A oportunidade de agir

Tendências e fatores por trás dos crimes econômicos no Brasil e no mundo

12%
das empresas brasileiras foram vítimas de crime econômico nos últimos 24 meses; globalmente foram 36%.

15%
das ocorrências foram crimes cibernéticos, um problema que cresce no mundo.

50%
das organizações pesquisadas no Brasil não acreditam que os agentes públicos estão preparados e treinados para investigar e punir crimes econômicos.

pwc

Apresentação

O Brasil vive nos últimos anos um momento crucial na sua história de combate à corrupção. De alguma forma, a nossa Pesquisa Global sobre Crimes Econômicos reflete essa situação. O índice de incidentes desse tipo relatados pelas empresas brasileiras vem caindo há cinco anos. Em 2016, no entanto, o recuo foi mais acentuado: o percentual de participantes do país que foram vítimas de um crime econômico caiu de 27% para 12%, um resultado a princípio surpreendente e uma das menores taxas entre os 115 países incluídos no estudo. No mundo, a tendência também foi de queda, mas o índice de crimes econômicos se manteve em patamar ainda elevado (36%), o que não dá trégua às organizações globais no combate a essa ameaça.

A situação brasileira pode ter sido influenciada por três possíveis fatores – ou por uma combinação deles. O primeiro seria uma consequência dos investimentos feitos em prevenção. Acreditamos que a nova Lei Anticorrupção, sancionada em 2013, possa ter melhorado os controles preventivos em muitas organizações. E a nossa pesquisa capturou alguns dados positivos nesse sentido.

Uma segunda explicação possível seria uma piora na detecção por mecanismos sob controle da administração, que caiu praticamente à metade em dois anos. Cresceu muito também o percentual dos incidentes revelados por mecanismos fora da influência da gestão, como a mídia ou os agentes públicos. Além disso, aumentou a importância das delações e dos canais formais de denúncia, um possível sinal da intolerância crescente da sociedade em relação a esses malfeitos.

No momento em que o país discute os maiores casos de corrupção da sua história, acreditamos que a pressão da mídia e dos órgãos públicos possa estar por trás de um terceiro fator, de caráter mais comportamental, que não encontra paralelo em outras partes do mundo. Com a forte repercussão das investigações, até mesmo no exterior, e punições pesadas para os envolvidos, é natural que a atuação dos criminosos tenha sido inibida, mesmo que temporariamente.

É certo que toda essa transformação representa para as empresas brasileiras uma oportunidade única de agir. Cabe a elas tomar as rédeas do combate ao crime econômico e influenciar o cenário que se instalará depois que diminuir a repercussão dos grandes escândalos revelados nos últimos anos. Os líderes podem aproveitar as mudanças culturais em curso para fortalecer suas defesas, sobretudo contra o avanço da fraude em compras, que registra no Brasil o maior percentual global.

Os dados da nossa pesquisa também mostram que os avanços tecnológicos estão mudando o perfil do crime econômico no mundo. As organizações devem se preparar para combater essa ameaça em novas frentes. Por esse motivo, o nosso relatório deste ano se concentra em três temas principais – o crime cibernético, os programas de ética e *compliance* e a prevenção à lavagem de dinheiro. E destacamos questões específicas que as empresas devem focar e o que elas podem melhorar para combater esses problemas.

Esperamos que o conteúdo das próximas páginas contribua para promover o debate franco sobre diferentes aspectos do crime econômico, uma ameaça preocupante para o crescimento das empresas e do país e um tema de interesse de toda a sociedade brasileira.

Fernando Alves
PwC Brasil
Sócio-presidente

Martin J. Whitehead
PwC Brasil
Sócio e líder de Forensic Services

Destaques

1 *Uma ameaça permanente*

- 36% das organizações globais foram vítimas de crimes econômicos. No Brasil, foram 12%, entre as menores taxas do mundo, após uma queda acentuada. A média dos BRICS ficou em 39%.
- Mercados desenvolvidos e emergentes afetados.
- Os métodos de detecção das empresas não acompanham a evolução das ameaças.

Quais são as oportunidades para combater o crime econômico de forma proativa?

No mundo, o índice se manteve estável. No Brasil, caiu de forma acentuada

2 *Os controles precisam estar embutidos na cultura organizacional*

- Globalmente, 22% dos participantes nunca realizaram uma avaliação de risco de fraude. No Brasil, foram 17%.

Que riscos a sua empresa enfrenta? Você identifica ativamente as áreas vulneráveis?

Os prejuízos financeiros ultrapassam centenas de milhões de dólares em alguns casos

3 *Empresas demonstram falta de preparo para lidar com o crime cibernético*

- O crime cibernético é o segundo tipo mais comum de crime econômico no mundo, com 32% das menções. O Brasil registrou uma queda na incidência, de 17% para 15%, mas 21% das empresas não sabem dizer se foram atacadas.
- A maioria das empresas ainda não está preparada nem mesmo para entender os riscos cibernéticos que enfrenta: apenas 37% das empresas no mundo, 29% no Brasil, têm um plano de resposta a incidentes.
- O comprometimento da liderança é essencial, mas menos de metade dos membros dos conselhos de administração solicita informações sobre o estado de prontidão cibernética da organização.

O seu plano de resposta cibernética está adequado à realidade?

O processo de fortalecimento da prontidão cibernética pode ser encarado como um teste de estresse organizacional

4 *Há uma desconexão entre o discurso e a realidade*

- Mais de 15% dos participantes no Brasil e no mundo desconhecem a existência de um programa formal de ética e *compliance*.
- No Brasil, 58% dos crimes econômicos são cometidos por agentes internos. No mundo, são 46%.
- Nas fraudes internas, 87% dos criminosos brasileiros estão em cargos de gerência executiva ou intermediária. No mundo, 51%.

A sua estratégia de negócios está alinhada com os valores da organização?

As pessoas e a cultura são a sua primeira linha de defesa

5 *A prevenção à lavagem de dinheiro ainda traz desafios*

- 41% das instituições financeiras brasileiras não passaram por inspeções regulatórias: uma em cada 10 teve problemas significativos na inspeção ou estava em um programa de remediação. **Os executivos podem ser responsabilizados pessoalmente por deixar de coibir práticas de negócios ilícitas.**
- Mais de 60% das instituições financeiras brasileiras não realizaram (ou não sabem se realizaram) uma avaliação de riscos de lavagem de dinheiro ou financiamento do terrorismo.
- Sistemas legados complexos comprometem os esforços de conformidade.
- A falta de equipes experientes em prevenção à lavagem de dinheiro e combate ao financiamento do terrorismo é um problema importante.

Como a sua organização se sairia em uma inspeção regulatória?

O custo da conformidade (e da não conformidade) continua a crescer

Conteúdo

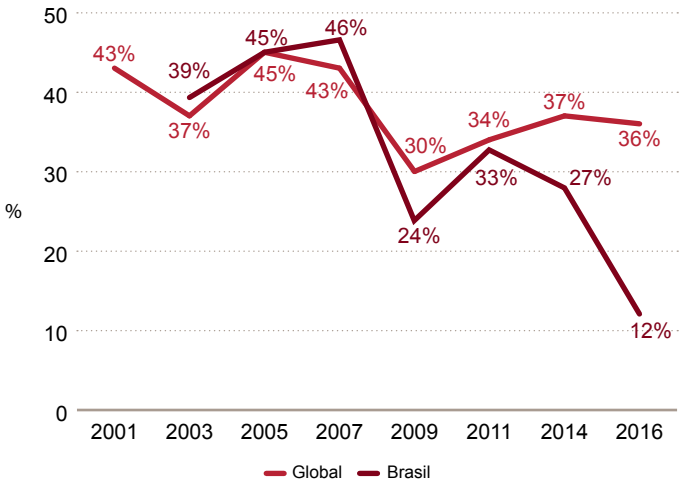
Visão geral

Fraudes despencam no Brasil: maturidade crescente, mudança temporária ou algo à espreita?

O Brasil passou a integrar o grupo de países com índices mais baixos de crimes econômicos no mundo. Na Pesquisa Global sobre Crimes Econômicos 2016 da PwC, apenas 12% dos respondentes brasileiros relataram ter sido vítimas de algum tipo de crime econômico nos últimos 24 meses. O percentual representa apenas um terço da média global deste ano e também é muito menor que o índice de 39% dos BRICS (bloco formado por África do Sul, Brasil, China, Índia e Rússia).

Esse resultado parece contrariar o senso comum a respeito do Brasil e também outros dados disponíveis sobre o ambiente corporativo nacional. Uma análise mais profunda das informações coletadas nesta oitava edição da nossa pesquisa bianual, no entanto, leva a crer que, nos últimos dois anos talvez tenha começado a se produzir uma mudança em consequência de alguns acontecimentos, como a investigação dos mais graves escândalos de corrupção da história do país, uma pressão crescente dos reguladores e a entrada em vigor de uma nova Lei Anticorrupção.

Fig 1: Evolução dos crimes econômicos



A queda do índice brasileiro segue uma tendência global, mas se revela muito mais pronunciada. Enquanto o mundo registrou uma queda de um ponto percentual em relação a 2014 (a primeira desde a crise financeira de 2008/2009) e o índice dos BRICS recuou 5 pontos percentuais, o Brasil teve uma redução de 15 pontos no mesmo período, após outra de 6 pontos observada entre 2011 e 2014. Em um momento em que esse tema está mais do que nunca no centro das discussões, o que se reflete também na piora da classificação do país no mais recente ranking de percepção da corrupção divulgado pela Transparência Internacional,[1] qual seria a explicação para uma mudança de rumos tão forte?

> **"A queda relatada na pesquisa parece coincidir com o que os clientes estão nos dizendo com base em sua experiência."**
>
> **Martin J. Whitehead, sócio e líder de Forensic Services da PwC Brasil**

Os dados e a nossa experiência na prevenção e no combate aos crimes econômicos apontam para três fatores que podem ter contribuído, de forma individual ou combinada, para esse fenômeno. Acreditamos que, em alguns casos, houve uma melhora nas medidas preventivas empregadas para conter o crime econômico na sua origem. Em contrapartida, porém, observamos que os mecanismos adotados para detectar esses incidentes talvez estejam falhando e que muitos crimes podem estar sendo cometidos sem ser notados. Em paralelo a essas duas tendências, acreditamos que as empresas estão vivendo uma transformação cultural importante como consequência dos escândalos recentes de corrupção, o que leva a uma espécie de "abstenção temporária" do fraudador. "Algo estranho parece ter acontecido no Brasil recentemente em relação à incidência dos crimes econômicos – mas a queda relatada na pesquisa parece coincidir com o que os clientes estão nos dizendo com base em sua experiência", afirma Martin J. Whitehead, sócio e líder de Forensic Services da PwC Brasil.

[1] Transparency International. Corruption Perceptions Index 2015 – o Brasil ocupa a 76ª posição entre 168 países, sete posições abaixo do ano anterior.

A melhora nos sistemas de prevenção pode estar associada a investimentos feitos nos últimos dois anos. Os dados mostram um aumento percentual de empresas que realizam uma avaliação de risco de fraudes no mínimo a cada semestre. Além disso, mais de 90% das organizações mantiveram ou ampliaram os gastos com programas e recursos de *compliance* nos últimos 24 meses. A maioria também afirma ter um código de conduta que estabelece valores e comportamentos esperados, além de realizar treinamentos e comunicações regulares sobre as regras nele contidas. Em relação a esse aspecto, é importante ressaltar também a influência da nova Lei Anticorrupção brasileira, sancionada em 2013. Sua entrada em vigor incentivou as empresas a implantar programas de *compliance* mais robustos para prevenir fraudes e evitar sanções. "A nova lei pode ter dado o impulso inicial nesse processo e, de fato, muitos dos nossos clientes estão levando o tema a sério e já implantaram controles preventivos melhores", afirma Leonardo Lopes, sócio da PwC Brasil e especialista em Forensic Services.

> **"A nova lei pode ter dado o impulso inicial nesse processo."**
>
> **Leonardo Lopes, sócio da PwC Brasil e especialista em Forensic Services**

Uma explicação mais pessimista para a forte diminuição do índice brasileiro de crimes econômicos poderia ser a redução na eficácia dos mecanismos de detecção. De fato, o percentual de incidentes revelados por métodos sob controle da administração caiu quase à metade no país (de 52% para 30%). O resultado reflete a tendência global, mas é bem mais acentuado. Além disso, mais que dobrou (de 13% para 30%) o percentual dos crimes identificados por métodos fora do controle da administração. O destaque nessa categoria foi o aumento relativo dos incidentes descobertos pela mídia ou por agentes públicos (de 3% para 17%). Esse dado parece demonstrar que a sociedade em geral está menos tolerante a esse tipo de conduta. A pesquisa também revela que a cultura corporativa mantém sua importância no combate ao crime econômico: a detecção relacionada a delações e sistemas formais de denúncias aumentou de 34% para 39%, também indicando um baixo nível de aceitação desse tipo de atividade no ambiente de negócios.

O terceiro fator – uma aparente e talvez temporária mudança de comportamento – é provavelmente o aspecto mais interessante e característico do Brasil no período coberto pelo estudo. No entanto, devemos ter cautela quanto a essa explicação, pois, embora ela esteja de acordo com as evidências que obtivemos em conversas informais regulares com clientes e executivos, é difícil obter dados que a comprovem.

Qualquer mudança aparente de comportamento – como a propensão reduzida para cometer crimes econômicos – pode estar associada a vários fatores, mas possivelmente o de maior impacto seja a pressão exercida pela mídia e pelos agentes públicos em relação à maior investigação de corrupção da história brasileira. Os dados sobre mecanismos de detecção mencionados antes parecem confirmar essa hipótese. Em um cenário de negócios marcado por vigilância crescente e grande atenção da opinião pública, é provável que os fraudadores estejam menos dispostos a correr riscos. Pode-se supor que toda essa pressão tenha coibido a ação dos criminosos.

Duas outras conclusões do estudo parecem ser bastante específicas do Brasil e diferentes das tendências globais. Em primeiro lugar, os dados revelam que os crimes cibernéticos estão em um patamar equivalente à metade da média global (15%, contra 32% no mundo) e caindo. Esse resultado contradiz as conclusões de outro estudo da PwC, a Pesquisa Global sobre Segurança da Informação 2016, que revela um aumento desses incidentes no país e no mundo. Nossa experiência também aponta para uma preocupação cada vez maior dos líderes com relação à ameaça que os crimes cibernéticos representam. Os dados sugerem, portanto, um possível problema de eficácia dos controles cibernéticos, que talvez não estejam detectando os ataques em andamento, um risco também observado na pesquisa global.

Em segundo lugar, a fraude em compras continua a ser um problema brasileiro. Em 2014, o país registrou o mais alto nível desse tipo de incidente (44%) no mundo. Naquela edição, esse tipo de crime econômico alcançou o segundo lugar na classificação brasileira, atrás apenas de roubo de ativos. Este ano, a incidência relativa da fraude em compras aumentou ainda mais: 58% e novamente a mais alta do mundo. Ao mesmo tempo, o índice de suborno e corrupção (o terceiro tipo de crime mais comum no país) caiu de 28% para 23%, espelhando a tendência global. A repercussão dos recentes acontecimentos no Brasil também poderia ser uma explicação para essa mudança. "A pressão pode ter ajudado a coibir os casos de suborno e corrupção e, ao mesmo tempo, a elevar a vigilância das empresas sobre seus contratos a fim de reduzir o risco de fraude em compras, um crime especialmente difícil de ser detectado e que costuma ser objeto de menos atenção", explica Whitehead.

Quando levamos em conta os resultados da Pesquisa Global com CEOs 2016 – em que quase três quartos dos executivos brasileiros afirmam que nunca houve tantas ameaças (dos mais diferentes tipos) ao crescimento das suas corporações – percebemos que uma abordagem passiva do crime econômico pode ser uma receita para o desastre. Afinal, quando toda a pressão da mídia e da Justiça brasileiras em relação aos acontecimentos recentes diminuir, há o risco de que os criminosos voltem silenciosamente a dilapidar as empresas.

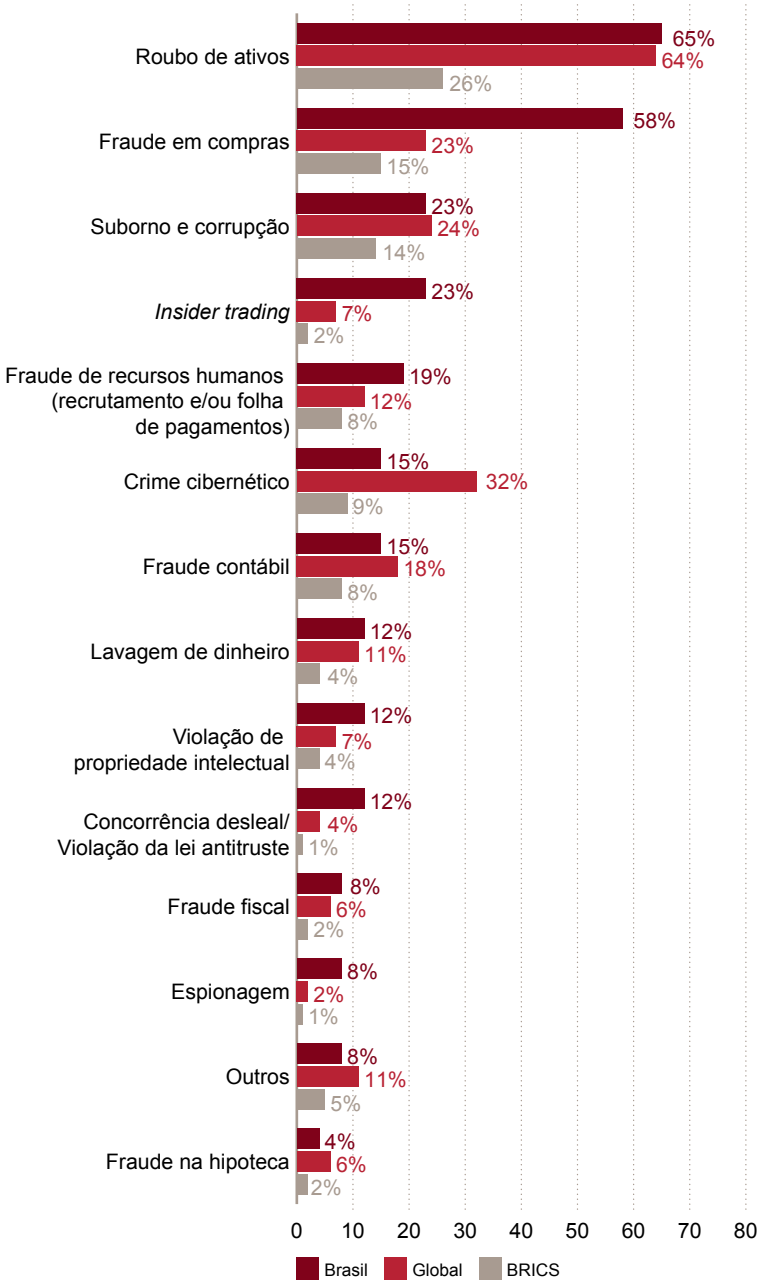
Para ajudar as organizações a agir em relação a esse sério problema, a nossa pesquisa sobre crimes econômicos deste ano se concentra em três áreas principais – o crime cibernético, os programas de ética e *compliance* e a prevenção à lavagem de dinheiro. Nas próximas páginas, exploramos alguns temas comuns nesse debate, como a gestão dos riscos associados à difusão crescente da tecnologia; o significado de conduzir negócios de forma responsável em um cenário cada vez mais complexo; e maneiras de integrar a conduta ética tradicional ao processo de tomada de decisões.

Além de destacarmos áreas específicas relacionadas aos crimes econômicos que as empresas devem focar, enfatizamos as práticas para melhor combater esse problema: implementar medidas mais sofisticadas e eficazes, capazes de reduzir riscos e tornar a empresa mais consciente sobre as ameaças existentes e confiante nas suas defesas.

A fraude em compras cresce no país

Os tipos mais comuns de crimes econômicos informados pelos participantes da nossa pesquisa este ano são destacados na figura a seguir.

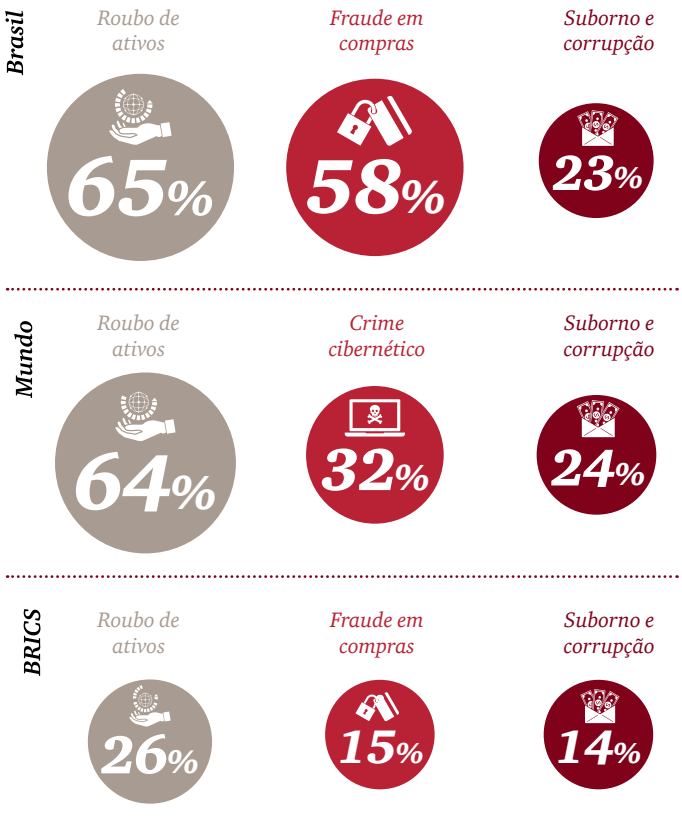
Fig 2: Tipos de fraude



No Brasil, a fraude em compras foi o tipo de crime econômico que mais cresceu em relação à edição anterior (de 44% para 58%). Em um cenário de intensa pressão da mídia e dos órgãos de investigação, é possível que as empresas estejam muito mais atentas aos seus contratos, o que explicaria o forte aumento do percentual de casos detectados. O roubo de ativos se manteve praticamente estável em primeiro lugar, enquanto suborno e corrupção aparece em terceiro lugar, mas recuou de 28% para 23%.

