

Combate a fraudes e crimes econômicos: uma batalha sem fim

Pesquisa Global sobre Fraudes e Crimes Econômicos **2020**

Apresentação

As fraudes e os crimes econômicos atingiram 46% das empresas brasileiras nos últimos dois anos*. O resultado é ligeiramente menor que o registrado na edição anterior da nossa Pesquisa Global sobre Fraudes e Crimes Econômicos e muito próximo da média global da edição atual.

Uma análise mais detalhada dos tipos de fraude relatados pelas empresas revela algumas tendências: suborno e corrupção, fraude contábil e fraude cometida pelo consumidor são as três formas mais comuns de crimes econômicos no País. Ao lado da lavagem de dinheiro, são também aquelas que registram maior tendência de aumento no período do nosso levantamento. No mundo, o crime cibernético e o roubo de ativos são mais frequentes do que no Brasil.

Com base em informações fornecidas por mais de 5 mil executivos em 99 países, este relatório explora como as empresas no Brasil e no mundo estão sendo afetadas por esses problemas e em quais áreas elas registram impactos mais relevantes.

A mensagem é clara para organizações de todos os portes: a ameaça da fraude e crimes econômicos é um problema permanente, que tende a se agravar em tempos de crise. Ignorá-la ou subestimá-la é um risco ao qual, infelizmente, muitas organizações estão expostas. Nas próximas páginas, apresentamos os resultados de nossa pesquisa e formas de como é possível enfrentar esses desafios de maneira eficaz.

* Referente ao biênio 2018-19.



Leonardo Lopes
Sócio e Líder de Forensic
Services PwC Brasil

Introdução



Sintonize qualquer canal de notícias ou folheie um jornal e provavelmente você encontrará uma reportagem sobre crimes econômicos ou fraudes.

- Suspeita de suborno em queda de edifício.
- Hacker viola prontuários médicos e dados financeiros de milhões de pessoas.
- Má conduta corporativa causou falha de produto.
- Preço de ações cai em meio a denúncias de fraude contábil.

Os índices de fraudes e crimes econômicos permanecem em níveis recordes, afetando cada vez mais empresas e de formas ainda mais variadas. Nesse cenário, é importante se perguntar:

Você está avaliando bem as ameaças ou brechas que o deixam vulnerável? As tecnologias de combate à fraude que você adotou estão gerando o resultado esperado? Quando ocorre algum incidente, você toma as medidas adequadas?

Essas são algumas das provocações que estão no centro das conclusões da Pesquisa Global sobre Fraudes e Crimes Econômicos deste ano. A fraude atingiu seu maior nível de ameaça em todos os tempos – causando também níveis inéditos de prejuízos. Nesse cenário, é fundamental que você avalie seu grau de preparação para enfrentá-la, adote medidas eficazes de combate e aja rapidamente quando for atingido.

Por mais de 20 anos, a Pesquisa Global sobre Fraudes e Crimes Econômicos da PwC analisa vários crimes registrados no ambiente corporativo, como:



Em números

Os destaques da nossa pesquisa

Casos de fraude: **um problema persistente**

Quase metade dos participantes da nossa pesquisa no Brasil e no mundo relataram ter sido vítimas de uma fraude nos últimos 24 meses. Esse resultado elevado demonstra a importância de conhecer os tipos de fraude mais recorrentes, quem está cometendo esses crimes e quais são os diferenciais das empresas que têm obtido mais sucesso na tentativa de coibir tais práticas.

5.018



participantes em
99 territórios

235



no Brasil

Estimativa de prejuízo

Brasil:
US\$ 2,5 bi

Mundo:
US\$ 42 bi



6



casos de fraude –
a média de incidentes de
que as empresas foram
vítimas no mundo nos
últimos 24 meses.

