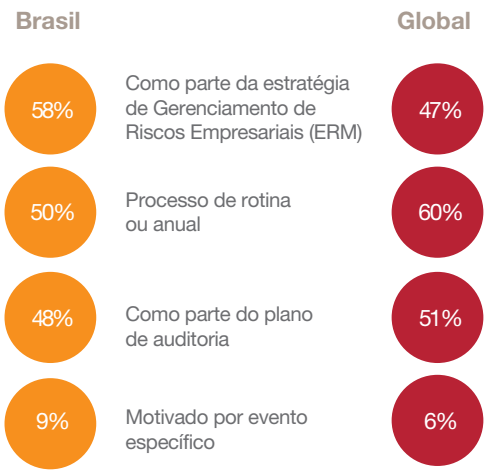
Fonte: *21ª Pesquisa Anual Global com CEOs* da PwC

Figura 4: Menos de metade de todas as organizações realizaram avaliações de risco específicas nos últimos dois anos



Q. Nos últimos 24 meses, sua organização realizou uma avaliação de risco de fraude em algumas das seguintes áreas?

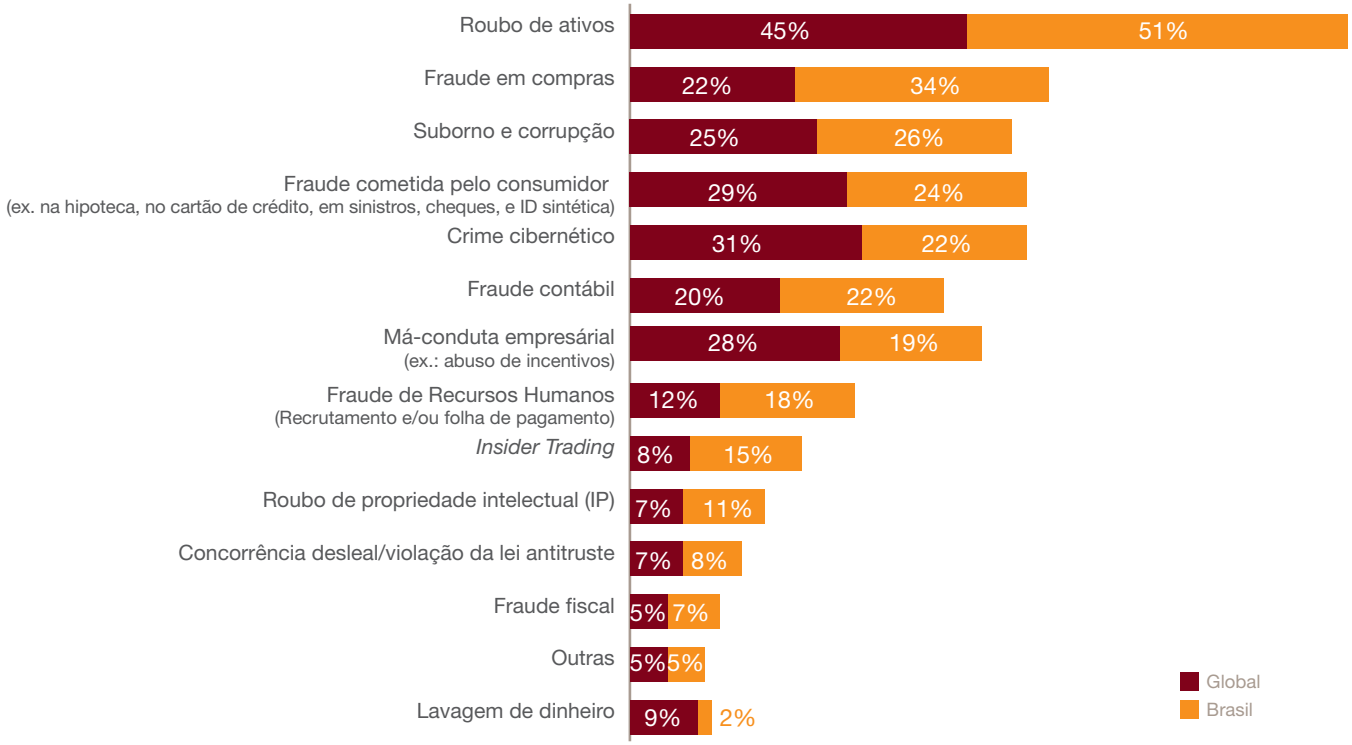
Fonte: *Pesquisa Global sobre Fraudes e Crimes Econômicos 2018* da PwC

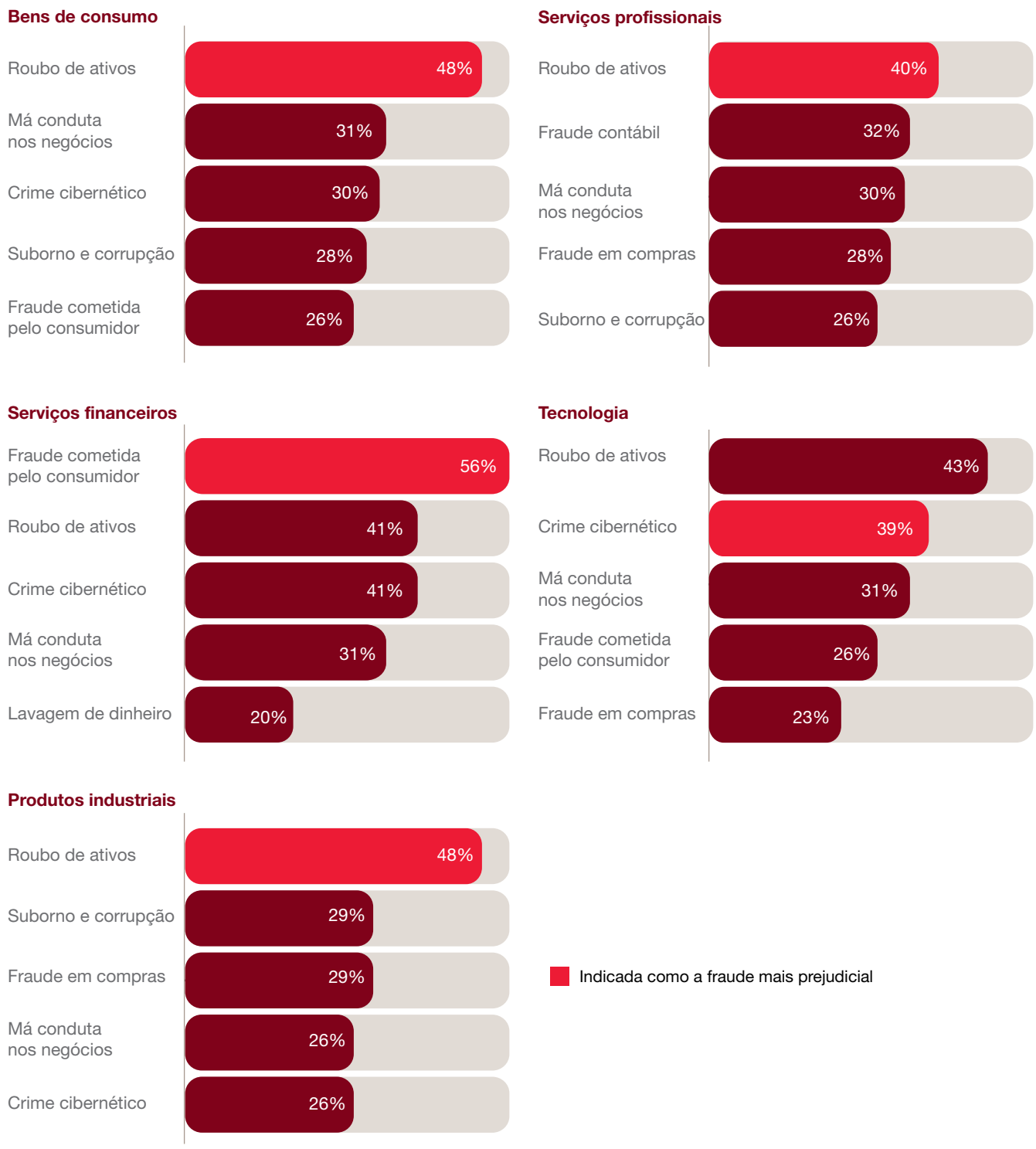


Q. O que o levou a sua organização a realizar a(s) avaliação(ões) de risco?

Fonte: *Pesquisa Global sobre Fraudes e Crimes Econômicos 2018* da PwC

Figura 5: O roubo de ativos, a fraude cometida pelo consumidor e o crime cibernético foram as fraudes relatadas com mais frequência em todas as indústrias no mundo. No Brasil, roubo de ativos e fraude em compras são os tipos mais frequentes.





Q. Quais tipos de fraudes e/ou crimes econômicos sua organização enfrentou em seu país nos últimos 24 meses?

Fonte: *Pesquisa Global sobre Fraudes e Crimes Econômicos 2018* da PwC

Risco de conduta: O “risco oculto” por trás da maioria das fraudes

Dois tipos de fraude cresceram a tal ponto que passamos a medi-las como ameaças separadas pela primeira vez. São elas a fraude cometida pelo consumidor (24% no Brasil e 29% no mundo) e a má conduta empresarial nos negócios (19% no Brasil e 29% no mundo), definida como qualquer tipo de fraude ou trapaça realizada por empresas contra o mercado ou o público em geral (práticas enganosas associadas a fabricação, vendas, marketing ou entrega de produtos ou serviços a clientes, consumidores ou público em geral). No mundo, essas fraudes representam, respectivamente, o terceiro e o quarto tipos relatados com mais frequência, atrás apenas de roubo de ativos e crimes cibernéticos. No Brasil, elas aparecem em quarto e quinto lugares entre os tipos relatados com mais frequência.

Essas mudanças de metodologia refletem o reconhecimento crescente de uma ampla categoria de riscos de fraude: o “risco de conduta”, ou seja, o risco de que as ações de seus empregados impeçam a entrega de resultados justos aos clientes ou a integridade do mercado. E, ao contrário de interrupções operacionais e ameaças externas (que podem ser verificadas por controles internos), o risco de conduta requer uma resposta mais holística – e uma mudança de atitude.

Atualmente, muitas empresas tratam o *compliance*, a ética e a gestão de riscos corporativos como funções separadas – que, em alguns casos, geralmente operam de maneira isolada. Mas, como acontece com todos os silos organizacionais, essas funções raramente representam (ou atuam como) um todo estratégico. As partes de uma organização que investigam a fraude, as partes que gerenciam o risco de fraude e as partes que relatam a fraude para o conselho ou para os reguladores são desarticuladas.

Quando isso acontece, surgem lacunas operacionais e as fraudes podem acabar sendo muito facilmente varridas para baixo do tapete ou encaradas como um “problema de outra pessoa” – em detrimento da eficácia geral da prevenção de fraudes, do desempenho financeiro e dos resultados regulatórios.

Uma abordagem mais inovadora é reformular essas funções como componentes do risco de conduta. Isso permite que a empresa meça e gerencie melhor o *compliance* de forma horizontal e incorpore essas questões em seu processo de decisão estratégica. Também significa que a fraude e os desvios éticos podem ser abordados de forma menos apaixonada, como um fato da vida com o qual toda organização precisa lidar. Além disso, adotar essa postura mais sistemática (e realista) em relação ao risco de conduta gera eficiência de custos entre os programas de ética, fraude e conformidade anticorrupção. É uma medida para romper barreiras entre as principais funções de combate à fraude e ajudar a tirá-la das sombras.

