

Protegendo o perímetro: o avanço da fraude externa

**Pesquisa Global sobre Fraudes e
Crimes Econômicos 2022**

PwC Brasil



pwc



As pressões ambientais, geopolíticas, financeiras e sociais estão criando um cenário volátil de riscos como jamais se viu. A situação torna ainda mais difícil prevenir fraudes e crimes econômicos. À medida que as organizações se adaptam rapidamente às mudanças, agentes mal-intencionados buscam explorar as brechas existentes nos mecanismos de defesa contra fraudes.

Os controles em vigor são suficientes para a gama de novas tecnologias digitais que está sendo desenvolvida? As empresas estão gerenciando riscos relacionados a um ambiente de trabalho híbrido que veio para ficar? Adotaram políticas e incentivos apropriados na transição do período de pandemia para um ambiente econômico incerto? **Qual são exatamente os riscos de fraude que as organizações enfrentam hoje?**

Anos de esforço para combater a fraude por meio de políticas, treinamento, controles internos e monitoramento ajudaram a reprimir más condutas internamente, mesmo em um ambiente volátil de riscos. Em paralelo, porém, **novas ameaças mais impactantes começaram a surgir**. A *Pesquisa Global sobre Fraudes e Crimes Econômicos* deste ano mostra que os perímetros das organizações estão vulneráveis, e que a ameaça dos fraudadores externos está crescendo.

Sumário

| | |
|--|----|
| Introdução | 2 |
| 1. As medidas de prevenção a fraudes estão funcionando – mas o cenário se agrava no Brasil | 4 |
| 2. O perímetro está vulnerável, e o jogo mudou | 13 |
| 3. Plataformas abrem nova fronteira para fraudes | 16 |
| 4. Principais medidas para proteger seu perímetro | 20 |
| Considerações finais | 21 |
| Sobre a pesquisa | 22 |
| Contatos | 23 |





1. As medidas de prevenção a fraudes estão funcionando – mas o cenário se agrava no Brasil

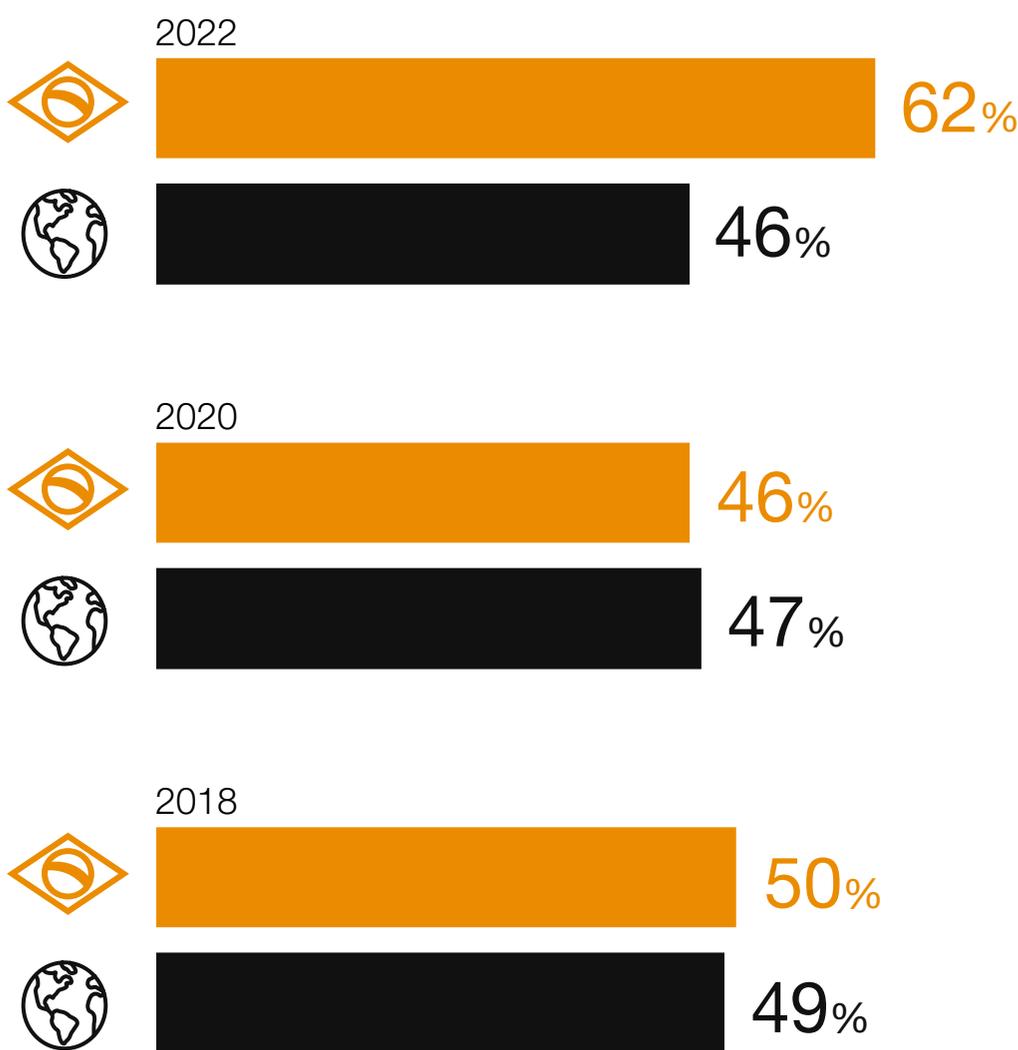
Apesar de problemas na cadeia de suprimentos, instabilidade ambiental e geopolítica, incerteza econômica, escassez de talentos e muitos novos riscos, o índice de fraude, corrupção e crimes econômicos não registra aumento no mundo desde 2018. No Brasil, no entanto, a tendência é diferente.