No cenário global, os tipos de fraudes que tradicionalmente lideram a pesquisa – como roubo de ativos, suborno e corrupção, fraude em compras e fraude contábil – registraram uma ligeira queda em relação aos números de 2014. No entanto, um tipo de crime vem crescendo de modo consistente desde que começou a ser medido pela nossa pesquisa: o crime cibernético, atualmente em segundo lugar no mundo e em sexto lugar no Brasil. Considerando a queda na taxa de detecção de incidentes por meios sob controle da administração no mundo, nossa dúvida é se a detecção desses crimes mais tradicionais está ficando mais difícil ou se simplesmente as empresas estão menos conscientes dos riscos que enfrentam para combatê-los.

Fig 3: Três tipos mais comuns de crimes econômicos em 2016



A prevalência do roubo de ativos na nossa pesquisa ano após ano é previsível, já que esse crime é tradicionalmente visto como o mais fácil de detectar. No entanto, desde 2011, observamos uma tendência de queda nos índices declarados nessa categoria no Brasil e no mundo. Isso pode ser um sinal de controles organizacionais mais rigorosos – e de que as empresas estão ficando melhores na prevenção do crime econômico tradicional – ou de que o roubo de ativos está evoluindo para fraudes mais sofisticadas e diferentes, difíceis de detectar, como o crime cibernético.

Está ficando mais difícil detectar alguns crimes econômicos ou as empresas estão menos conscientes dos riscos que enfrentam?

Essa é uma das questões que buscamos investigar na Pesquisa Global sobre Crimes Econômicos 2016. Como, em média, um quinto de todos os participantes acredita que, nos próximos 24 meses, sua organização provavelmente será vítima de um dos principais crimes econômicos aqui destacados, o momento de rever sua atuação é agora.

Um problema global, com diferenças regionais

Região	Crimes econômicos relatados em 2016	Crimes econômicos relatados em 2014
África	57%	50%
Europa Ocidental	40%	35%
América do Norte	37%	41%
Europa Oriental	33%	39%
Ásia-Pacífico	30%	32%
América Latina	28%	35%
Oriente Médio	21%	21%
Global	**36%**	**37%**

A maioria das regiões relatou índices menores de crimes econômicos, com exceção da África, da Europa Ocidental e do Oriente Médio. Na América Latina, os maiores índices foram registrados no Chile (39%, 7 pontos acima do resultado de 2014) e no México (37%, alta de apenas um ponto). Venezuela (33%, 12 pontos a menos que na edição anterior) e Colômbia (32%, em sua primeira participação expressiva na pesquisa) ficaram quase empatadas em terceiro lugar.

Os principais países africanos responsáveis pelo aumento dos índices de crime econômico na região foram a África do Sul (69%, inalterado desde 2014), seguida por Quênia (61%, 17 pontos percentuais acima da taxa de 2014) e Zâmbia (61%, com um aumento de 35 pontos).

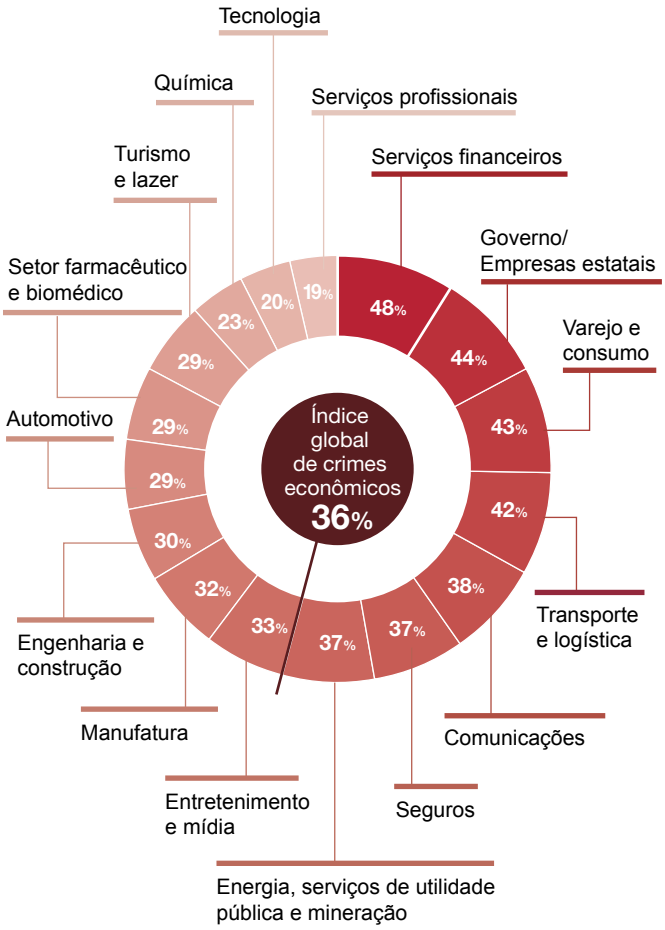
O resultado da Europa foi liderado pela França (68%) e pelo Reino Unido (55%), com 13 e 11 pontos percentuais a mais do que em 2014, respectivamente. Esses números mostram que o crime econômico não está restrito aos mercados emergentes, mas é uma questão importante para as nações desenvolvidas também.

Embora a maioria dos países desenvolvidos tenha aumentado a sua vigilância regulatória – especialmente em torno de aspectos críticos, como o crime cibernético, a lavagem de dinheiro, o suborno e a corrupção – a natureza transnacional das atividades criminosas está levando a um crescente nível de cooperação internacional em termos de regulação e fiscalização.

As organizações têm, portanto, uma oportunidade – não importa seu tamanho ou sua diversidade geográfica – de adotar uma visão global e aplicar padrões internacionais a seus esforços de combate ao crime econômico.

Como o crime econômico afeta as diferentes indústrias?

Fig 4: Que setores estão em mais risco no mundo?



O setor de serviços financeiros é o mais suscetível ao crime econômico, sobretudo por atender as necessidades financeiras de todas as outras indústrias. No entanto, com o mercado evoluindo para soluções de negócios integradas, várias organizações de serviços tradicionalmente não financeiras estão atendendo às demandas de seus clientes nessa área.. Muitas empresas de serviços não financeiros nos setores automotivo, varejo e consumo e comunicações, para citar apenas alguns exemplos, estão atuando em parceria com empresas de serviços financeiros ou têm suas próprias licenças de operação para prestar serviços nesse segmento, o que amplia o universo de alvos para ocorrências em operações financeiras.

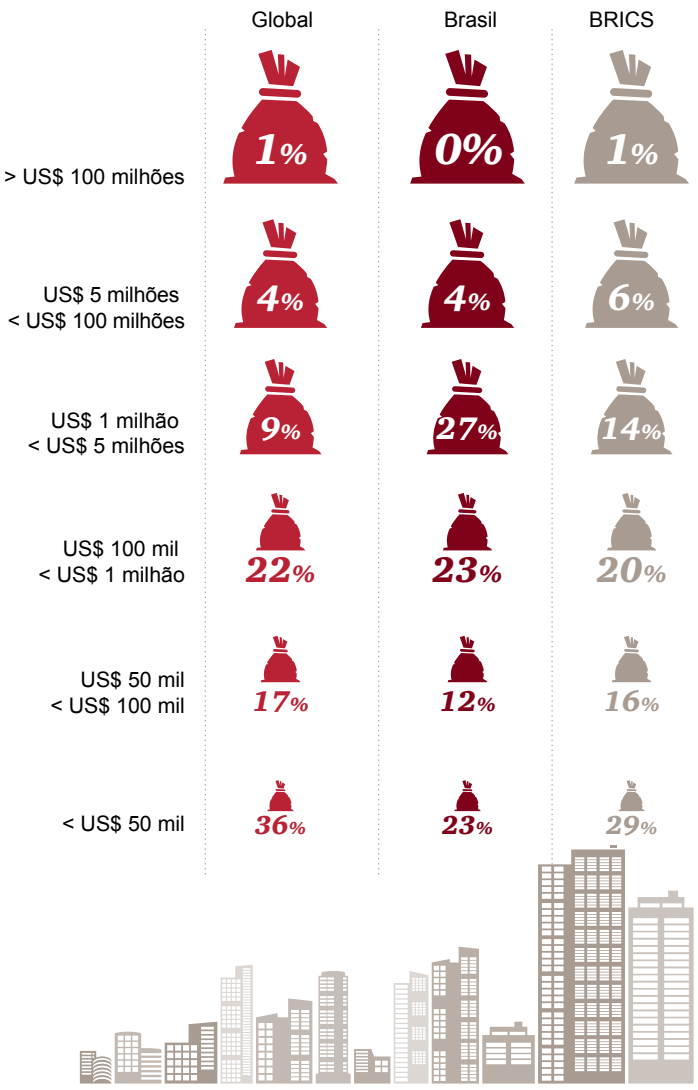
Ao longo de décadas, o setor de serviços financeiros, em virtude do seu ambiente altamente regulado, construiu mecanismos de controle, metodologias de detecção e ferramentas de gestão de riscos altamente sofisticadas. Mas as organizações híbridas ainda precisam evoluir na gestão dos riscos ou das mudanças do ambiente de *compliance* no qual agora atuam.

Os prejuízos financeiros

Nos últimos 24 meses, 54% das empresas brasileiras participantes da nossa pesquisa tiveram prejuízos financeiros relacionados a crimes econômicos entre US$ 100 mil e US$ 100 milhões. Houve uma queda em relação aos 59% registrados na pesquisa de 2014. Mas o resultado foi superior à média global (35%) e ao percentual registrado entre os BRICS (41%) em 2016. A maioria das empresas globais (53%) teve prejuízos abaixo de US$ 100 mil. Nessa faixa, ficaram 35% das empresas brasileiras e 45% das classificadas entre os BRICS. Apenas 1% dos participantes globais foi vítima de crimes econômicos com prejuízos acima de US$ 100 milhões, predominantemente na América do Norte e na região da Ásia-Pacífico. No Brasil, nenhuma empresa entrevistada informou prejuízos acima desse valor.

O verdadeiro custo do crime econômico para a economia global é difícil de estimar, especialmente considerando que o prejuízo financeiro real geralmente é só um pequeno componente do rol de consequências de um incidente grave. Interrupções no negócio, medidas de remediação, intervenções para investigação e prevenção, multas regulatórias, honorários legais, entre outras despesas, tudo isso tem um impacto nos resultados, e esses custos podem ser enormes, embora, em grande parte, inestimáveis.

Fig 5: Impacto financeiro



O perfil do fraudador

Os agentes internos continuam a dominar o perfil dos fraudadores que atacam as organizações, embora em um percentual um pouco menor do que na última edição da nossa pesquisa. No Brasil, foram 58%, contra 64% em 2014, e, no mundo, foram 46%, em comparação com 56% na pesquisa anterior.

Quase 90% dos fraudadores internos fazem parte da gerência média ou executiva das empresas brasileiras, um percentual que cresceu muito em relação aos 56% da edição anterior da pesquisa. Esse aumento segue em tendência contrária à observada no mundo. Os dados globais mostram uma redução do percentual de fraudadores nesses níveis hierárquicos de 62%, em 2014, para 51%, este ano. Nos BRICS, mesmo com a alta acentuada do Brasil nos últimos dois anos, eles representavam 74%, em 2014, e, atualmente, são 62% do total.

Esses resultados apontam para uma possível fragilidade dos controles internos, cujas medidas servem mais como exercícios burocráticos para "cumprir tabela" do que processos incorporados à cultura da organização. Tal hipótese é reforçada pelo fato de que 17% dos respondentes no Brasil (22% no mundo e 19% nos BRICS) nunca realizaram uma avaliação de risco de fraude. Outros 28% realizam esse tipo de avaliação apenas anualmente no país (31% no mundo e 29% nos BRICS).

Atualmente, as organizações têm a oportunidade de repensar suas estruturas de controle e fortalecer seus fundamentos. Criar uma cultura de controles e consciência sobre riscos, em vez de atividades ritualizadas, e adotar a tolerância zero em relação às práticas desonestas pode ajudar a proteger as organizações de prejuízos evitáveis causados por fraudes internas.

Fig 6: Nível hirárquico

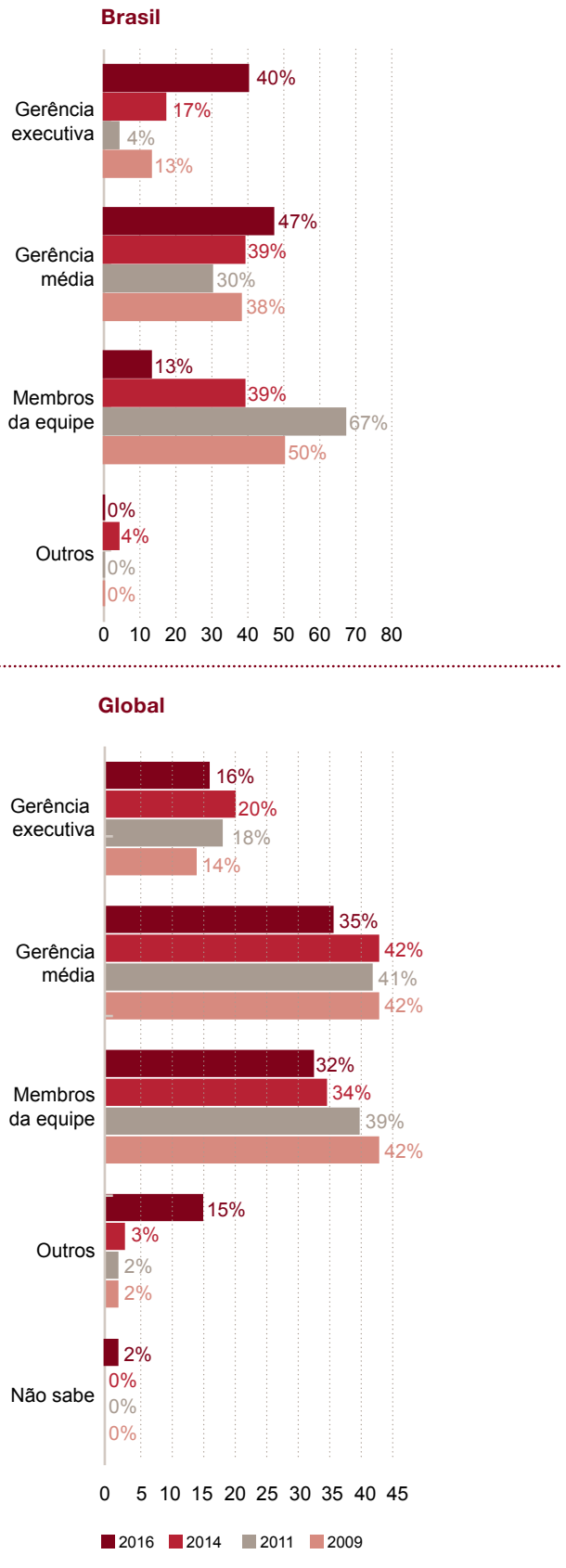
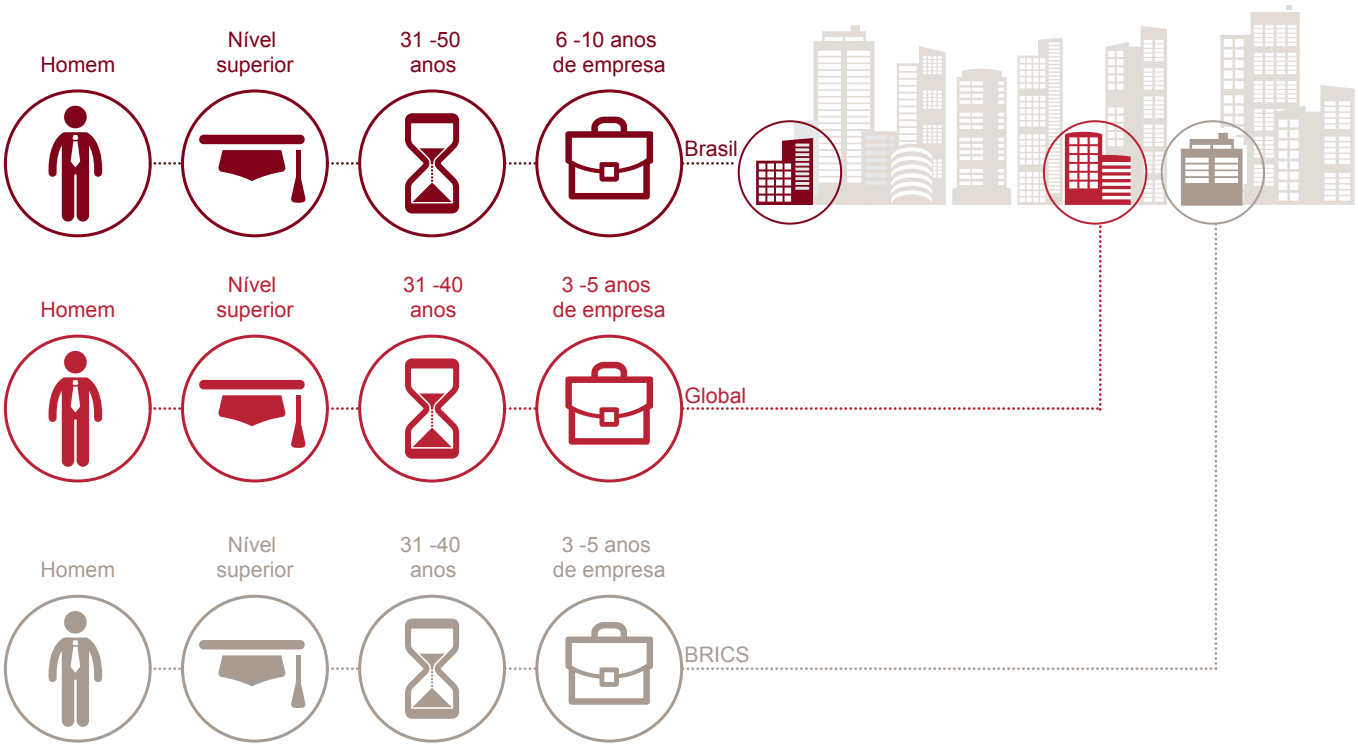


Fig 7: Características mais prováveis do fraudador interno



Os mecanismos de detecção

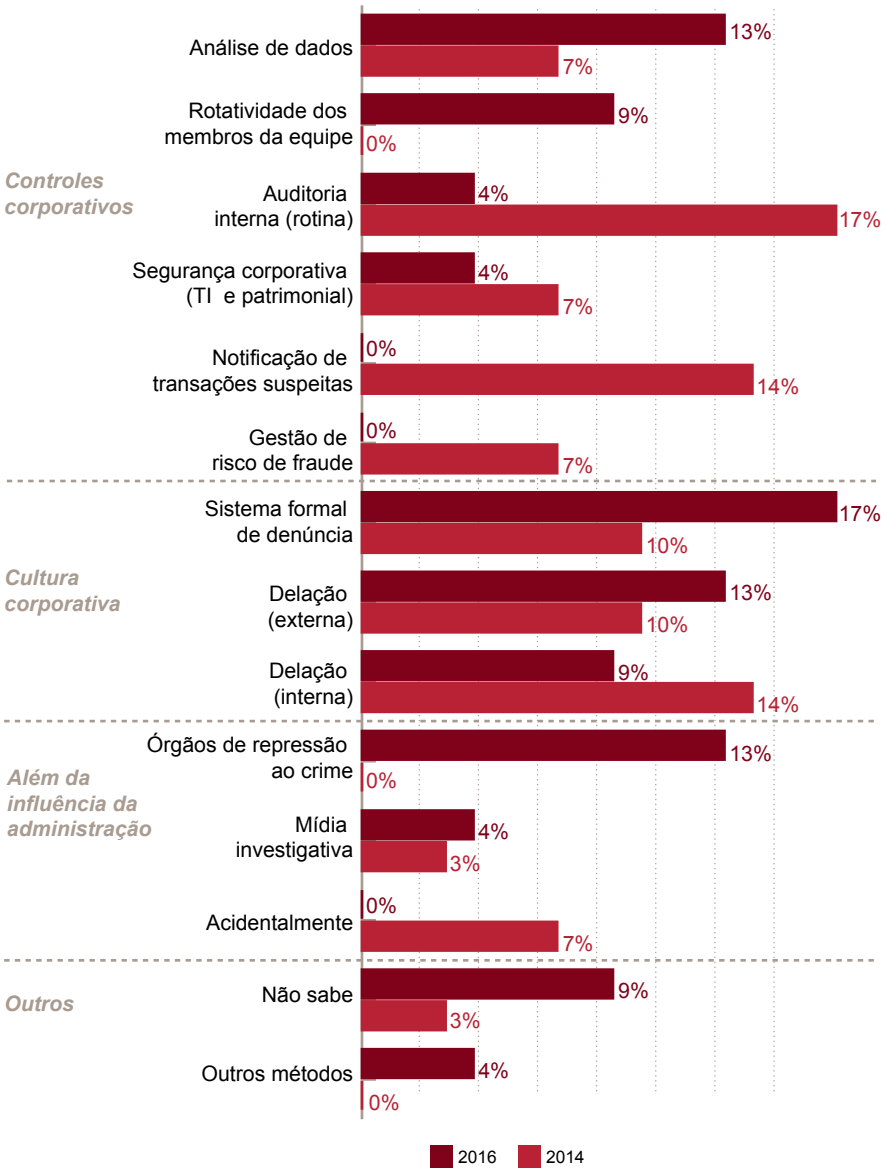
De forma geral, no Brasil e no mundo, houve uma redução no índice de crimes detectados por mecanismos sob controle da administração. Globalmente, essa queda foi de 55% para 48%; no Brasil, o percentual despencou de 52% para 30%. A análise de dados se tornou o principal método de descoberta de crimes nessa categoria no Brasil, enquanto, no mundo, a notificação de transações suspeitas manteve a liderança. Em termos globais, houve também um forte aumento dos crimes detectados por acidente, um índice que foi zerado pelo Brasil.