Como procurar a fraude nos lugares certos

Nossa pesquisa global revelou um aumento significativo da participação de agentes internos nos crimes econômicos: de 46%, em 2016, para 52% este ano (no Brasil, o índice ficou estável, em 58%). Houve também no mundo um aumento acentuado na proporção desses crimes atribuídos à gerência executiva, de 16% para 24%. O Brasil seguiu tendência contrária: o índice caiu de 40%, em 2016, para 26% este ano. O mesmo aconteceu na gerência média, que registrou uma queda de 47% para 26%, enquanto no mundo o índice permaneceu praticamente estável em 37%. A análise dos dados permite observar que, no Brasil, os agentes internos têm quase o dobro da propensão dos externos para cometer as fraudes mais graves em uma empresa. No mundo, essa diferença é de apenas um terço para os agentes internos.

No entanto, um dos maiores pontos cegos – e uma das maiores ameaças – em uma empresa em relação à fraude tem a ver não com os empregados, mas com as pessoas com as quais ela faz negócios. São os terceiros com os quais as empresas têm relações regulares e rentáveis: agentes, fornecedores, provedores de serviços compartilhados e clientes. Em outras palavras, pessoas e organizações de quem se espera um certo grau de confiança mútua, mas que, na verdade, podem estar roubando da empresa.

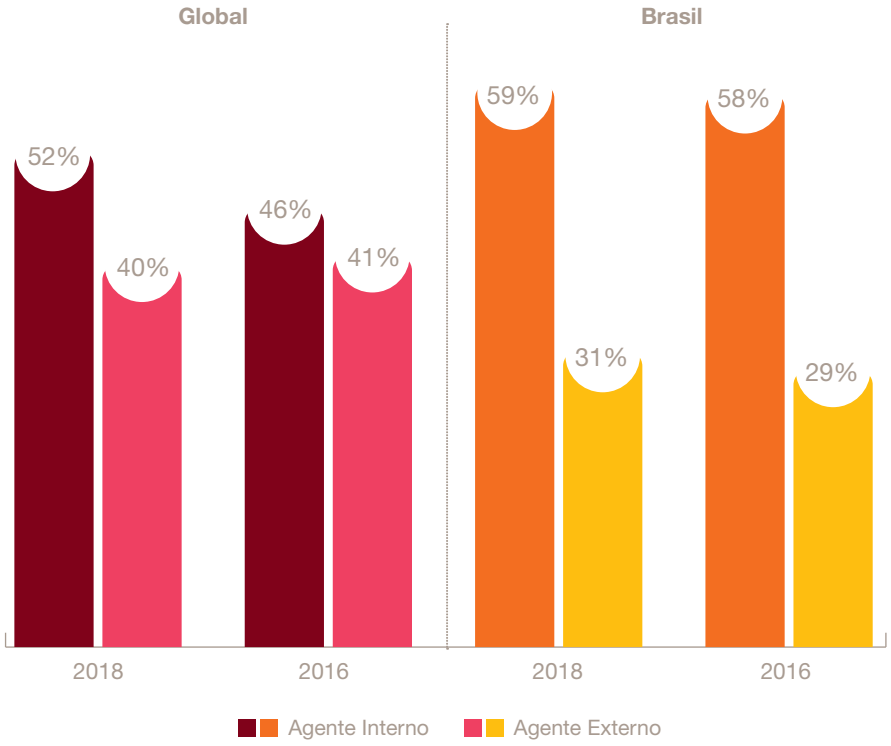
26%

das fraudes internas relatadas no Brasil foram cometidas por agentes internos. Houve queda em relação a 2016; no mundo, onde a tendência é de alta, foram 24%.

63%

dos autores externos de fraudes no Brasil eram "falsos amigos" da organização – intermediários, fornecedores, provedores de serviços compartilhados e clientes.

Figura 6: Os agentes internos são os principais autores das fraudes



Q. Qual foi o principal autor da fraude mais grave?

Fonte: *Pesquisa Global sobre Fraudes e Crimes Econômicos 2018* da PwC

Adote uma abordagem dinâmica

Os líderes executivos são responsáveis

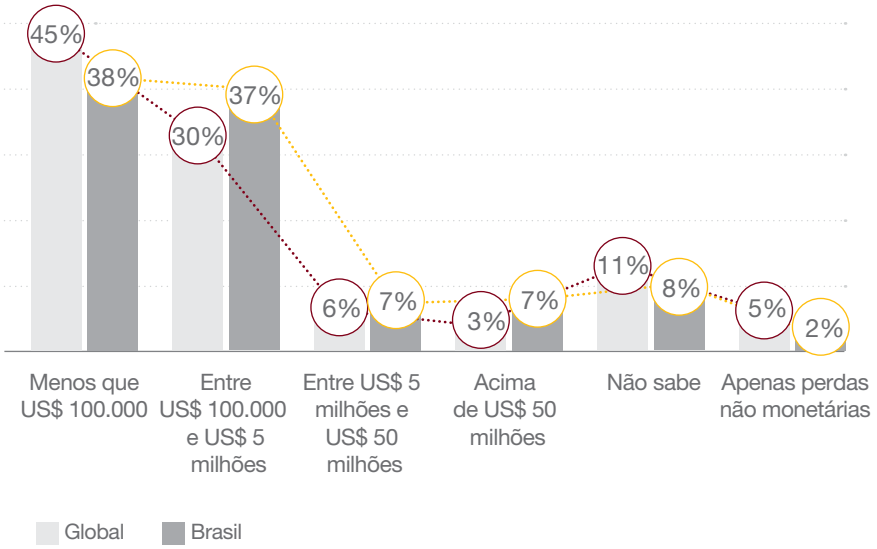
Nossa pesquisa destaca que o custo direto da fraude – e de suas consequências – pode ser substancial. E, após a avaliação dos custos secundários, como investigações e outras intervenções, a despesa total pode disparar.

Quando os custos financeiros de uma fraude afetam os resultados, é natural que a gerência executiva tenha de prestar contas ao conselho e aos acionistas. Hoje, essa responsabilidade não termina aí. Na verdade, ela apenas começa.

43%

dos brasileiros disseram que suas organizações gastaram tanto ou mais em investigações e outras intervenções do que perderam diretamente com a fraude; no mundo, foram 46%.

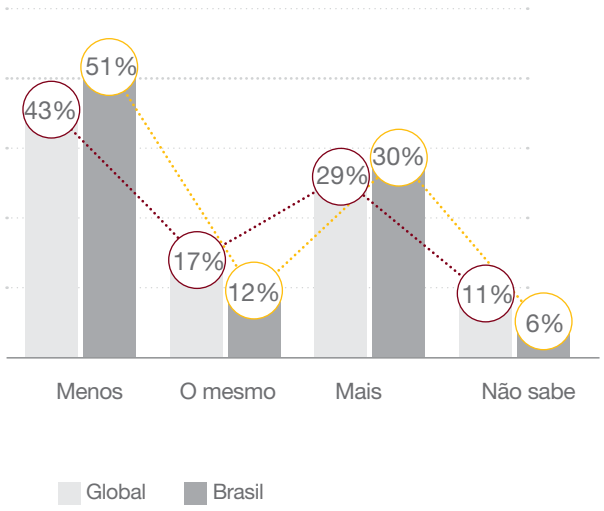
Figura 7: As perdas monetárias diretas causadas pela fraude podem ser substanciais



Q. Em termos financeiros, aproximadamente quanto você acha que sua organização pode ter perdido diretamente com o crime econômico mais grave nos últimos 24 meses?

Fonte: *Pesquisa Global sobre Fraudes e Crimes Econômicos 2018* da PwC

Figura 8: O montante gasto em investigações e outras intervenções em consequência da fraude é significativo



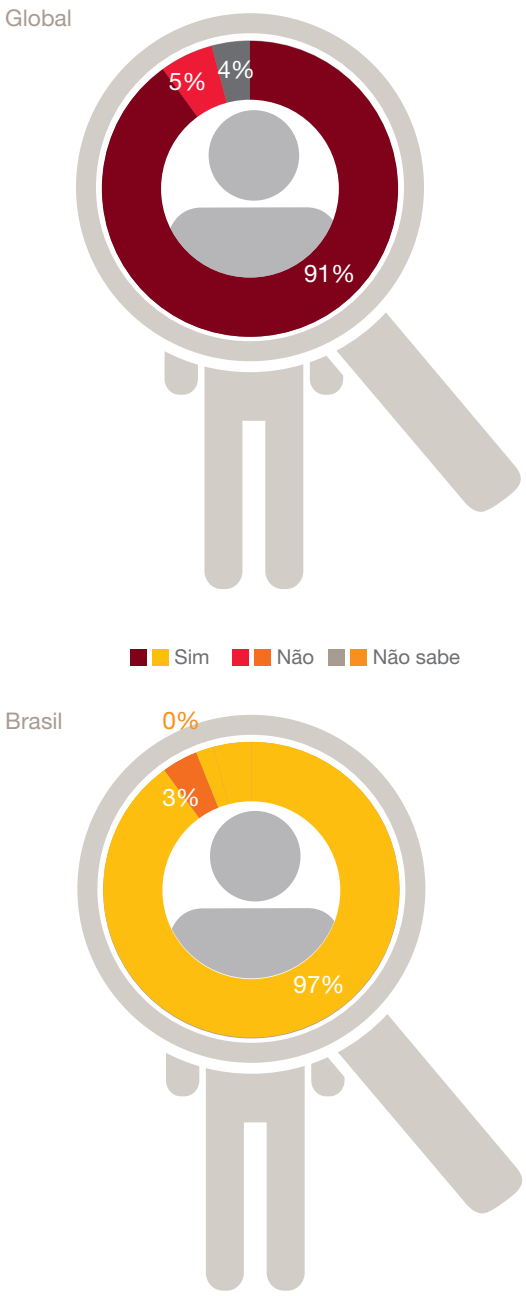
Q. Como resultado do mais grave crime econômico ocorrido nos últimos 24 meses, o valor gasto pela sua organização em investigações e/ou outras intervenções é maior, menor ou o mesmo que o valor perdido com o crime?

Fonte: *Pesquisa Global sobre Fraudes e Crimes Econômicos 2018* da PwC

Os líderes executivos são vistos cada vez mais como a personificação de uma organização – capazes de avaliar precisamente, em todos os momentos, cada aspecto da cultura e da operação organizacional. Assim, quando ocorrem problemas éticos ou de *compliance*, esses líderes muitas vezes são responsabilizados pessoalmente – tanto pela opinião pública quanto pelos reguladores. Seja isso merecido ou não, uma coisa é clara: a gerência executiva não pode mais recorrer à ignorância como desculpa.

Nossa pesquisa mostra que a esmagadora maioria dos incidentes mais graves de fraude foi informada à gerência executiva: 91% no mundo e 97% no Brasil. Além disso, 17% dos participantes no mundo indicaram que o CEO é o principal responsável pelo programa de ética e *compliance* em suas organizações. No Brasil, o percentual foi de apenas 8%. Isso mostra nitidamente a maneira como o *front office* está gerenciando a crise – e até que ponto as empresas estão (ou não) ajustando seus perfis de risco de forma adequada.