46%



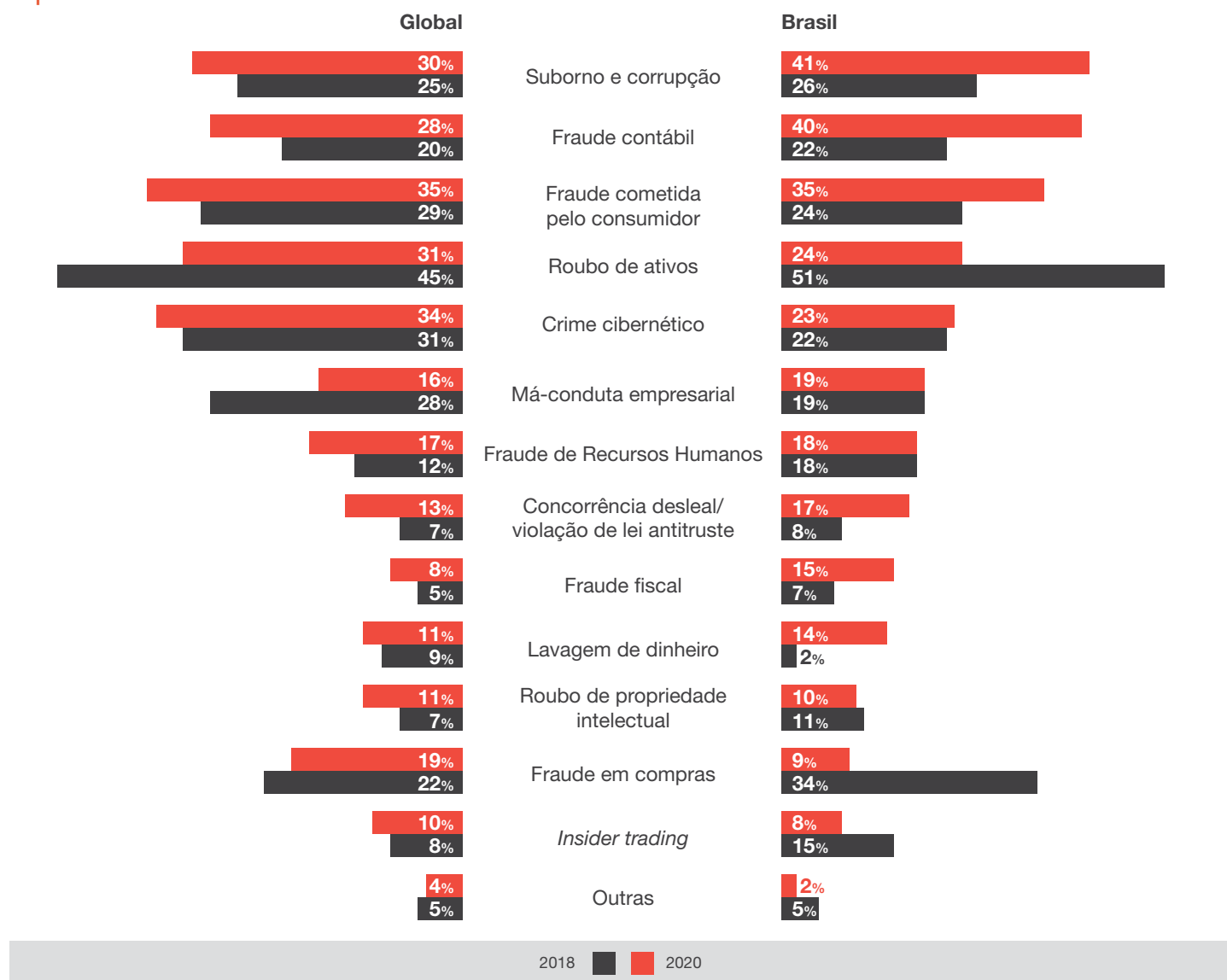
é o percentual de participantes brasileiros que foram vítimas de pelo menos um caso de fraude nos últimos 24 meses, valor muito próximo da média global (47%) e do resultado da América Latina (49%). É o segundo nível mais alto relatado desde o início do levantamento, abaixo apenas dos 50% registrados em 2018 (49% no mundo e 53% na América Latina).

