A fraude vista à lupa

Global Economic Crime and Fraud Survey 2018 - Perspetiva sobre Portugal

34%

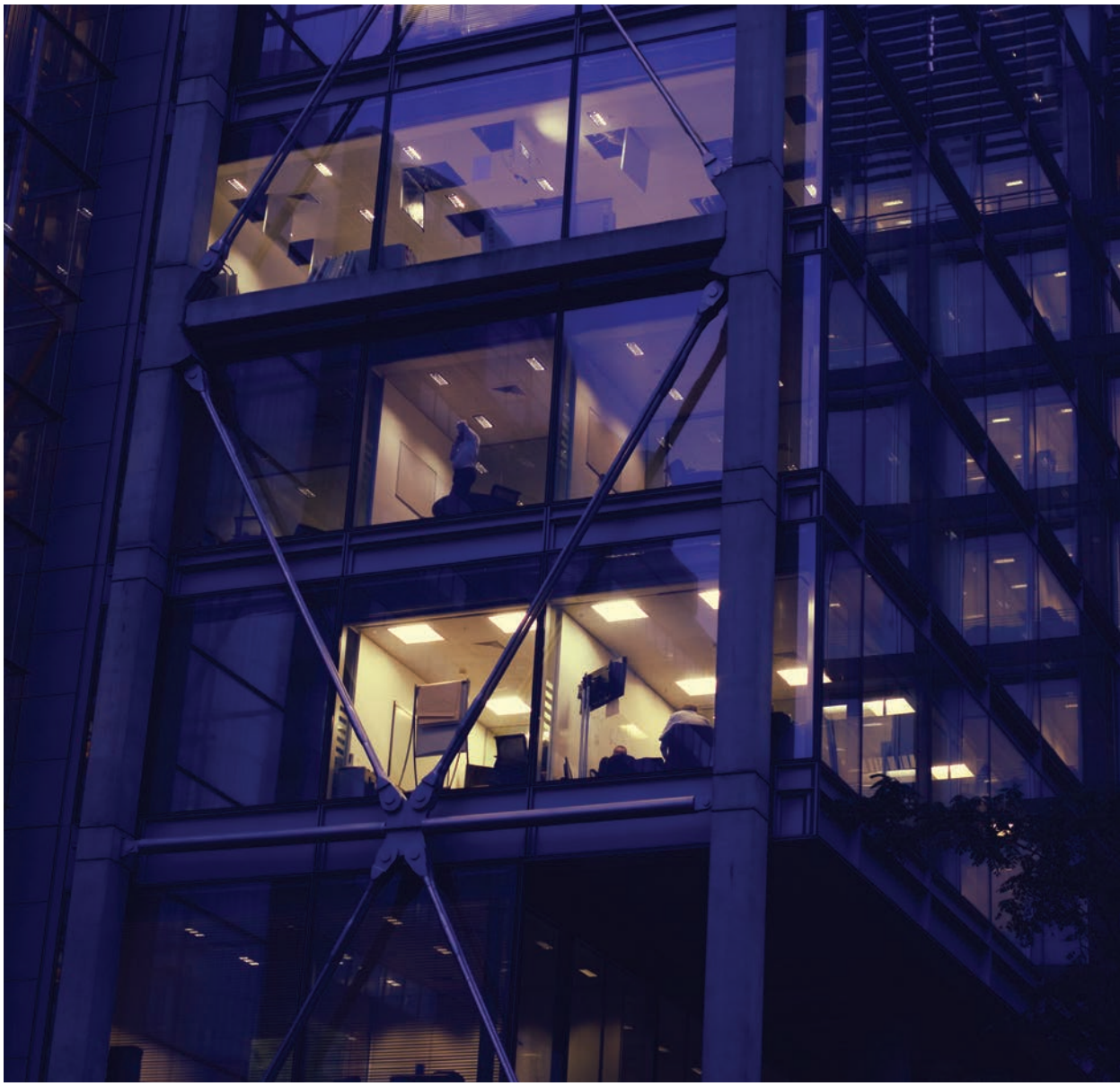
das organizações em Portugal afirmam ter sido vítimas de fraude ou crime económico

57%

destas afirmam que a fraude foi cometida por elementos externos

53%

dos inquiridos em Portugal acreditam que as recentes mudanças no ambiente regulatório e geopolítico terão um impacto acrescido nas suas organizações nos próximos dois anos



pwc

www.pwc.pt/forensics

Sumário Executivo

Patrique Fernandes
Partner da PwC Portugal
Forensic Services

O Global Economic Crime and Fraud Survey de 2018 da PwC confirma a tendência global de crescimento dos níveis de fraude e do impacto significativo que esta crescente onda de crimes económicos tem nas organizações hoje em dia.

Em Portugal, apenas 34% das organizações afirma ter sido vítima de fraude e crime económico, o que contrasta com os 49% a nível global. No entanto estima-se que o número de organizações que são de facto vítimas de fraude seja significativamente superior. Na realidade, são ainda poucas as organizações que estão plenamente conscientes dos riscos de fraude que enfrentam.

O Global Economic Crime and Fraud Survey reuniu dados valiosos de mais de 7.200 participantes em 123 países, incluindo Portugal com 86 participantes (parte significativa do setor financeiro) com o propósito de realçar alguns dos desafios estratégicos que as organizações enfrentam atualmente no que se refere à fraude e crime económico.

A fraude que não se vê é tão importante como a fraude que se observa

O Global Economic Crime and Fraud Survey de 2018 revela que, embora exista uma crescente consciencialização do risco de fraude e crime económico, poucas organizações estão conscientes da plenitude dos riscos que existem nas suas próprias estruturas orgânicas e funcionais.

O presente *Survey* pretende suprir essa falha de conhecimento, explorando não apenas a fraude "factual" e visível que as empresas dizem estar a enfrentar, mas também as "caixas negras" que não permitem uma visão clara e global, e o que pode e deve ser efetuado relativamente a esta matéria. Que ações podem ser tomadas para que o combate à fraude e ao crime económico seja efetuado de forma eficaz?

Combater a fraude

Reconhecer a fraude quando a vemos

A fraude está efetivamente a aumentar ou estaremos apenas mais atentos?