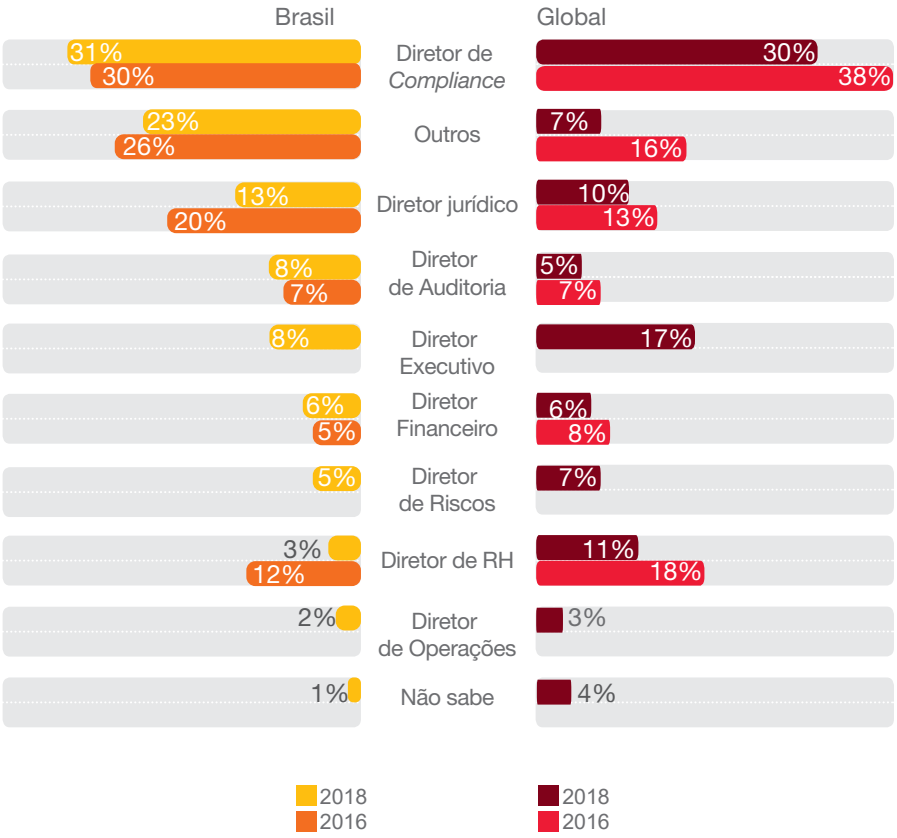
Figura 9: As organizações estão relatando fraudes graves à gerência executiva



Q. O incidente mais grave que você indicou foi levado ao conhecimento e à atenção dos integrantes do conselho ou dos líderes seniores encarregados da governança?

Fonte: *Pesquisa Global sobre Fraudes e Crimes Econômicos 2018* da PwC

Figura 10: A responsabilidade pelo programa de ética e *compliance* é principalmente da gerência executiva



Q. Quem tem a responsabilidade principal pelo programa de ética e *compliance* em sua organização?

Fonte: *Pesquisa Global sobre Fraudes e Crimes Econômicos 2018* da PwC (Algumas alternativas não estavam presentes no questionário de 2016)

Embora tradicionalmente a prevenção e a detecção de fraudes sejam uma atribuição da segunda linha de defesa da organização – gestão de riscos, departamento jurídico, área de conformidade, entre outras – as empresas hoje incorporam cada vez mais suas medidas de prevenção a fraude na primeira linha de defesa.

Isso pode indicar o início de uma mudança importante, por meio da qual os recursos de prevenção e detecção de fraudes da primeira linha de defesa amadureçam e se fortaleçam. Ao fazerem isso, eles permitirão que a segunda linha de defesa adote uma abordagem mais tradicional – de governança e supervisão e de definição de políticas, modelos e tolerância a riscos.

Essa é uma questão importante em um mundo no qual os limites entre as indústrias, a tecnologia e os órgãos reguladores são menos claros – e no qual os fraudadores miram além dos alvos tradicionais e altamente protegidos dos serviços financeiros em busca de pontos fracos que facilitem suas ações.

As más notícias voam: o risco de reputação ultrapassa o risco regulatório

Uma forte mudança na maneira como o mundo encara a fraude e a corrupção aconteceu ao longo dos últimos anos. E os dados da nossa pesquisa refletem essa demanda, hoje acentuada, por responsabilidade, tanto do público como de reguladores, nos setores público e privado.

Esse fenômeno não se limita aos mercados desenvolvidos. Nas mais diferentes culturas, de todas as regiões do planeta, estamos vendo sinais de convergência entre as normas relacionadas à transparência e as expectativas de conduta, um movimento impulsionado pelos órgãos reguladores e pela opinião pública. Em países onde a legislação e a transparência tradicionalmente eram frágeis, observamos nas ruas a indignação do público – políticos e líderes empresariais foram presos e até governos derrubados.

Para a organização que foi vítima do crime, que talvez só tenha informações fragmentadas ou indícios sobre o que aconteceu, isso pode representar um sério risco reputacional. Ela pode ser fortemente punida pelos mais diferentes públicos por demonstrar incapacidade de reagir adequadamente ao problema – muito antes que a gerência executiva da empresa tenha um plano sobre o que fazer.

Figura 11: A detecção da fraude sobe para a primeira linha de defesa

Sua reputação não está sujeita a nenhuma jurisdição, lei ou garantia processual.

55%

dos brasileiros (54% no mundo) esperam que mudanças no ambiente regulatório exerçam impacto maior na suas organizações nos próximos dois anos.

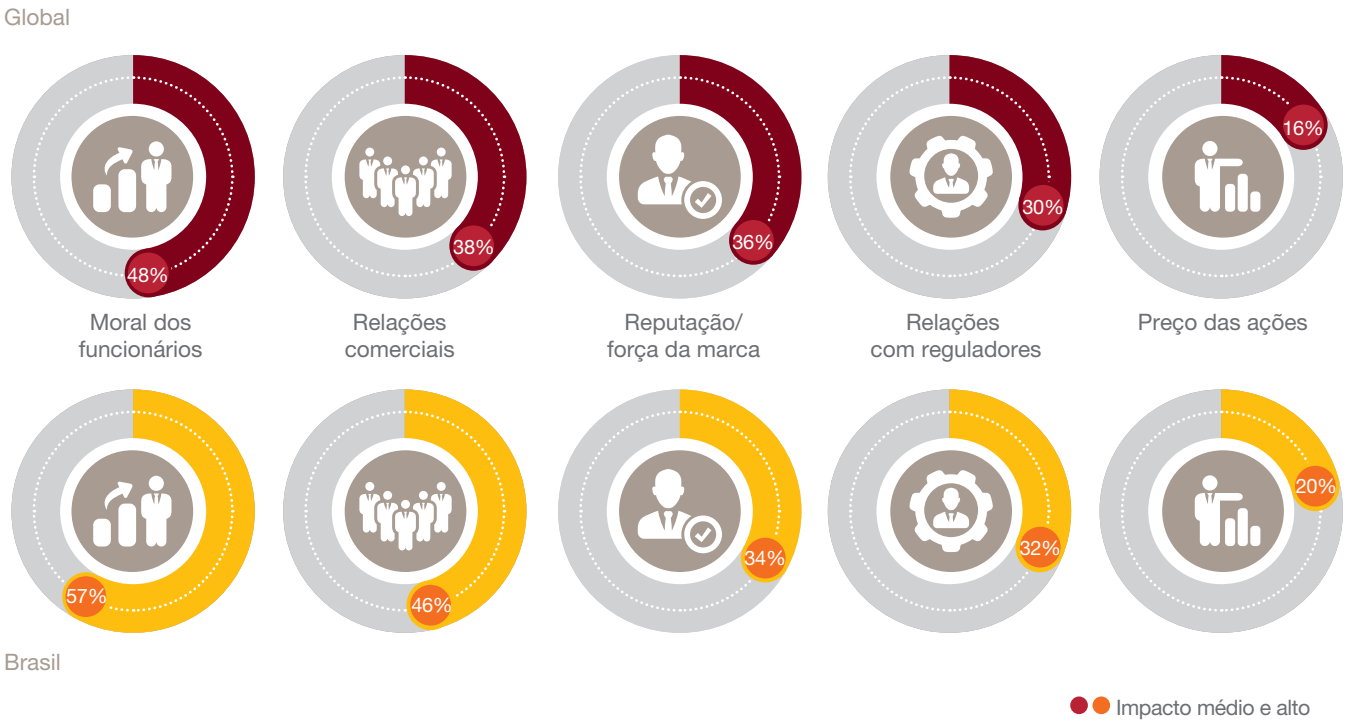
Isso ocorre porque, na era da transparência radical, as empresas costumam ter dificuldade para enxergar quando um problema pode se tornar uma crise. Isso acaba ficando a cargo da opinião pública. Além disso, as regras da sociedade mudam mais rapidamente que as dos órgãos reguladores, e a tolerância em relação a quem as desobedece é pequena. Os reguladores, por definição, operam dentro de uma jurisdição limitada e sob regras bem definidas. Já a reputação de uma empresa não está sujeita a nenhuma jurisdição, lei ou garantia processual.

Os executivos que ouvimos classificaram de forma consistente o dano à reputação como um dos principais impactos negativos de várias formas de crime econômico, sendo a percepção do público (reputação/força da marca, relações comerciais e preço das ações) a mais afetada.

O *compliance* regulatório continua essencial – talvez até mais do que antes. De modo geral, os requisitos regulatórios e de prestação de informações, que envolvem comportamentos legais e éticos, estão ficando cada vez mais rigorosos. A vigilância e a repressão ao crime também estão aumentando em todo o mundo, enquanto a cooperação regulatória entre os países se torna mais rotineira.

No Brasil, 62% das empresas envolvidas na movimentação de dinheiro (e/ou em qualquer uma das seguintes linhas de negócios: instituições financeiras, fundos mútuos, empresas de serviços monetários, corretores, companhias de seguros ou revendedores de metais preciosos, pedras ou joias) disseram ter passado por uma ação regulatória ou uma inspeção relacionada à lavagem de dinheiro nos últimos dois anos. O percentual mais que dobrou em relação ao resultado de 2016 (28%). No mundo, embora também tenha sido registrado um aumento, ele foi muito menos expressivo: de 50% para 54%. Pouco mais de metade dos participantes (55% no Brasil e 54% no mundo) espera que mudanças recentes no ambiente geopolítico em termos regulatórios exerçam um impacto maior nas suas organizações nos próximos dois anos.

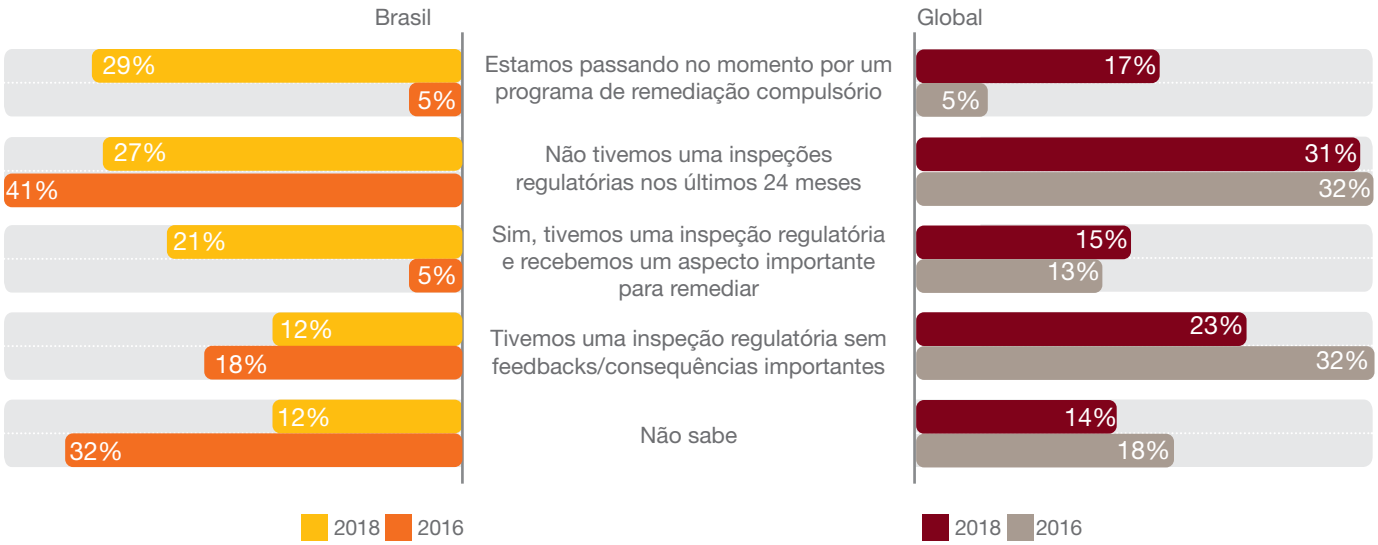
Figura 12: : A fraude e o crime econômico impactam todos os elementos do negócio



Q. Qual foi o impacto do crime econômico mais grave nos seguintes aspectos das operações da sua empresa?

Fonte: *Pesquisa Global sobre Fraudes e Crimes Econômicos 2018* da PwC

Figura 13: O número de inspeções e execuções regulatórias continua a crescer



Q. A sua organização passou por alguma execução/inspeção regulatória relacionada a lavagem de dinheiro nos últimos 24 meses?