Suborno e corrupção, fraude contábil e fraude cometida pelo consumidor – são os três tipos de fraude mais comuns no Brasil. Há dois anos, roubo de ativos, fraude em compras e suborno e corrupção ocupavam os primeiros lugares. No mundo, a fraude cometida pelo consumidor, o crime cibernético e o roubo de ativos encabeçam a lista.

Fraude contábil, suborno e corrupção, lavagem de dinheiro e fraude cometida pelo consumidor – esses incidentes registraram os maiores aumentos percentuais este ano no Brasil. No mundo, as maiores altas foram, na ordem, fraude cometida pelo consumidor, fraude contábil, concorrência desleal, fraude de recursos humanos e suborno e corrupção.

Os tipos de crime mais comuns

Suborno e corrupção, fraude contábil e fraude cometida pelo consumidor estão no topo da lista no Brasil



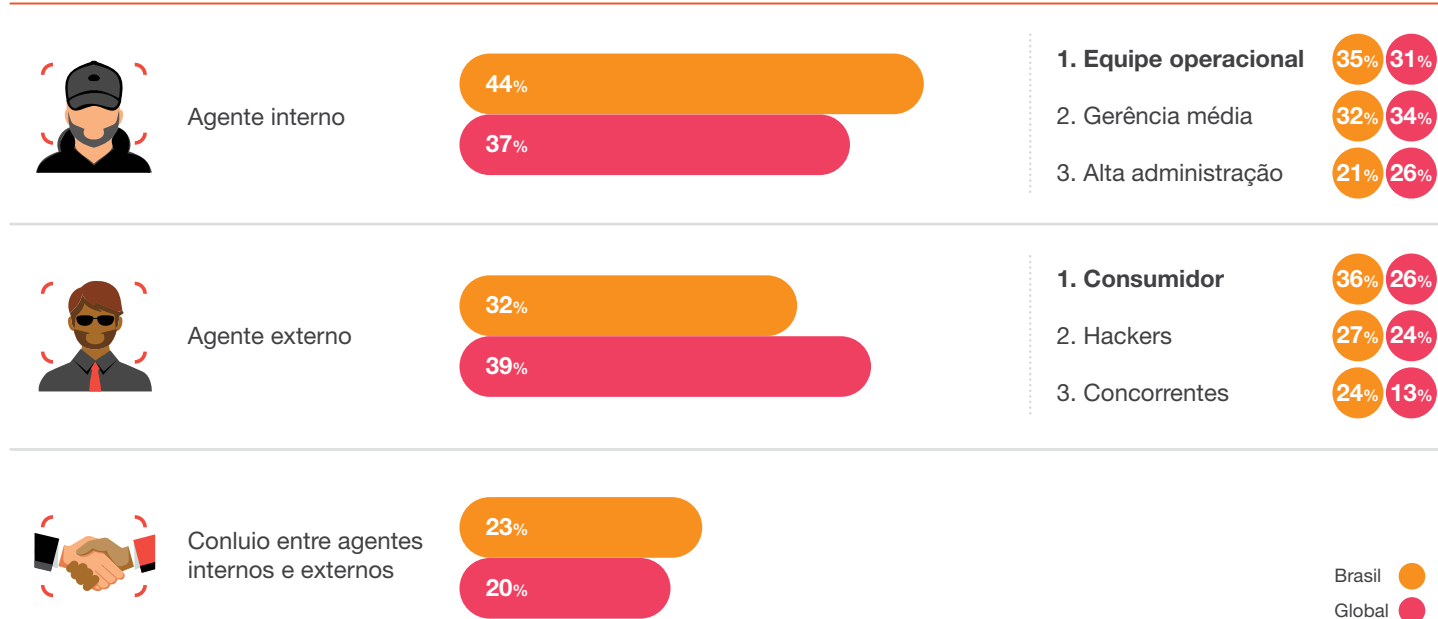
Crimes considerados mais graves



Os fraudadores: quem são eles

A fraude atinge as empresas por todos os ângulos – os fraudadores podem ser internos, externos ou, em muitos casos, pode haver conluio. No Brasil, o autor do crime está dentro da organização grande parte das vezes, sendo que as equipes operacionais e gerência média oferecem mais riscos que a alta administração.