Pouco menos da metade das organizações globais (46%) relatou ter sofrido alguma forma de fraude ou outro crime econômico nos últimos 24 meses. Já no Brasil o percentual passou de 46% em 2020 para 62% neste ano.

A indústria de tecnologia é uma exceção à tendência global. Com a maturidade crescente do setor, foi possível identificar um aumento significativo na atividade de fraude globalmente desde 2020. Quase dois terços das empresas de tecnologia, mídia e telecomunicações sofreram algum tipo de fraude, a maior incidência entre todos os setores.

Quais são os maiores riscos? Em organizações de todos os portes, o crime cibernético representa a maior ameaça, seguido pela fraude do consumidor e pelo roubo de ativos – nossa pesquisa de 2020 chegou a conclusões semelhantes.

Empresas vítimas de fraude, corrupção ou outros crimes econômicos



Fonte: Pesquisa Global sobre Fraudes e Crimes Econômicos 2022, PwC.

Embora os índices de fraudes e crimes econômicos e financeiros permaneçam estáveis globalmente, os impactos desses crimes são altos para organizações de pequeno e grande portes (classificadas pelo volume de receitas anuais).

Entre as empresas com receita anual global acima de US\$ 10 bilhões, 52% sofreram fraude nos últimos 24 meses. Nesse grupo, quase uma em cada cinco informou que o incidente mais grave registrado teve impacto financeiro superior a US\$ 50 milhões. A parcela de empresas afetadas com menos de US\$ 100 milhões em receitas foi inferior: 38% sofreram fraude, sendo que cerca de uma em cada quatro registrou impacto total de mais de US\$ 1 milhão.

Índice global de fraude e seu impacto financeiro para as empresas

Empresas com receita acima de US\$ 10 bilhões



52%

sofreram fraude nos últimos 24 meses.



18%

registraram impacto financeiro de US\$ 50 milhões ou mais em consequência do incidente de fraude mais grave sofrido.

Fonte: Pesquisa Global sobre Fraudes e Crimes Econômicos 2022, PwC.

Empresas com receita abaixo de US\$ 100 milhões



38%

sofreram fraude nos últimos 24 meses.