Fonte: *Pesquisa Global sobre Fraudes e Crimes Econômicos 2018* da PwC

Há relação entre desenvolvimento econômico e fraude?

Nossa pesquisa revela aspectos interessantes sobre abordagens globais em relação à fraude, que poderiam oferecer indicadores valiosos para as nações em sua jornada de desenvolvimento econômico.

Nos países em desenvolvimento, 58% das empresas envolvidas com movimentação de dinheiro (e/ou em qualquer uma das seguintes linhas de negócios: instituições financeiras, fundos mútuos, empresas de serviços monetários, corretores, companhias de seguros ou revendedores de metais preciosos, pedras ou joias) registraram ações de repressão e inspeção regulatória relacionadas a lavagem de dinheiro nos últimos dois anos, em comparação com 48% nos países desenvolvidos.

Nesses mesmos países, 15% das empresas relataram que esperam aumentar significativamente os recursos destinados a investimentos para combater a fraude nos próximos 24 meses. Nos países desenvolvidos, esse percentual é de 9% apenas.

Os participantes da pesquisa em países em desenvolvimento afirmaram que o crime econômico é cometido com mais frequência por agentes internos (59%, contra 39% nos países desenvolvidos).

83%

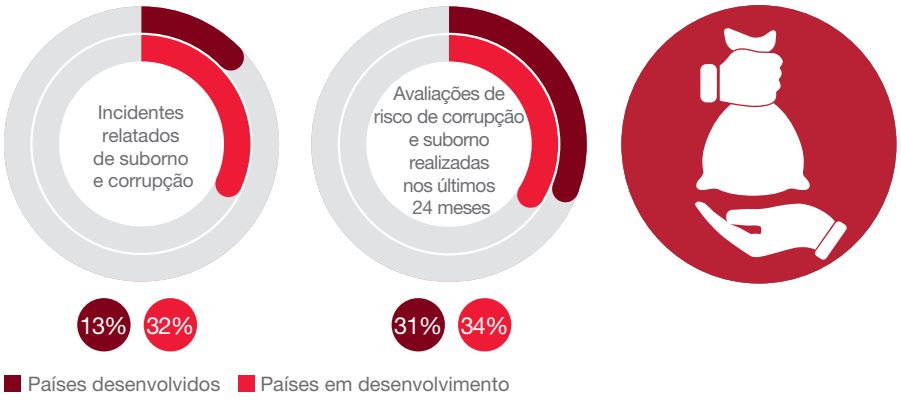
dos CEOs não registraram impactos negativos no crescimento da receita após uma crise bem gerenciada.

Fonte: *CEO Pulse on Crises,* da PwC

"O tom da liderança não deve ser superestimado. O mais importante são as ações e o comprometimento da liderança com o combate a determinadas práticas"

José Figueira,
Sócio, PwC Brasil

Figura 14:Os países em desenvolvimento continuam a ser desafiados pelo risco de corrupção



Fonte: *Pesquisa Global sobre Fraudes e Crimes Econômicos 2018* da PwC

Organizações de países em desenvolvimento são quase três vezes mais propensas a serem vítimas corrupção que as de países desenvolvidos. No entanto, apenas um terço realiza avaliações de risco sobre medidas antissuborno e corrupção, quase o mesmo que o registrado em países desenvolvidos.

Aproveite as pequenas crises para se fortalecer

Em qualquer organização, interrupções operacionais e contratempos são inevitáveis. E os nossos dados sugerem que há uma grande vantagem em aprender com as pequenas crises. De fato, elas podem ser encaradas como um mal que vem para o bem – uma oportunidade para testar seus sistemas e fazer melhorias.

O amadurecimento de um processo – tanto para as empresas quanto para os países – acontece em parte graças ao aprendizado de sobrevivência a crises. Quando um evento não planejado é bem gerenciado, 83% dos CEOs relatam não registrar impactos negativos para o crescimento das receitas. E a gerência executiva será julgada não só pelos resultados financeiros alcançados, mas também pela forma de lidar com o que poderia se tornar uma crise.

É natural que uma empresa relativamente inexperiente apresente respostas automáticas a uma crise que a "ceguem". No entanto, quanto mais a empresa aprende a reagir a pequenas perturbações de maneira eficaz, mais ela fica preparada para responder a megacrises. Ela adquire uma "memória muscular" e passa a adotar uma abordagem mais proativa, desenvolvendo programas de ética e *compliance* maduros e um *front office* testado em situações difíceis.

Utilize o poder defensivo da tecnologia

Como descobrir a abordagem ideal para a tecnologia

Quando o assunto é fraude, a tecnologia pode ser uma faca de dois gumes: ela funciona tanto como ameaça, quanto como defesa para os negócios. Assim, à medida que as empresas passam a ver a fraude essencialmente como um problema de negócios que pode prejudicar seriamente o crescimento, muitas estão fazendo uma mudança estratégica em sua abordagem da tecnologia, por meio de um *business case* para novos investimentos sólidos em áreas como detecção, autenticação e redução de atritos no relacionamento com o consumidor.

As organizações hoje dispõem de uma variedade de tecnologias inovadoras e sofisticadas voltadas para monitorar, analisar, aprender e prever o comportamento humano. Entre elas, estão o aprendizado de máquina, a análise preditiva e outras técnicas de inteligência artificial. E a nossa pesquisa mostra que as empresas estão usando essas tecnologias em graus variados, dependendo do setor.

É caro comprar e implantar tecnologia em uma grande organização – é algo proibitivo para algumas delas. E a decisão sobre o que comprar (e quando) é delicada. Algumas organizações investem em tecnologias novas ou inovadoras, mas não as utilizam de forma ideal, por exemplo. Outras se atrasam no processo e ficam em desvantagem.

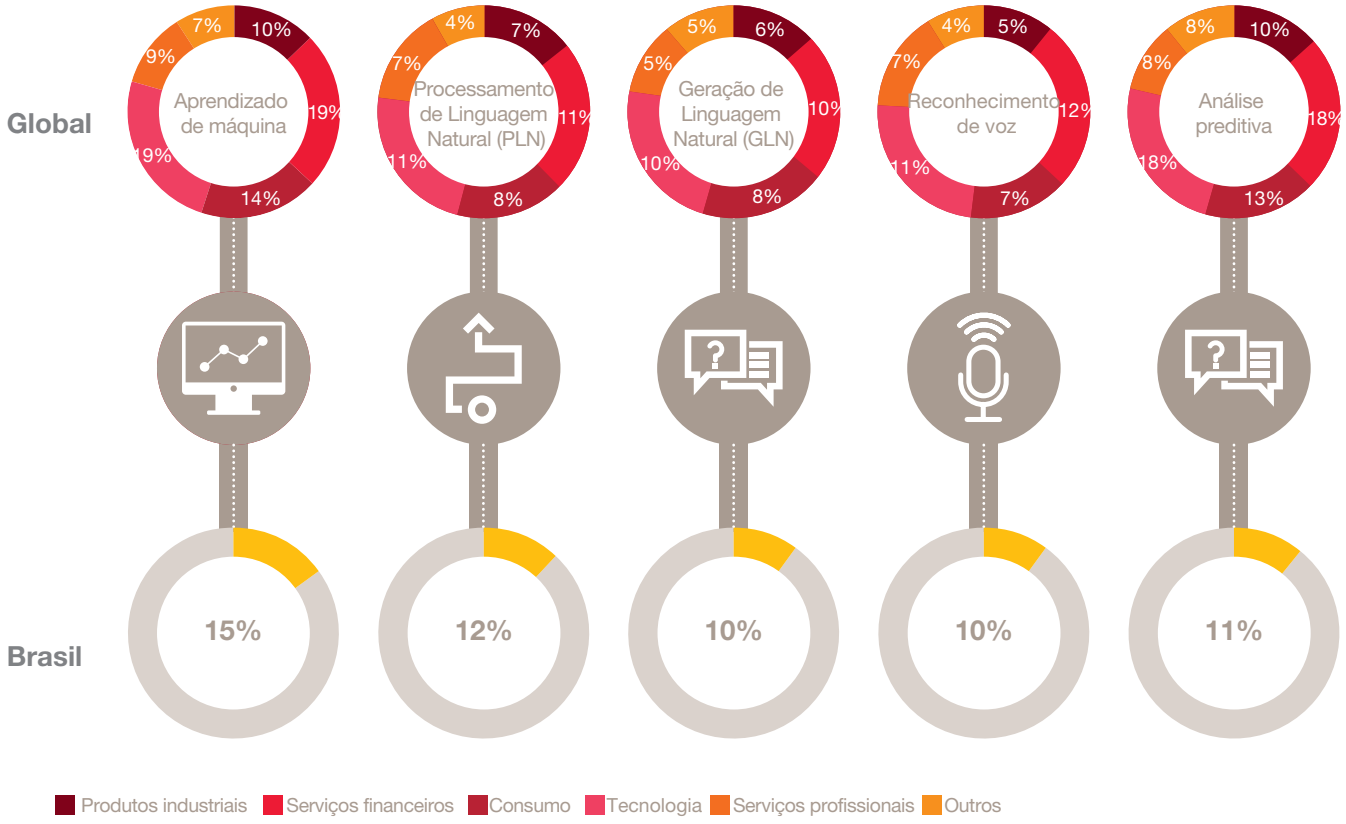
31%

das empresas brasileiras afirmam ter gasto com investigação e prevenção pelo menos o dobro dos prejuízos registrados como resultado do crime econômico mais grave.

52%

das organizações ouvidas no Brasil aumentaram os recursos destinados a combater a fraude e o crime econômico.