Quem são os principais autores



Terceiros. As empresas terceirizam cada vez mais competências não essenciais para reduzir custos. Mas esses parceiros de negócios podem representar uma fonte de riscos, que muitas organizações não avaliam de forma estruturada.

- 14% dos participantes brasileiros e 19% dos globais citam os fornecedores como autores da fraude mais grave sofrida cometida por um agente externo.
- Metade ainda não tem um programa formal para gerenciar o risco de terceiros – e 24% (21% no mundo) não possuem um programa de monitoramento ou *due diligence* de terceiros.

Fraudes cometidas pelo consumidor. Esse tipo de fraude está no topo não apenas da lista das principais fraudes cometidas por um agente externo no Brasil e no mundo (36% ante 26%), como também da lista de todos os crimes sofridos pelas participantes globais – com 35%, em alta desde 2018. No Brasil, essa opção aparece em terceiro lugar na lista geral de fraudes sofridas, embora o percentual registrado seja o mesmo que o global e esteja crescendo.

- Não surpreende que a fraude cometida por consumidores tenha especial destaque nos segmentos de serviços financeiros e bens de consumo. É um dado relevante a ser considerado quando diferentes indústrias se dedicam a implantar estratégias de relacionamento direto com o consumidor.
- A boa notícia é que essa é uma das fraudes para as quais o emprego de recursos dedicados, processos robustos e tecnologia se mostram eficazes como medida de prevenção.

Alta administração. Esses crimes geralmente estão entre os piores por causa da capacidade que os altos executivos têm de anular (ou conspirar para anular) os controles internos – seja pelo nível de autoridade delegada, conhecimento do sistema ou influência.

Quase metade das fraudes relatadas no mundo que resultaram em prejuízo **acima de US\$ 100 milhões** foram cometidas por pessoas de dentro da empresa.

Acusados. Pela primeira vez este ano, perguntamos aos entrevistados se suas organizações haviam sido acusadas de cometer uma fraude. Globalmente, entre os que relataram ter sido vítimas de um evento desse tipo, quase 30% também foram acusados de cometer alguma fraude.

Mais de 750 empresas no mundo (42 no Brasil) foram acusadas de cometer fraudes.

- Concorrentes e empregados são os principais denunciadores no Brasil (40% e 33% respectivamente). No mundo, concorrentes, reguladores, empregados e consumidores ocupam o topo da lista, com resultados semelhantes.
- Um foco regulatório maior e, em alguns países, incentivos à delação dos crimes podem contribuir para essa tendência.



Impacto: **o custo da fraude**

A análise dos prejuízos é complexa. É possível quantificar alguns custos, como perdas financeiras diretas ou gastos com multas, sanções e ações de resposta ou remediação. Mas outros prejuízos não são facilmente quantificáveis – como danos à marca, perda de posição no mercado ou de engajamento dos funcionários e perda de oportunidades futuras não aproveitadas.

Algumas fraudes – como as causadas por agentes externos – geralmente ocorrem fora da empresa, são de natureza transacional e podem ser objeto de um monitoramento ativo, além de causar impacto financeiro potencialmente mais limitado. Em relação a outros crimes, como suborno e corrupção ou aqueles cometidos internamente, o trabalho é de gerenciamento e mitigação de riscos. Esses crimes tendem a ser mais difíceis de prever e monitorar, resultam em multas mais altas e têm repercussões indiretas, como perda de negócios ou danos à marca.

No total, 19% dos participantes no Brasil que foram vítimas de uma fraude nos últimos 24 meses informaram ter perdido mais de US\$ 50 milhões em todos os incidentes registrados. No mundo, foram 13%.