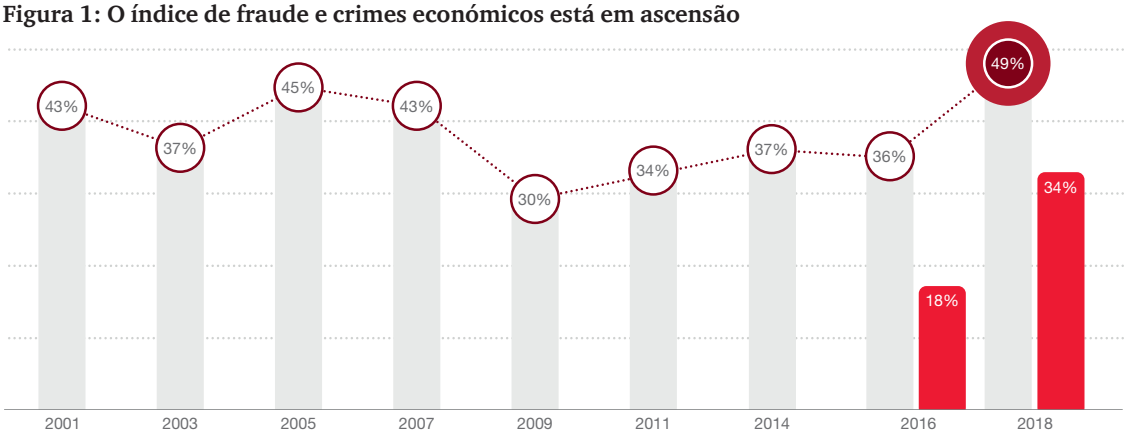
Este ano, 49% dos inquiridos do Global Economic Crime and Fraud Survey disseram que as suas organizações tinham sido vítimas de fraude ou crime económico, o que contrasta com os 36% obtidos em 2016. Em Portugal, 34% das organizações foram objeto de crimes económicos nos últimos 24 meses o que representa um crescimento significativo face ao anterior *Survey* (18% em 2016).

Este aumento pode ser explicado por uma combinação de fatores:

- a crescente consciência global de fraude;
- um número maior de respostas ao *Survey*;
- e uma maior clareza sobre o que "fraude" realmente significa.

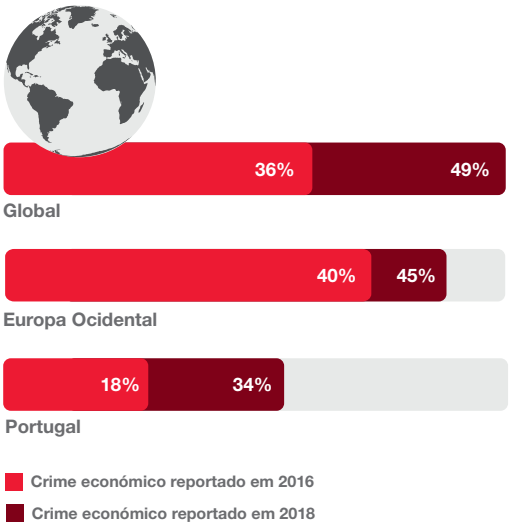
Mas toda a organização, por mais atenta que seja, é vulnerável a "ângulos mortos". E como esses "ângulos mortos" geralmente só se tornam visíveis depois da fraude ocorrer, é necessário aumentar os esforços de combate à fraude através de procedimentos de identificação desses mesmos "ângulos mortos".

Figura 1: O índice de fraude e crimes económicos está em ascensão



As empresas estão hoje mais expostas ao risco de fraude (interna e externa), regulatório e reputacional.

Figura 2: O índice de fraude e crimes económicos aumentou em todas as regiões geográficas



Q. A sua organização sofreu alguma fraude e/ou crime económico nos últimos 24 meses?

Fonte: PwC's 2018 Global Economic Crime and Fraud Survey

Apropriação indevida de ativos é, a nível global, o crime económico mais reportado nos últimos 24 meses

Q. Que tipos de crime económico foram sofridos pela sua organização nos últimos 24 meses

Fonte: PwC's 2018 Global Economic Crime and Fraud Survey

Do mesmo modo que o índice de criminalidade económica aumentou desde 2016, tanto em Portugal como a nível global, o mesmo sucedeu com o montante que as empresas estão a gastar para combater a fraude:

- 36% dos inquiridos em Portugal, afirmam que as suas organizações aumentaram os gastos com o combate à fraude e ao crime económico nos últimos dois anos, o que compara com 42% a nível Global (39% no Global em 2016).
- 50% dos inquiridos em Portugal, afirmam que as suas organizações planeiam aumentar os gastos com o combate à fraude e ao crime económico nos próximos dois anos, o que compara com 44% a nível Global.

Onde está este dinheiro a ser gasto? As organizações estão a utilizar tecnologias cada vez mais poderosas e ferramentas de análise de dados mais robustas para combater a fraude e o crime económico.

Para além dos controlos baseados na tecnologia, muitas organizações estão também a implementar canais de denúncias *(whistle-blowing)* e a tomar medidas para manter a gestão de topo envolvida no tema da fraude.

Mas será que estas medidas representam uma mudança genuína para abordagens mais proativas relativamente à fraude e à corrupção? Ou são apenas uma reação, impulsionada principalmente por uma legislação reforçada relativamente a temas como o combate ao suborno e à corrupção e formas cada vez mais globalizadas de fiscalização? Por outras palavras, será que ainda estamos a deixar escapar algo de fundamental na luta contra a fraude? Os resultados do nosso *Survey* sugerem fortemente que estamos.

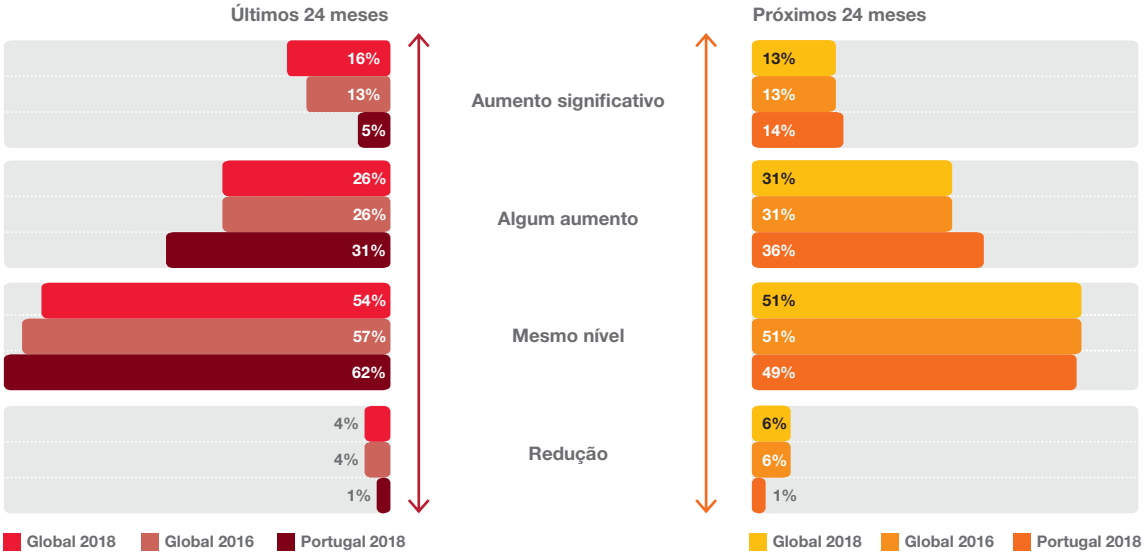
36%

dos inquiridos em Portugal, afirmam ter aumentado os gastos no combate à fraude e aos crimes económicos

50%

das organizações inquiridas em Portugal manifestaram a intenção de aumentar esses mesmos gastos nos próximos dois anos

Figura 3: As organizações continuam a aumentar os gastos com combate à fraude



Q. De que forma a sua organização ajusta o montante a gastar no combate à fraude e/ou crimes económicos?

Fonte: PwC's 2018 Global Economic Crime and Fraud Survey

Dado o contínuo aumento da fraude, é preocupante que nos últimos dois anos, 46% dos inquiridos em Portugal não tenham realizado uma avaliação geral do risco de fraude, analisando os principais riscos que enfrentam os seus negócios ou atividades.