Chama a atenção no Brasil o peso conquistado pelos sistemas formais de denúncias, por delações externas e pelos órgãos públicos na identificação dos incidentes, o que de certa forma reflete a forte repercussão dos grandes casos de corrupção revelados nos últimos dois anos no país e o aumento da intolerância da sociedade em relação a esses crimes. A mídia também aumentou ligeiramente sua participação.

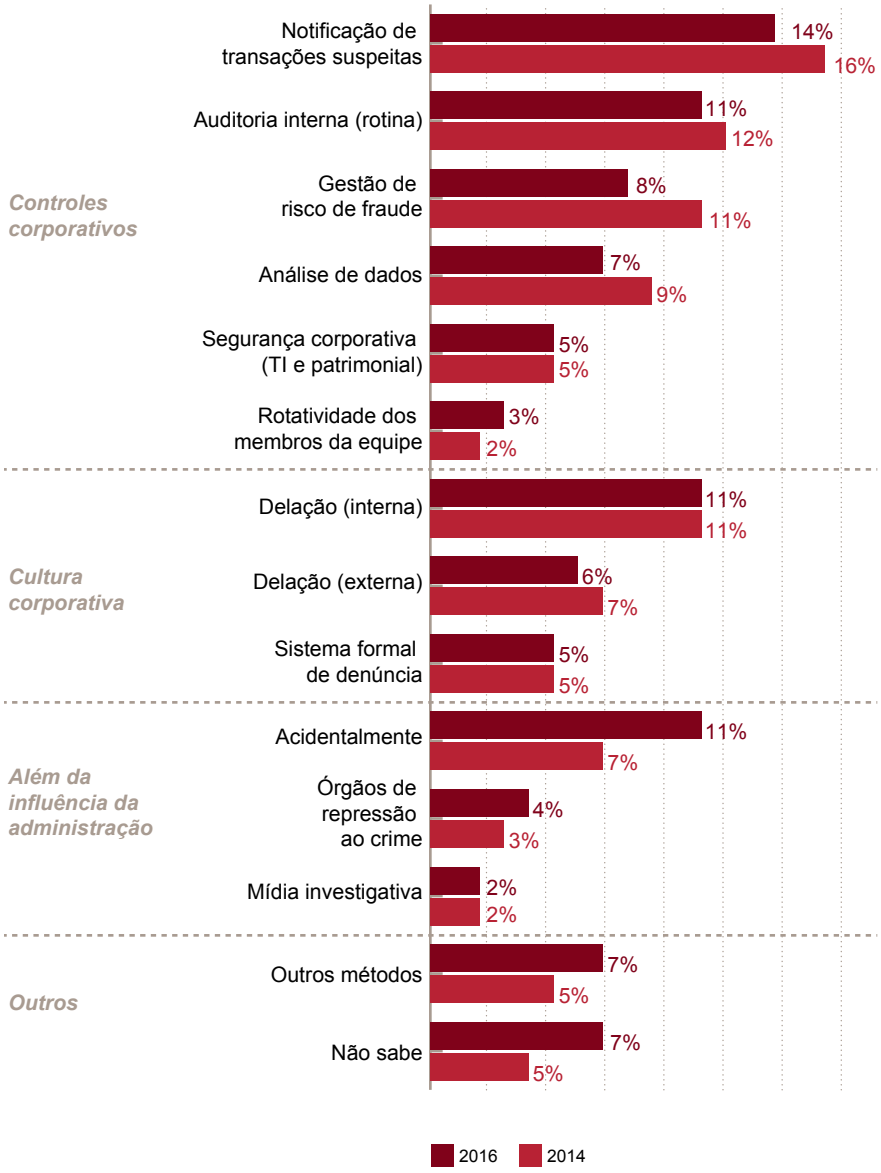
De modo geral, o resultado dos BRICS na classificação dos principais métodos de detecção de crimes econômicos foi bastante semelhante ao global.

Fig 8: Principais métodos de detecção

Brasil

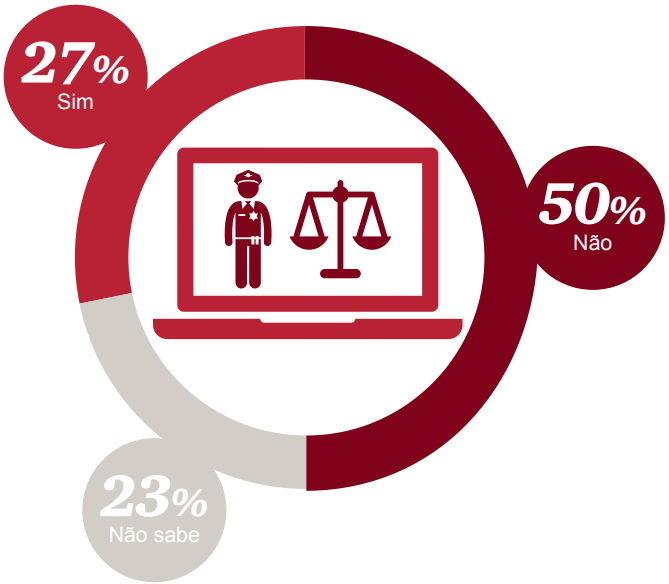


Global


Controles corporativos
Notificação de transações suspeitas
14%
16%
Auditoria interna (rotina)
11%
12%
Gestão de risco de fraude
8%
11%
Análise de dados
7%
9%
Segurança corporativa (TI e patrimonial)
5%
5%
Rotatividade dos membros da equipe
3%
2%
Cultura corporativa
Delação (interna)
11%
11%
Delação (externa)
6%
7%
Sistema formal de denúncia
5%
5%
Além da influência da administração
Acidentalmente
11%
7%
Órgãos de repressão ao crime
4%
3%
Mídia investigativa
2%
2%
Outros
Outros métodos
7%
5%
Não sabe
7%
5%
2016
2014

Percepção sobre a aplicação da lei

Fig 9: Você acredita que os agentes de repressão ao crime no Brasil estão adequadamente preparados e treinados para investigar e processar crimes econômicos?



No mundo, 45%, em média, forneceram uma resposta negativa a essa pergunta, enquanto 31% disseram não saber. Entre os BRICS, esses percentuais foram, respectivamente, 51% e 23%, em média, considerando a situação de cada país que compõe o bloco.

10 países com maior índice de crimes econômicos

1	África do Sul	69%
2	França	68%
3	Quênia	61%
4	Zâmbia	61%
5	Espanha	55%
6	Reino Unido	55%
7	Austrália	52%
8	Rússia	48%
9	Bélgica	45%
10	Holanda	45%

Obs.: A lista contém apenas países com mais de 40 participantes.

Os participantes do Quênia e da África do Sul são os menos confiantes na capacidade dos órgãos locais de repressão ao crime de investigar e processar crimes econômicos, e isso está correlacionado aos altos índices de incidentes informados nesses países.

No entanto, não estamos lidando com uma ciência perfeita. Uma análise mais detalhada sugere que essa métrica pode ser influenciada por vários fatores. Entre eles, a divulgação feita pelos órgãos de repressão ao crime de cada país sobre sua expertise em determinadas áreas, como crime cibernético, e o grau de interferência política que eles aparentam sofrer.

15 países com menor índice de confiança na capacidade dos órgãos de repressão ao crime

1	Quênia	73%
2	África do Sul	70%
3	Zâmbia	67%
4	Nigéria	62%
5	Luxemburgo	59%
6	Estados Unidos	58%
7	Ucrânia	57%
8	Reino Unido	57%
9	México	57%
10	Turquia	56%
11	Croácia	55%
12	Bulgária	53%
13	Filipinas	52%
14	Polônia	52%
15	Venezuela	52%

Obs.: A lista contém apenas países com mais de 40 participantes.

Oportunidade para avançar

Ao longo das próximas páginas do relatório, enfatizamos o aspecto mais estratégico da *oportunidade* e não tanto os números da pesquisa – por mais importantes que essas métricas possam ser. Nosso objetivo foi responder à seguinte pergunta: O que esses dados realmente representam para a *sua* empresa?

Os números da pesquisa podem ajudar a revelar não só sinais de alerta e tendências preocupantes, conforme abordamos nas três próximas seções, dedicadas a temas altamente estratégicos (crime cibernético, prevenção à lavagem de dinheiro e programas de ética e *compliance*). Os dados também servem como indicadores importantes de áreas em que as organizações têm oportunidade para avançar. Estar prevenido é estar preparado para o sucesso.

Crimes cibernéticos

Embora os ativos militares sejam considerados altamente seguros, os criminosos descobriram que fornecedores de "baixo risco" têm vulnerabilidades de segurança que podem ser facilmente exploradas e usadas para controlar o destino desses suprimentos.

Uma ameaça sem fronteiras

A tecnologia digital continua a transformar e revolucionar o mundo dos negócios, expondo as organizações a oportunidades e riscos. Não surpreende, portanto, que o crime cibernético continue crescendo no mundo – classificado como o segundo tipo de crime econômico mais comum nesta edição da nossa pesquisa.

Como todos os outros aspectos dos negócios, o crime econômico, de alguma forma, também se tornou digital. Em um ambiente de negócios hiperconectado, que muitas vezes atravessa as jurisdições, uma falha em qualquer conexão desse sistema – incluindo terceiros, como provedores de serviços, parceiros de negócios ou órgãos governamentais – pode comprometer de várias maneiras o cenário digital da organização.

Além disso, o risco cibernético já abrange mais do que a nossa visão tradicional de computadores. Observamos um aumento acentuado de ataques envolvendo a chamada Internet das Coisas, direcionados até mesmo a carros e eletrodomésticos.

É o paradoxo digital: as empresas hoje são capazes de cobrir um território mais amplo, de forma mais rápida – graças a novas conexões digitais, ferramentas e plataformas que conseguem conectá-las em tempo real com clientes, fornecedores e parceiros. Mas, ao mesmo tempo, o crime cibernético tornou-se uma poderosa força de oposição que limita o potencial das organizações.

E os líderes das empresas temem que isso esteja freando seu crescimento. Na 19ª Pesquisa Anual Global com CEOs da PwC, 6 em cada 10 executivos classificaram os riscos cibernéticos e a velocidade da mudança tecnológica como as principais ameaças à expansão dos seus negócios.

A pesquisa deste ano aponta um fato preocupante: muitas organizações estão deixando a resposta imediata a esses incidentes a cargo das equipes de TI, sem a intervenção ou o apoio adequado da alta liderança e de outros grupos importantes. Além disso, a composição dessas equipes de resposta geralmente tem falhas, o que acaba por afetar o tratamento das violações.

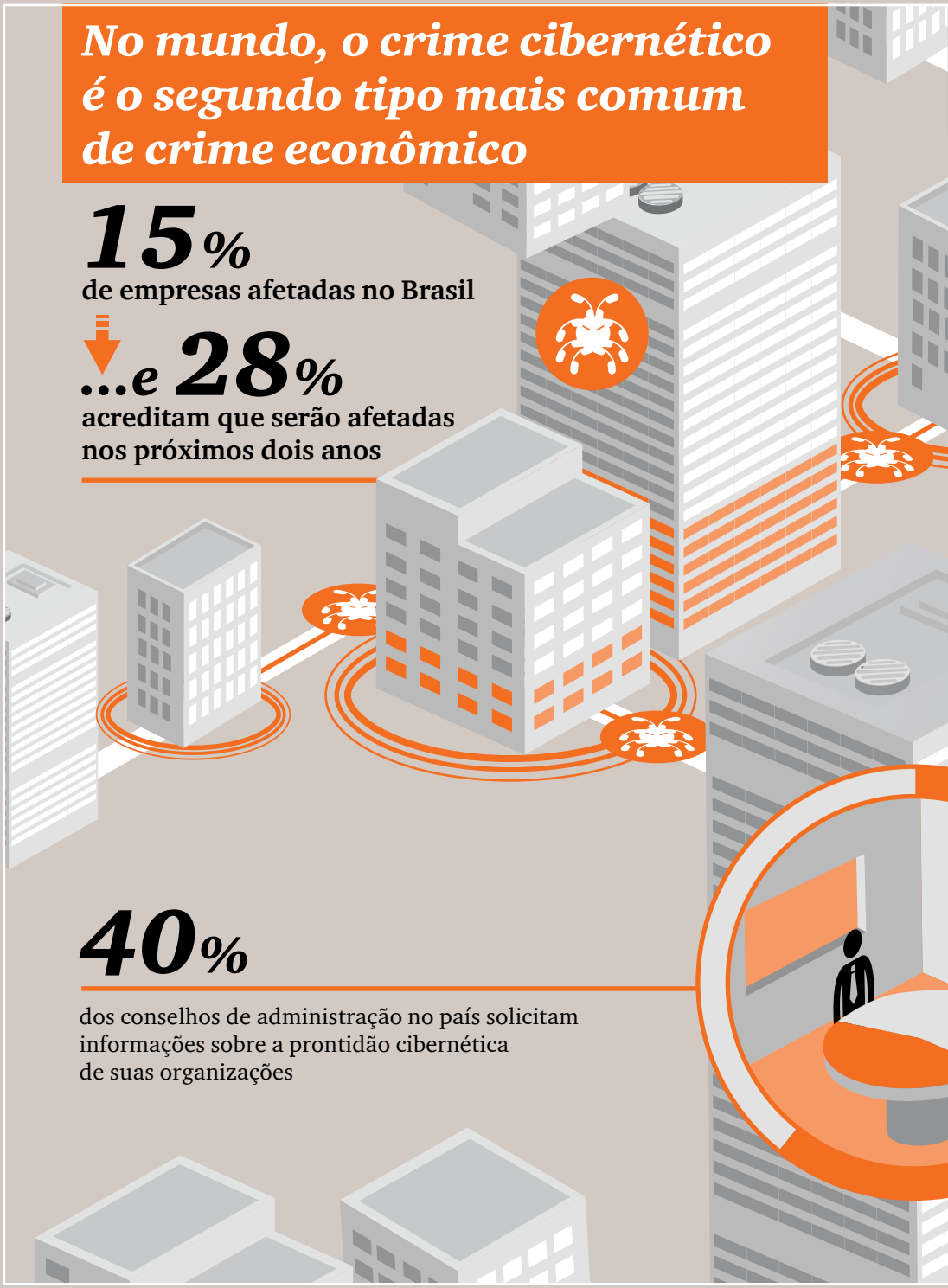
Com base no nosso trabalho relacionado à estratégia e à execução digital em milhares de empresas no mundo, identificamos práticas que distinguem os líderes da era digital. A principal delas é *uma postura proativa em relação à cibersegurança e à privacidade*. Para isso, é preciso que todos na organização – desde a liderança até à base – encarem essa questão como sua responsabilidade.

O crime cibernético é uma ameaça constante e, muitas vezes, silenciosa em um ecossistema de negócios totalmente conectado

No mundo, o crime cibernético é o segundo tipo mais comum de crime econômico

15%
de empresas afetadas no Brasil

...e 28%
acreditam que serão afetadas nos próximos dois anos



40%

dos conselhos de administração no país solicitam informações sobre a prontidão cibernética de suas organizações

Apenas 29%

das organizações brasileiras têm um plano de resposta a incidentes em vigor

A maioria das empresas ainda não está adequadamente preparada ou desconhece os riscos enfrentados

O seu plano de resposta cibernética é adequado à realidade?

O crime cibernético avança

A incidência de crimes cibernéticos informados pelos participantes da pesquisa global cresceu muito este ano, de 24% para 32%, saltando do 4º para o 2º lugar entre os tipos de crimes econômicos mais comuns. Foi o único tipo de crime a registrar crescimento no mundo. O Brasil seguiu tendência contrária: o índice caiu de 17% para 15%. Entre os BRICS, o percentual ficou em 9% este ano. De forma preocupante, porém, cerca de um quinto de todos os participantes da pesquisa global – e também da amostra brasileira e dos BRICS – disseram não saber se tinham sido afetados ou não pelo problema.

Uma quantidade muito grande de organizações, portanto, revela falta de conhecimentos ou de instrumentos adequados para detectar um ataque. “No nosso relacionamento com as empresas, observamos que muitos executivos ainda não entendem bem os riscos cibernéticos e os impactos que um ataque desse tipo pode ter para o negócio”, afirma Edgar D’Andrea, sócio e líder de Cybersecurity e Segurança da Informação da PwC Brasil. Metade da amostra brasileira, por exemplo, considera improvável sofrer um incidente nos próximos 24 meses. Outras pesquisas realizadas pela PwC revelam, porém, que esses incidentes estão aumentando em todo o mundo e de forma significativa no Brasil.

A análise dos resultados deste estudo e a nossa própria experiência no dia a dia levam a crer que a queda na detecção de crimes cibernéticos pelas empresas brasileiras se deva mais à falta de controles robustos para detectar os ataques do que a um aumento na prevenção. Além disso, acredita D'Andrea, talvez os participantes da Pesquisa sobre Crimes Econômicos no Brasil não estejam sendo envolvidos nos debates sobre riscos cibernéticos dentro das suas organizações. "A visão de que os ataques estão ligados sobretudo a roubos de dinheiro acoberta os riscos reais e está ultrapassada. As empresas precisam entender que detêm informações importantes que as diferenciam no mercado e que esses ativos podem ser alvo de criminosos para comercialização futura no submundo cibernético", ressalta.

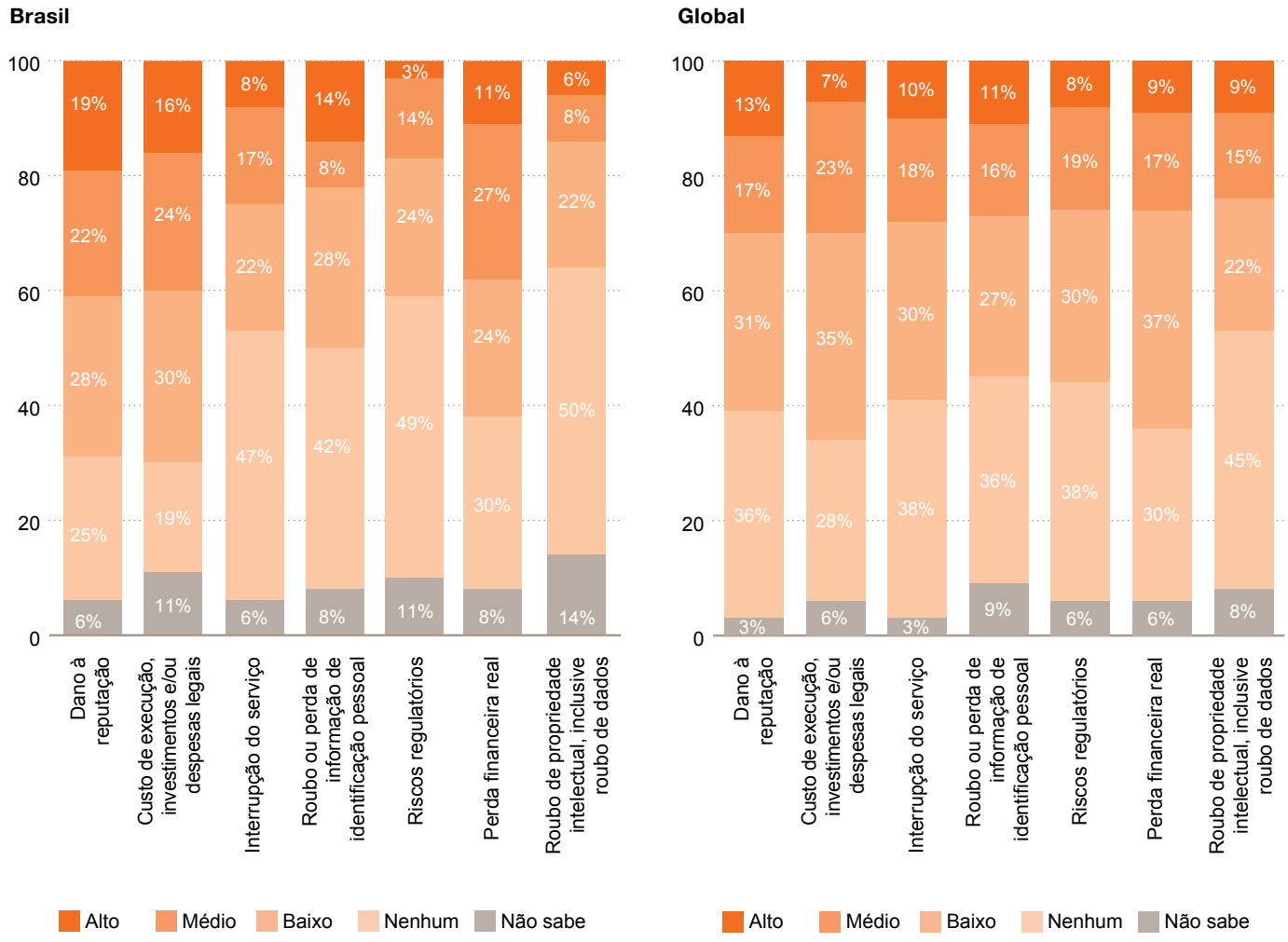
Os prejuízos podem ser altos. Aproximadamente 50 organizações participantes da pesquisa global sofreram perdas acima de US$ 5 milhões (nenhuma no Brasil e 6% entre os BRICS, resultado afetado sobretudo pelos dados da África do Sul). Um terço desse total informou ter perdido mais de US$ 100 milhões.