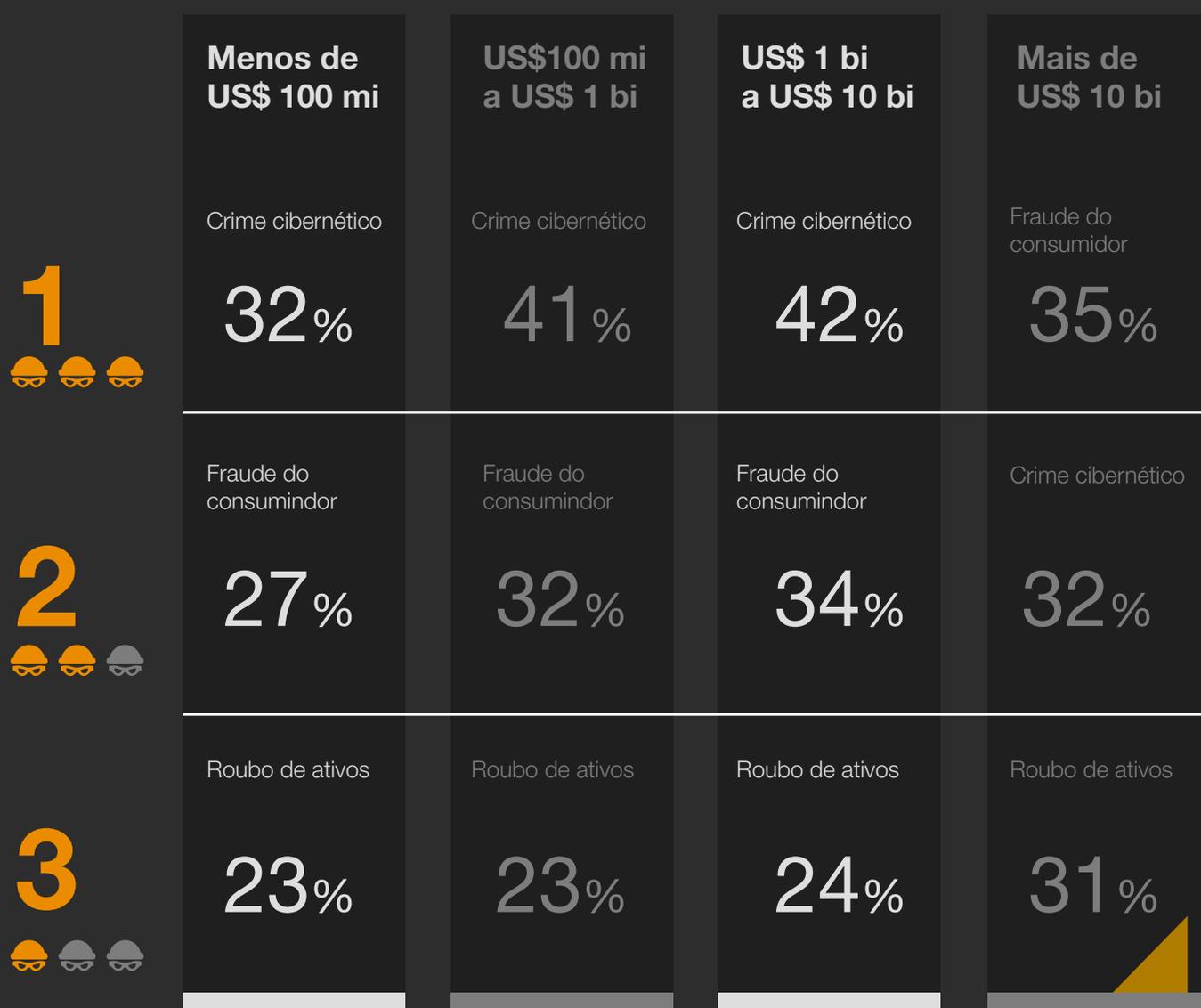
22%

registraram impacto financeiro de US\$ 1 milhão ou mais em consequência de todos os incidentes de fraude sofridos.

Fonte: Pesquisa Global sobre Fraudes e Crimes Econômicos 2022, PwC.