Na nossa perspetiva, uma avaliação do risco de fraude, ponderada, objetiva e focalizada, constitui o pilar para o desenho das restantes atividades antifraude. A ausência de uma avaliação de risco de fraude, significa que os processos de negócios e antifraude implementados pela organização podem ser mal direcionados e não possuírem a eficácia e especificidade necessárias.

De uma forma mais positiva, algumas empresas referem ter realizado avaliações de risco de fraude, mais focadas em áreas de risco acrescido, como a vulnerabilidade a ataques cibernéticos (49%), obrigações regulamentares específicas da indústria (37%), plano de resposta cibernética (31%), prevenção de branqueamento de capitais (29%) e anti suborno e anti corrupção (28%).

No entanto, fica claro que a cobertura é insuficiente em todas as áreas.

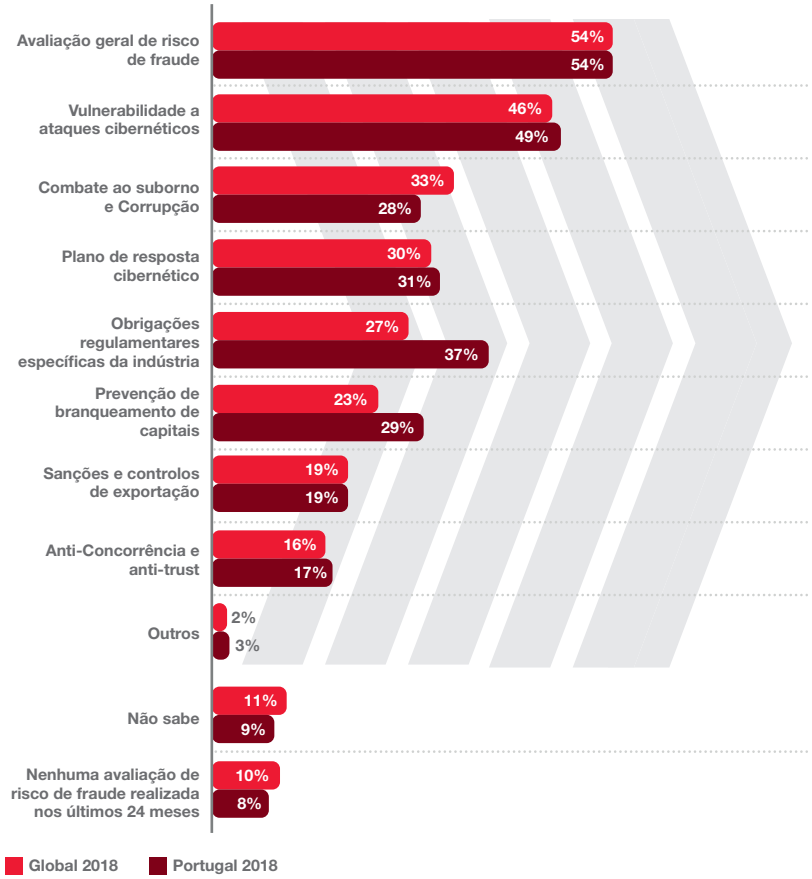
Da nossa experiência, são poucas as organizações que implementaram processos para identificar grandes alterações ao perfil de risco do negócio ou partes do negócio. As avaliações de risco de fraude, quando existentes, são frequentemente documentos estáticos, refletindo um momento no tempo, em vez de responder a um ambiente complexo e em permanente evolução. Este tipo de avaliação estática é manifestamente insuficiente.

O risco de fraude é uma questão cada vez mais multifacetada e complexa que tem evoluído ao longo do tempo. Tanto as técnicas de combate à fraude, como as ameaças evoluem ao mesmo ritmo que as atividades, operações, pessoas e estruturas do negócio, o que torna fundamental que as avaliações de risco sejam atualizadas regularmente para garantir que as ameaças sejam devidamente tratadas. A ausência de atualizações regulares é uma preocupação significativa.

46%

das organizações em Portugal não realizaram uma avaliação geral do risco de fraude. A nível Global foram obtidos os mesmos resultados

Figura 4: Menos de metade das organizações realizaram avaliações de risco "direcionadas" nos últimos dois anos



Q. Nos últimos 24 meses, a sua organização realizou alguma avaliação de risco em alguma das seguintes áreas?

Fonte: PwC's 2018 Global Economic Crime and Fraud Survey

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

Fonte: PwC's 2018 Global Economic Crime and Fraud Survey

Adotar uma abordagem proativa no combate à fraude

A responsabilidade da administração

O nosso *Survey* refere que o custo direto da fraude e as suas consequências podem ser significativos. Mas quando os custos indiretos (como investigações e outras intervenções) são incluídos, o custo total é bastante superior. As intervenções e investigações de fraude e/ou crime económico têm de ser planeadas e executadas por especialistas de forma a maximizar os resultados alcançados e, com isto, diminuir estes custos indiretos.

Quando os custos com a fraude atingem os resultados de uma organização, é natural que o conselho de administração e os acionistas exijam explicações. No entanto, no mundo de hoje, a responsabilidade da administração não fica por aí. Na verdade, isso é apenas o início.

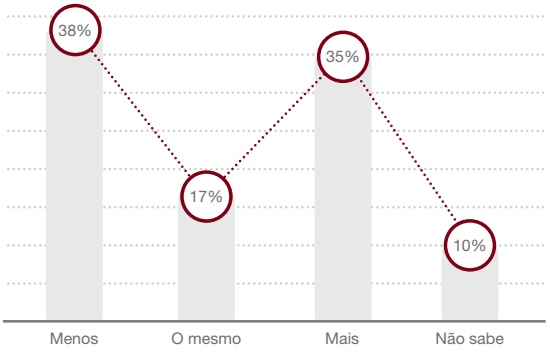
Um administrador é cada vez mais visto como a personificação de uma organização. Assim, quando se verificam falhas ao nível ético ou ao nível do *compliance*, esses indivíduos são muitas vezes responsabilizados individualmente - tanto pelos media e opinião pública, como pelos reguladores e tribunais. Se é merecido ou não, uma coisa é certa: os principais diretores executivos ("C-suite") não podem mais alegar a falta de conhecimento como desculpa.

O nosso *Survey* mostra que, a nível global, nove em cada dez casos de incidentes graves de fraude foram reportados à administração. Além disso, 25% dos inquiridos portugueses indicaram que o CEO é o principal responsável pelo programa de ética e *compliance* da sua organização, o que coloca o foco em como a gestão de topo se encontra a gerir o tema da fraude e crimes económicos, ajustando (ou não) o seu perfil de risco.