Figura 15: As indústrias de serviços financeiros e tecnologia estão obtendo mais valor da inteligência artificial e das análises avançadas



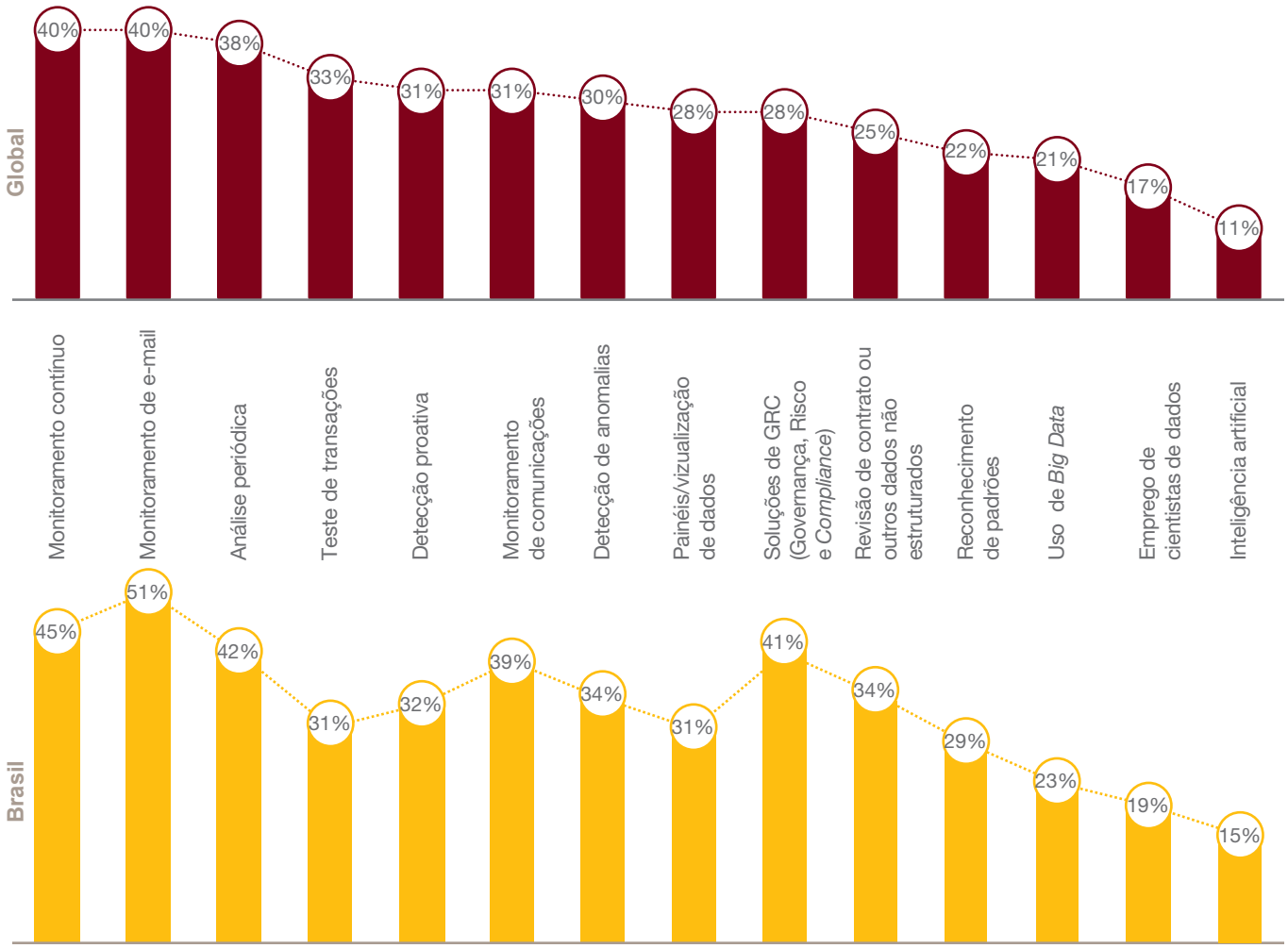
Q. Até que ponto a sua organização está aproveitando a inteligência artificial ou análises avançadas para combater/monitorar fraudes e outros crimes econômicos? (% de participantes cuja organização usa e entende que agrega valor)

Fonte: *Pesquisa Global sobre Fraudes e Crimes Econômicos 2018* da PwC

"O uso de tecnologias inovadoras é fundamental para o combate às fraudes e os países em desenvolvimento estão sendo pioneiros em sua adoção"

Francisco Macedo
Sócio, PwC Brasil

Figura 16: As organizações estão começando a obter valor de tecnologias alternativas e disruptivas de combate à fraude



Q. Até que ponto a sua organização está aproveitando a inteligência artificial ou análises avançadas para combater/monitorar fraudes e outros crimes econômicos? (% de participantes que a organização usa e entende que agrega valor)

Fonte: *Pesquisa Global sobre Fraudes e Crimes Econômicos 2018* da PwC

O uso de tecnologias inovadoras para combater a fraude é hoje um fenômeno mundial. De fato, nossa pesquisa mostra que as empresas de países em desenvolvimento estão investindo em tecnologias avançadas a um ritmo mais rápido do que as nações desenvolvidas. Descobrimos que 27% das empresas de países em desenvolvimento atualmente usam ou planejam implementar a inteligência artificial para combater fraudes, em comparação com 22% das empresas nos países desenvolvidos.

Para os países em desenvolvimento, essa abordagem poderia representar um meio efetivo de progresso em uma área na qual outras nações já incorreram em custos de infraestrutura consideráveis.

Em última análise, a onipresença da tecnologia cria um duplo desafio para todas as organizações: como encontrar a abordagem ideal para a tecnologia, que equilibre eficiência e custo, mantendo-se à frente dos fraudadores.

O que é atrito na relação com o consumidor?

Para um consumidor, a princípio, talvez seja tranquilizador saber que uma empresa está monitorando continuamente a ocorrência de fraudes nos serviços que ela presta. Mas se esse monitoramento resultar em alertas frequentes ou repetitivos, essa tranquilidade pode se transformar rapidamente em irritação.

Esse é o significado de atrito na relação com o consumidor, um desafio crescente para as organizações, que se esforçam para encontrar o equilíbrio entre agir em relação aos alertas de fraude e enviar notificações aos clientes de forma exagerada.

Não é um equilíbrio fácil de ser alcançado – e a margem de erro é pequena. Se for muito passivo, você corre o risco de ser vítima de uma transação fraudulenta (com as consequências financeiras e de reputação associadas). Mas, por excesso de proatividade, você pode incomodar (e até perder) a sua base de clientes.

"Quando se trata de adoção de novas tecnologias, o mundo em desenvolvimento está avançando mais que o desenvolvido."

Philip Upton,
Sócio, PwC EUA

44%

dos brasileiros acreditam que a tecnologia usada por suas empresas para combater a fraude e/ou o crime econômico estava produzindo muitos falsos positivos. No mundo esse percentual é de 34%.

Os clientes não são apenas um aspecto do negócio – eles são o negócio

Os clientes são a força vital de qualquer negócio. Mas, à medida que os modelos de negócios evoluem para acompanhar a revolução digital, muitos desses clientes estão ficando expostos a fraudes de pagamento pela primeira vez. A maneira de lidar com esse problema afetará profundamente os resultados das empresas. Estas são algumas características e desafios da fraude digital atualmente:

- ***Novos produtos digitais estão criando novas superfícies de ataque***
  Para lançar produtos, as empresas seguiam um processo B2B bem constituído envolvendo revendedores, distribuidores e varejistas. As inovadoras plataformas digitais B2C atuais têm uma superfície de ataque muito mais ampla – e com muito mais espaço para fraudes.
- ***As linhas que separam as indústrias estão ficando cada vez menos claras***
  Empresas de serviços não financeiros estão se aventurando no setor de sistemas de pagamentos. Esses novos entrantes em geral não dispõem da experiência e do conhecimento da indústria tradicional de serviços financeiros no combate à fraude e à lavagem de dinheiro, o que torna essas empresas (e seu ecossistema de terceiros) vulneráveis a riscos regulatórios e de fraude.
- ***A sofisticação técnica dos fraudadores externos continua a crescer***
  Os ataques de fraude digital se tornam cada vez mais sofisticados, amplos e devastadores. Um único ataque de *ransomware* pode paralisar organizações, permitindo que os fraudadores movimentem milhões de dólares.
- ***Você pode alterar seu número de cartão de crédito, mas não sua data de nascimento***
  As ferramentas de autenticação baseadas em conhecimento usadas para controlar fraudes estão desatualizadas. Novas técnicas – como identificação digital de dispositivos e biometria de voz – são hoje necessárias para proteger os ativos dos clientes. Mas a maioria das empresas ainda precisa adotá-las. Essa é uma questão importante porque um grande roubo de dados em nada se compara à perda de ativos substituíveis como dinheiro. O prejuízo envolve marcadores de identidade únicos, permanentes e estritamente pessoais, como datas de nascimento ou números da previdência social. Como esses são os dados normalmente usados pelas ferramentas de autenticação baseadas em conhecimento para verificar identidades e evitar fraudes, seu roubo abre caminho para que fraudadores possam assumir a identidade de outra pessoa.

Ataques cibernéticos: pela porta arrombada ou aberta?

O crime cibernético há muito tempo passou da infância e da adolescência. Os "cibercriminosos" atuais são tão experientes e profissionais quanto as empresas que eles atacam. Essa maturidade exige uma nova visão sobre os diferentes aspectos das ameaças cibernéticas e das fraudes associadas.

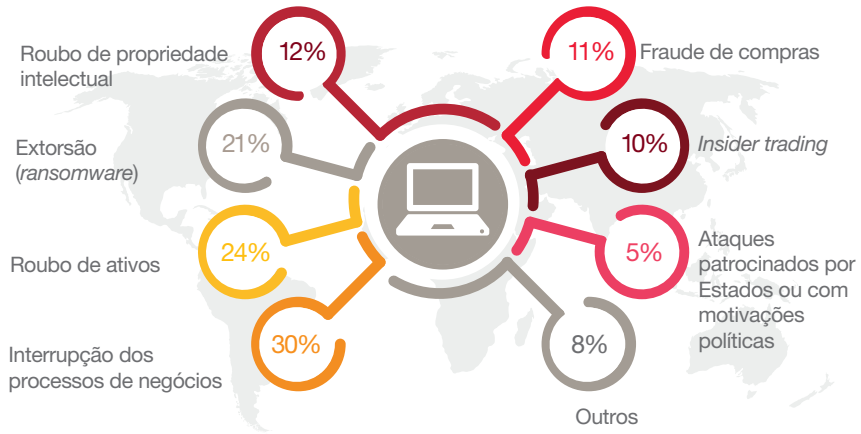
Muitas vezes, o primeiro sinal de que há um problema sistêmico na organização é a detecção de um ataque cibernético, como *phishing*, *malware* ou um ataque tradicional de força bruta. A frequência, a sofisticação e a letalidade crescentes desses ataques estimulam as empresas a procurar em suas operações maneiras de antecipá-los. O benefício adicional dessa abordagem é o foco mais agressivo na prevenção de fraudes.

Embora seja difícil para as empresas medir precisamente os impactos financeiros dos ataques cibernéticos, 14% dos participantes da pesquisa global que indicaram o crime cibernético como o mais grave tipo de fraude de que foram vítimas disseram ter perdido mais de US$ 1 milhão como consequência; 1% indicaram ter perdido mais de US$ 100 milhões.

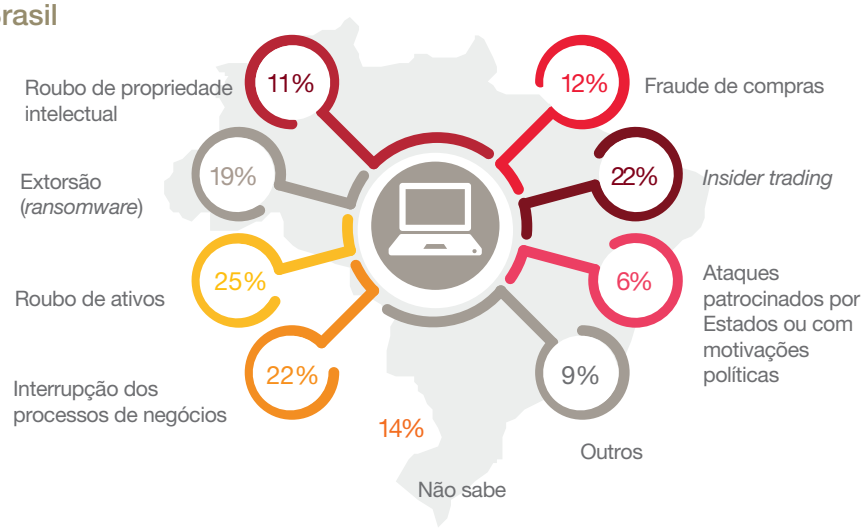
O crime cibernético, de fato, está entre as ameaças mais sérias para as empresas. No Brasil, 14% dos participantes acreditam que ele será o crime mais grave e impactante que enfrentarão nos próximos dois anos, atrás apenas de suborno e corrupção (com 20%). No mundo, ele aparece no topo da lista, com 26%, muito à frente de suborno e corrupção (12%) e roubo de ativos (11%). Os ataques cibernéticos se difundiram tanto que medir sua ocorrência e seus impactos está se tornando menos útil estrategicamente do que se concentrar no mecanismo que o fraudador usou para atacar.