As 5 fraudes mais caras. Práticas anticoncorrenciais, uso de informação privilegiada, fraude fiscal, lavagem de dinheiro e suborno e corrupção encabeçam a lista de fraudes no mundo em termos de perdas diretas – às vezes agravadas pelo custo significativo de reparação e de multas posteriores ao fato.

As principais fraudes cometidas dentro da organização causam potencialmente muito mais prejuízos do que os crimes praticados por agentes externos — e não apenas porque a perda financeira tende a ser maior – nos casos em que o criminoso está dentro da empresa, 43% relatam perder US\$ 100 milhões ou mais. Esses crimes também costumam resultar em ações civis ou criminais contra a empresa e os envolvidos, em danos à reputação, desvio de foco da administração e perda de negócios.

Suborno e corrupção

Principal tipo de crime econômico relatado no Brasil, suborno e corrupção continuam sendo um grande desafio.

Quase metade dos brasileiros (48%, ante 30% no mundo) acredita ter perdido uma oportunidade porque um concorrente teria pago suborno. Cerca de um terço (36% no Brasil e 29% no mundo) informa ter recebido um pedido de pagamento de suborno.

As respostas revelam alguns pontos cegos e surpresas:

- **6 em cada 10 empresas não têm um programa para lidar com o risco de suborno e corrupção.**
- 53% dos participantes no Brasil e 47% no mundo não realizam avaliações de riscos ou fazem apenas avaliações informais.
- 30% dos participantes brasileiros (28% no mundo) realizam testes limitados da eficácia operacional de seus controles, enquanto 14% (12% no mundo) não realizam nenhum tipo de teste.
- Cerca de metade dos participantes no Brasil e no mundo não realiza ou realiza apenas informalmente o monitoramento contínuo de terceiros e o *due diligence* com base em riscos – embora os terceiros representem um dos maiores riscos de suborno e corrupção.



Prepare-se, responda e saia da crise ainda mais forte



Ação: **Prepare-se**

O que você está fazendo para prevenir e identificar fraudes? Quais programas, métodos e tecnologias estão funcionando – e quais não estão? Que falhas de percepção ainda existem – e que oportunidades de melhoria podem ser aproveitadas?

Combater a fraude compensa... mas o que você faz é suficiente? Embora 56% das empresas brasileiras (64% das globais) tenham políticas e procedimentos em vigor e a maioria (6 em 10) inclua treinamento e monitoramento, **menos de metade das organizações dedica recursos à avaliação de riscos, investigações e gerenciamento de terceiros.**

Quais ações seriam mais eficazes?

1. Identifique, classifique e enfrente seus riscos. As empresas podem realizar avaliações de risco robustas, reunindo informações internas de *stakeholders* de toda a organização e em diferentes regiões geográficas, para identificar riscos e avaliar fatores mitigadores. Essas avaliações também devem incorporar fatores externos. Uma vasta quantidade de informações está disponível em domínio público, e ignorá-la pode resultar em uma falha grave. Os riscos devem ser avaliados com regularidade (não de forma pontual).

2. Suporte seus recursos de tecnologia com governança, experiência e monitoramento adequados. É importante reconhecer que uma única ferramenta não é capaz de lidar com todas as fraudes – e a tecnologia sozinha não mantém sua empresa protegida. A eficácia da tecnologia geralmente está associada ao uso de recursos especializados e do monitoramento regular dedicado a ela.

3. Fique atento. A capacidade de reagir a uma fraude assim que ela é identificada é um elemento importante de um programa eficaz de fraude. Mobilizar rapidamente a combinação certa de pessoas, processos e tecnologia pode limitar o dano potencial. Em alguns casos, uma fraude pode ser uma oportunidade – ou um ponto de inflexão estratégico – para desencadear uma transformação organizacional mais ampla para a proteção da marca.



A tecnologia é apenas uma parte da resposta

Várias organizações investiram pesadamente em novas ferramentas e técnicas nos últimos anos, mas muitos participantes da pesquisa revelaram preocupações com a implantação da tecnologia.