25%

dos inquiridos afirmam que a responsabilidade pela ética e *compliance* na organização é do CEO

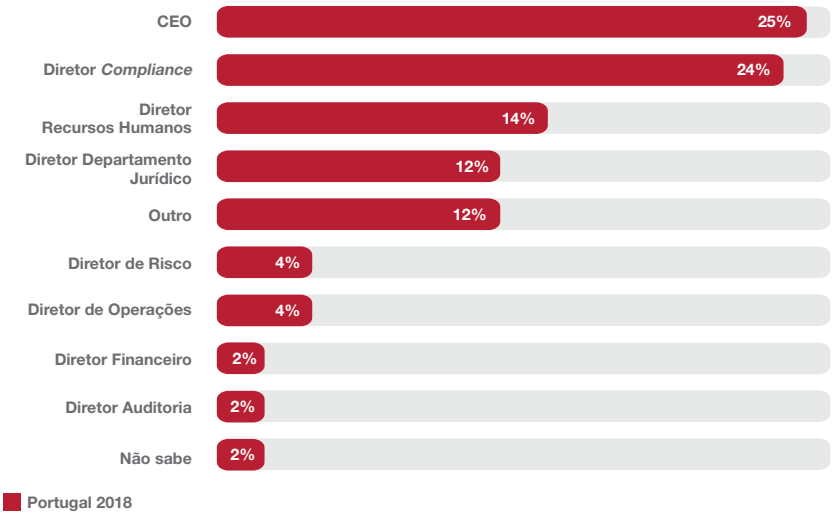
Figura 5: O valor gasto em investigações e outras intervenções como resultado de fraude é significativo



Q. Como resultado do crime mais disruptivo sofrido nos últimos 24 meses, qual o montante dispendido pela sua organização em investigações e/ou outras intervenções: mais, menos ou igual ao que foi sofrido através deste crime?

Fonte: PwC's 2018 Global Economic Crime and Fraud Survey

Figura 6: A responsabilidade pela implementação de programas de ética e de *compliance* incide principalmente no "C-suite"



Q. Quem é o principal responsável pelo programa de ética e *compliance* na sua organização?

Fonte: PwC's 2018 Global Economic Crime and Fraud Surve

As más notícias sabem-se rápido: o risco reputacional supera o risco regulatório

Uma mudança acentuada na maneira como o mundo olha para a fraude e para a corrupção tem ocorrido nos últimos anos. Os dados do nosso *Survey* refletem essa mesma realidade, tanto por parte dos media e opinião pública como por parte dos reguladores, no setor público e privado.

Este não é um fenómeno limitado a mercados desenvolvidos mas sim transversal a diferentes culturas, em todas as regiões do mundo, sendo evidente a existência de sinais de convergência em torno de padrões de transparência e códigos de conduta. Em Portugal, tem-se assistido, nos últimos anos, a uma grande atenção mediática sobre a ética e o combate à corrupção. As expectativas sobre o poder judicial são neste momento elevadíssimas, e a credibilidade das autoridades de investigação e dos reguladores sairá reforçada ou abalada, em função do desfecho dos casos mais mediáticos. Também as expetativas sobre a ética nos negócios são mais elevadas do que nunca.

Nos dias de hoje, as empresas não decidem quando um problema se torna uma crise, pelo contrário é a opinião pública (veiculada pelos media tradicionais ou crescentemente através das redes sociais) que numa era de transparência radical exerce o papel de júri.

Além disso, as regras da sociedade podem mudar mais rapidamente do que a regulamentação - e há pouca tolerância pública para aqueles que as quebram. Os reguladores, por definição, operam dentro de uma jurisdição limitada e de acordo com regras bem definidas.

A reputação de uma empresa, por outro lado, não está sujeita a uma jurisdição fixa, lei ou processo obrigatório.

Os inquiridos classificam consistentemente os danos reputacionais no topo dos impactos negativos oriundos de crimes económicos, com a perceção pública (reputação, relações comerciais e cotação das ações) a ter o maior impacto.

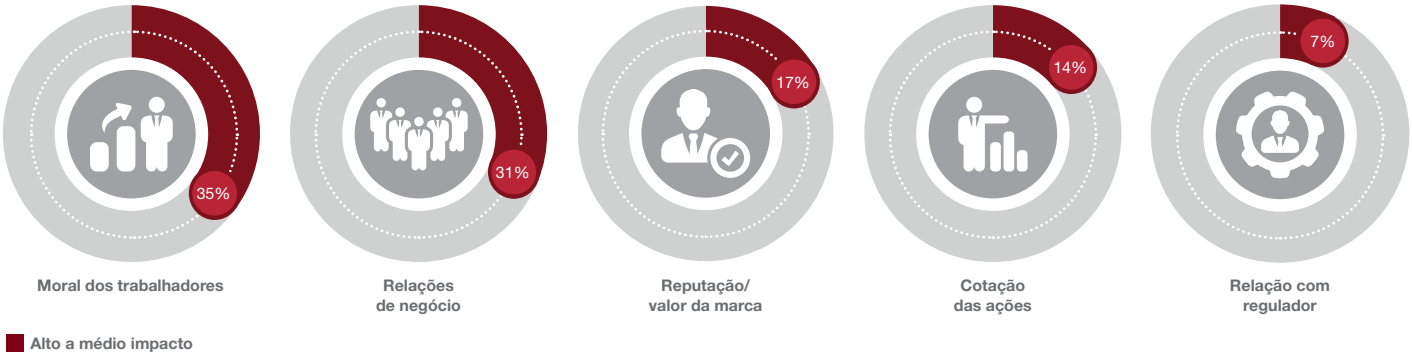
O *compliance* continua a ser um fator crítico com uma importância nunca vista. Independentemente de nos aproximarmos de níveis de regulação excessiva, verifica-se de uma forma transversal que as exigências regulatórias e de reporte, incluindo em matéria de comportamento ético e legal, continuam a aumentar.

O escrutínio e a fiscalização também estão em ascensão global e a cooperação regulatória internacional está a tornar-se cada vez mais habitual.

53%

dos inquiridos em Portugal acreditam que as mudanças no ambiente regulatório terão um maior impacto na sua organização nos próximos 2 anos

Figura 7: Os danos que causaram maior impacto nas organizações em Portugal



Q. Qual foi o nível de impacto do crime económico mais diruptivo sofrido sobre os seguintes aspetos das suas operações comerciais?

Fonte: PwC's 2018 Global Economic Crime and Fraud Survey

Explorar o poder da tecnologia

Implementar hoje a tecnologia certa

Quando se trata de fraude, a tecnologia pode ser uma faca de dois gumes. Por um lado, vivemos num momento de inovação estimulante: inteligência artificial (IA), *big data* e *blockchain* são apenas alguns dos principais avanços tecnológicos que testemunhamos.