As organizações estão trabalhando para aprimorar capacidades técnicas e implementar controles internos mais fortes.

Tipos de fraude sofridos, por tamanho da organização (em receita global) – mundo



Uma exceção ao domínio do crime cibernético é o setor de energia, *utilities* e recursos, onde a fraude em compras é a maior ameaça. Entre o grupo de 31% de empresas do segmento que sofreram crimes econômicos, quase metade relatou fraude em compras. Por ter uma presença digital menor e menos interações com o consumidor do que muitas outras indústrias, o setor tem um perfil de fraudes diferente. No entanto, eventos recentes mostraram que ataques cibernéticos contra infraestrutura podem representar uma ameaça no futuro próximo.

Mudanças sistemáticas estão fortalecendo as organizações contra fraudes e outros crimes econômicos. Especificamente, elas vêm implementando políticas, procedimentos e treinamento para ajudar os empregados que querem fazer a coisa certa. A pesquisa mostra que as organizações estão trabalhando para aprimorar capacidades técnicas e implementar canais de reporte de irregularidades e controles internos mais robustos.

Dois terços das **empresas que foram vítimas de crimes econômicos no mundo descobriram o incidente mais grave de fraude com a ajuda de controles corporativos**, um resultado sete pontos percentuais acima do registrado em 2020.

Tipos de fraude sofridos, por indústria – mundo

| Produção industrial | Serviços financeiros | Energia, utilities e recursos | Varejo e consumo | Governo e setor público | Saúde | Tecnologia, mídia e telecom |
|---|--|--|-----------------------------|-----------------------------|-----------------------------|-----------------------------|
| Crime cibernético 32% | Fraude do consumidor 44% | Fraude em compras 45% | Fraude do consumidor 37% | Crime cibernético 36% | Crime cibernético 40% | Crime cibernético 50% |
| Roubo de ativos 28% | Crime cibernético 38% | Crime cibernético 29% | Roubo de ativos 31% | Roubo de ativos 33% | Roubo de ativos 30% | Fraude do consumidor 35% |
| Fraude nas demonstrações contábeis/financeiras 24% | Falha <i>know-your-customer</i> 29% | Fraude na cadeia de suprimentos 29% | Crime cibernético 27% | Fraude do consumidor 28% | Fraude do consumidor 27% | Fraude em compras 26% |

Fonte: Pesquisa Global sobre Fraudes e Crimes Econômicos 2022, PwC.



Marcos Panassol

Sócio e líder de Forensics



“Estamos vivendo um cenário de riscos mais volátil. Observamos um aumento de ameaças trazidas por agentes externos organizados para se infiltrar em plataformas digitais. Para responder a esses riscos, as organizações precisam ser ainda mais ágeis e adotar novas abordagens e tecnologias de prevenção e combate a fraudes.”

Em foco

Fraude durante a pandemia

A crise criou uma vulnerabilidade preocupante para as empresas que aceleravam a transição para operações digitais. **Um ponto positivo nos últimos 24 meses foi a queda nos roubos de ativos, que ainda é, no entanto, uma das principais categorias de fraude.** Talvez isso se deva, em parte, ao fato de que mais empregados estão trabalhando remotamente, com acesso limitado aos ativos da empresa.

Ao mesmo tempo, o trabalho remoto aumentou riscos que vão além da segurança digital. Por exemplo, algumas empresas perceberam mais riscos para a segurança dos empregados. Cresceram as ameaças de chantagem ou danos físicos aos empregados que trabalhavam em casa com acesso a dados corporativos valiosos. O índice global de empresas que sofreram **fraude baseada em desinformação** nos últimos 24 meses foi de 15%. Isso sugere que as organizações precisam investir na conscientização sobre esse risco emergente.

Crises anteriores, como a recessão de 2007 a 2009, oferecem lições valiosas para as organizações que enfrentam a volatilidade pós-pandemia. A história mostra que as tendências de fraude em tempos de turbulência não surgem imediatamente. Muitas vezes, leva entre 18 e 24 meses para que esses eventos se tornem conhecidos. No entanto, pontos de inflexão, como a transição de uma economia em contração para uma economia em expansão, podem dar sinais para a identificação de fraudes internas.