Figura 17: Tipos de fraudes de que as organizações foram vítimas através de um ataque cibernético

Global



Brasil



Q. De quais dos seguintes tipos de fraude e/ou crime econômico sua organização foi vítima por meio de um ataque cibernético?

Fonte: *Pesquisa Global sobre Fraudes e Crimes Econômicos 2018* da PwC

41%

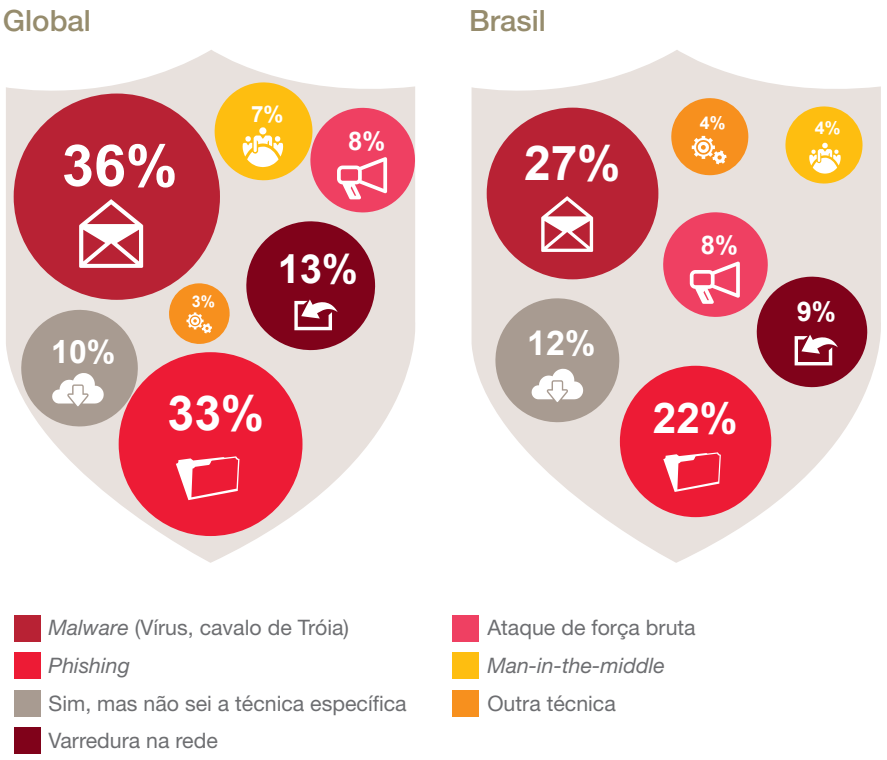
dos executivos ouvidos no mundo disseram que gastaram com investigações e outras intervenções pelo menos o dobro do que perderam para o crime cibernético.

Todas as fraudes digitais são classificadas como fraudes, mas o contrário não é verdade. Portanto, é importante definir as duas formas de encarar o crime cibernético:

1. ***Como roubo digital*** (os artigos roubados, não a violação). O crime pode incluir roubo de dinheiro, informações pessoais, propriedade intelectual, extorsão e pedido de resgate (*ransomware*) ou uma série de outros crimes.

2. ***Como fraude digital.*** Em muitos aspectos, esse é o tipo de ataque mais perigoso, porque o fraudador penetra por uma porta aberta (normalmente, mas não sempre, um ponto de acesso para clientes ou empregados) e usa os processos de negócios da empresa para atacá-la. Para combater esse tipo de fraude, a organização deve usar métodos digitais – como vacina ou remédio para tratar a infestação.

Figura 18: Técnicas de ataque cibernético usadas contra organizações



Q. Nos últimos 24 meses, a sua organização foi alvo de ataques cibernéticos usando qualquer das técnicas a seguir?

Fonte: *Pesquisa Global sobre Fraudes e Crimes Econômicos 2018* da PwC

Quase um quarto dos brasileiros (22%) e 31% dos participantes globais foram alvo de ataques cibernéticos, seja por *malware* ou *phishing*. A maioria desses ataques, que podem afetar seriamente os processos de negócios, também levou a prejuízos substanciais para as empresas: cerca de um quarto dos atingidos sofreu também roubo de ativos e um quinto foi vítima de extorsão digital.

O consumidor é ressarcido, mas para onde vai o dinheiro roubado?

Ressarcir os clientes no caso de fraude é uma prioridade, mas é importante também entender as dimensões mais profundas da prevenção desse problema, que envolve o submundo do crime e os regimes de regulação e fiscalização que têm por missão controlá-lo.

Em um caso de roubo de identidade, por exemplo, o banco ou o varejista cobrirá o prejuízo, isentando o cliente de responsabilidades adicionais se um fraudador abrir um cartão de crédito em nome dele e gastar uma quantia elevada. Até hoje, o sistema de reparação desse tipo de fraude externa tem funcionado assim, e todas as partes envolvidas – bancos, varejistas, consumidores e reguladores – aceitaram isso como parte do custo de fazer negócios juntos.

Embora essas atividades fraudulentas possam ser detectadas pelos sistemas existentes de monitoramento de transações criados em resposta à regulamentação americana do BSA (Bank Secrecy Act) e a regras similares adotadas em outros países, como o Brasil, é provável que tanto os bancos quanto as MSBs (sigla em inglês para empresas de serviços monetários) estejam deixando de identificar como essas transações se manifestam no sistema – conforme foi demonstrado, por exemplo, em uma execução regulatória recente relacionada a falhas de detecção no contexto de tráfico de seres humanos.

Empresas não financeiras talvez não precisem cumprir as mesmas exigências regulatórias que as prestadoras de serviços financeiros, mas elas também podem enfrentar problemas com a lei. Isso porque os órgãos reguladores e de repressão ao crime agora estão atentos a elementos que vão além do impacto primário de um crime – por exemplo, o comércio de produtos falsificados – para examinar que atividades ilícitas acabaram sendo financiadas pelos ativos roubados. Como parte de suas atribuições, eles examinam as medidas antifraude e de *compliance* que as empresas não financeiras adotam para detectar sinais de que elas possam ter "auxiliado e incentivado" tais atividades criminosas, conscientemente ou não – outro exemplo de que as fronteiras da prevenção a fraudes se tornam cada vez mais difusas em todas as indústrias.

O *business case*

O *business case* de investimento em tecnologia de combate a fraudes vai além da proteção contra danos à reputação, regulatórios ou financeiros. Também é preciso reduzir os custos de prevenção com base em ganhos de eficiência e garantir que a empresa tenha segurança para desenvolver e vender novos produtos e serviços em uma plataforma digital. Além disso, permite que a empresa aperfeiçoe seu programa contra fraudes para reduzir os "atritos com o consumidor" – de tal forma que os clientes interajam mais livremente com sua plataforma e seu produto.

Invista em pessoas, não apenas em máquinas

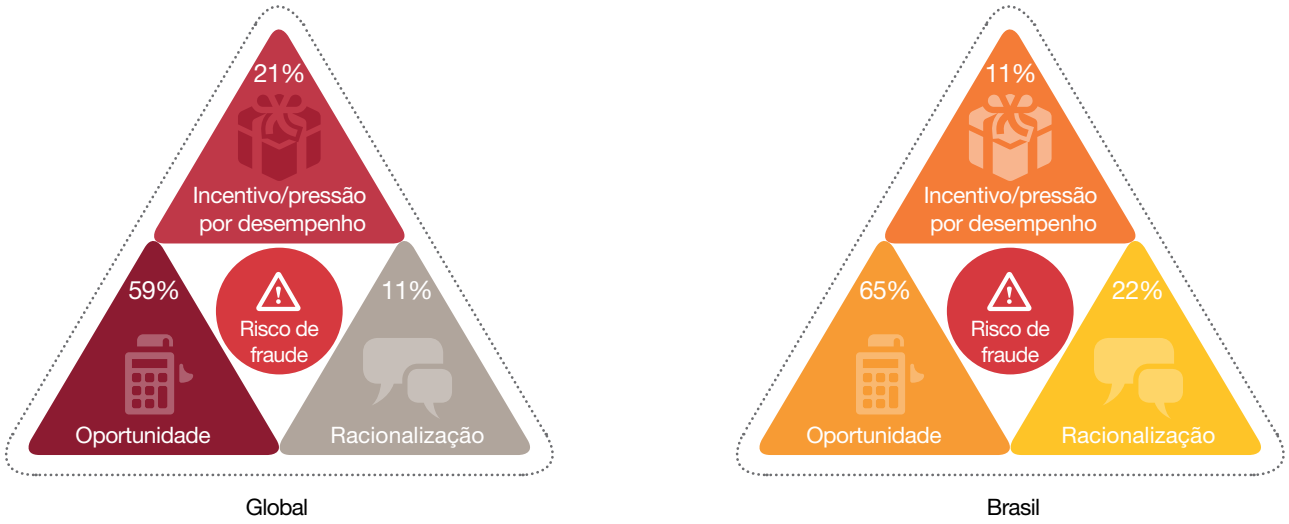
Um pequeno investimento nas pessoas pode gerar grandes dividendos

Pressionadas pelas dificuldades para solucionar a fraude, muitas organizações decidem investir mais recursos em tecnologia. No entanto, esses investimentos acabam por registrar retornos decrescentes, especialmente no caso da fraude interna. A tecnologia é uma ferramenta essencial na luta contra a fraude, mas não é a única. Talvez nem seja a mais estratégica.

Isso ocorre porque a fraude é produto de uma combinação complexa de condições e motivações, algumas das quais só podem ser desafiadas por máquinas ou processos. O fator mais crítico na decisão de cometer uma fraude é, em última análise, um comportamento humano – e isso cria a melhor oportunidade de combatê-la. Existe um método poderoso para entender e medir os fatores individuais por trás da fraude interna: o triângulo da fraude.

Ele começa com um incentivo (geralmente uma pressão por desempenho originada dentro da organização), é seguido de uma oportunidade e termina com um processo interno de racionalização. Esses três fatores precisam estar presentes para que um ato fraudulento ocorra. Todos, portanto, devem ser enfrentados individualmente.