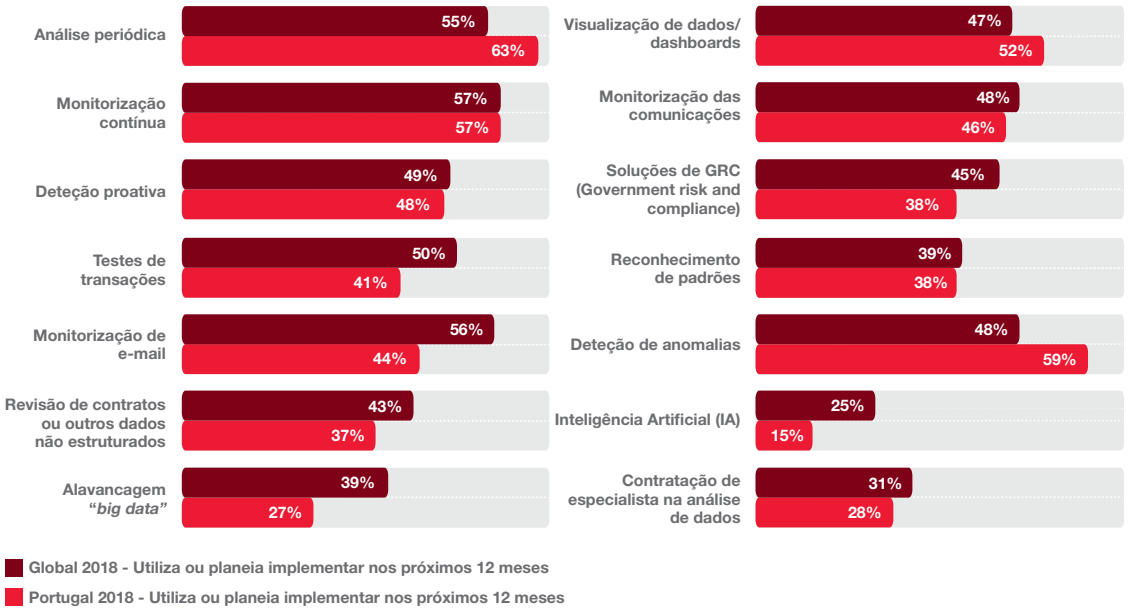
Muitas dessas tecnologias podem ser aproveitadas para combater a fraude e atuar como linhas adicionais de defesa para as organizações.

Por outro lado, a tecnologia tornou-se omnipresente e oferece mais oportunidades para os que cometem fraude atingirem organizações em diferentes níveis e agirem sob o anonimato.

Apenas 15%

dos inquiridos em Portugal afirmam que têm implementado ou tencionam implementar inteligência artificial (IA) nos próximos 12 meses para ajudar a combater fraudes e crimes económicos

Figura 8: As organizações começam a obter o valor das tecnologias alternativas e disruptivas no combate à fraude, no entanto, há muito por fazer no domínio da alavancagem sobre grandes volumes de dados (big data) e da inteligência artificial

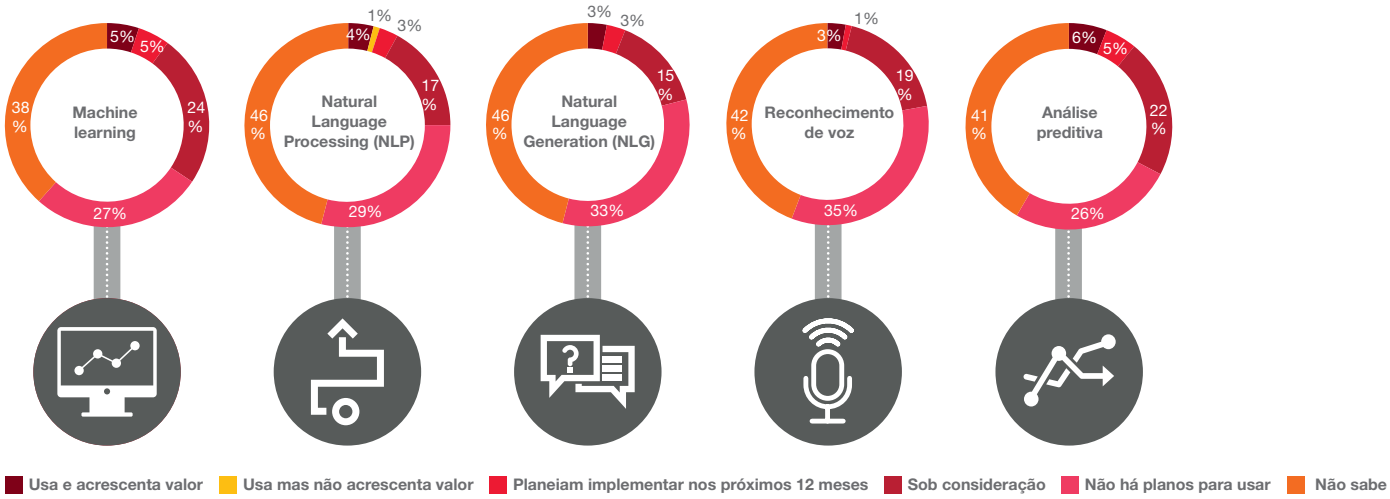


Q. Em que medida é que a sua organização utiliza, ou tem em conta, as seguintes tecnologias alternativas e técnicas disruptivas no seu ambiente para combater a fraude e/ou o crime económico?

Fonte: PwC's 2018 Global Economic Crime and Fraud Survey

As organizações precisam ser cautelosas ao implementar novas tecnologias, protegendo essas plataformas ou produtos contra os riscos e educando toda a organização a ser vigilante e a estar preparada contra as ameaças existentes. Quando se trata de usar a tecnologia para combater a fraude e o crime económico, torna-se claro que as organizações portuguesas não estão a usar toda a sua extensão - ou, pior, nem sequer a usam. Os resultados de Portugal do nosso *Survey* indicam que apenas 15% dos inquiridos têm implementado ou estão a planear implementar a Inteligência Artificial nos próximos 12 meses como meio de combate à fraude e crimes económicos.

Figura 9: A maioria dos entrevistados portugueses não tenciona usar IA ou tecnologia para tratamento de dados



Q. Até que ponto é que a sua empresa está a retirar utilidade da inteligência artificial ou das técnicas avançadas de análise para combater/monitorizar a fraude e outros crimes económicos?

Fonte: PwC's 2018 Global Economic Crime and Fraud Survey

Cibercrime: uma desconexão entre fins e meios

O cibercrime ultrapassou a infância e a adolescência. Os cibercriminosos de hoje são tão experientes e profissionais quanto os negócios que atacam. Essa maturidade exige uma nova perspetiva sobre a natureza multifacetada das ameaças cibernéticas e das fraudes que as acompanham.