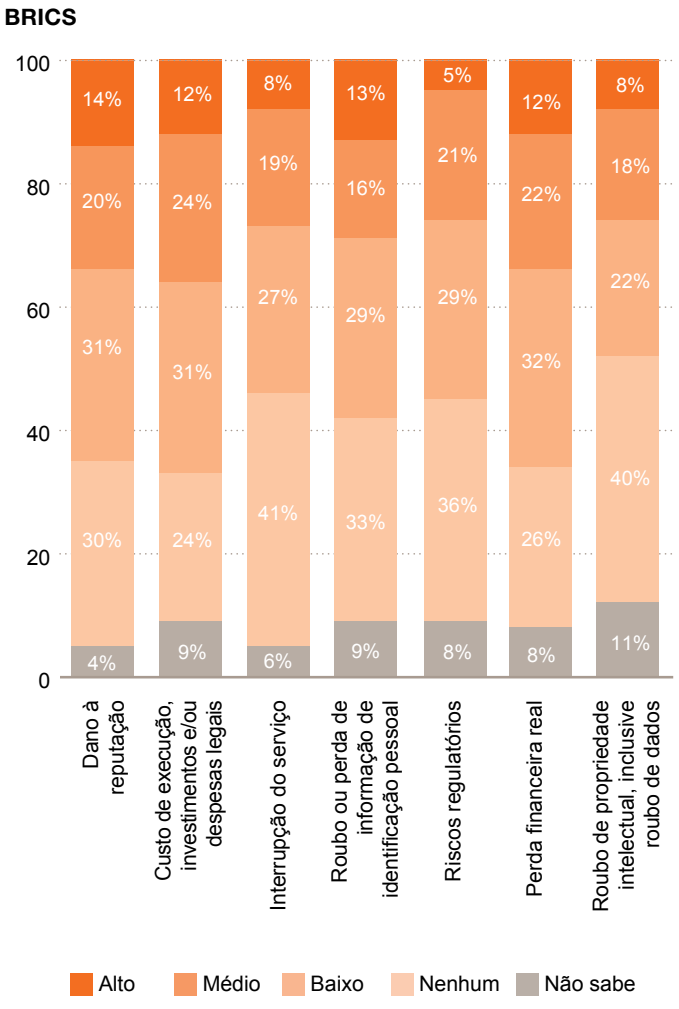
Que indústrias estão em risco?

Atualmente, todas as indústrias estão ameaçadas, inclusive algumas que talvez tenham se considerado alvos improváveis no passado. De acordo com a Pesquisa Global de Segurança da Informação da PwC 2016, o setor de varejo registrou o aumento mais significativo na atividade de crimes cibernéticos em 2015, enquanto o de serviços financeiros – ainda um dos setores mais atacados – se estabilizou, com um aumento muito pequeno no número de ataques nos últimos três anos.

Entre os participantes globais, os danos à reputação foram considerados os impactos mais prejudiciais de uma violação cibernética. O Brasil relata também o alto impacto dos custos de execução, investimentos e/ou despesas legais. O resultado pode ser um reflexo dos elevados custos judiciais no país, mas também um sinal de que os problemas não são identificados de forma proativa e de que grande parte das empresas age tardiamente, o que gera custos adicionais na resposta a incidentes.

Fig 10: Principais impactos do crime cibernético - Brasil





O crime cibernético é uma ameaça tão perigosa, que muitos participantes que consideram não ter sido vítimas do problema (56% no mundo, 61% no Brasil e 57% nos BRICS) podem ter sido atingidos sem saber. “O principal risco é a falta de mecanismos para identificar em tempo real os primeiros sinais do ataque, para que seja possível atuar e conter a invasão antes que ela se torne um problema maior”, afirma João Castilho, gerente da área de Forensic Technology Solutions da PwC Brasil. Além disso, segundo Castilho, os departamentos de TI e SI devem ser aliados estratégicos importantes das áreas de negócio na prevenção dos crimes cibernéticos, e não encarados como áreas de suporte, envolvidas de maneira reativa.

Uma tendência preocupante é a dos atacantes que conseguem permanecer nas redes das organizações por longos períodos sem ser detectados. Os criminosos também costumam realizar ataques diversionistas para ocultar atividades mais prejudiciais. Uma dessas técnicas é o uso de ataques distribuídos de negação de serviço como um meio de criar distração e muita confusão, enquanto o verdadeiro ataque transcorre de modo lento e silencioso.

Os dois tipos de crime cibernético – e o que eles representam para a sua empresa

Percorremos um longo caminho desde que a ameaça cibernética era personificada por adolescentes que atacavam os sistemas de cartões bancários. Houve um aumento significativo e louvável de consciência e sofisticação na detecção da identidade (ou da origem) dos criminosos. Mas o fato é que "a queda de braço" entre os criminosos e as empresas continua forte. E as organizações podem ter certeza de que nunca a vencerão totalmente.

Nos últimos anos, o crime econômico cibernético evoluiu e foi dividido basicamente em duas categorias: o que envolve roubo de dinheiro e danos a reputações; e o que rouba propriedade intelectual e pode devastar toda uma empresa.

- **Fraude cibernética.** O crime cibernético que pode ser facilmente convertido em dinheiro, como roubo de identidades, senhas e cartões de pagamento, é o evento que tende a produzir manchetes na mídia, em geral com prejuízos de muitos milhões de dólares (e muitas vítimas). Apesar da forte repercussão, esses incidentes raramente representam uma ameaça à sobrevivência das empresas.

- **Ataques de transferência de patrimônio/ propriedade intelectual.** O crime econômico mais grave que as organizações enfrentam é o da espionagem cibernética: o roubo de propriedade intelectual — segredos comerciais, informações sobre produtos, estratégias de negociação e questões semelhantes. Os profissionais cibernéticos chamam essas violações de "eventos de extinção" e por uma boa razão: os danos podem alcançar bilhões de dólares e destruir uma linha de negócios, uma empresa ou até mesmo um ecossistema econômico maior. Esses tipos de ataques não são apenas difíceis de ser detectados: eles talvez nem estejam no radar de ameaças das empresas.

Embora o dano de longo prazo, tanto para a organização quanto para a economia, seja potencialmente muito maior no caso de ataques de transferência de patrimônio, as penas impostas pelos reguladores e a pressão da mídia associadas a roubo de cartões de crédito ou informações de identificação pessoal podem ser muito mais pesadas.

Por que empresas (e nações) roubam propriedade intelectual?

- Muitas nações desenvolvidas estão verificando um padrão nas violações de grande porte focadas em propriedade intelectual. Não são ataques aleatórios a empresas individuais, mas sim uma campanha maior e estrategicamente organizada.

- Embora algumas nações estejam por trás desses ataques em larga escala, não se trata de uma ação terrorista (para tentar paralisar a infraestrutura essencial), mas um crime econômico.

- Há uma lógica econômica em roubar propriedade intelectual de outra empresa. É mais barato e rápido do que realizar seu próprio trabalho de pesquisa e desenvolvimento.

Agentes de ameaças

Estados nacionais

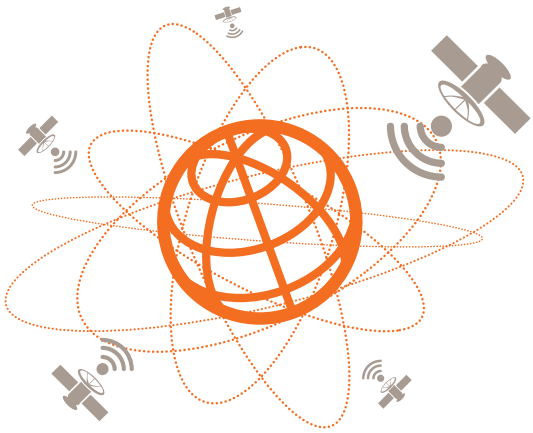
As ameaças incluem espionagem e guerra cibernética; entre as vítimas estão agências governamentais, infraestrutura, energia e organizações ricas em propriedade intelectual.

Pessoas com informação privilegiada

Não só os empregados, mas também terceiros confiáveis com acesso a dados confidenciais não diretamente sob seu controle.

Terroristas

Embora relativamente incipiente, inclui ameaças como interrupção de serviços e guerra cibernética; as vítimas podem ser agências governamentais, infraestrutura e energia.



Grupos de crime organizado

Entre as ameaças estão o roubo de informações financeiras ou pessoais (às vezes com a colaboração de agentes internos); as vítimas são instituições financeiras, varejistas, empresas médicas e do ramo de hospedagens, entre outras.

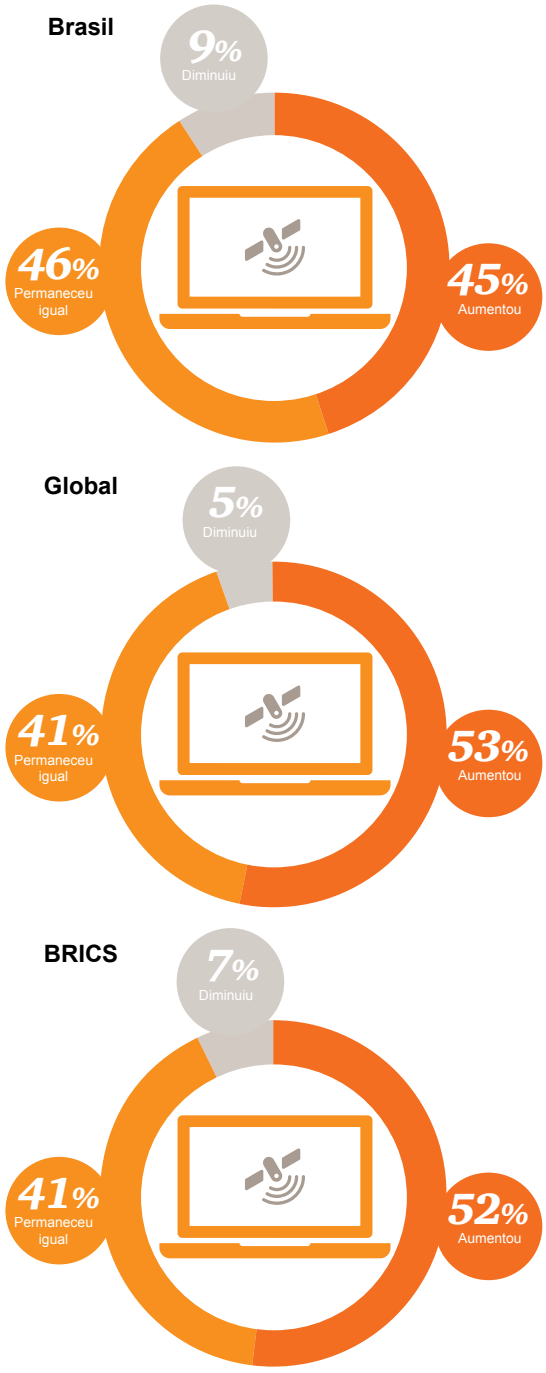
Hacktivistas

Algumas ameaças são interrupção de serviços ou dano à reputação; as vítimas incluem governos e organizações de destaque (exemplos: Edward Snowden, Wikileaks); todos os tipos de organizações podem ser vítimas.

Preparadas ou não?

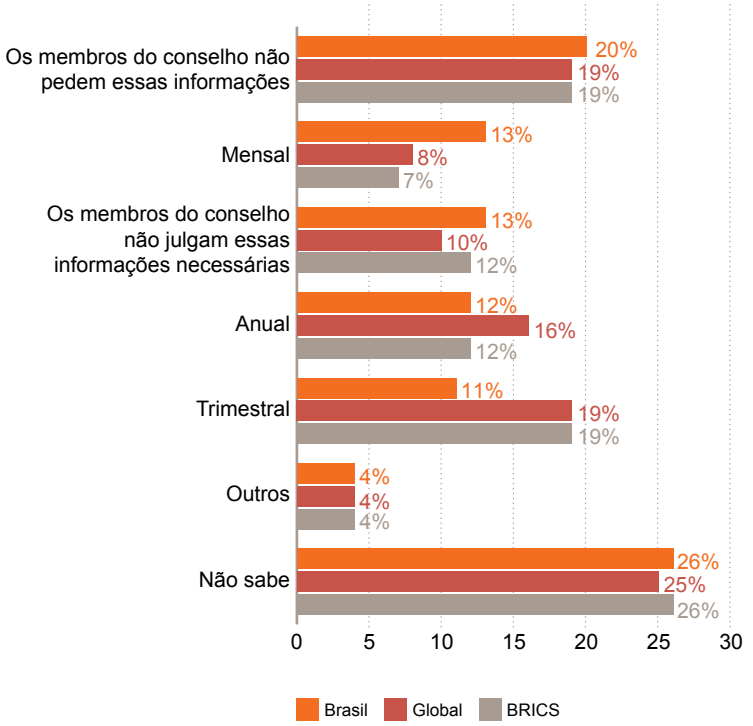
No Brasil, mesmo tendo caído nos últimos dois anos, o percentual de respondentes que percebem o aumento dos riscos do crime cibernético continua alto (45%, contra 52% em 2014). No mundo, esse percentual cresceu de 48% para 53% no mesmo período, talvez em consequência da maior cobertura da mídia. A nossa pesquisa sugere que as empresas não estão adequadamente preparadas para enfrentar as ameaças cibernéticas atuais, diante de um adversário que sofistica cada vez mais seus mecanismos de atuação.

Fig 11: Percepção de riscos dos crimes cibernéticos



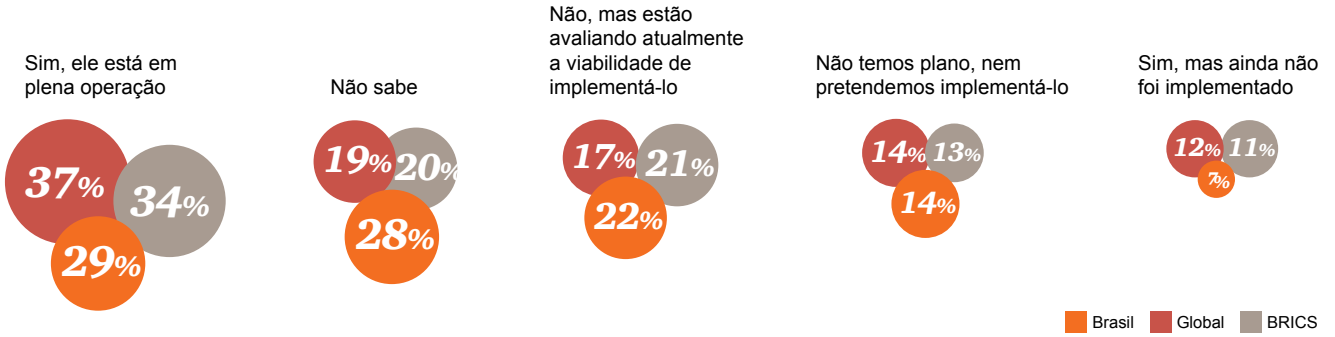
A responsabilidade por corrigir vulnerabilidades cibernéticas começa no topo da empresa. No entanto, os dados coletados indicam que muitos conselhos de administração não são suficientemente proativos em relação a essas ameaças. “Por se tratar de um tema relativamente novo, os conselhos de administração desconhecem os riscos e os impactos das ameaças cibernéticas para aos negócios e a reputação das suas organizações”, afirma Francisco Macedo, sócio da área de Forensic Technology Solutions da PwC Brasil. Em geral, os conselheiros não compreendem a presença digital das suas organizações suficientemente bem para avaliar os riscos de modo adequado – isso ocorre apesar de, em muitos países, os conselhos terem responsabilidade fiduciária perante os acionistas em relação aos riscos cibernéticos. Por exemplo, nos Estados Unidos, a Securities and Exchange Commission (SEC) divulgou um aviso de que inspeções futuras levarão em conta as competências de resposta cibernética das empresas. Hoje, no entanto, menos de metade dos conselhos (47%) solicita informações sobre a situação de prontidão cibernética de suas organizações, segundo dados da nossa pesquisa global. No Brasil, o percentual é de 40%; entre os BRICS, 42%.

Fig 12: Frequência com que o conselho pede informações sobre prontidão cibernética



Apenas 29% das empresas brasileiras, 37% das globais e 34% dos BRICS – a maioria no setor de serviços financeiros altamente regulado – têm um plano de resposta a incidentes em plena operação. Cerca de um terço não tem qualquer plano e, destas, quase metade acredita que não precisa de um. O mais grave no caso do Brasil: 28% dos participantes nem mesmo sabem se esse plano existe.

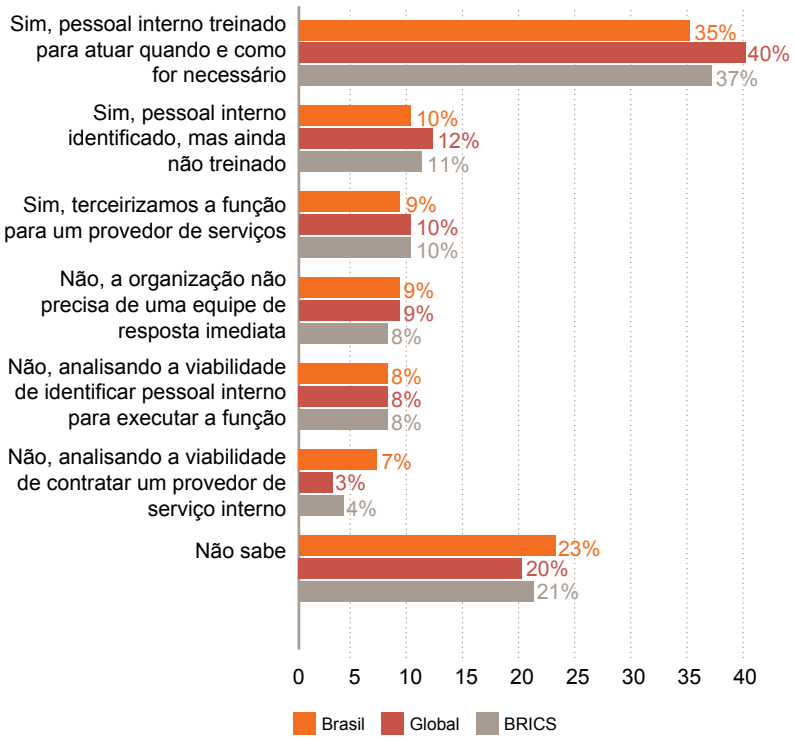
Fig 13: Há um plano de resposta a incidentes?



No caso de uma crise cibernética, apenas 4 em cada 10 empresas têm pessoal "totalmente treinado" para agir como uma equipe de resposta imediata, e a maioria esmagadora dessa equipe (cerca de 75%) é da área de TI.

Obviamente, a área de TI tem uma função essencial a desempenhar na detecção e na tentativa de conter o ataque, mas impressiona que apenas cerca de metade das equipes de resposta imediata inclua membros com foco na administração mais ampla da crise – gestores seniores (46%), advogados (25%), RH (14%) e assemelhados. Menos de 2 em cada 10 equipes de resposta a incidentes incluem investigadores forenses digitais, que são fundamentais na preservação de evidências não só para entender a origem dos ataques como também para identificar e processar os criminosos.

Fig 14: Equipe de resposta imediata identificada

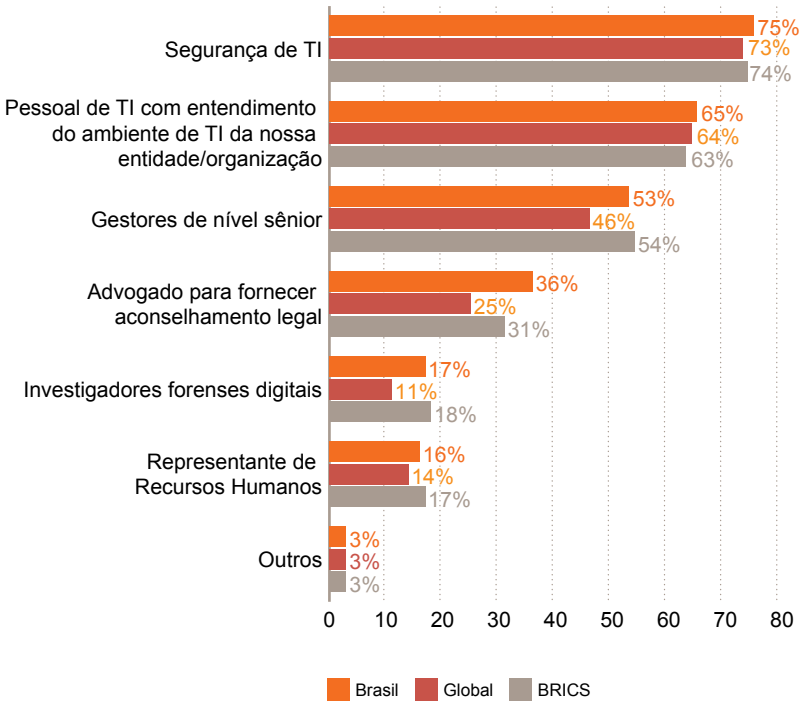


Esses resultados sugerem que muitas organizações, na pressa compreensível para conter a violação e colocar seus sistemas em funcionamento novamente, correm o risco de negligenciar provas cruciais – o que pode dificultar a sua capacidade de iniciar um processo judicial e, mais importante, entender como a violação ocorreu.