- 43% dos participantes brasileiros (29% no mundo) afirmam categoricamente que conseguiram implementar ou atualizar sua tecnologia. Aspectos como custos, recursos limitados e falta de sistemas são os principais obstáculos citados pelos outros participantes.

- Globalmente, entre os que não estão implementando novas tecnologias antifraude, quase um terço afirma que isso acontece porque têm dificuldade em perceber o valor delas.
- Considerando tecnologias e técnicas alternativas/disruptivas, no Brasil aproximadamente 40% estão usando inteligência artificial (IA) – uma tecnologia cada vez mais predominante– em comparação com apenas 25% no mundo. Mais de 60% dos que usam IA no mundo percebem seu valor como ferramenta de combate à fraude.

Uma única ferramenta ou tecnologia por si só não chega a ser um programa antifraude. Você está coletando os dados certos de acordo com as regras e os requisitos adequados? Como a empresa analisa esses dados? Você está realimentando seu programa com as conclusões obtidas para torná-lo mais robusto? As empresas geralmente deixam de perceber o valor da tecnologia quando falham em fornecer os recursos certos para gerenciá-la, com a expertise adequada.



Ação: **Faça a coisa certa**

Sua resposta a uma fraude pode fazer toda a diferença para a continuidade da empresa. No mundo, cerca de 60% das organizações que conduziram uma investigação do problema acabaram em situação melhor – mas quase metade dos participantes da pesquisa não fazem essa investigação. E apenas cerca de um terço relata o problema ao conselho de administração.

Os reguladores – e a opinião pública – estão cada vez mais exigentes. Reagir de forma muito lenta pode não apenas causar danos imediatos, como também ampliar a crise.

55% das organizações no Brasil conduziram uma investigação do seu pior caso de fraude. Apenas 29% o informaram ao conselho de administração.

Globalmente, quais foram as principais medidas adotadas pelas organizações que saíram mais fortes de uma fraude?

Conduzir uma investigação (71%) — Chegar à raiz do problema é essencial para evitar mais fraudes. As empresas geralmente buscam ajuda externa para investigar a fraude quando a objetividade é crucial ou quando não têm a experiência nem os recursos necessários para fazer isso.

Divulgar o incidente às autoridades (37%) — A divulgação tempestiva pode levar a um resultado mais favorável na relação com os reguladores.

Reforçar controles internos, políticas e procedimentos (58%) — Embora algumas políticas e procedimentos sejam mais comuns, é importante avaliar as operações globalmente e identificar outros controles que possam estar faltando.

Aplicar medidas disciplinares aos infratores (44%) — A aplicação das medidas previstas em um programa de *compliance* é uma das chaves da sua eficácia. De acordo com as diretrizes regulatórias, os programas de *compliance* devem ser aplicados a todos: ninguém deve estar fora de seu alcance. Nenhuma pessoa deve ser considerada importante demais para escapar de ações disciplinares.

Realizar treinamentos (32%) — O treinamento não apenas informa melhor a equipe sobre novas políticas e procedimentos, como também fortalece a cultura de combate à fraude.



89%

reagiram com sentimentos/
emoções negativas

Não surpreende que a maioria dos participantes no mundo (89%) tenham experimentado emoções negativas após um incidente de fraude. Globalmente, os sentimentos mais positivos surgiram, por sua vez, quando:

- O principal autor era externo à organização (“fomos atacados”), não interno (“um de nós”) (48%).
- A organização encomendou uma investigação (71%) e implementou controles internos melhores (58%) depois que a fraude foi revelada.
- As empresas disseram ter se mantido fiéis aos seus valores, agido como equipe, além de ter preparado e implementado um plano.

A importância de fazer um balanço da crise

Ninguém quer ser vítima de uma fraude – muito menos ser acusado de cometer uma. Mas um incidente pode ser encarado de outra forma, como um ponto de inflexão, um possível gatilho para uma transformação organizacional. Se ela será positiva ou negativa – a chance de alcançar uma posição de mercado melhor, por exemplo, ou mergulhar em uma crise absoluta – depende do quanto você está preparado para enfrentar o evento e de como o gerencia.