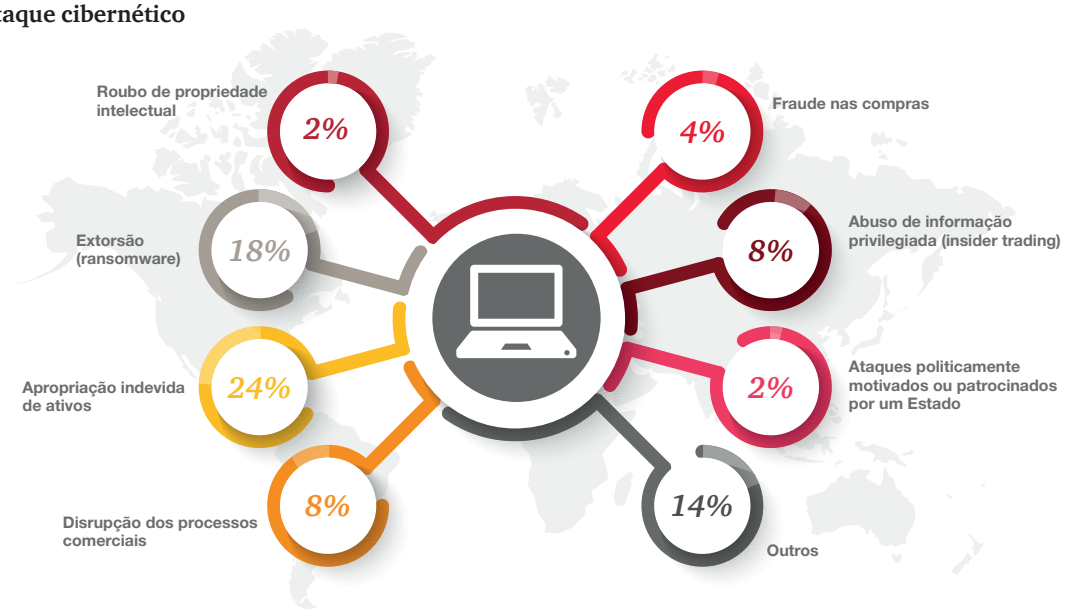
Normalmente, o primeiro sinal para uma organização perceber que algo sistémico está a acontecer é quando deteta um possível ciber-ataque, como por exemplo o *phishing* ou o *malware*. A crescente frequência, sofisticação e magnitude desses ataques está a levar as organizações a implementar medidas preventivas.

Esta abordagem permite um maior enfoque na prevenção de fraudes. O cibercrime foi considerado como o crime económico mais sério e disruptivo a acontecer nos próximos dois anos, com um impacto económico expectável significativo (25% dos inquiridos em Portugal disseram prever um ataque cibernético e que este seria o mais prejudicial, 15% disseram que esperavam que o branqueamento de capitais fosse o mais prejudicial para a organização). Na verdade, os ataques cibernéticos tornaram-se tão difundidos que medir a sua ocorrência e impacto está a tornar-se estrategicamente menos útil do que manter o foco no mecanismo que os defraudadores usaram caso a caso.

25%

dos executivos inquiridos prevêm a ocorrência de um ataque cibernético e que seria este o mais prejudicial para a organização

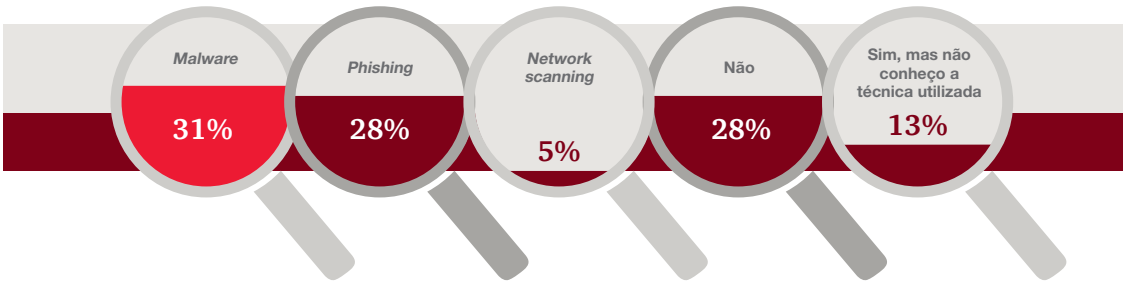
Figura 10: Os tipos de fraude de que as organizações foram vítimas, em Portugal, por meio de um ataque cibernético



Q. De qual dos seguintes tipos de fraude e/ou crime económico é que a sua organização foi vítima através de um ciber-ataque?

Fonte: PwC's 2018 Global Economic Crime and Fraud Survey

Figura 11: Técnicas de ciber-crime usadas contra as organizações de Portugal

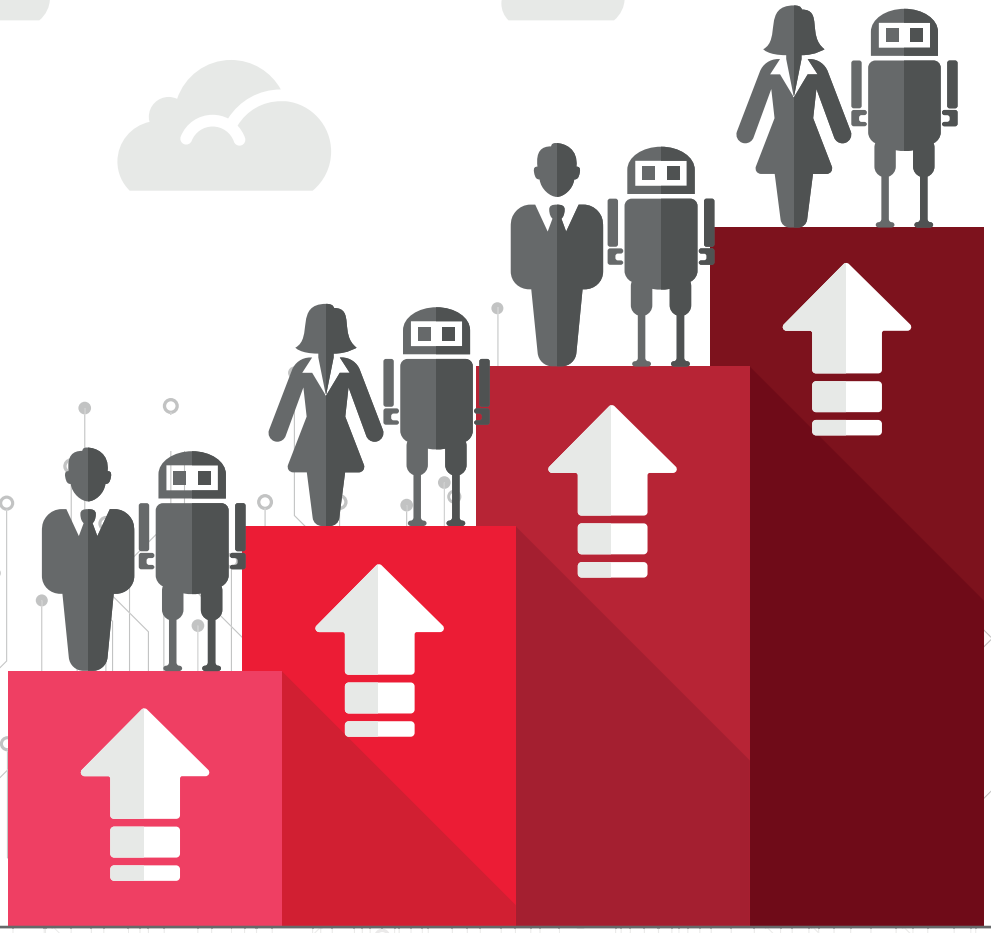


3% respondeu "outros"

Q. Nos últimos 24 meses a sua organização foi alvo de ciber-ataque através de uma das seguintes técnicas?

Fonte: PwC's 2018 Global Economic Crime and Fraud Survey

Investir em pessoas, não apenas em máquinas



Um pequeno investimento em pessoas pode render enormes dividendos

Confrontada com a crescente complexidade da fraude, muitas organizações decidem investir cada vez mais em tecnologia. No entanto, esses investimentos invariavelmente atingem um ponto de retorno decrescente, particularmente no combate à fraude interna. Assim, embora a tecnologia seja claramente uma ferramenta vital na luta contra a fraude, ela só consegue ser parte da solução.