Em termos imediatos, uma resposta mal coordenada talvez também limite a capacidade da organização de investigar todas as áreas que foram de fato violadas, o que é especialmente importante, considerando o uso frequente de técnicas de distração pelos atacantes.

A pressa também pode prejudicar a comunicação com *stakeholders* internos e externos, inclusive a mídia, elevando o risco de danos reputacionais (classificados como o maior impacto da violação cibernética na pesquisa deste ano).

Fig 15: Composição das equipes de resposta imediata



Como detectar uma violação: gestão de crises

O que acontece quando você toma conhecimento de uma violação? É fundamental reduzir o intervalo entre a detecção e a resposta eficaz – interrompendo os impactos nocivos ao negócio o quanto antes. Depois de convocar a sua equipe de crise e resposta imediata, você pode seguir estes passos:

- Obtenha e preserve os dados essenciais sobre a violação e descubra se o processo ainda está em andamento. Com a crescente complexidade das redes, talvez seja difícil identificar como um invasor pode ter entrado na rede. Ferramentas forenses e de análise de dados sofisticadas – algumas delas fornecidas por especialistas externos, outras pelos agentes públicos – são essenciais nesta fase.
- Leve em conta que o ataque identificado pode, às vezes, mascarar incursões mais profundas na organização e que, em algumas situações, talvez demore semanas, não horas, para detectar uma violação e começar a conter os danos.
- Decida se e até que ponto você quer envolver os agentes de segurança pública — e se o órgão correto é local ou federal. Há muitos fatores a serem considerados, e eles variam de acordo com o tipo e a escala do ataque. (Essa é uma questão importante, considerando que aproximadamente metade dos respondentes põe em dúvida a capacidade do governo de investigar o crime cibernético.)
- Avalie os riscos secundários. Por exemplo, uma simples violação de e-mail pode revelar segredos para competidores. No caso de invasão de uma rede, e a empresa usar um serviço telefônico por VOIP/rede, os telefones provavelmente também foram violados.
- Por fim, quando ocorre uma violação, lembre-se: uma investigação cibernética é, essencialmente, uma investigação, e a ela se aplicam os princípios de investigação criminal. Ao se concentrar em interromper o ataque e voltar a operar normalmente, é preciso evitar destruir por acidente evidências relevantes para o processo investigativo e para a prevenção de novos ataques.

A importância da defesa em várias camadas

Ameaças cibernéticas e mitigações são responsabilidade de toda a empresa; todos têm um papel vital a desempenhar. Apesar disso, embora tenhamos observado avanços importantes em termos de sofisticação e prontidão cibernética desde a nossa última pesquisa, a maioria das empresas ainda não está adequadamente preparada para entender os riscos enfrentados, nem para prever e gerenciar os incidentes de modo eficaz.

Muitas organizações estão sofrendo prejuízos cibernéticos porque não fazem o básico corretamente. Do envolvimento insuficiente do conselho de administração (ou consciência sobre a prontidão) a configurações de sistemas malfeitas e controles inadequados sobre terceiros com acesso à rede, as empresas estão expostas a erros não forçados, geralmente deixando portas entreabertas para intrusos.

É essencial que os conselhos incorporem o crime cibernético em suas indagações regulares sobre riscos do ponto de vista dos avanços da tecnologia digital e do perfil de exposição da empresa. Os executivos devem atuar na gestão adequada dos riscos cibernéticos e garantir os fundamentos da resposta a incidentes.

A prontidão para o crime cibernético deve estar embutida no escopo mais amplo da gestão de crises.

A empresa deve entender as ameaças cibernéticas e se preparar adequadamente da mesma maneira que em qualquer outra possível interrupção ou ameaça ao negócio (como atos de terrorismo ou um desastre natural): com um plano de resposta, funções e responsabilidades, monitoramento e planejamento de cenários. É por isso que grandes empresas estão incorporando exercícios regulares de gestão de crises como elemento central das suas estratégias de segurança cibernética e resposta a incidentes. Elas convocam exercícios constantemente para examinar cenários específicos e testar seus planos de resposta a incidentes sob pressão, identificando eventuais lacunas ou deficiências.

"As organizações devem rever os fundamentos estratégicos, táticos e operacionais de *cyber* à luz dos riscos cibernéticos a que estão expostas", afirma Eduardo Batista, diretor de Cybersecurity da PwC Brasil. "Nesse contexto, é essencial que as empresas identifiquem e monitorem seu perfil de risco cibernético, assim como o de seus acionistas e dirigentes", complementa.

Gestão de crises/exercícios de simulação: Planos não valem nada — planejamento é tudo

Parafraseando um general prussiano, os planos raramente sobrevivem ao primeiro contato com a realidade. Os acontecimentos costumam apresentar circunstâncias imprevistas às equipes de resposta a incidentes e aos gestores de crises.

Uma resposta eficaz à crise requer as competências, o conhecimento e a experiência de uma gama de departamentos corporativos trabalhando juntos, entre eles, os departamentos jurídico, de recursos humanos, finanças, comunicação, relações públicas, relações com acionistas e reguladores, conselho de auditoria e riscos, segurança corporativa, além das unidades de negócios de primeira linha e da administração regional.

O processo — o "planejamento de um plano" — associado a um programa de exercício regular é muito mais valioso do que os planos que ele produz. Ele gera "memória" de resposta a incidentes, tornando o processo, o ambiente e a tomada de decisões aspectos intuitivos para os *stakeholders* que estarão sob pressão em uma crise. Assim, eles poderão se concentrar em resolver o problema em questão.

Ameaças cibernéticas e sua mitigação são responsabilidade de toda a organização

Nível executivo:

- Institui uma estratégia sólida de segurança cibernética.
- Acompanha a evolução dos principais indicadores de riscos e incidentes cibernéticos.
- Apoia iniciativas do programa de mudanças da cultura empresarial a respeito dos riscos cibernéticos (ex.: evento de conscientização sobre segurança para funcionários e terceiros).
- Autoriza investimentos com segurança baseados na estratégia.

Gestão de riscos e *compliance*:

- Garante o mapeamento adequado e sistemático dos riscos cibernéticos e das contramedidas necessárias.
- Monitora o cumprimento das contramedidas e dos limites de riscos individuais.
- Garante o *compliance* operacional e regulatório dos riscos cibernéticos.

Jurídico:

- Acompanha o ambiente regulatório cibernético em constante evolução.
- Monitora decisões tomadas por reguladores em resposta a incidentes cibernéticos.
- Toma ciência dos fatores que podem anular o seguro cibernético.

Segurança da informação:

- Estabelece os fundamentos da segurança cibernética e os riscos associados, na perspectiva dos processos de negócio, da força de trabalho (pessoas) e da tecnologia digital empregada.
- Conduz avaliações de prontidão forense.
- Toma conhecimento da evolução no ambiente de ameaças e vetores de ataque.
- Testa planos de resposta a incidentes.
- Implementa processos de monitoramento eficazes.
- Emprega novas estratégias: simulações de ataques cibernéticos, gamificação do treinamento de segurança e sessões de conscientização e análise de dados de segurança.

Auditoria interna:

- Assegura entendimento e cobertura ampla dos riscos cibernéticos e tecnológicos na matriz de riscos da organização.
- Considera riscos cibernéticos no plano anual de auditoria e nos programas de trabalho.
- Considera os perfis técnicos apropriados para avaliação e julgamento de riscos cibernéticos.

Uma crise cibernética corporativa é um dos problemas mais complexos e desafiadores que uma organização pode enfrentar. Violações cibernéticas exigem comunicações e estratégias investigativas sofisticadas (inclusive recursos analíticos e forenses expressivos), executadas com precisão, agilidade e sangue-frio.

Embora pareça uma tarefa muita pesada, fortalecer a prontidão tem seu lado positivo: você pode encará-la como um teste de estresse organizacional – que pode e deve levar a avanços nos processos corporativos. No cenário de riscos atual, o grau de prontidão de uma empresa para lidar com uma crise cibernética também pode ser um indicador de vantagem competitiva e, em última análise, significar a sua sobrevivência.

Ética e compliance

Gerenciar o equilíbrio entre confiança e *compliance* pode significar a diferença entre reter ou perder os grandes talentos. No mercado atual em constante evolução, é essencial ter uma estratégia para alinhar ética e *compliance* com os riscos do negócio.

Como alinhar riscos e responsabilidades com valores e estratégia

Os resultados da nossa pesquisa mostram que não só os riscos de* compliance *estão aumentando, como também a sua complexidade e o papel que a tecnologia desempenha na sua evolução. Isso não chega a ser surpresa em um ambiente de negócios caracterizado pela globalização crescente, por uma vigilância cada vez mais rigorosa das autoridades e uma demanda maior do público por responsabilidade.

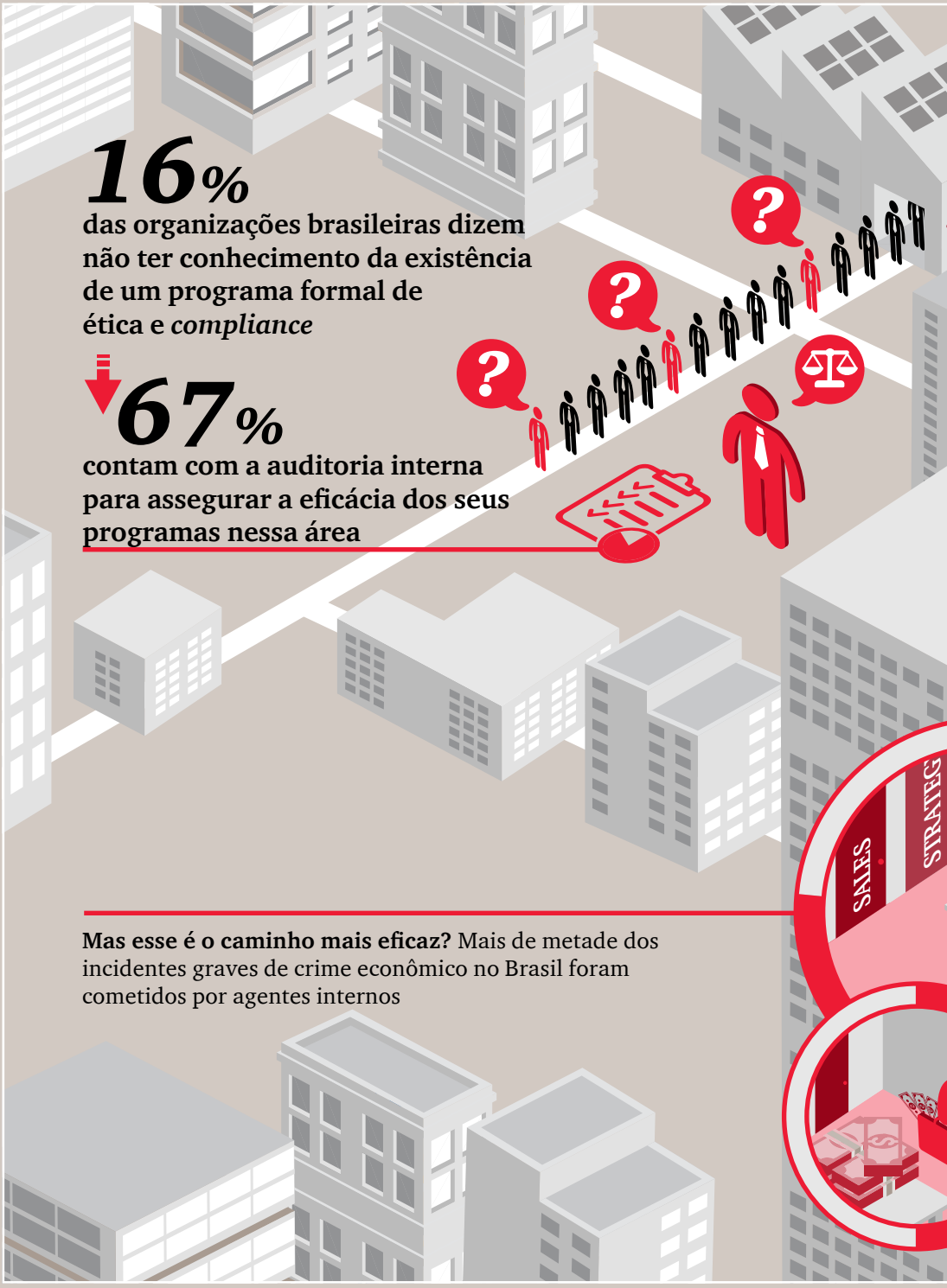
Esses são os motivos pelos quais a sua capacidade de identificar e mitigar riscos de *compliance* precisa evoluir rapidamente. Um dado preocupante é que, mesmo nesse cenário, 17% das organizações brasileiras (22% no mundo e 19% nos BRICS) não realizaram nenhuma avaliação de riscos de fraudes nos últimos 24 meses.

Uma abordagem de ética e *compliance* baseada em riscos – que comece com um entendimento holístico dos seus riscos de crimes econômicos e com uma compreensão de onde estão as suas fragilidades – é uma obrigação. Com base nessa posição clara você pode criar um programa eficaz que mitigue esses riscos e o posicione para alcançar seus objetivos de negócios.

O suborno e a corrupção representam apenas uma área do crime financeiro, mas podem servir como um termômetro importante das tendências de *compliance* atuais. A nossa pesquisa mostra que um quarto das empresas que foram vítimas de um crime econômico no Brasil e no mundo (23% e 24%, respectivamente, em comparação com 14% entre os BRICS) registrou um incidente desse tipo nos últimos 24 meses – um pouco menos do que na pesquisa de 2014. Além disso, 18% das empresas brasileiras receberam um pedido de pagamento de propina (13% no mundo e 20% nos BRICS). Outras 37% não sabem se receberam (29% no mundo e 35% nos BRICS).

No mundo, a maioria dos outros crimes financeiros seguiu tendência semelhante de estabilização desde 2014. No Brasil, alguns tipos cresceram: fraude em compras, de recursos humanos, lavagem de dinheiro, *insider trading*, competição desleal e violação das leis antitruste e espionagem.

Pessoas responsáveis querem trabalhar para empresas responsáveis – que colocam em prática seus valores éticos e cumprem sua palavra



17%
das empresas acham que provavelmente serão vítimas de suborno e corrupção nos próximos dois anos

... e 52%
citaram a redução do moral dos funcionários como o maior dano nas empresas atingidas por crimes econômicos

Como a sua estratégia de negócios está alinhada com os seus valores organizacionais?

O problema na ligeira redução em alguns tipos de crimes é que ela pode estar alimentando uma falsa sensação de segurança. Há risco de que algumas empresas deixem de perceber o valor que há em investir mais recursos em programas de ética e *compliance* quando não registram um aumento nas métricas de crimes econômicos. De fato, muitas organizações cortaram custos com pessoal e treinamento ou ampliaram as responsabilidades de suas equipes de *compliance* para incluir tarefas adicionais.

Isso pode ser um erro estratégico: em várias indústrias e lugares, os riscos de crimes econômicos não estão diminuindo – e uma memória corporativa curta pode representar perigo. A principal questão é que, para ter sucesso, um programa de *compliance* precisa prever a evolução dos riscos e combatê-los adequadamente.

Desconexão

Pense nos incidentes recentes e de grande repercussão envolvendo importantes montadoras e instituições financeiras globais com programas de *compliance*, valores e ética muito bem implantados. Esses lapsos indicariam que tais programas não estão acompanhando a evolução dos riscos de negócio? Que estão enviando mensagens confusas? Ou há uma razão mais profunda para essa desconexão?

Os números indicam uma diferença de percepção entre as suposições e afirmações de CEOs e conselhos de administração e aquilo que realmente está acontecendo nas empresas, sobretudo na gerência média e executiva. Segundo a nossa pesquisa, a gerência média continua tendendo mais a cometer fraudes (com algumas variações regionais) e a perceber que os valores não estão sendo claramente expressos ou que os programas de incentivos não são justos.

A nossa 19ª Pesquisa Global com CEOs corrobora essa ideia de um gap entre intenção e execução. Entre as principais ameaças que as organizações enfrentam, o item suborno e corrupção foi o que registrou maior crescimento percentual, de 51% para 56%. A falta de confiança no negócio foi outra ameaça apontada, o que ressalta a importância de as equipes de liderança terem um programa sofisticado e confiável de ética empresarial.

Como elaborar um programa adequado

Como a liderança executiva pode assegurar que aquilo que ela defende está realmente sendo colocado em prática pelos gestores? Como o *compliance* está sendo incentivado? Como ele está sendo medido?

Apresentamos a seguir as quatro áreas de foco para aprimorar a eficácia dos programas de ética e *compliance*. Elas serão analisadas nas próximas páginas:

- **Pessoas e cultura.** Manter um programa baseado em valores, medir e recompensar os comportamentos desejados.
- **Papéis e responsabilidades.** Assegurar que estejam clara e corretamente alinhados com os riscos atuais.
- **Áreas de alto risco.** Melhor implementação e teste do programa em mercados e divisões de alto risco.
- **Tecnologia.** Melhor uso de ferramentas de detecção e prevenção, inclusive análise de *big data*.

Cinco etapas para um programa de compliance mais eficaz

1. Comunique e posicione o seu programa de acordo com a estratégia corporativa.
2. Avalie e possivelmente repense a identidade da sua área de *compliance,* de tal forma que ela possa se adaptar a um ambiente em que os riscos e as ameaças estão sempre evoluindo.
3. Certifique-se de que todos os responsáveis pelas obrigações de *compliance* entendam plenamente o programa geral da organização como um todo e o escopo das suas próprias responsabilidades.
4. Lembre-se de que políticas e treinamento sobre valores não bastam: o engajamento de toda a organização, de forma coerente e confiável, é essencial.
5. Não reduza as atividades quando os riscos estiverem crescendo.

Pessoas e cultura: sua primeira linha de defesa

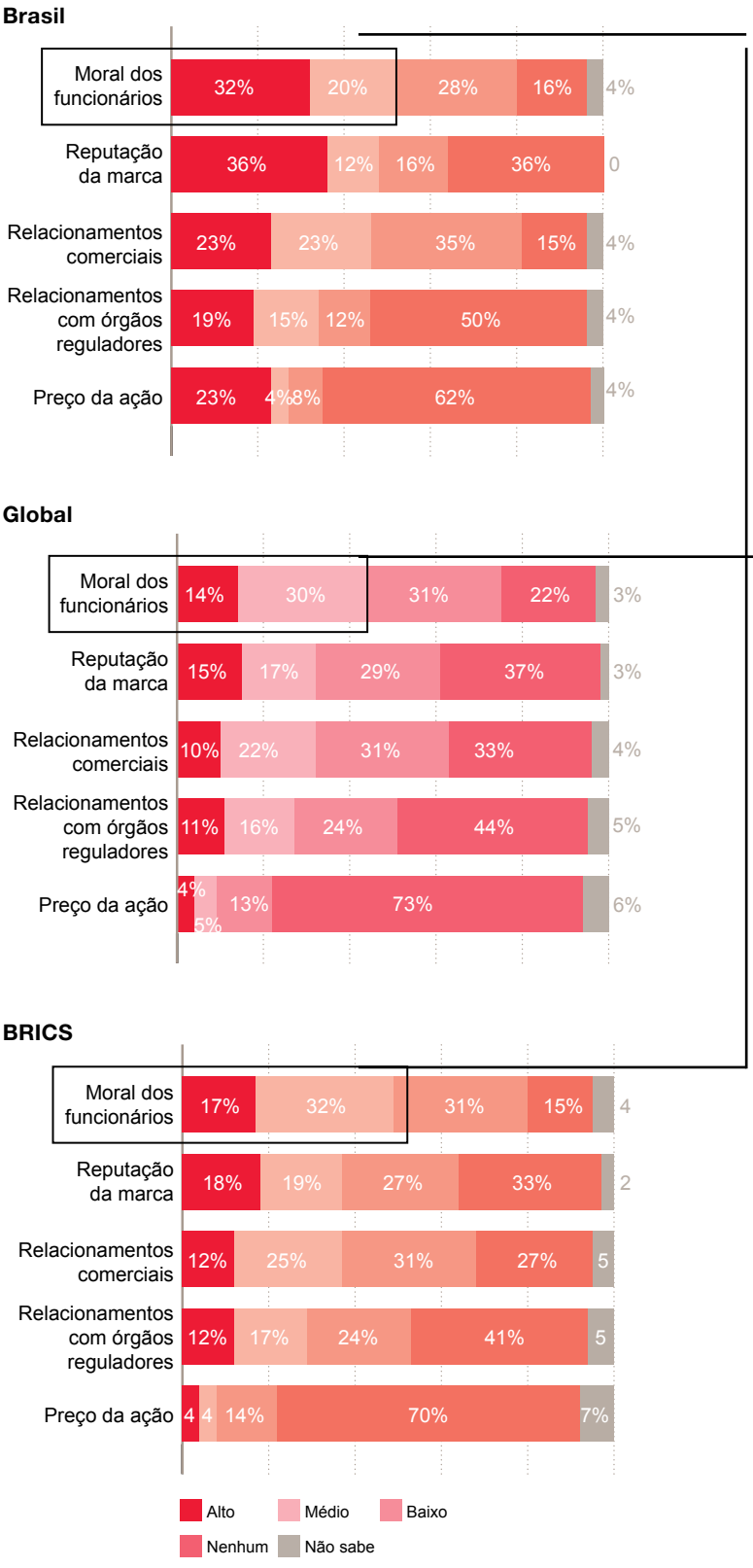
No centro de qualquer crime econômico está uma decisão ruim, impulsionada pelo comportamento humano. Concluímos assim que a solução desse problema deve começar pelas pessoas. Isso significa não só estabelecer princípios e processos claros para os empregados, mas também criar uma cultura na qual o *compliance* **esteja diretamente conectado aos valores** – e à estratégia global da organização.