Os dados mostram que há uma grande vantagem em fazer um balanço do incidente. Quase metade dos participantes que sofreram um crime econômico (43% no Brasil e 45% no mundo) dizem ter saído da crise em situação melhor – citando aspectos como avanços no ambiente de controle, operações mais simples, menos perdas e melhor ânimo dos funcionários. Grandes empresas tendem ainda mais (52%) a dizer que saíram melhores da situação, citando a adoção de novas tecnologias e menor repetição de incidentes, em conjunto com um ambiente melhor e operações simplificadas.



Eficácia: **Como medir o sucesso**

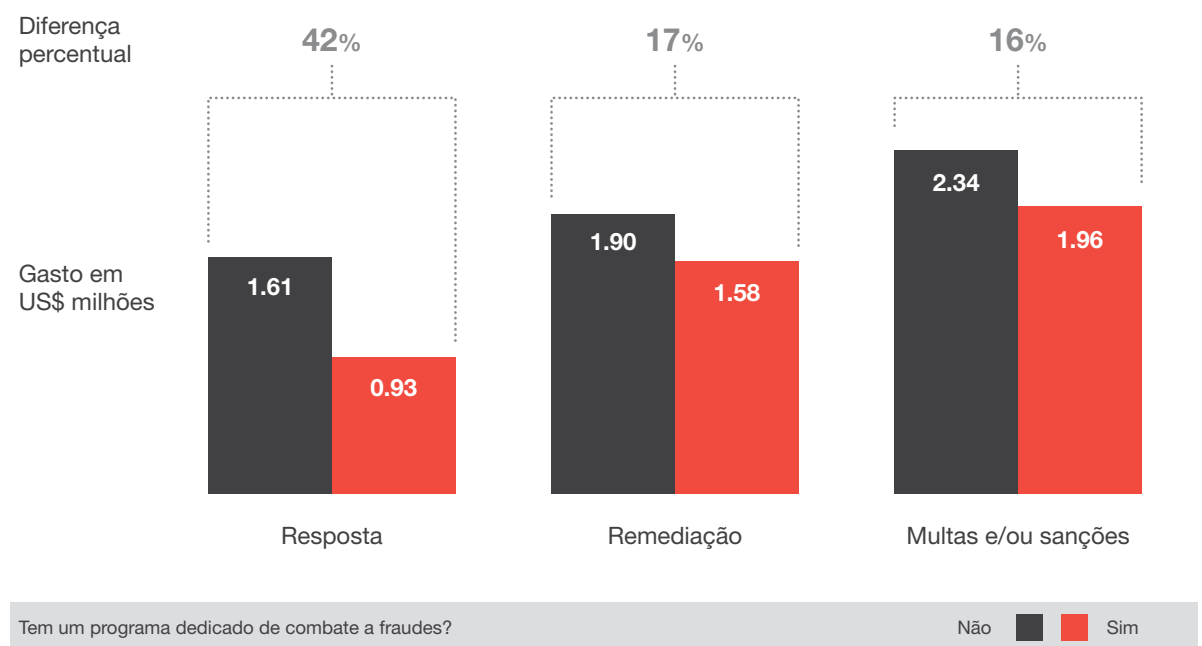
Os responsáveis pelo combate à fraude costumam se esforçar para aumentar seu orçamento a fim de investir em novas tecnologias, implementar novos programas ou contratar recursos adicionais. Ao todo, 43% no Brasil (40% no mundo) planejam aumentar seus gastos com prevenção a fraudes nos próximos dois anos. Mas será que as medidas adotadas serão eficazes e eles verão um retorno de seu investimento?

Quantificar os benefícios de uma ferramenta de combate à fraude é difícil, mas sabemos que um programa de prevenção efetivo reduz os efeitos e a magnitude de uma futura fraude. Com base nos resultados da pesquisa, observamos uma clara conexão entre os investimentos em mecanismos de prevenção a fraudes e custos reduzidos quando a fraude ocorre.