Isto ocorre porque a fraude é o resultado de uma mistura complexa de condições e motivações humanas. O fator mais crítico na decisão de cometer fraude é, em última instância, o comportamento humano - e isso oferece a melhor oportunidade para combatê-lo.

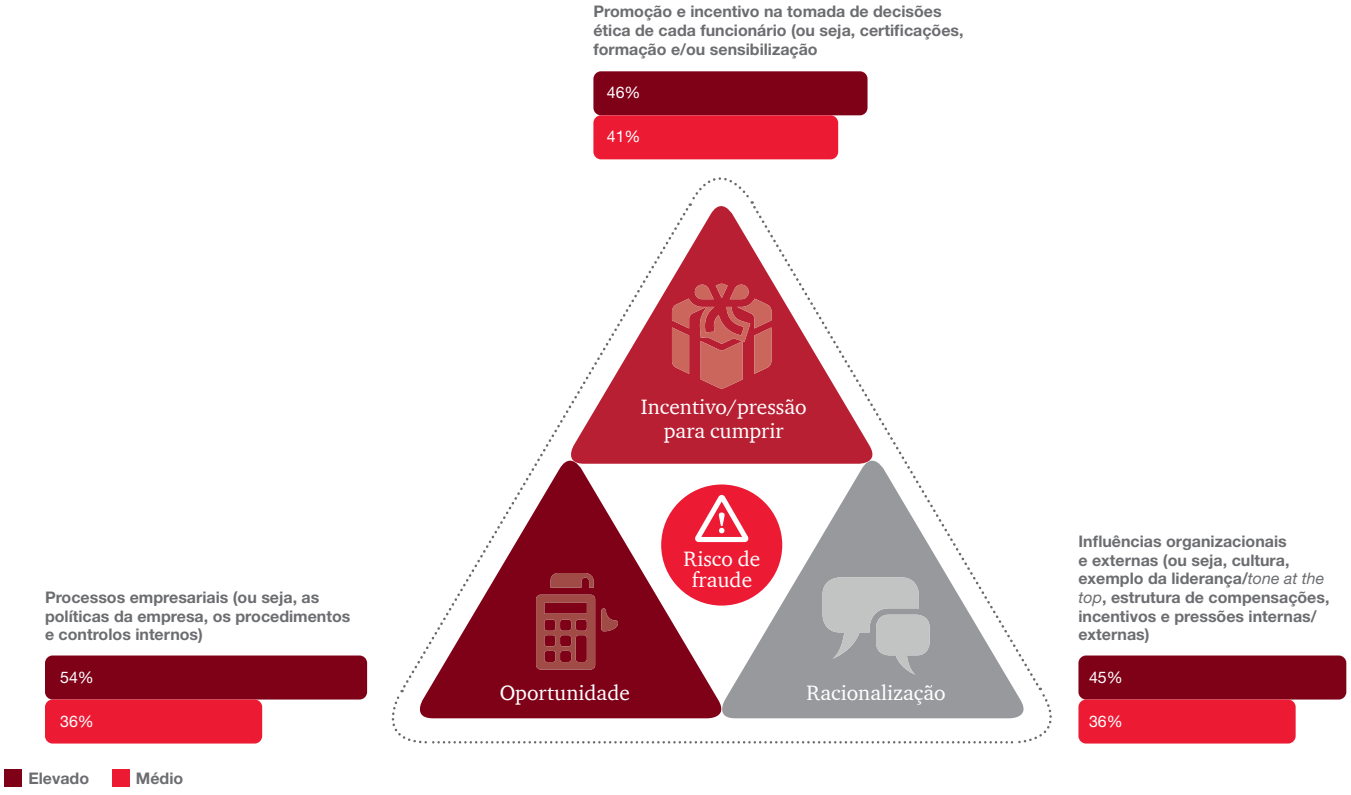
Existe um método poderoso para entender e prevenir os três principais fatores da fraude interna - o triângulo da fraude. Um dos vértices do triângulo da fraude é o incentivo (geralmente uma pressão para atuar dentro da organização). Os restantes vértices são a oportunidade e o processo de racionalização interna. Como todos esses três fatores devem estar presentes para que um ato de fraude ocorra, cada um deles deve ser tratado individualmente.

Uma oportunidade para os controlos

A maioria dos esforços de combate à fraude nos últimos anos têm sido concentrados em reduzir as oportunidades de que sejam praticados atos fraudulentos: 50% dos inquiridos, a nível global, afirmam que colocaram um maior enfoque no desenho de processos de negócio, nomeadamente na vertente de controlo interno, com o propósito de reduzir as oportunidades de cometer fraude.

Enquanto 59% dos inquiridos a nível global classificam a oportunidade como o principal responsável pelas fraudes mais prejudiciais cometidas por agentes internos, esta percentagem encontra-se 10 pontos percentuais abaixo dos resultados de 2016 (69%). Esta é uma evidência de que a tecnologia tem um papel fundamental a desempenhar - e, mais especificamente, que as empresas geralmente a empregam de uma forma cada vez mais eficaz.

Figura 12: Triângulo da fraude: O que leva um colaborador a cometer fraude em Portugal?



Q. Que nível de esforço é aplicado na sua organização nas seguintes categorias para a luta contra a fraude e/ou o crime económico?

Fonte: PwC's 2018 Global Economic Crime and Fraud Survey

Procurar a fraude nos lugares certos

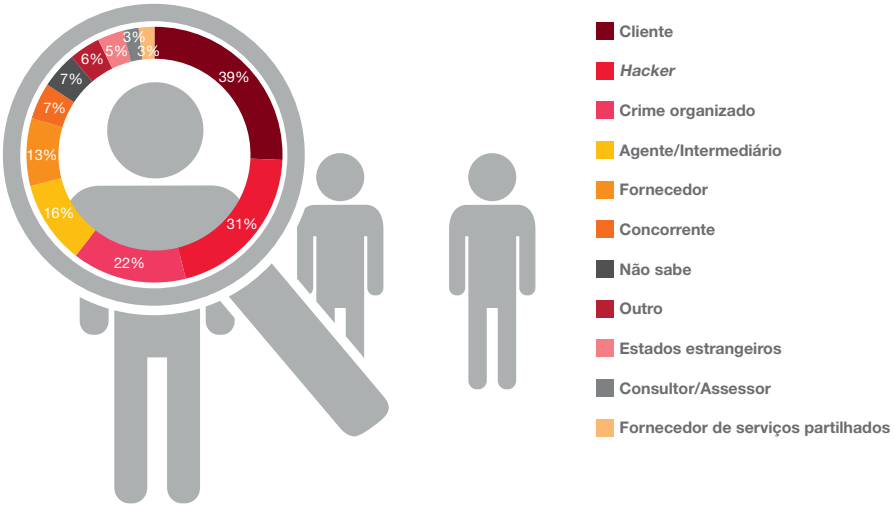
O *Survey* em Portugal revelou um decréscimo significativo na parcela de crimes económicos cometidos por agentes internos (de 50% em 2016 para 38% em 2018). De acordo com os nossos inquiridos, em Portugal, a fraude externa supera a fraude interna ao contrário do que se verifica globalmente. Em Portugal são os agentes externos os principais responsáveis por cometer fraude.