Os participantes da nossa pesquisa afirmaram que o maior dano organizacional que sofreram como consequência do crime econômico não foi registrado nos preços das ações, nem mesmo no relacionamento com os reguladores. Ele foi sentido principalmente no moral dos empregados e, em segundo lugar, na reputação da empresa. Em ambos os casos, a forma como a empresa é percebida – interna ou externamente – foi a área mais atingida. Isso ressalta o papel fundamental desempenhado pelos valores em uma estratégia de negócios bem-sucedida.

Uma pesquisa recente da PwC e da London School of Business sobre a promoção do comportamento ético no setor de serviços financeiros mostra que a adoção de uma abordagem "rígida" à gestão do desempenho cria um clima de medo que, por sua vez, leva a comportamentos não éticos.
O estudo revelou que a ansiedade causada por essa cultura de culpa destrói a capacidade das pessoas de tomar boas decisões – e geralmente as leva a se comportar de forma pior do que as pessoas que são motivadas pelas possíveis consequências positivas do sucesso.

"Stand out for the right reasons" – Pesquisa da PwC e da London Business School, junho/2015.

Fig 16: Principais impactos do crime econômico



52% *no Brasil,*

44% *no mundo e*

49% *nos BRICS citaram a redução do moral dos funcionários como o maior impacto dos crimes econômicos*

Spotlight (Ética e Compliance)

Muitas organizações estão se esforçando para coletar dados relevantes que as ajudem a monitorar e tratar seus riscos comportamentais. Além dessas pressões internas, existem outras externas: o crivo da opinião pública e a ampla disponibilidade de informações significam que investidores, consumidores, fornecedores e terceiros em geral exigem mais evidências do compromisso de uma organização de agir corretamente.

Conforme demonstrado por eventos recentes de ampla divulgação, uma abordagem estática do problema da ética e do *compliance* não é suficiente para promover o comportamento ético em toda a organização.

O **Spotlight™**, ferramenta da PwC baseada na Web, permite quantificar o seu risco comportamental, fornecendo ao mesmo tempo uma avaliação da eficácia do seu programa de ética e *compliance*. Ele mede o alinhamento entre o que você quer que os seus funcionários façam e o que está acontecendo na prática – usando uma pesquisa on-line e outras métricas subjetivas e objetivas (inclusive entrevistas, grupos de foco e análise de documentos).

Um programa de *compliance* baseado em valores faz mais do que contornar o problema do enfraquecimento da sua base de talentos. Ele também trata de atrair os melhores profissionais para a sua organização. Pessoas responsáveis querem trabalhar para empresas responsáveis – que colocam em prática suas crenças éticas e "cumprem o que prometem". Um programa de *compliance* bem projetado – com foco no apoio a comportamentos éticos – pode proporcionar um benefício estratégico claro para o negócio.

Mas, para ser eficaz, seu programa de *compliance* também deve abranger mais do que um código de conduta atualizado, uma política e algumas horas de treinamento. Em essência, ele deve abordar a profunda conexão entre valores, comportamentos e a tomada de decisões.

Em vez de tentar antecipar cada risco individual, a abordagem sofisticada busca fortalecer as pessoas com uma avaliação básica de como e por que tomar as decisões certas em determinadas circunstâncias. A necessidade dessa abordagem é confirmada pelas conclusões da nossa pesquisa de que, nas regiões em que gestores mais sêniores estavam envolvidos na realização de fraudes econômicas (como Ásia-Pacífico, América do Norte e Europa Ocidental), um dos principais fatores por trás disso era o incentivo ou a pressão por resultados (ou seja, eles tomavam a decisão errada quando era mais importante para a organização).

Observe e meça as diferenças (de percepção)

Mais de 80% dos participantes concordam que suas organizações têm valores claramente especificados e bem entendidos. CEOs e CFOs expressam essa visão de forma especialmente forte. Mas a nossa pesquisa identificou áreas nas quais a gerência executiva e o conselho não estavam percebendo a realidade da mesma forma que a gerência média. Enquanto 90% dos CEOs acreditam que os valores são claros e compreendidos, entre os gerentes esse percentual cai para 84%.

Na nossa experiência, essa diferença estatística – entre o que os líderes executivos pensam e dizem e o que a gerência média percebe – pode criar um vácuo no qual, mesmo com as melhoras intenções, talvez as atividades antiéticas se disseminem.

Diferenças de percepção

As diferenças de percepção são um tema constante nos resultados da nossa pesquisa e podem ter consequências indesejadas. Elas se dividem em três categorias básicas:

- A diferença entre aquilo em que o conselho acredita e promove e o que as pessoas dentro da organização realmente veem, acreditam e fazem no dia a dia.
- A diferença entre as intenções e o que é financiado.
- A diferença entre a alta administração e os gerentes médios na supervisão da conformidade.

Fig 17: Ética de negócios e *compliance*

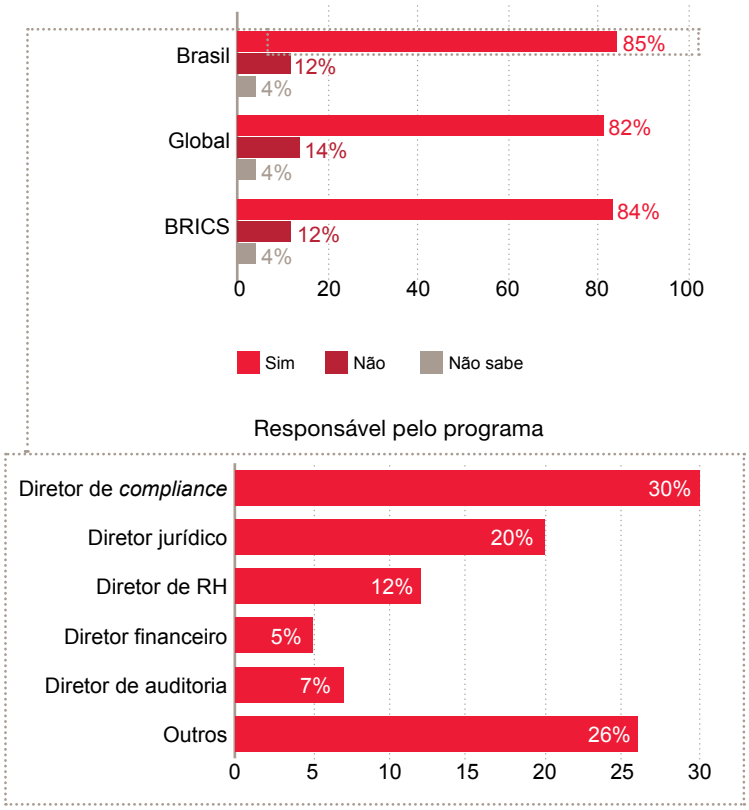

Global
A organização tem valores claramente especificados e bem entendidos
44%
42%
9%
4
1%
Há um Código de COnduta que abrange as principais áreas de riscos/ políticas e estabelece os valores organizacionais e os comportamentos esperados de todos
48%
38%
9%
5
0%
A conduta ética nos negócios é um componente essencial dos nossos procedimentos de RH, o que inclui objetivos, promoções, remuneração, reconhecimento e procedimentos disciplinares
38%
40%
14%
6%
2%
Líderes executivos e gerentes transmitem a importância da conduta ética nos negócios em tudo o que fazem, estabelecendo um exemplo positivo e tratando isso como prioridade
36%
42%
15%
6%
1%
Há canais confidenciais para levantar preocupações (inclusive um procedimento e uma política clara de denúncias)
41%
33%
14%
9%
3%
As preocupações podem ser comunicadas de forma confidencial, sem medo de retaliação, e o feedback é fornecido em tempo hábil
31%
42%
18%
7%
2%
Independentemente de nível, função, departamento ou local, os procedimentos e as penalidades disciplinares são aplicadas de modo coerente
24%
43%
21%
10%
2%
O treinamento sobre o Código de Conduta (e as políticas de apoio) é fornecido regularmente, apoiado em comunicações regulares e vários canais de aconselhamento
28%
42%
24%
11%
3%
Independentemente de nível, função, departamento ou local, as remunerações são justas e coerentes
21%
42%
24%
11%
3%
BRICS
A organização tem valores claramente especificados e bem entendidos
53%
36%
6%
3
1%
Há um Código de COnduta que abrange as principais áreas de riscos/ políticas e estabelece os valores organizacionais e os comportamentos esperados de todos
53%
36%
6%
3
1%
A conduta ética nos negócios é um componente essencial dos nossos procedimentos de RH, o que inclui objetivos, promoções, remuneração, reconhecimento e procedimentos disciplinares
43%
38%
13%
5%
2%
Líderes executivos e gerentes transmitem a importância da conduta ética nos negócios em tudo o que fazem, estabelecendo um exemplo positivo e tratando isso como prioridade
41%
40%
11%
6%
2%
Há canais confidenciais para levantar preocupações (inclusive um procedimento e uma política clara de denúncias)
51%
31%
9%
7%
2%
As preocupações podem ser comunicadas de forma confidencial, sem medo de retaliação, e o feedback é fornecido em tempo hábil
36%
40%
14%
7%
3%
Independentemente de nível, função, departamento ou local, os procedimentos e as penalidades disciplinares são aplicadas de modo coerente
28%
43%
16%
11%
3%
O treinamento sobre o Código de Conduta (e as políticas de apoio) é fornecido regularmente, apoiado em comunicações regulares e vários canais de aconselhamento
37%
43%
19%
14%
3%
Independentemente de nível, função, departamento ou local, as remunerações são justas e coerentes
25%
43%
19%
11%
3%
Concordo fortemente
Concordo
Nem concordo nem discordo
Discordo
Discordo fortemente

Alinhamento de papéis e responsabilidades: Quem está no comando?

A nossa pesquisa revelou que 15% dos participantes no Brasil (18% no mundo e 16% entre os BRICS) não sabem se suas empresas têm um programa formal de ética e *compliance*. Curiosamente, na pesquisa global, a porcentagem de CEOs, membros dos conselhos e diretores de operações que mostraram desconhecimento foi maior, 23%.

Entre as organizações que têm um programa formal, a responsabilidade por ele é bastante distribuída.

Fig 18: Programa formal de ética e *compliance*



Organizações com menos de mil funcionários tendem menos a apresentar um programa formal de ética e *compliance* nos negócios. Embora elas possam estar focando as reais necessidades da empresa, abrindo mão de uma abordagem cheia de recursos não essenciais, isso pode representar um desafio, pois muitas enfrentam um cenário de riscos semelhante ao das empresas maiores.

Quem é o responsável? Como adotar uma abordagem baseada em riscos

É importante que todas as pessoas da empresa – não só os profissionais de *compliance* – entendam suas funções e responsabilidades no sentido de garantir que a empresa esteja alinhada e cumprindo seu programa e suas prioridades de ética e *compliance*. Além disso, muitas empresas demonstram um certo grau de confusão sobre quem é responsável pelo quê.

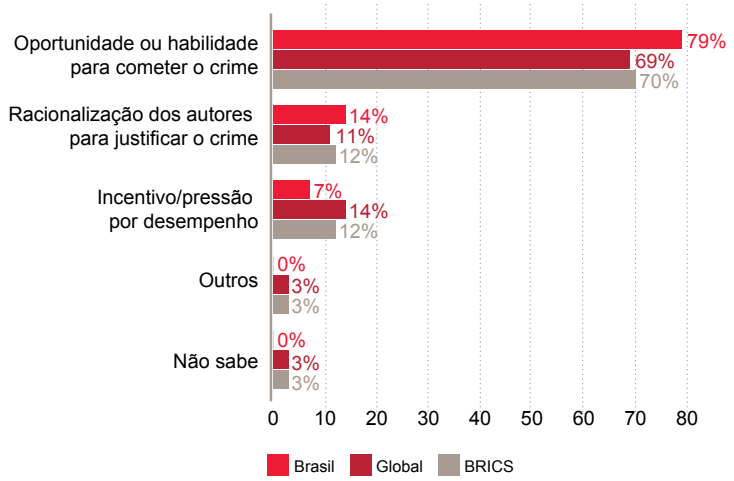
O "domínio" do programa é das equipes de linha de frente – a administração das unidades de negócios –, cuja responsabilidade é entender os riscos e determinar o apetite da unidade para esse risco. O papel da área de *compliance*, por sua vez, é a supervisão e a orientação. Em algumas organizações, porém, há uma tendência de encarar o *compliance* como um tipo de apólice de seguros sobre o qual deve haver uma responsabilidade passiva.

Em última análise, todos os integrantes da empresa precisam trabalhar para alcançar os mesmos resultados de *compliance*. Organizações com visão de futuro se posicionam como uma "comunidade de *compliance*" mais ampla, em que os papéis e as responsabilidades pela ética e o *compliance* se tornam parte do dia a dia dos negócios para todos.

A oportunidade (para o crime) bate à porta. Mas quem ouve?

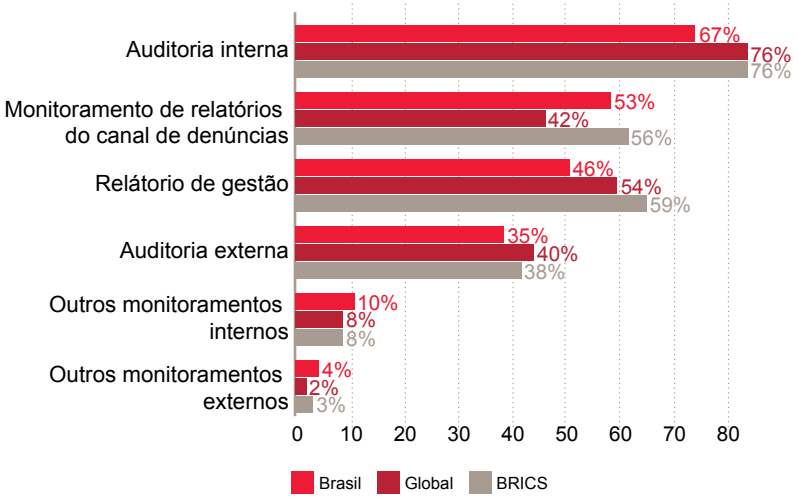
Mais de dois terços das organizações acreditam que a oportunidade é a motivação principal para o crime econômico interno – superando de longe os outros dois elementos do triângulo da fraude, que são incentivo/pressão por desempenho e racionalização do crime.

Fig 19: Motivações de fraudador interno



Uma ampla maioria parece preferir ambientes mais fortes de controle para reduzir as oportunidades oferecidas ao fraudador, mas a nossa pesquisa mostra que os mecanismos sob controle da administração estão agora muito menos eficazes em detectar o crime econômico do que em 2014: a queda foi de 22 pontos percentuais no Brasil e 7 pontos no mundo. No Brasil, 67% contam com a área de auditoria interna como parte da sua abordagem para avaliar a eficácia dos programas de *compliance*. No mundo e entre os BRICS, esse percentual sobe para 76%.

Fig 20: Mecanismo para assegurar a eficácia do programa de *compliance*



Embora seja uma peça importante do modelo de avaliação da eficácia de um programa de *compliance*, a auditoria interna sozinha não consegue assegurar o *compliance*, já que suas intervenções são periódicas e históricas. Além disso, a incidência de alguns tipos de fraude está crescendo ou persiste em determinados tipos de organização. Por exemplo, grandes organizações se mostram mais suscetíveis à fraude em compras e ao suborno e à corrupção (7% e 3% mais, respectivamente, do que a média global), pois os esquemas de fraude encontram uma maneira de contornar as estruturas de controle estabelecidas. Na verdade, algumas abordagens de monitoramento tornaram-se bem conhecidas e fáceis de contornar.

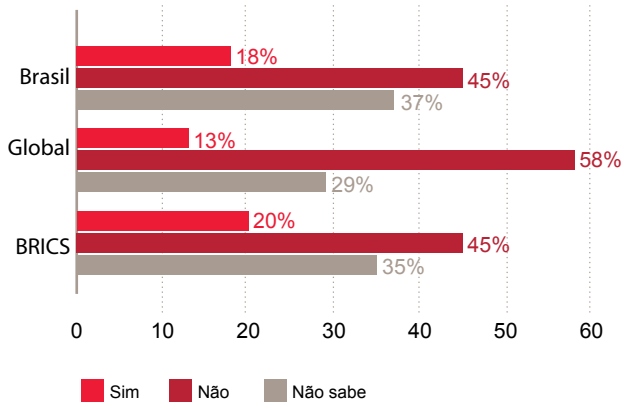
Como a prevenção deve ocorrer, de modo ideal, no momento da tomada das decisões, os mecanismos da auditoria interna devem ser integrados aos relatórios de gestão e monitoramento do negócio em tempo real, de maneira que os problemas sejam detectados e prevenidos de forma ágil. Os participantes do setor financeiro, especialmente, indicam o relatório de gestão como uma ferramenta essencial para assegurar a eficácia dos programas de *compliance*. Atualmente, apenas 8% dos participantes globais dizem que estão usando outras abordagens mais promissoras de monitoramento interno, como análise de dados ou preditiva, mais difíceis de burlar.

Implementação em áreas de alto risco: o diabo mora nos detalhes

Estabelecer um comportamento ético em uma organização global exige melhor treinamento, comunicação coerente e relatórios de gestão. Mas também deve incluir um entendimento de que os riscos de cada país são diferentes (mesmo considerando as áreas de alto risco) – e que um programa de *compliance* global sofisticado deve ser precisamente ajustado às realidades locais específicas.

Pensemos no risco transnacional conhecido do suborno e da corrupção. Os reguladores têm demonstrado cada vez mais a disposição de responsabilizar as empresas pelo comportamento antiético que ocorre fora da sede, e a administração está tendo de lidar com o problema de como garantir que todo o seu pessoal esteja fazendo a coisa certa o tempo todo.

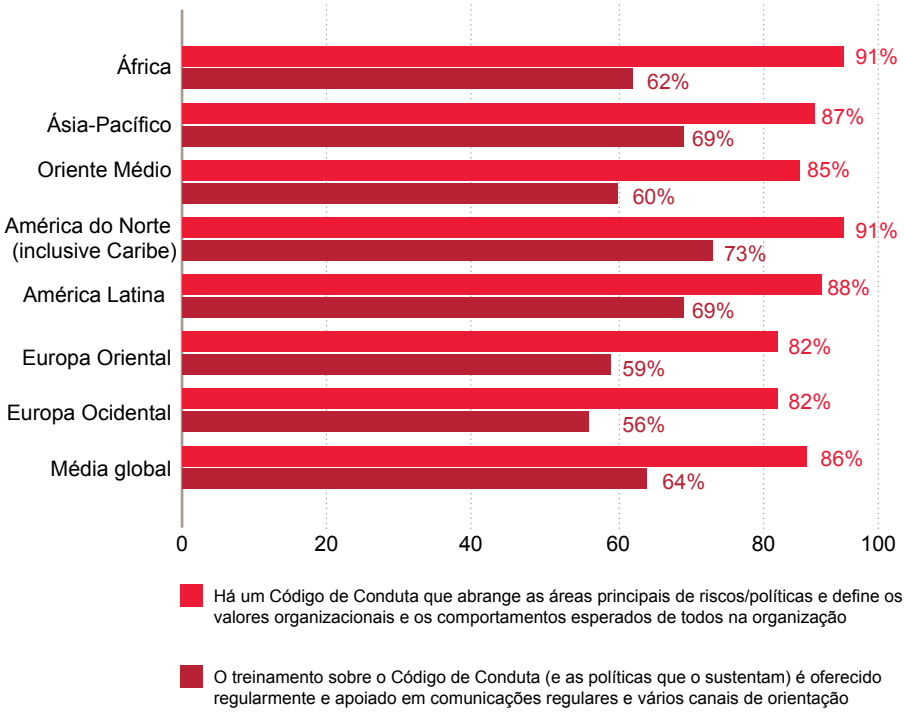
Fig 21: Organizações que receberam pedido para pagar propina



Como as organizações respondem aos riscos? Ter um código de conduta reconhecido é um começo, mas se os empregados não sabem como usá-lo para tomar decisões no dia a dia, ele vale pouco para reduzir os riscos de *compliance*. O código e outras políticas precisam ser dominados por meio de treinamento, comunicações regulares, remuneração e reconhecimento das boas decisões – e de procedimentos disciplinares no caso de decisões ruins.

Embora quase 88% das organizações brasileiras (86% das globais e 89% dos BRICS) afirmem ter um código de conduta em vigor, um percentual menor (70%, em comparação com 64% das globais e 80% dos BRICS) diz que o treinamento é fornecido regularmente e apoiado em comunicação e aconselhamento regular. Essa discrepância foi especialmente pronunciada na África, na Europa Ocidental e no Oriente Médio.

Fig 22: Código de conduta e treinamento nas empresas



Ao todo, segundo 91% dos participantes globais (90% no Brasil e 91% nos BRICS), a alta liderança deixa claro que o suborno é uma prática ilegítima. Esse resultado foi uniforme para todas as regiões e indústrias. No entanto, ainda estamos observando um grande número de incidentes relatados – e, em muitas regiões, um número crescente de organizações que esperam ser vítimas de suborno e corrupção nos próximos 24 meses.

As regiões que acreditam ter mais probabilidade de registrar suborno e corrupção nos próximos 24 meses – África, Oriente Médio e Ásia-Pacífico – são também aquelas com maior número de respondentes que relatam um aumento planejado de gastos com *compliance* nos próximos 24 meses (59%, 48% e 47%, respectivamente). Porém, o aumento de gastos nem sempre corrige o problema. As organizações precisam ter certeza de que estão usando as ferramentas, tecnologias e técnicas certas para obter o máximo de retorno sobre os investimentos em *compliance*.