Em tempos de transição, muitas fraudes internas se tornam visíveis porque o comportamento do fraudador exibe um atraso em relação à mudança para novos objetivos e metas. Por exemplo, alguns colaboradores mal intencionados podem estar praticando ações ilegais para atingir metas de vendas que, na visão dos líderes, são inalcançáveis em uma economia em crise e, portanto, suspeitas.

Os fraudadores externos também aproveitam pontos de inflexão, explorando a confusão do mercado, principalmente com esquemas focados no consumidor. Grupos do crime organizado podem recrutar parceiros mais facilmente em uma economia em crise, incorporando à equipe novos membros que ficaram desempregados. Sendo assim, há todos os motivos para aumentar a vigilância sobre os riscos de fraude em uma crise, com atenção especial para aqueles que a organização pode não ter observado antes.



Crimes econômicos amplificados pela covid-19

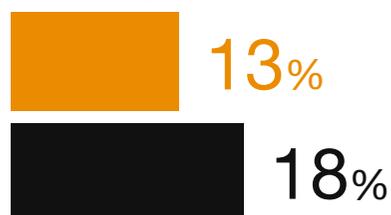
Porcentagem de empresas que dizem ter sofrido novas fraudes e aumento do risco por causa da covid-19 no mundo

■ Novo tipo de fraude sofrido ■ Áreas em que o risco aumentou

Risco de má conduta



Risco legal



Crime cibernético



Informação privilegiada



Risco de plataformas



Fonte: Pesquisa Global sobre Fraudes e Crimes Econômicos 2022, PwC.



70%

dos que foram vítimas de fraudes no mundo registraram novos incidentes em consequência da turbulência causada pela covid-19.



2. O perímetro está vulnerável, e o jogo mudou

A pesquisa identifica o surgimento de um novo perfil de ameaça. Agentes perigosos – entidades externas que não podem ser controladas nem facilmente influenciadas – estão ganhando força e eficácia rapidamente. **No resultado global, quase 70% das organizações que reportaram ter sofrido fraudes relataram que o incidente mais grave teve como base um ataque externo ou conluio entre agentes externos e internos.** O problema é que fraudadores externos são imunes aos mecanismos tradicionais de prevenção de fraudes, como códigos de conduta, treinamento e investigações.

O impacto dos *hackers* e das redes do crime organizado, que estão entre os criminosos externos mais comuns, aumentou substancialmente nos últimos dois anos. Globalmente, cerca de um terço dos ataques externos foi cometido por *hackers* e 28% foram conduzidos pelo crime organizado. Ambos os números refletem aumentos em relação à nossa pesquisa de 2020.

Principal autor da fraude mais grave sofrida – mundo



43% Agente externo (41% em 2020)



31% Agente interno (38% em 2020)



26% Conluio entre agentes internos e externos (21% em 2020)

Fonte: Pesquisa Global sobre Fraudes e Crimes Econômicos 2022, PwC.

Os grupos de criminosos organizados estão se tornando mais especializados e profissionais, com metas, incentivos e estruturas de bônus. Eles aproveitam as vulnerabilidades e investem continuamente para enganar suas vítimas. O combate a esses agentes mal-intencionados é diferente do esforço para conter a fraude interna, porque as empresas têm pouca capacidade de influenciar ou controlar as ações dos criminosos.

Vários fatores estão convergindo para impulsionar o aumento da fraude externa. O crescimento da frequência de violações de dados observado nos últimos anos continuará e vai elevar consideravelmente as exigências para empresas que são obrigadas a proteger os dados pessoais de seus clientes. As violações também desafiarão as estratégias de autenticação que as organizações adotaram para se proteger contra fraudadores.