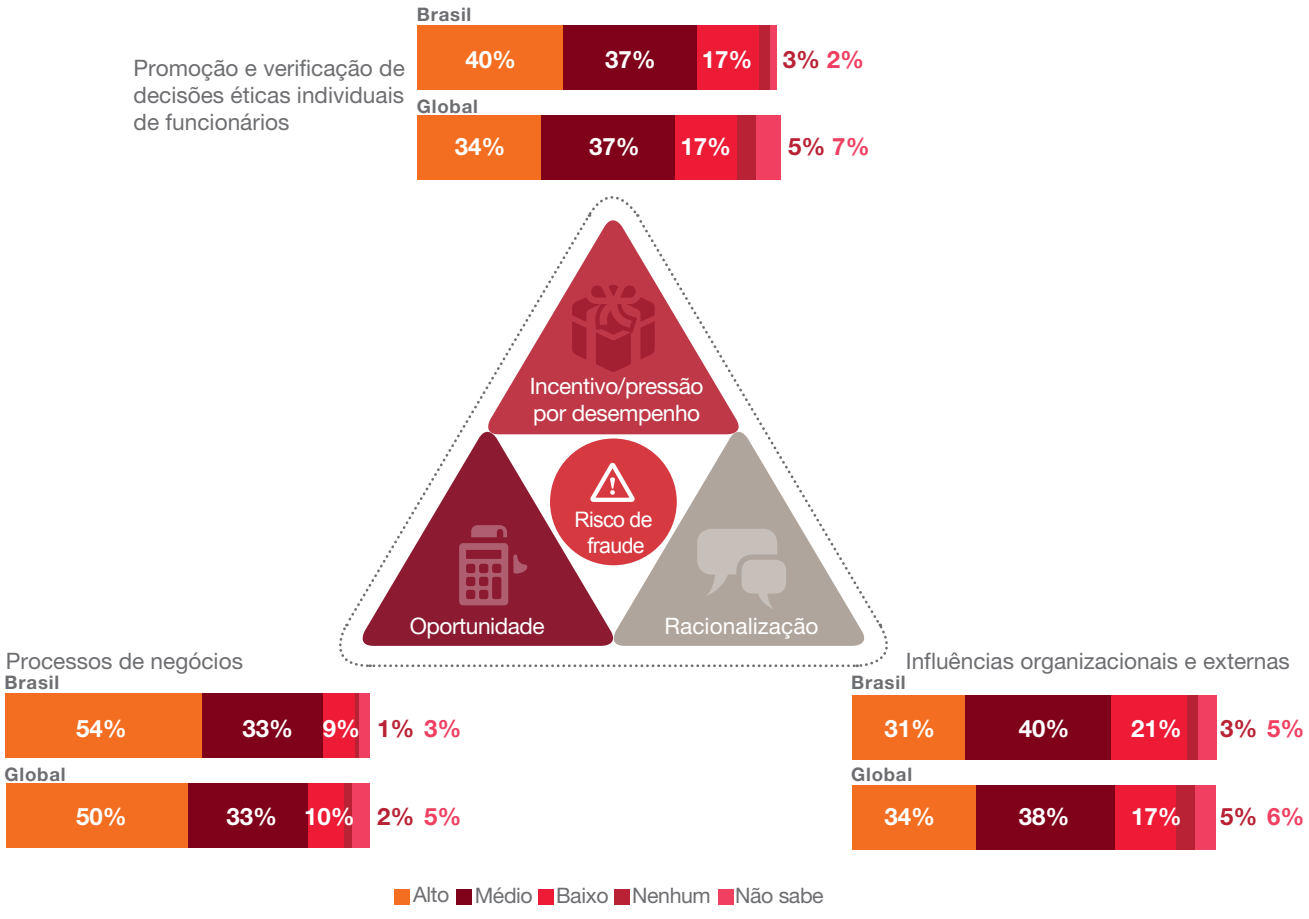
Figura 19: O triângulo da fraude: o que leva um empregado a cometê-la?



Q. Até que ponto cada um dos seguintes fatores contribuiu para a fraude e/ou o crime econômico provocado por agentes internos? Classifique em ordem de contribuição para o incidente? (% dos participantes que classificaram o fator como o principal)

Fonte: *Pesquisa Global sobre Fraudes e Crimes Econômicos 2018* da PwC

Figura 20: O nível de esforço organizacional exigido para combater a fraude



Q. Qual é o nível de esforço que a sua organização aplica nas seguintes categorias para combater fraudes e/ou crimes econômicos internamente?

Fonte: *Pesquisa Global sobre Fraudes e Crimes Econômicos 2018* da PwC

Prevenção da oportunidade: controles

A maior parte do empenho das empresas no combate à fraude nos últimos dois anos foi feito para reduzir as oportunidades do crime –54% das empresas brasileiras (50% das globais) disseram ter feito um esforço alto para desenvolver processos de negócios, como controles internos, voltados para combater as oportunidades de cometer fraudes. E, embora 65% dos brasileiros tenham indicado a oportunidade como principal fator por trás dos incidentes mais graves do tipo cometidos por agentes internos, esse percentual é 14 pontos mais baixo que o resultado de 2016 (no mundo, a queda foi alta, de 10 pontos). Essa é uma prova positiva de que a tecnologia tem um papel fundamental a desempenhar – e, mais precisamente, que as empresas, em geral, a estão empregando de forma eficaz.

Infelizmente, as empresas estão colocando muito menos esforço em medidas para neutralizar os incentivos e a racionalização: menos de metade delas (40% no Brasil e 34% no mundo) disseram dedicar um esforço alto para lidar com esses fatores. Nossa pesquisa destaca os resultados dessas escolhas: o percentual dos brasileiros que indicam o incentivo como principal fator por trás da fraude mais grave que sofreram aumentou de 14% para 22% em dois anos (no mundo o aumento foi de 14% para 21%). A racionalização foi apontada por 11% dos participantes (há dois anos, o resultado foi de 7% no Brasil e também de 11% em escala global).

Essa ênfase menor em medidas culturais/éticas indica um possível ponto cego e pode ser a razão para a resistência tão alta da fraude interna. Como ela é resultado da interseção de escolhas humanas com falhas do sistema, é importante desconfiar da falsa sensação de segurança que os controles internos, mesmo quando bem desenhados, podem trazer.

De fato, há uma falha essencial na crença de que controles internos baseados na tecnologia, por si só, podem interceptar a fraude: ela presume que a administração sempre se comportará de forma ética. Na verdade, a experiência mostra que a maioria das fraudes internas graves ocorre por desrespeito a esses controles pela administração (*management override of controls*).

Nossa pesquisa confirma esse fenômeno em âmbito global: houve um aumento acentuado na proporção desses crimes atribuídos à gerência executiva no mundo: de 16% para 24 %. O Brasil seguiu tendência contrária: o índice caiu de 40%, em 2016, para 26% este ano. O mesmo aconteceu na gerência média, que registrou uma queda de 47% para 26%, enquanto no mundo o índice permaneceu praticamente estável em 37%.

Para superar esse problema estrutural, o caminho para as organizações é criar controles que realmente consigam lidar com o conluio da administração ou o desrespeito às normas em áreas específicas.

Prevenção do incentivo: transparência

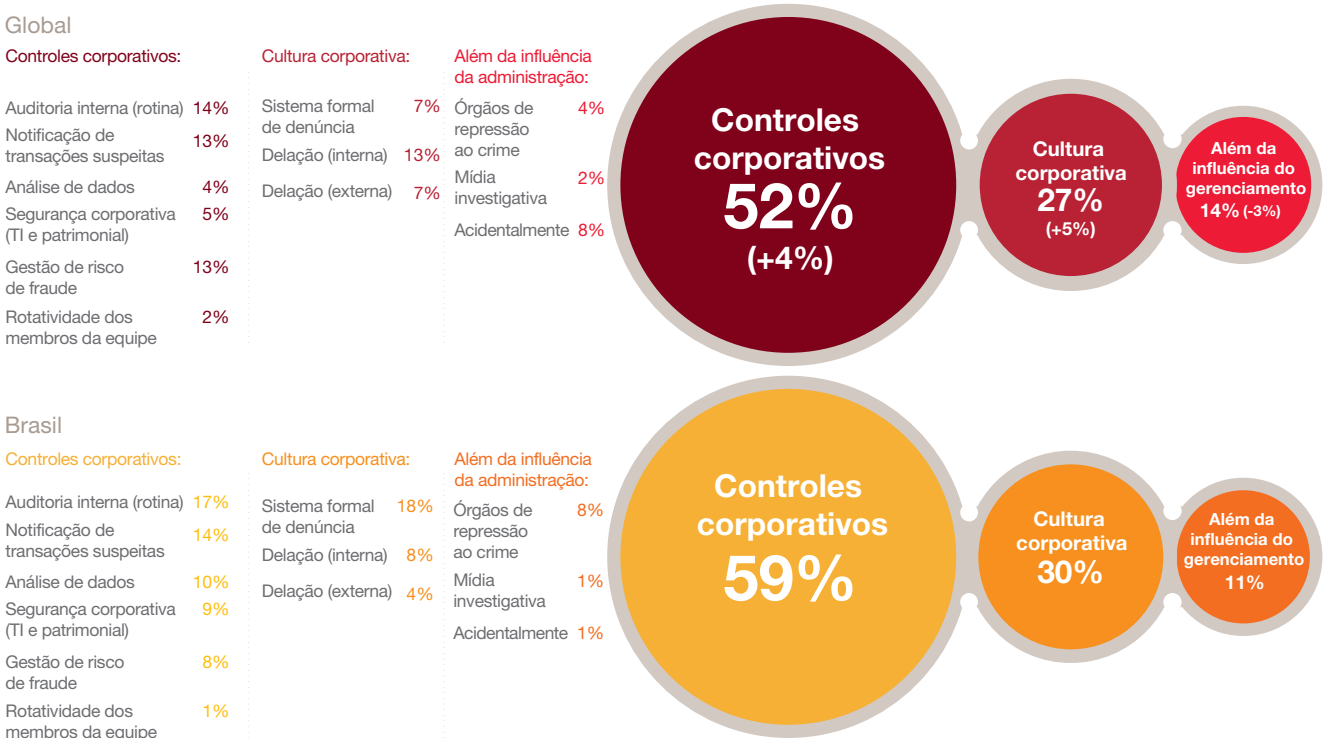
As fraudes corporativas geralmente estão associadas a pressões corporativas – e a pressão para cometer uma fraude pode surgir em qualquer nível da organização.

Nossa pesquisa revela que 19% das organizações brasileiras que registraram fraudes nos últimos dois anos (28% no mundo) foram vítimas da má conduta nos negócios (abuso de incentivos) e 13% das que têm escritórios em outros territórios (16% no mundo) experimentaram o mesmo problema nesses locais. Além disso, 24% dos participantes globais indicaram que a gerência executiva foi responsável pelo crime econômico mais grave que registraram, uma alta de 8 pontos percentuais em dois anos. O Brasil seguiu tendência contrária: a parcela das fraudes internas graves cometidas pela gerência executiva caiu de 40% para 26% nos últimos dois anos.

É importante não enfatizar demais os incentivos financeiros ao avaliar o que pode levar uma pessoa a cometer fraudes. Medo e vergonha de admitir um erro podem ter a mesma relevância. Sendo assim, os incentivos que vêm dos altos escalões da organização precisam ser examinados: até que ponto eles cumprem os regulamentos e são coerentes com "aquilo que é certo"?

Além disso, controles de curto prazo e elaborados sob medida podem servir para confirmar se programas agressivos de vendas estão levando a comportamentos fraudulentos ou ilegais. E uma política de denúncias ou de portas abertas bem divulgada também pode funcionar como um valioso sistema de alerta precoce de possíveis problemas na organização.