Tecnologia: uma poderosa ferramenta, não uma panaceia

Existem várias ferramentas sofisticadas atualmente – inclusive análise de *big data* capaz de um monitoramento muito mais efetivo – que podem ajudar a aproximar o *compliance* da operação, manipulando uma variedade de dados estruturados ou não. Além disso, fora dos sistemas de monitoramento de transações (usados principalmente por clientes do setor financeiro), muito poucas organizações estão usando essas tecnologias para ajudar a detectar e prevenir o crime econômico. Atualmente, apenas 13% dos participantes brasileiros, quase o dobro do percentual global (7%) e dos BRICS (6%), mencionaram o uso de outras abordagens de monitoramento interno, como a análise de dados.

Mas cuidado: as organizações podem ser vítimas de erros relacionados à tecnologia. Orientadas por um processo desconectado de avaliação de riscos, algumas realizam monitoramento em demasia em alguns lugares (com efeito limitado) e nenhum monitoramento em outros. Outras empresas, sem saber, duplicam seus gastos com diferentes ferramentas. Há ainda as que seguem uma abordagem burocrática do *compliance* – e nem sempre reúnem ou usam os dados certos, muitas vezes abandonando os exercícios de análise de dados antes que eles demonstrem o seu valor.

Observamos que o melhor lugar para começar não é o espaço do *big data* de monitoramento das transações, mas sim o *small data* das avaliações de risco. O que mais importa é coletar dados comparáveis consistentes – uma tarefa que parece simples, mas não é.

O modelo ideal abrange a propagação de riscos que uma organização enfrenta e permite gerar relatórios por unidade de negócios, geografia ou terceiros. Para isso, três condições são necessárias:

- Uma taxonomia de riscos coerente.
- Transparência na medição de riscos.
- Uma plataforma de dados comuns.

Esses pré-requisitos, além de um modelo centralizado de operação e governança, podem ajudar você a começar a avaliar os esforços mais amplos de monitoramento de transações em uso no momento - e concentrá-los nas ameaças reais para a sua empresa. Em última análise, o foco não deve estar na tecnologia por si só, mas naquilo que ela possibilita. Os dados nunca serão uma panaceia, mas, usados de forma eficaz, podem conferir às empresas um poder adicional para se manter à frente dos riscos de *compliance*.

Prevenção à lavagem de dinheiro

A lavagem de dinheiro destrói valor

Ao facilitar o crime econômico e outras atividades ilícitas, como a corrupção, o terrorismo, a evasão fiscal e o tráfico de drogas e seres humanos, a lavagem de dinheiro também prejudica a reputação de uma organização – e seus resultados financeiros.

As transações globais de lavagem de dinheiro estão estimadas em 2 a 5% do PIB global, ou cerca de US$ 1-2 trilhões anuais. Mas, segundo o Escritório das Nações Unidas sobre Drogas e Crime (UNODC), menos de 1% dos fluxos financeiros ilícitos globais são atualmente apreendidos pelas autoridades.

Com a visibilidade crescente dos ataques terroristas, a lavagem de dinheiro e o financiamento do terrorismo estão subindo na lista de prioridades dos governos de todo o mundo. Ao longo dos últimos anos, somente nos Estados Unidos, mais de 10 instituições financeiras globais receberam multas no valor de centenas de milhões a bilhões de dólares por lavagem de dinheiro e/ou violações de sanções. Há fortes indícios de que outros países seguirão a tendência de regulação e repressão mais firmes.

Mas o problema não está só nessas instituições. Qualquer organização que facilite transações financeiras – inclusive negócios não bancários envolvendo dinheiro, como serviços de pagamento móvel ou digital, seguradoras do ramo vida e varejistas, para citar apenas alguns – também começa a ser objeto da legislação de combate à lavagem de dinheiro em todo o mundo. É preocupante, mas não surpreende, que muitos desses novos participantes da economia ainda não estejam familiarizados com as exigências que devem cumprir ou com os programas de *compliance* de que precisarão.

Com o aumento da complexidade e do escopo da regulamentação, o custo do *compliance* cresce. De acordo com novos números da Research and Markets,[2] os gastos globais com o *compliance* relacionado à prevenção da lavagem de dinheiro devem superar US$ 8 bilhões até 2017[3] (uma taxa anual composta de crescimento de quase 9%). Mas muitas instituições relutam em aumentar seus gastos com o *compliance* - mesmo diante do custo das ações de fiscalização e de sanções em larga escala decorrentes de falhas de conformidade.

[2] 2020 Foresight Report: The Impact of Anti-Money Laundering Regulations on Wealth Management. http://www.researchandmarkets.com/research/lqd7k4/2020_foresight.
[3] Estatísticas gentilmente fornecidas pela WealthInsight.

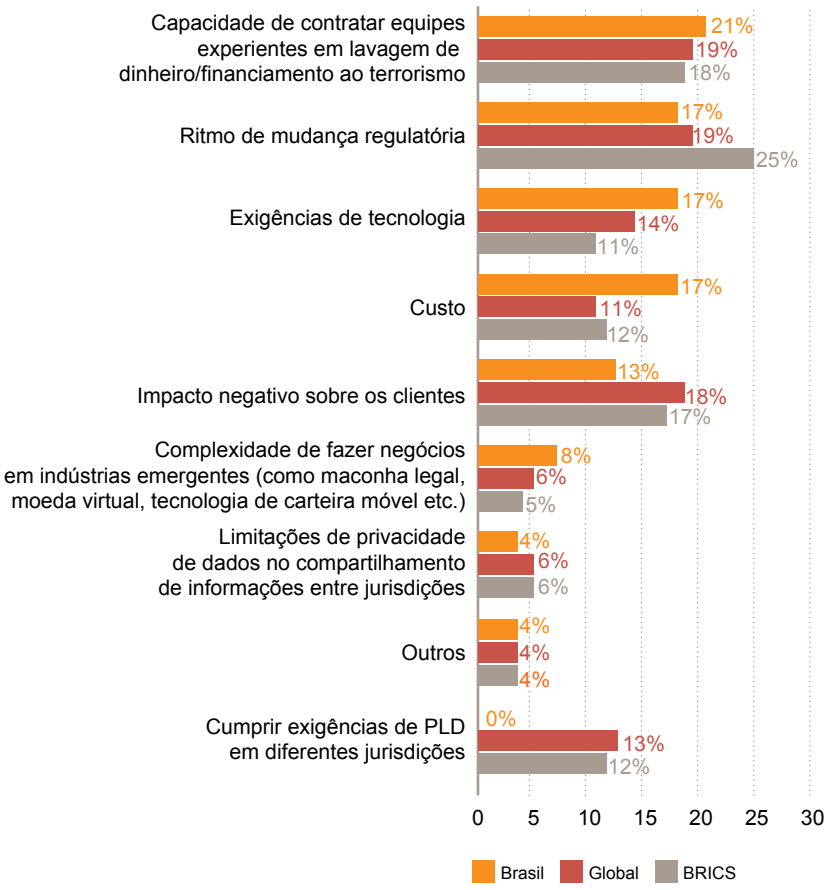
O aumento dos padrões regulatórios está ampliando as ações de repressão


Mais de 25%
das instituições financeiras globais não realizaram uma avaliação de riscos de lavagem de dinheiro ou financiamento do terrorismo em suas instalações globais
BANK
Como a sua organização agiria diante de uma inspeção regulatória?

Regulação por inspeção

Normas regulatórias mais rígidas estão impulsionando fortemente as ações coercitivas. A nossa pesquisa mostra que o nível das medidas de repressão à lavagem de dinheiro e ao financiamento do terrorismo criou desafios até para instituições financeiras com os mais sofisticados e robustos programas de *compliance* de PLD.

Fig 23: Desafios no cumprimento de requisitos de PLD/CFT



Órgãos de fiscalização e regulação sobre a lavagem de dinheiro

- O **GAFI** (Grupo de Ação Financeira) é um organismo intergovernamental de normalização e formulação de políticas criado pelo G-7 (sete países mais industrializados), em 1989. Sua missão atual é promover políticas para combater a lavagem de dinheiro e o financiamento do terrorismo monitorando tendências globais relacionadas a esses temas e definindo padrões internacionais de combate a essa combinação de ameaças.
  O GAFI formulou suas "40 Recomendações" – estabelecendo um padrão mínimo global de um sistema eficaz de prevenção à lavagem de dinheiro. Atualmente, 34 países-membros adotaram as "40 Recomendações" como parte de sua legislação e regulamentação de combate à lavagem de dinheiro, entre eles o Brasil.
- O **Conselho de Segurança das Nações Unidas** emite resoluções contendo listas *inter alia* de pessoas e organismos contra os quais foram impostas sanções, como organizações terroristas conhecidas. Essas listas são geralmente usadas por governos participantes para apoiar medidas contra atividades terroristas.
- O **OFAC** (Office of Foreign Assets Control, vinculado ao Departamento do Tesouro dos EUA) mantém e administra vários embargos e programas de sanções econômicas nos Estados Unidos.

Alguns governos impuseram multas – e, em certos casos, iniciaram ações criminais – contra instituições financeiras que não implementaram controles suficientes para monitorar suas transações globais. Mais recentemente, os mesmos governos reafirmaram a necessidade de abrir processos criminais contra indivíduos, além dos acordos e das pesadas multas já aplicadas às empresas. Em resumo, eles buscam a responsabilização pessoal por essas falhas. O período em que as pessoas eram protegidas por acordos corporativos está com seus dias contados. Os indivíduos agora enfrentam a possibilidade de prisão caso sejam considerados cúmplices de práticas comerciais ilícitas ou até mesmo de falhas substanciais de *compliance*.

Algumas instituições financeiras entraram na mira de reguladores de um determinado país por práticas de negócios ilícitas em outro. De modo geral, existem conflitos em relação aos países em que as instituições estão autorizadas a atuar enquanto sofrem sanções de outros países.

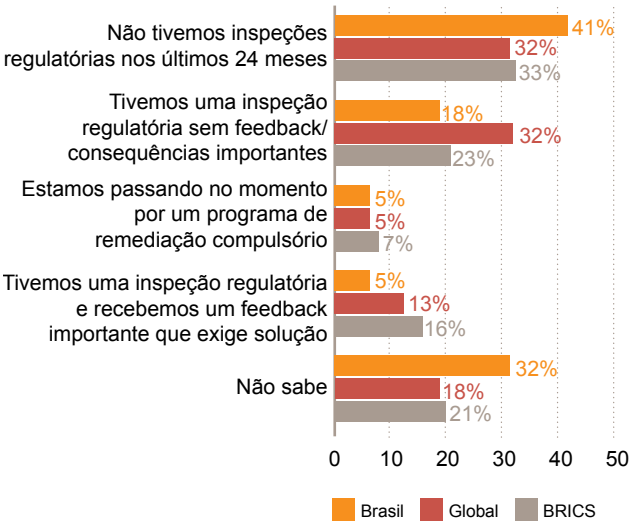
Inspeções e remediações estão crescendo. Com o crescimento das organizações de serviços financeiros por aquisição, seus veículos legais, negócios e mercados não são consolidados imediatamente de acordo com os processos ou padrões do grupo. Muitos ainda enfrentam dificuldades em consequência de ações ou sanções regulatórias. Todos esses fatores aumentam o perfil de risco para ações de PLD. Nossa pesquisa indica que 18% dos bancos – um percentual muito alto – sofreram recentemente medidas coercitivas de um órgão regulador.

Repressão desigual?

Embora a maioria das nações disponha de algum mecanismo para inspeções de PLD, o rigor dessas inspeções varia substancialmente.

Os Estados Unidos e alguns outros países desenvolvidos têm equipes de inspeção dedicadas a PLD e sanções. Mas muitos outros países empregam generalistas em riscos ou *compliance*, em vez de especialistas em PLD, e realizam inspeções menos frequentes.

Fig 24: Inspeção/medida regulatória e remediação



Outro desafio para as organizações que se esforçam em relação ao *compliance* global de PLD/CFT é o fato de que as expectativas regulatórias estão substituindo, cada vez mais, requisitos legais claros. Isso é mais notável em áreas de *due diligence* de clientes e monitoramento de transações, nas quais os inspetores podem aplicar uma norma em uma instituição com base nas práticas de outra. Essa tendência, também chamada de "regulação por inspeção", desafia o conceito bem conhecido da abordagem baseada em riscos que as organizações e seus *stakeholders* são obrigados a aplicar.

GAFI: novo foco em eficácia

O GAFI modificou seu padrão de avaliação de normas nacionais de PLD/CFT do *compliance* técnico para a eficácia, de forma que todas as organizações são avaliadas segundo um critério semelhante.

Esse novo foco em eficácia levará alguns países em desenvolvimento a fazer mudanças em suas práticas de repressão ao crime, o que terá repercussões para as instituições – e, por sua vez, considerando a natureza global das iniciativas de PLD, para outras jurisdições. Com isso, pode haver também uma diferença de percepção temporária sobre o significado de "eficácia" entre mercados mais maduros e em desenvolvimento.

O *compliance* global não é uma questão de seguir as leis de uma única jurisdição. Independentemente da sua jurisdição de origem, as organizações devem considerar que as questões de PLD/CFT são reguladas mundialmente por três razões principais:

- O GAFI define padrões internacionais para gestão de riscos e aplicação da lei em relação a questões de PLD/CFT. Assim, ele constitui a base das regulamentações nacionais - e das obrigações de bancos e outras instituições reguladas.
- Em conjunto com outros tesouros nacionais, como o britânico, o OFAC administra programas de sanções econômicas – e, com esse objetivo, investiga a movimentação de mercadorias, serviços e fundos entre países.
- É praticamente impossível para as instituições financeiras evitar as leis das jurisdições em que atuam gerenciando negócios em importantes moedas globais como o dólar americano, a libra inglesa e o euro. O simples ato de liquidar uma transação nos Estados Unidos ou em dólares americanos – ou até mesmo de contatar uma pessoa nos Estados Unidos por telefone ou e-mail – é suficiente para estabelecer uma conexão e abrir caminho para processos naquele país.

Cada vez mais, os *frameworks* regulatórios dos principais centros financeiros – Hong Kong, Cingapura, Londres e Nova York, por exemplo – estão convergindo, o que exige das instituições a incorporação dos padrões mais elevados, tanto internacionalmente quanto em suas jurisdições locais.

Em conjunto, esses eventos imprevisíveis e em rápida evolução podem levar a uma espécie de inércia estratégica, à medida que as instituições tentam prever o cenário regulatório futuro que devem enfrentar. Uma coisa é muito clara: uma boa dose de bom senso será necessária para que essas organizações elaborem seus programas de *compliance* relacionados a crimes financeiros.

O que tudo isso significa para a sua empresa?

A corrida rumo ao topo. Com a globalização dos padrões de PLD/CFT, é importante lembrar que você pode ser avaliado pelos mais elevados padrões internacionais de *compliance*. Apresentamos a seguir três pontos de ação a ser considerados:

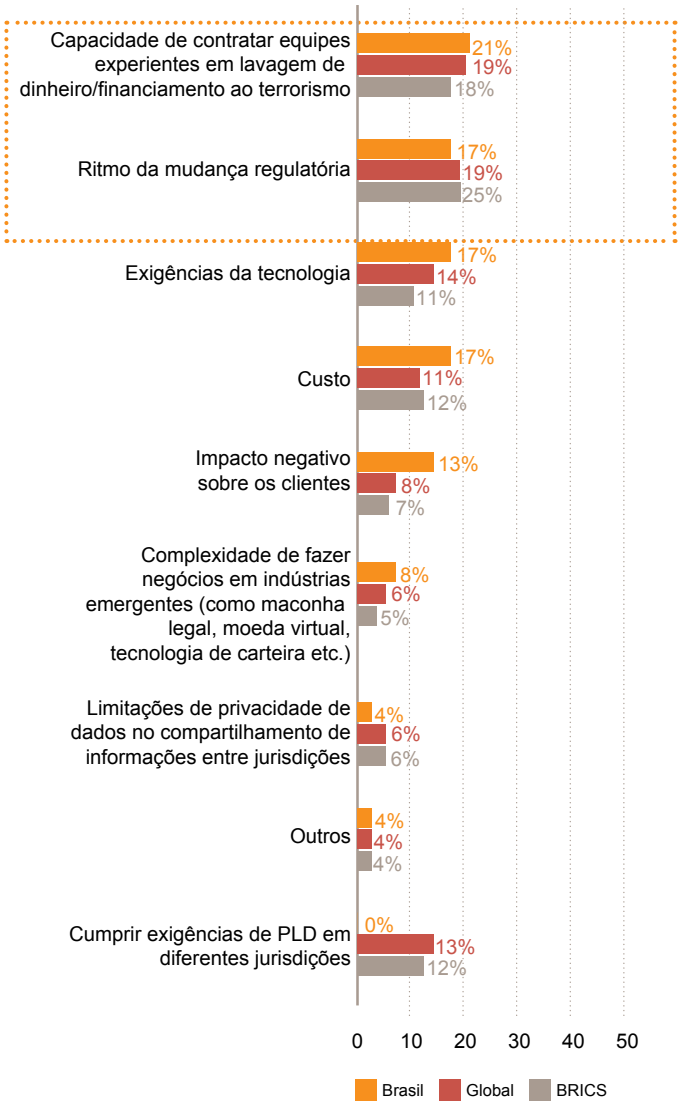
- **Mantenha-se na vanguarda regulatória.** Vá além do *compliance* burocrático com a legislação atual. Antecipe-se e avalie como se estruturar adequadamente para acompanhar as tendências legislativas. Concentre-se em manter uma área dentro da organização com as condições adequadas para acompanhar as regulamentações pendentes nessa área.
- **Seja líder, não seguidor.** Ficando no meio da multidão, você corre o risco de estar sempre um passo atrás em relação à regulamentação. Busque ser ágil estrategicamente e inovador para tentar antecipar as mudanças regulatórias.
- **Aprenda com os erros dos outros.** Poucas organizações são reconhecidas por investigar de forma ativa a causa raiz dos problemas significativos identificados pelos reguladores. A remediação geralmente serve como uma solução rápida para lidar com achados dos reguladores - embora o custo de remediar violações geralmente supere as multas impostas pelos reguladores. Como a maioria das transações tem um componente financeiro multinacional, é uma boa prática assumir como padrão a mais elevada norma global de *compliance*, sempre que possível, e promover autoavaliações mais rigorosas de PLD/CFT. Estabeleça requisitos para toda a empresa a fim de assegurar a uniformidade entre diferentes regiões.

Pessoas e processos

No Brasil e no mundo, os respondentes da nossa pesquisa afirmam que contratar equipes experientes é o desafio mais importante que enfrentam no âmbito da PLD, seguido de perto pelo ritmo da mudança regulatória.

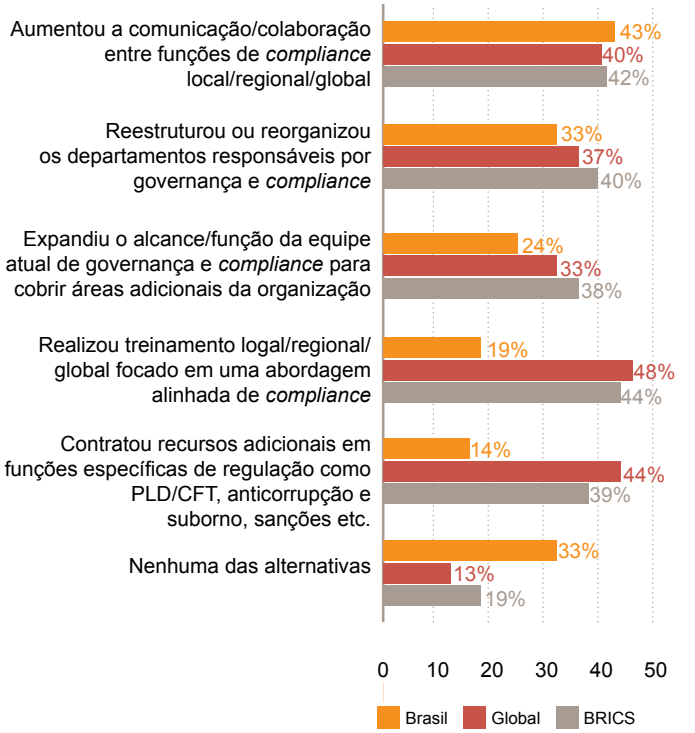
Infelizmente, a oferta de talentos continua abaixo da demanda. A rotatividade nas equipes de PLD e *compliance* é alta, e a concorrência por profissionais de alto nível é significativa para organizações de serviços financeiros e não financeiros.

Fig 25: Desafios de *compliance* em relação a lavagem de dinheiro/financiamento do terrorismo



Algumas organizações estão enfrentando o desafio do talento recorrendo ao treinamento de recursos internos, com um foco significativo em recursos PLD/CFT e anticorrupção.

Fig 26: Medidas adotadas para atender às crescentes expectativas regulatórias



Avaliações de risco são essenciais. Ao longo da última década, o aperfeiçoamento das medidas de controle de lavagem de dinheiro nos sistemas financeiros formais obrigou os criminosos a buscar novas maneiras de "movimentar" o produto dos seus crimes. Por isso, a avaliação regular de riscos é essencial para ajudar a organização a identificar e minimizar os riscos de lavagem de dinheiro e financiamento do terrorismo - em qualquer lugar ou com qualquer pessoa com quem ela faça negócios.

Apesar dos claros benefícios, 27% da amostra global de empresas de serviços financeiros que participaram da nossa pesquisa não estão realizando uma avaliação de riscos de PLD/CFT em todas as suas operações de negócios globais no momento, ou não sabem se estão. No Brasil, esse percentual salta para 64%, em comparação com 36% dos BRICS.

Pessoas certas, competências certas, nos lugares certos. De que competências você precisa?