Os agentes mal-intencionados também estão colaborando entre si, o que aumenta o volume e a sofisticação dos ataques. Usando salas de *chat*, *dark web* e criptomoedas, os especialistas em violação de dados, criação de identidades falsas, metodologias de ataque e outras áreas podem se conectar, coordenar e realizar transações como parte de uma economia criminosa em ascensão.

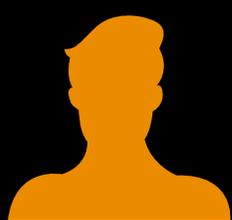
Além disso, há uma tendência cada vez maior de pessoas que antes agiam dentro da legalidade se juntarem a grupos de fraudadores. Ela prevalece sobretudo em países com más condições socioeconômicas, pois as pessoas encontram justificativas na falta de oportunidades legítimas para racionalizar essas ações.

No mundo

Tipo de agente externo, 2022



Principais agentes externos, 2020



1
Consumidor

26%



2
Hacker

24%



3
Fornecedor/provedor

19%



3. Plataformas abrem nova fronteira para fraudes

Globalmente, das organizações que sofreram fraudes nos últimos dois anos, quatro em cada dez registraram algum tipo de delito associado a plataformas digitais, seja relacionado a violações de *know-your-customer* (KYC – “conheça seu cliente”, em tradução livre), desinformação, lavagem de dinheiro, financiamento do terrorismo ou atividades antiembargo. A ascensão das plataformas digitais, como mídias sociais, comércio eletrônico ou serviços (por exemplo, carros compartilhados ou hospedagens) abre caminho para uma gama de riscos de fraude e outros crimes econômicos que a maioria das empresas está apenas começando a conhecer.

Os riscos das plataformas podem criar um efeito cascata, com o impacto das fraudes alcançando várias áreas da organização. Como a fraude associada às plataformas é um problema de toda a empresa, combatê-la requer um esforço multifuncional e uma comunidade diversificada de profissionais envolvidos.

Em foco

Ameaças no horizonte

Os riscos que estão surgindo podem causar grandes perturbações nos próximos anos. Por definição, esses novos riscos quase não aparecem no radar, mas podem ir para o primeiro plano rapidamente. Por exemplo, apenas 6% das organizações globais disseram ter sofrido fraudes antiembargo nos últimos 24 meses. No entanto, esse cenário pode mudar nos próximos dois anos, uma vez que as sanções globais atingiram os níveis mais altos da história recente.

O desafio de gerenciar os riscos de novas fraudes é evitar cair na armadilha de ver apenas o que é conhecido. Quais são os riscos mais preocupantes de novas fraudes?

A PwC acredita que pelo menos dois riscos devem estar no radar.



Fraude em relatórios ESG

A confiança se tornou um fator-chave para a geração de valor. A nossa [25ª Global CEO Survey](#) destacou a existência de um vínculo entre empresas com alto nível de confiança e sua capacidade de impulsionar mudanças. Mas a confiança é algo frágil. Uma falha de transparência, percebida ou real, pode causar estragos em termos de reputação da marca e confiança.

Com a importância crescente das questões ambientais, sociais e de governança (ESG, na sigla em inglês) para os *stakeholders*, a precisão nos relatórios ESG é essencial. Globalmente, apenas 8% das organizações que foram vítimas de crimes econômicos nos últimos 24 meses registraram delitos associados a relatórios ESG, como *greenwashing* ou manipulação de indicadores de performance ESG base para remuneração variável. O incentivo, porém, para cometer fraudes nessa área só aumentará, assim como as consequências delas.



Fraude na cadeia de suprimentos

Uma em cada oito organizações no mundo registrou novos incidentes de fraude na cadeia de suprimentos como resultado da turbulência causada pela covid-19. Um em cada cinco vê a fraude nessa área como um risco crescente por causa da pandemia. Poucas empresas estão cientes dos riscos de fraude e de condutas impróprias em sua cadeia de suprimentos, o que torna essa área um foco de exposição hoje e no futuro.



6%

das organizações* disseram ter sofrido fraude antiembargo nos últimos 24 meses.



8%

das organizações* que sofreram fraudes nos últimos 24 meses registraram delitos associados a relatórios ESG.