Figura 21: Pouco mais de metade das fraudes mais graves foram detectadas pelos controles corporativos



Q. Como foi detectada a fraude e/ou o crime econômico mais grave?

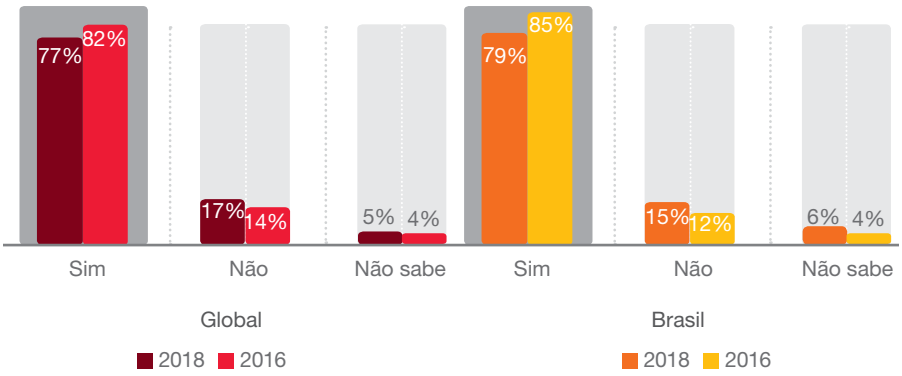
Fonte: *Pesquisa Global sobre Fraudes e Crimes Econômicos 2018* da PwC

A fraude pode ser motivada pela melhor das intenções

A fraude não necessariamente é um ato mal-intencionado e egoísta. Do ponto de vista jurídico, na verdade, existem dois tipos de fraude – a cometida para obter vantagens pessoais (como desfalque ou informações financeiras falsificadas para alavancar a remuneração) e a fraude cometida por "motivos corporativos" (como a sobrevivência da empresa ou a proteção da força de trabalho).

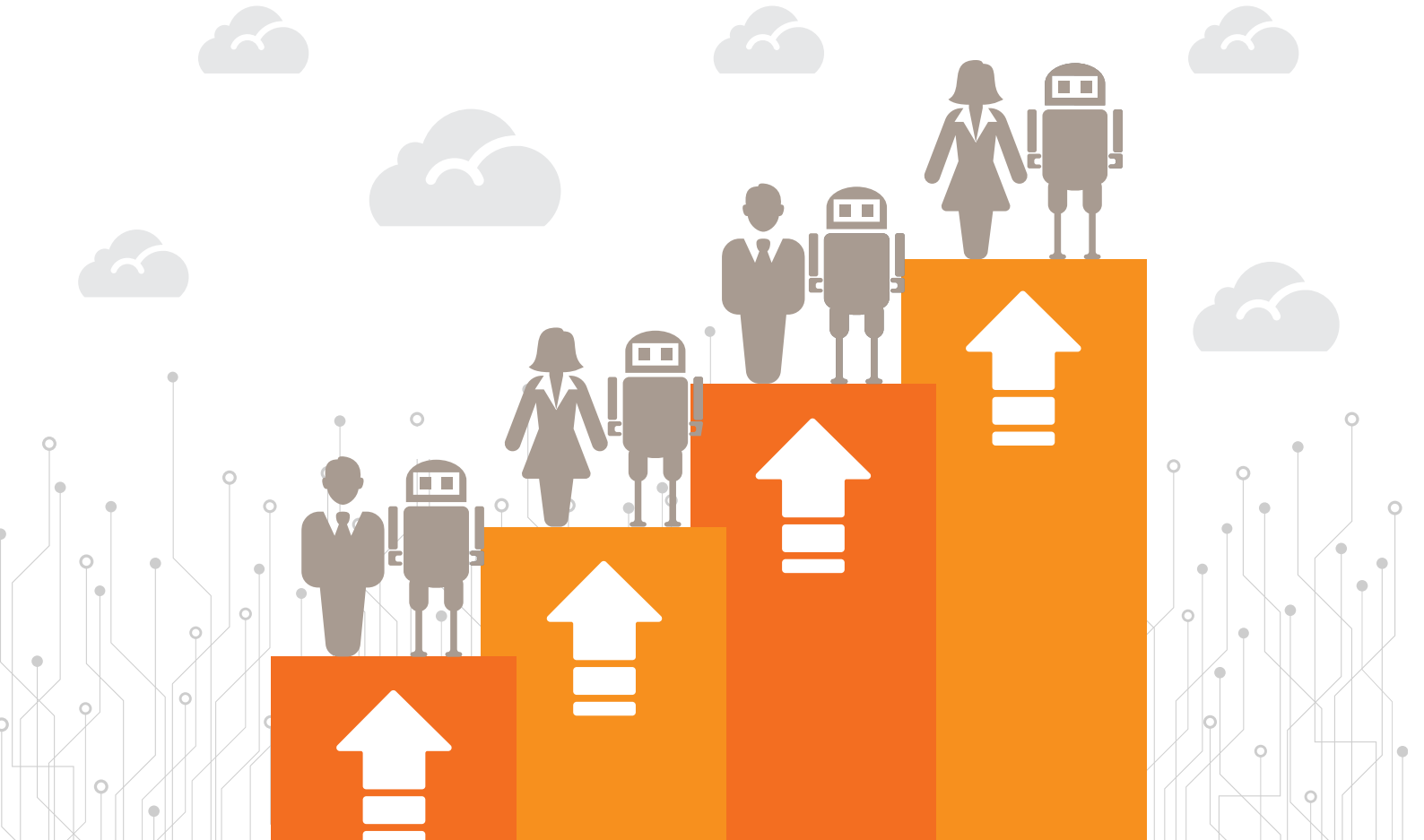
O segundo tipo pode ocorrer com a melhor das intenções: a de promover o sucesso da organização. Por exemplo, o que talvez começasse como uma estratégia de vendas voltada para aumentar a participação de mercado e a lucratividade (em benefício dos funcionários) pode, em última análise, se transformar em uma tática de vendas fraudulenta. Em qualquer caso, o resultado é o mesmo: a gerência executiva será responsável.

Figura 22: Menos empresas dizem ter programas de ética e *compliance*



Q. Você tem um programa de *compliance* e ética nos negócios em sua organização?

Fonte: *Pesquisa Global sobre Fraudes e Crimes Econômicos 2018* da PwC



Prevenção da racionalização: cultura

A pressão e a oportunidade podem ser influenciadas e controladas pela organização (pelo menos até certo ponto), mas prevenir a racionalização é um desafio maior. Esse é um processo que ocorre inteiramente dentro da mente humana e, portanto, é mais difícil de ser influenciado.

Uma das características da fraude interna é que seus autores geralmente a veem como um crime sem vítimas e não conseguem enxergar qualquer pessoa diretamente prejudicada. Isso ajuda a explicar por que, em quase três quartos dos incidentes relatados na nossa pesquisa global, um agente interno é o principal autor dos seguintes crimes econômicos mais graves: fraude de recursos humanos (81%), roubo de ativos (75%), *insider trading* (75%), fraude contábil (74%) e fraude em compras (73%).

O primeiro passo para prevenir a racionalização é se concentrar em entender o ambiente que determina o comportamento dos empregados – a cultura da organização. Pesquisas, grupos de foco e entrevistas em profundidade devem ser usados para avaliar os pontos fortes e fracos dessa cultura. Um treinamento consistente também é essencial. Quando as pessoas entendem claramente o que é uma ação inaceitável – e por quê – é mais difícil racionalizar uma atividade fraudulenta.

Infelizmente, nossa pesquisa revela um número decrescente de organizações que investem no tipo de treinamento capaz de fazer uma diferença substancial na prevenção da fraude. A porcentagem de participantes que disseram ter um programa formal de *compliance* e ética nos negócios caiu de 85% para 79% no Brasil e de 82% para 77% no mundo desde a nossa pesquisa de 2016. E apenas 58% das empresas com esse tipo de programa no Brasil e no mundo disseram ter políticas específicas voltadas para a fraude.

A tarefa de detectar e prevenir o crime econômico ou a fraude é, sem dúvida, complexa. É preciso encontrar uma fórmula que associe de maneira adequada medidas relacionadas às pessoas e à tecnologia, orientadas por um claro entendimento das motivações por trás dos atos fraudulentos e das circunstâncias em que eles ocorrem. As organizações precisam não se conformar com a ideia de que a tecnologia é a única solução ou de que um certo volume de fraude é parte do custo de fazer negócios. Em vez disso, ao estabelecer uma cultura de honestidade e transparência, desde os escalões mais altos, elas conseguem incutir em suas organizações um espírito de transparência e responsabilidade – e tirar a fraude das sombras.

"A conscientização dos colaboradores de uma organização e de seus stakeholders, *somada às ações de prevenção e detecção no nível transacional, eleva a percepção de que desvios podem ser detectados, contribuindo de forma significativa para reduzir a incidência de fraudes."*

Leonardo Lopes,
Sócio, PwC Brasil

Conclusão

Prepare-se, combata a fraude e se fortaleça

Nossa pesquisa mostra que muitas empresas estão despreparadas para enfrentar a fraude, por razões tanto internas quanto externas. Por isso, é tão importante lançar luz sobre os pontos cegos de uma organização em relação à fraude e compartilhar de forma ampla o significado claro da fraude – incluindo quais medidas podem e devem ser tomadas para preveni-la.

Fazer isso também cria oportunidades importantes, pois ajuda a realizar melhorias estruturais positivas em toda a organização – que podem torná-la mais forte e estratégica nos bons e maus momentos. As melhorias compreendem integrar melhor áreas como *compliance*, ética, gestão de riscos e assuntos jurídicos – e promover uma cultura mais positiva, coesa e resiliente.

Talvez seja difícil quantificar a proposta de valor de um programa de fraude robusto, e isso pode dificultar a obtenção dos investimentos necessários. Mas o custo de oportunidade – financeiro, legal, regulatório e de reputação – de deixar de criar uma cultura de *compliance* e transparência pode ser muito maior.

Não só a ameaça do crime econômico se intensificou nos últimos anos como as regras e as expectativas de todos os *stakeholders* – reguladores, empregados, o público em geral e as redes sociais – mudaram de maneira irrevogável. A transparência e o respeito às leis nunca foram tão essenciais quanto hoje.

E isso é bom, porque, no tribunal da opinião pública, em que uma reputação pode mudar do dia para a noite, você será responsabilizado amanhã pelo que acontecer hoje. Portanto, o modo como a empresa responde a um evento de fraude ou problema de *compliance* é tão importante quanto o evento em si.

Entender esse princípio permite que a empresa se antecipe a eventos que evoluem rapidamente e demonstre aos *stakeholders* internos e externos que ela está no controle da situação. Agir com transparência, em uma atmosfera de tolerância zero, traz benefícios consideráveis em termos de reputação, mas não só isso: pode ajudar também a preservar a segurança dos altos executivos em seus cargos, além de atrair a futura geração de líderes para a organização.

Um evento não planejado é capaz de se transformar rapidamente em uma crise se não for resolvido da maneira correta, mas, ao empregar os mecanismos certos – uma cultura de coesão e abertura, um ambiente de controles sofisticado –, a empresa estará bem posicionada para absorver o choque, desenvolver "memória muscular" e se fortalecer. Os imperativos são claros: inclua a transparência como aspecto essencial do propósito da sua organização, use-a para vincular estratégia, governança, gestão de riscos e *compliance*, e você estará mais bem posicionado para transformar qualquer problema de fraude em uma oportunidade para avançar.

Contatos

Quer saber mais sobre o que você pode fazer na luta contra a fraude?

Entre em contato com um dos nossos especialistas no assunto

Leonardo Lopes
Sócio – Forensic Services
leonardo.lopes@pwc.com
T.: +55 (11) 3674 3826

Francisco Macedo
Sócio – Forensic Services
francisco.macedo@pwc.com
T.: +55 (11) 3674 3826

José Figueira
Sócio – Forensic Services
j.figueira@pwc.com
T.: +55 (11) 3674 3826

Sobre a pesquisa

A *Pesquisa Global sobre Fraudes e Crimes Econômicos 2018* da PwC contou com a participação de 7.228 pessoas de 123 países. Do total de participantes, 52% eram líderes executivos de suas organizações, 42% representavam empresas de capital aberto e 55% representavam organizações com mais de mil funcionários.