Quando a sua melhor linha de defesa para combater a lavagem de dinheiro é ter as pessoas certas, nas funções certas e com as habilidades certas, você precisa saber o que está procurando. Há uma forte demanda por competências e conhecimentos específicos:

- Requisitos e padrões globais.
- Regulação e obrigações das jurisdições.
- O ecossistema regulatório global.
- *Due diligence* de clientes.
- Relacionamentos sólidos com reguladores.
- Conhecimento técnico em monitoramento de transações.
- Análise de dados.

E com a sofisticação crescente da lavagem de dinheiro, essa é uma atividade que não pode ser descartada. A lavagem de dinheiro com base no comércio, por exemplo – um sistema complexo de documentações falsas por meio do qual os criminosos obtêm e movimentam valores pelo mundo como se estivessem fazendo comércio legítimo –, está se tornando mais difícil de detectar com sistemas tradicionais de monitoramento de transações.

As avaliações de riscos devem ser conduzidas de forma periódica. Elas devem estar em perfeita sintonia com mudanças nas circunstâncias, como o ambiente operacional, as normas globais e a regulação nos países em que a empresa opera. As avaliações também devem incluir a classificação do perfil dos clientes em diferentes categorias de risco de lavagem de dinheiro e financiamento do terrorismo. Essa também é a norma global recomendada pelo GAFI e pelos reguladores para conter as ameaças.

Fig 27: Porcentagem de organizações que realizam avaliações de riscos de PLD/CFT

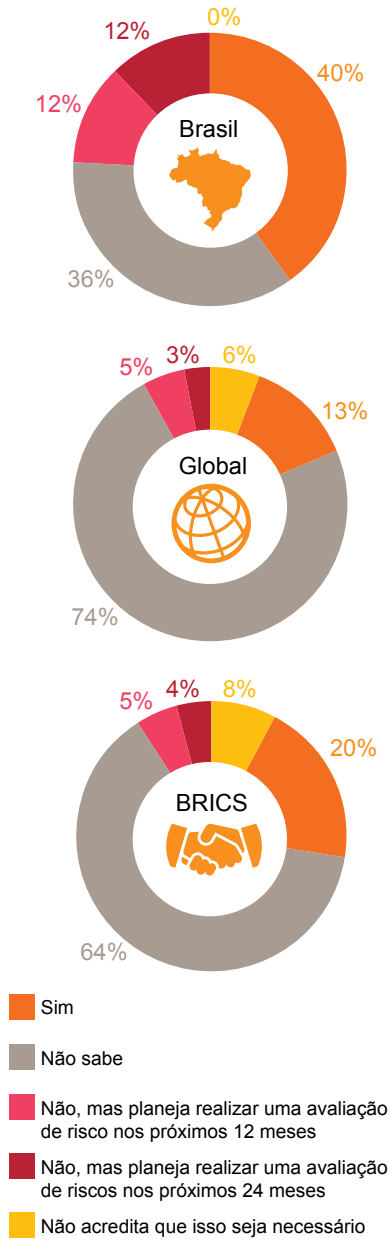


Fig 28: Técnicas comuns de lavagem de dinheiro baseadas no comércio

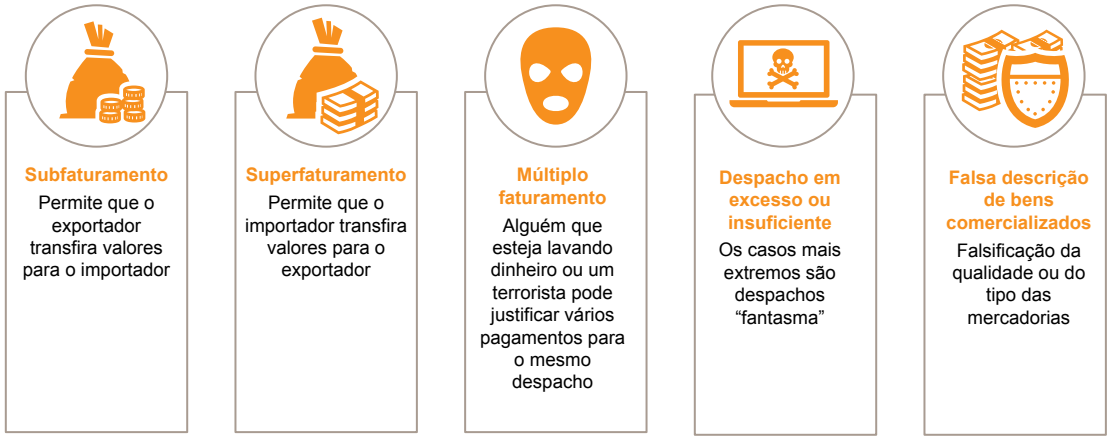
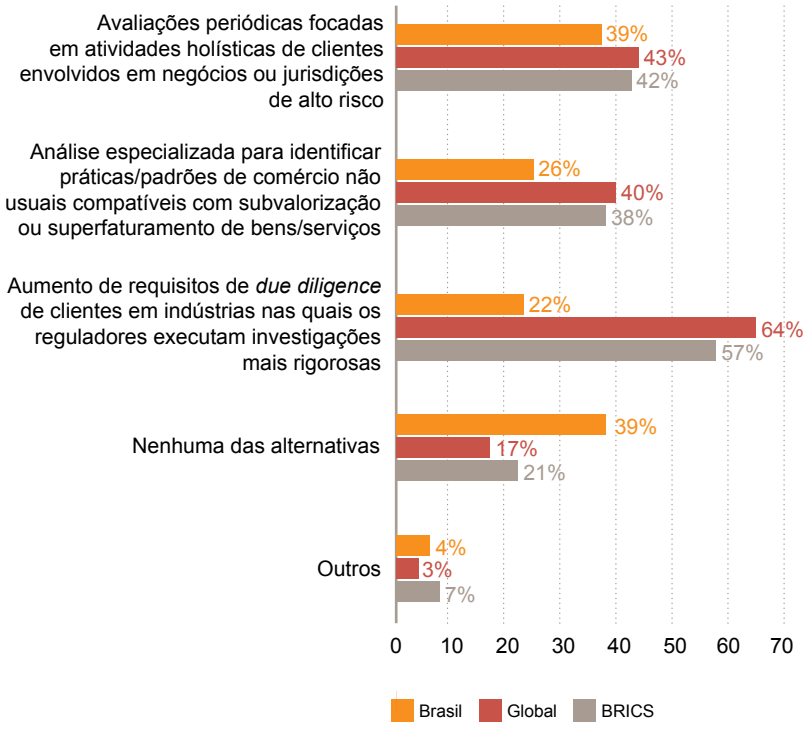
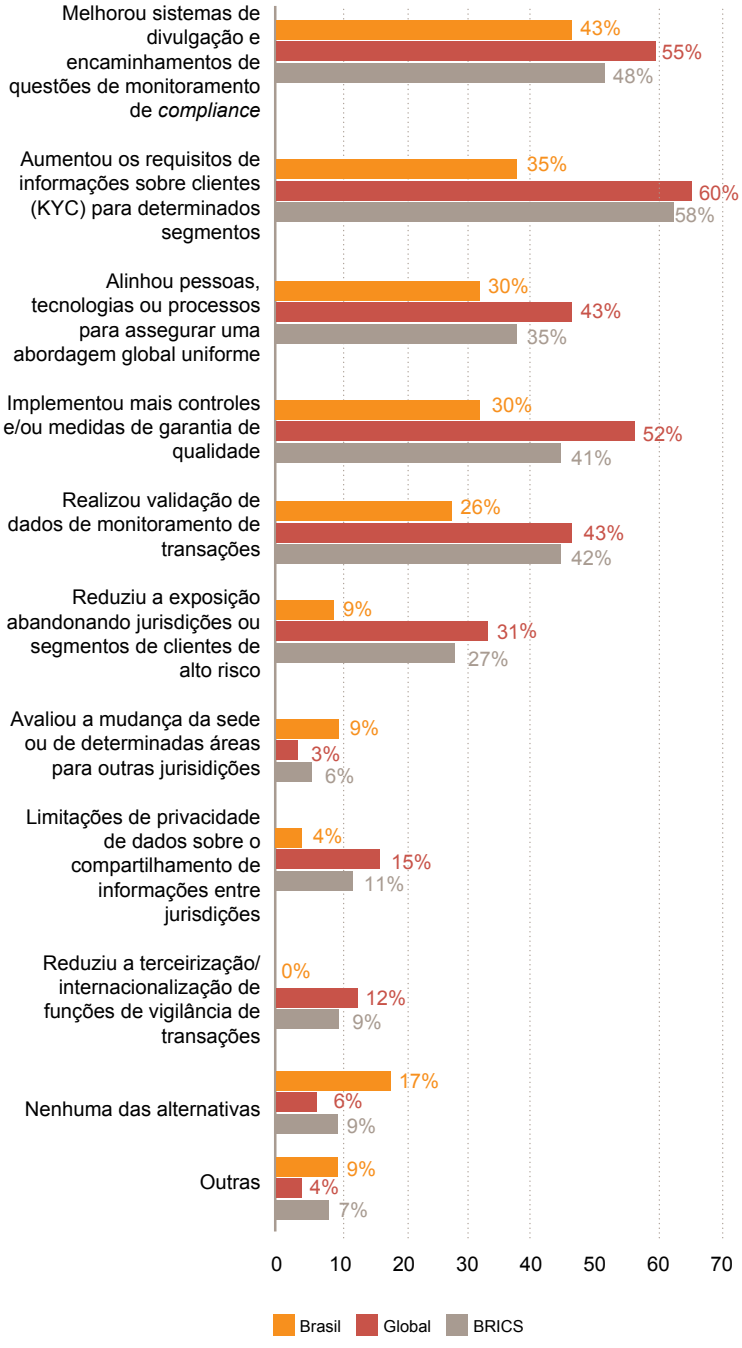


Fig 29: Medidas para detectar e frear a lavagem de dinheiro baseada em comércio



Conheça o seu cliente, hoje e amanhã. Uma visão transparente da sua base de clientes significa mais do que simplesmente identificar e confirmar as informações que eles fornecem. Deve ser uma ação dinâmica, não estática. É essencial continuar monitorando sinais de alerta e atividades suspeitas regularmente. Uma atenção especial deve ser dada a relacionamentos e transações comerciais de clientes – especialmente quando eles têm negócios com pessoas que residem em países com regulamentação PLD fraca ou insuficiente.

Fig 30: Medidas contra riscos de PLD/CFT



Tecnologia

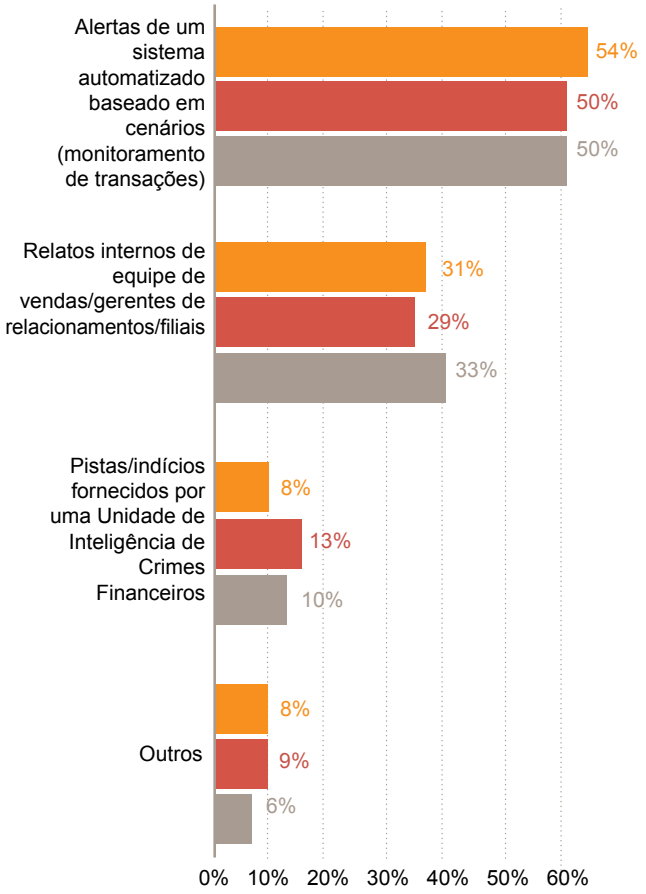
As empresas globais de todos os setores parecem estar presas numa difícil situação. A maioria - sobretudo as instituições financeiras – enfrenta as dificuldades de "redimensionar" seus programas de PLD de acordo com a evolução dos negócios e do cenário regulatório global. Os participantes da pesquisa no segmento de serviços financeiros demonstram estar bastante cientes dos desafios desses sistemas. A qualidade dos dados foi citada por um terço deles como a questão técnica mais importante atualmente.

O Brasil, no entanto, parece estar um passo atrás do restante do mundo em relação a esse tema. Mais de metade dos participantes ainda está às voltas com os desafios de implementação e atualização dos sistemas. A qualidade dos dados, que costuma ser um foco de atenção depois que os sistemas estão em pleno funcionamento, é citada por apenas 17% dos respondentes, em comparação com 32% dos BRICS.

Fig 31: Maior dificuldade atual em relação aos sistemas de combate à lavagem de dinheiro/financiamento de terrorismo

Para agravar o problema, o monitoramento de alertas de PLD apresenta um desempenho fraco. Apenas 54% das atividades identificadas como suspeitas de lavagem de dinheiro ou financiamento do terrorismo (50% no mundo e nos BRICS) estão sendo sinalizadas por sistemas de monitoramento de transações. As tipologias atuais de PLD talvez não capturem as nuances e estruturas complexas necessárias para identificar transações de alto risco.

Fig 32: Método usado para identificar atividade de LD/FT



Obs.: Considera apenas as respostas dos participantes que detectaram uma atividade suspeita.

A conversão para novas plataformas e modelos analíticos não é, pelo menos por enquanto, um fenômeno generalizado. Isso pode indicar que as instituições "precificaram" um certo grau de ineficácia nos seus sistemas legados de detecção – talvez para seu próprio prejuízo.

O que faz então uma empresa dar um salto tecnológico?

Geralmente, essa mudança é impulsionada por um evento – uma remediação provocada por sanções regulatórias, uma fusão, aquisição ou outra transação que revele que os sistemas legados não são mais adequados às necessidades. Pode ser também a entrada de um novo concorrente no mercado, causando transformações para todos os *players*.

Mas, às vezes, é simplesmente pelo fato de a organização alcançar um ponto de virada, no qual ela percebe que o retorno esperado do investimento necessário para adotar uma nova plataforma tecnológica é maior que o custo de abandonar os sistemas nos quais foram gastos milhões de dólares em configuração e manutenção.

E pode haver outras vantagens na adoção de novas tecnologias. Além do *compliance* para prevenção à lavagem de dinheiro, outras funções essenciais de *compliance* talvez sejam aprimoradas nesse processo – como medidas anticorrupção, sanções à exportação, monitoramento e resposta a fraudes, controles e investigações financeiras – fortalecendo possivelmente a governança geral.

Estatísticas de participação

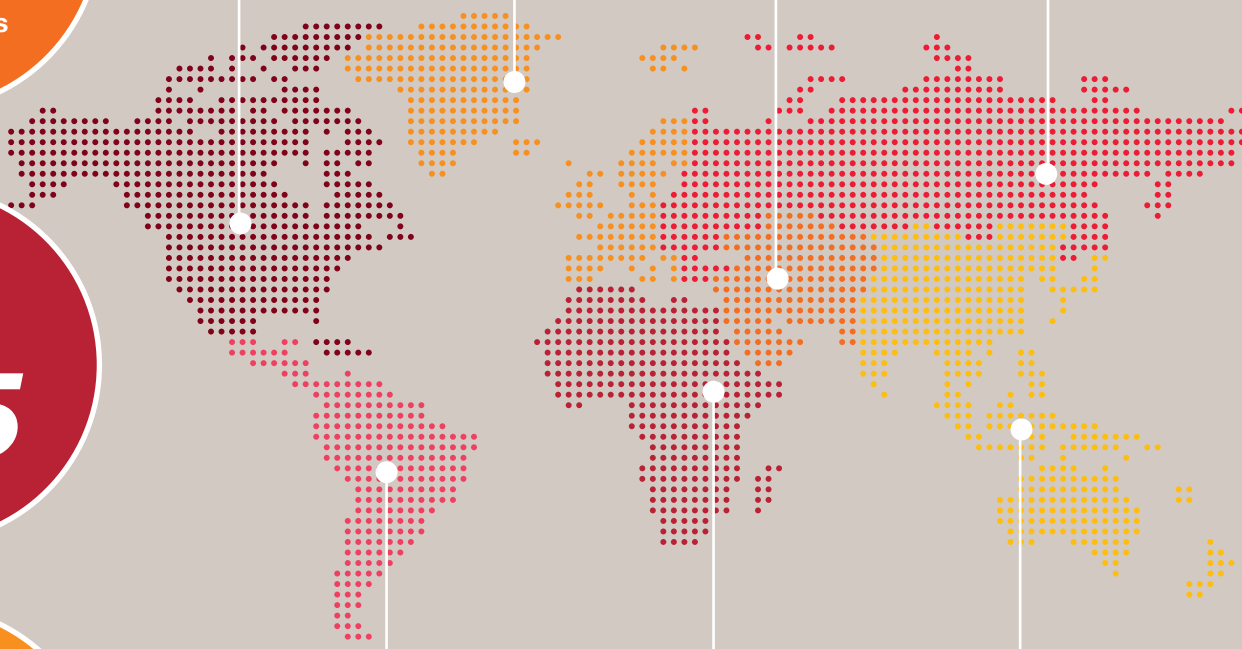
Estatísticas de participação

6.337
questionários preenchidos

115
países

17
diferentes idiomas

Participação por região



- **8%** América do Norte
- **22%** Europa Ocidental
- **5%** Oriente Médio
- **17%** Europa Oriental
- **18%** América Latina
- **10%** África
- **20%** Ásia-Pacífico

Respondentes

45%
Líderes executivos

30%
Chefes de departamentos ou unidades de negócios

70%
dos participantes em cargos de gestão executiva, finanças, auditoria, *compliance* ou gestão de riscos

54%
dos participantes contratados por organizações com mais de 1 mil empregados

48%
com mais de 10 mil empregados

37%
da amostra da pesquisa representaram empresas abertas

59%
dos participantes eram de organizações multinacionais

Setores

35%
Industrial

24%
Serviços financeiros

14%
Consumo

7%
Tecnologia

6%
Serviços profissionais

13%
Outros

Fontes de dados

Precisa de mais dados?

O nosso site www.pwc.com/crimesurvey foi projetado como uma extensão da pesquisa sobre crimes econômicos. Ele contém vários recursos úteis para os leitores que desejam se aprofundar na análise dos dados, com informações como:

- Metodologia
- Terminologia
- Comparações entre países
- Informações adicionais sobre o perfil dos participantes

Além disso, os dados da pesquisa deste ano alimentaram uma ferramenta inovadora chamada Global Data Explorer, que permite personalizar a análise dos dados de acordo com as necessidades do usuário.

Colaboradores

Líderes da pesquisa

Trevor White
Sócio, África do Sul
+27 (31) 271 2020
trevor.white@za.pwc.com

Mark Anderson
Sócio, Reino Unido
+44 (0) 207 8042564
mark.r.anderson@uk.pwc.com

Didier Lavion
Principal, Estados Unidos
+1 (646) 471 8440
didier.lavion@pwc.com

Membros do comitê editorial

Alex Tan
Diretor Executivo, Malásia
+60 (3) 2173 1338
alex.tan@my.pwc.com

Claudia Nestler
Sócia, Alemanha
+49 (69) 9585 5552
claudia.nestler@de.pwc.com

Martin Whitehead
Sócio, Brasil
+55 (11) 3674 3843
martin.j.whitehead@pwc.com

Antoinette Lau
Sócia, China
+86 (21) 2323 5533
antoinette.yy.lau@cn.pwc.com

Dinesh Anand
Sócio, Índia
+91 9818267114
dinesh.anand@in.pwc.com

Equipe de gestão da pesquisa

Moazam Fakey
Gerente sênior, África do Sul
+27 (11) 797 4750
moazam.fakey@za.pwc.com

Anjali Fehon
Diretora, Estados Unidos
+1 (973) 263 4310
anjali.t.fehon@pwc.com

Equipe de marketing da pesquisa

Gemma Peart
Gerente Global de Marketing, Reino Unido
+44 (0) 771 1589 331
gemma.peart@uk.pwc.com

Kate Glenn
Diretora de Marketing, Estados Unidos
+1 (571) 265 1497
kate.n.glenn@pwc.com

Equipe de dados e pesquisa

Colin McIlheney
Diretor de Pesquisa, Irlanda do Norte
+44 (0) 289 0415719
colin.mcilheney@uk.pwc.com

Sabrina McCotter
Gerente, Irlanda do Norte
+44 (0) 289 0415598
sabrina.c.mccotter@uk.pwc.com

Líderes de Forensic Services

Andrew Gordon
Líder Global, Reino Unido
+44 (0) 20 7804 4187
andrew.gordon@uk.pwc.com

Andrew Palmer
Líder EMEA, Reino Unido
+44 (0) 20 7212 8656
andrew.palmer@uk.pwc.com

Erik Skramstad
Líder APA, Estados Unidos
+1 (617) 530 6156
erik.skramstad@pwc.com

Contatos

Martin Whitehead
Sócio

t: +55 (11) 3674 3843
e: martin.whitehead@pwc.com

Leonardo Lopes
Sócio

t: +55 (11) 3674 3826
e: leonardo.lopes@pwc.com

Francisco Macedo
Sócio

t: +55 (11) 3674 2583
e: francisco.macedo@pwc.com

www.pwc.com/crimesurvey