1 em 8

organizações* sofreram novos incidentes de fraude na cadeia de suprimentos por causa da turbulência provocada pela covid-19.

4. Principais medidas para proteger seu perímetro

1

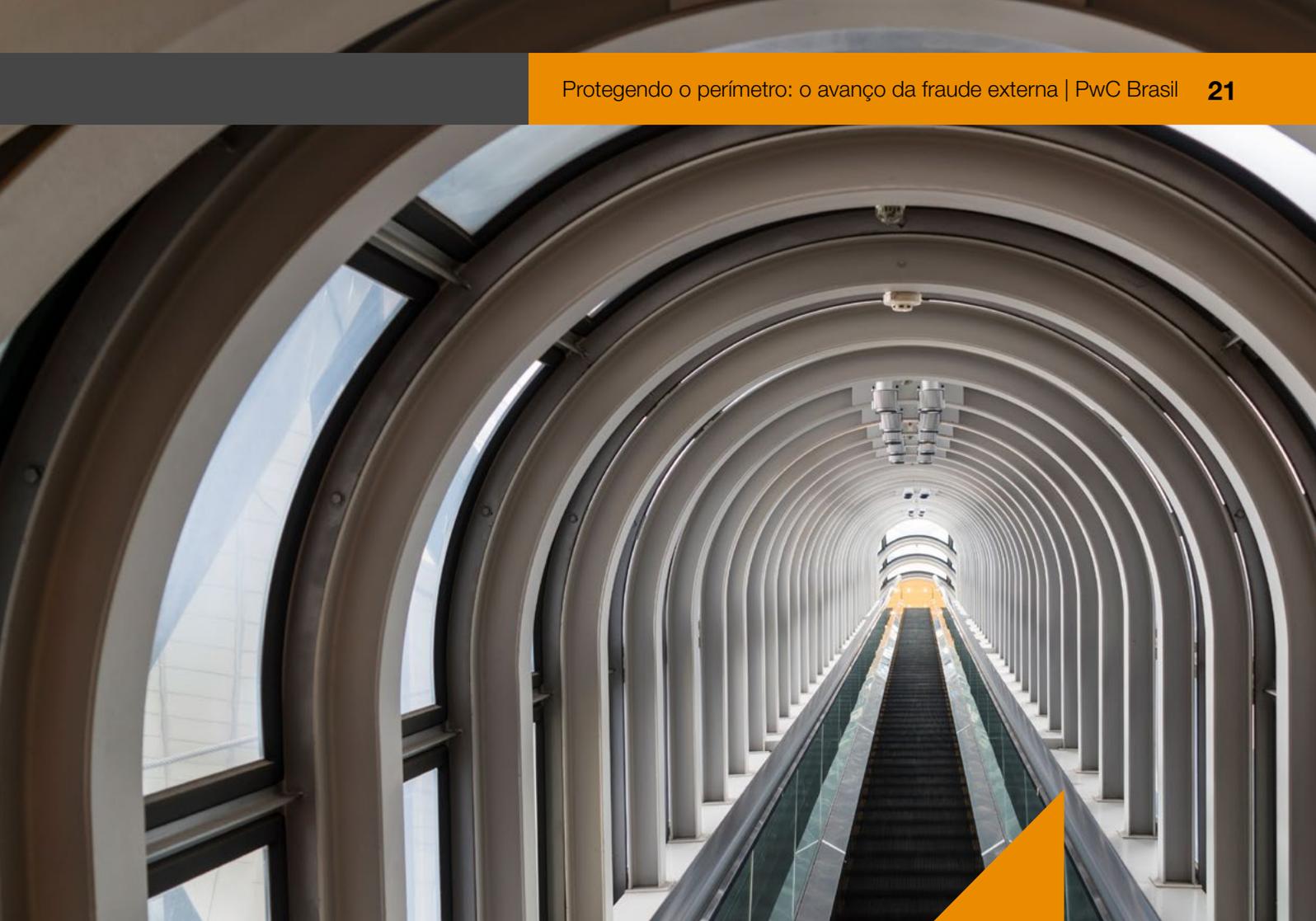
Entenda o ciclo de vida dos produtos voltados para o consumidor. Dedique tempo a identificar onde um fraudador pode encontrar oportunidades para explorar um produto e causar danos financeiros, legais ou de reputação. Como isso poderia acontecer? O que seria necessário para evitar que acontecesse e que tipo de resposta precisa ser dada caso aconteça?