As empresas que têm um programa dedicado de combate a fraudes geralmente gastam menos (em relação à sua receita) com ações de resposta, remediação e com o pagamento de multas.

- As organizações com um programa dedicado de combate a fraudes gastaram 42% menos com ações de resposta e 17% menos com ações de remediação do que aquelas que não possuem um programa estabelecido.
- Nos casos em que houve suborno ou corrupção, as empresas com um programa dedicado a combater esse problema gastaram 58% menos em remediação do que as outras que não possuem o programa.

Empresas com programas estruturados de combate a fraudes gastam menos com resposta, remediação e multas (amostra global)



Quando se tem um programa em vigor, é essencial avaliá-lo e ajustá-lo periodicamente. Por quê?

- Os modelos de negócios costumam evoluir mais rápido que os programas de risco, deixando as empresas expostas a riscos inesperados.
- Há uma convergência cada vez maior em certas indústrias – por exemplo, empresas de tecnologia que oferecem serviços financeiros ou empresas de saúde que entram no mercado de produtos de consumo. Os programas de gerenciamento de riscos precisam ser adaptados para lidar com esses riscos novos ou em evolução.
- Um canal de denúncias ou uma constatação da auditoria pode trazer à tona um risco não considerado até então.

O mais importante em todo esse cenário talvez seja que os reguladores estão prestando mais atenção aos programas de *compliance* e esperam que as empresas apresentem evidências de que eles são realmente eficazes.

Muitos reconhecem que os programas de *compliance* devem ser baseados em riscos e ser dimensionados de forma adequada. Também há consenso que nenhum programa é capaz de identificar toda e qualquer atividade irregular. Não existe uma abordagem de *compliance* padrão: um programa de uma grande empresa de telecomunicações certamente deve ser diferente de outro de um pequeno varejista. No entanto, ambos devem ser adequados para lidar com os riscos específicos que cada organização enfrenta.

Da mesma forma, não há um método prescrito para avaliar a eficácia das ações. Muitos artigos acadêmicos sobre como avaliar a eficácia do treinamento fornecem informações úteis. No entanto, não há muitos recursos disponíveis sobre a avaliação da eficácia de um programa de gerenciamento de terceiros, por exemplo. Isso cria uma oportunidade para as empresas definirem seu próprio sistema de avaliação, que pode incluir aspectos como: estatísticas de racionalização de fornecedores, estatísticas de rejeição de fornecedores, participação de fornecedores em programas de treinamento, certificações de fornecedores ou menor número de pontos de atenção levantados pela auditoria de terceiros. A chave é adotar uma métrica defensável, capaz de demonstrar que a área do programa foi testada e como ela impediria ou detectaria problemas de conduta no futuro.

Contatos

Entenda melhor seus riscos de fraude e crime econômico e avalie seus programas em relação ao mercado e aos participantes globais da nossa pesquisa. Fale conosco.



Leonardo Lopes

Sócio – Forensic Services
leonardo.lobes@pwc.com
+55 (11) 3674 3826



José Figueira

Sócio – Forensic Services
jose.figueira@pwc.com
+55 (11) 3674 3826



Adriano Vargas

Sócio – Forensic Services
adriano.s.vargas@pwc.com
+55 (11) 3674 3843

PwC. Traga desafios. Leve confiança.
www.pwc.com.br



Neste documento, "PwC" refere-se à PricewaterhouseCoopers Contadores Públicos Ltda., firma membro do network da PricewaterhouseCoopers, ou conforme o contexto sugerir, ao próprio network. Cada firma membro da rede PwC constitui uma pessoa jurídica separada e independente. Para mais detalhes acerca do network PwC, acesse: www.pwc.com/structure

© 2020 PricewaterhouseCoopers Contadores Públicos Ltda. Todos os direitos reservados.

(DC0) Informação Pública