2

Encontre o equilíbrio entre a experiência do usuário e os controles de fraude. Proteger os canais de contato com o cliente exigirá um equilíbrio delicado entre garantir que os usuários tenham uma ótima experiência e detectar e deter os fraudadores. O duplo objetivo de manter os falsos positivos no nível mais baixo possível e detectar fraudes verdadeiras pode ser alcançado por meio de uma combinação de processos, estratégia e tecnologia de fraudes.

3

Orquestre os dados. Muitas vezes, os sinais de fraude virão de sistemas diferentes e desconectados e só serão detectados por uma revisão manual ocasional. É essencial que os indicadores de fraude sejam orquestrados em uma plataforma centralizada que possa monitorar todo o ciclo de vida dos usuários (fraudadores ou não) e gerar alertas que sejam relevantes.



Considerações finais

Prevenir a fraude e outros crimes econômicos é um desafio complexo. É preciso manter o foco em políticas, treinamento e controles internos e – cada vez mais – usar tecnologias sofisticadas. Em um ambiente de incertezas, proteger o perímetro é essencial, pois todos os sinais apontam para criminosos se tornando cada vez melhores em explorar as brechas.



Sobre a pesquisa

A **Pesquisa Global sobre Fraudes e Crimes Econômicos** deste ano perguntou sobre as atitudes das organizações em relação à fraude e ao crime financeiro e econômico no ambiente atual e obteve respostas de 1.296 participantes em 53 países e regiões. Esta publicação se concentrou nas tendências de fraude e nos riscos de conduta.

Há mais de 20 anos, a **Pesquisa Global sobre Fraudes e Crimes Econômicos da PwC** analisa vários crimes, como:

- Fraude nas demonstrações contábeis/financeiras
- Violação de leis de concorrência/antitruste
- Roubo de ativos
- Suborno e corrupção
- Fraude do consumidor
- Crime cibernético
- Práticas comerciais enganosas
- Fraude de recursos humanos
- Transações não autorizadas/com informações privilegiadas
- Roubo de propriedade intelectual (PI)
- Lavagem de dinheiro e sanções
- Fraude em compras
- Fraude fiscal



61%

dos participantes da pesquisa são diretores executivos.



39%

das organizações participantes têm receita anual superior a US\$ 1 bilhão (e 65% têm receita superior a US\$ 100 milhões).

Contatos

Marcos Panassol

Sócio e líder de Forensics
marcos.panassol@pwc.com

Leonardo Lopes

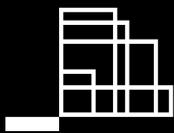
Sócio
leonardo.lopes@pwc.com

Elisa Mayor

Sócia
elisa.mayor@pwc.com

Adriano Vargas

Sócio
adriano.s.vargas@pwc.com



pwc

www.pwc.com.br

 PwC Brasil  @PwCBrasil  PwC Brasil  @PwCBrasil  PwC Brasil  @PwCBrasil

O conteúdo deste material destina-se apenas à informação geral, não constitui uma opinião, ou entendimento da PwC, e nem pode ser utilizado como, ou em substituição, a uma consulta formal a um profissional habilitado.

© 2022 PricewaterhouseCoopers Brasil Ltda. Todos os direitos reservados. Neste documento, “PwC” refere-se à PricewaterhouseCoopers Brasil, firma membro do network da PricewaterhouseCoopers, ou conforme o contexto sugerir, ao próprio network. Cada firma membro da rede PwC constitui uma pessoa jurídica separada e independente. Para mais detalhes acerca do network PwC, acesse: www.pwc.com/structure