No entanto, um dos maiores pontos críticos e uma das maiores ameaças de fraude, geralmente não está relacionada com os colaboradores, mas sim com as pessoas com quem estes mantêm relações de negócio. Esses são os terceiros com os quais as empresas mantêm relacionamentos comerciais regulares: agentes, fornecedores, prestadores de serviços e clientes. Por outras palavras, as pessoas e organizações de quem se espera um elevado grau de confiança, mas que podem estar efetivamente a intentar fraude contra a organização.

13%

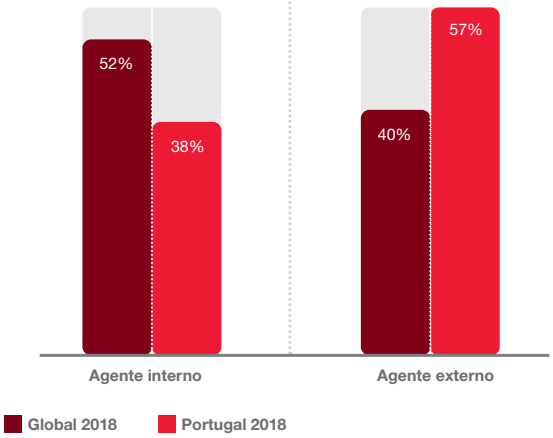
das fraudes internas reportadas foram cometidas por altos dirigentes

Figura 13: Mais de um terço dos crimes económicos, a nível global, são praticados por clientes



Q. Quem foram os autores da fraude externa contra a sua organização?
Fonte: PwC's 2018 Global Economic Crime and Fraud Survey

Figura 14: Em Portugal, os agentes externos são os principais responsáveis por cometer fraude

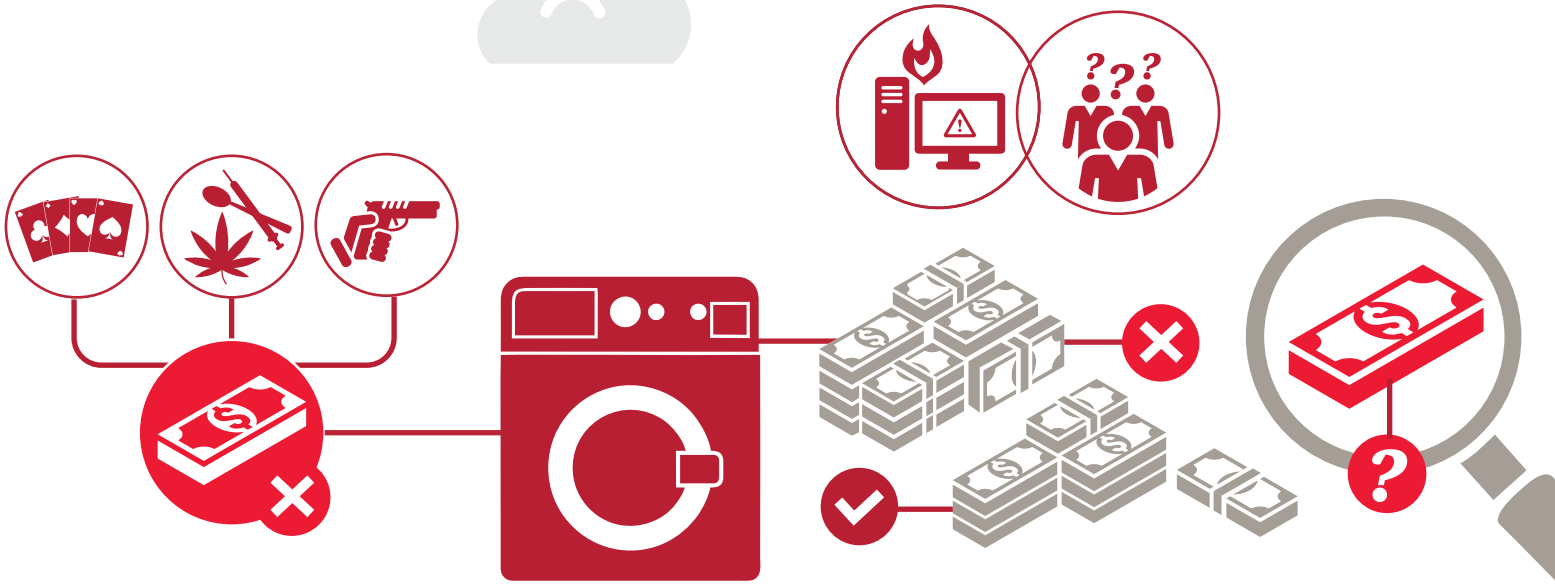


Mais de 1/3

dos agentes externos que cometeram fraude na organização, a nível global, são clientes

Q. Quem foi o principal autor desta fraude?
Fonte: PwC's 2018 Global Economic Crime and Fraud Survey

Branqueamento de capitais: suprir falhas e consolidar processos



Avaliação de Risco é hoje uma ferramenta indispensável

À medida que se alcança um nível superior de maturidade, um número cada vez maior de organizações solicita apoio para a Avaliações de Risco em Prevenção de Branqueamento de Capitais e Combate ao Financiamento do Terrorismo (PBC/CFT). As organizações expõem-se a um risco considerável ao adotarem uma abordagem de "tick in the box" e o nosso Survey mostra que 10% das organizações (sujeitas a regras de PBC/CFT) inquiridas em Portugal não consideraram necessário realizar uma avaliação de risco de PBC/CFT. Este resultado sugere que algumas das organizações que participaram no nosso Survey tratam as suas avaliações de risco como documentos estáticos, contrariando os requisitos da Lei de Prevenção de Branqueamento de Capitais e Combate ao Financiamento do Terrorismo (Lei nº 83/2017).

Cerca de 30% das organizações inquiridas em Portugal indicaram que tinham sido objeto de fiscalização/inspeção regulatória no âmbito da PBC/CFT nos últimos dois anos, o que significa que as entidades de supervisão estão atentas e inconformidades serão identificadas, o que representa um risco regulatório real. Este facto é particularmente relevante, na medida em que os planos de remediação quando ocorrem sob pressão do regulador são mais dispendiosos e morosos para a gestão do que uma implementação proativa.

Verifica-se, por outro lado, que a maturidade das entidades sujeitas e também das entidades de supervisão quanto aos temas de PBC/CFT é ainda heterogénea. O setor bancário parece estar com um nível de maturidade moderada a elevada, mas muito há ainda por fazer noutros setores de atividade.

Para as organizações que estão a iniciar uma avaliação de PBC/CFT, importa que entendam que essa é uma tarefa demorada, dispendiosa e stressante, especialmente se for deixada para o último minuto.

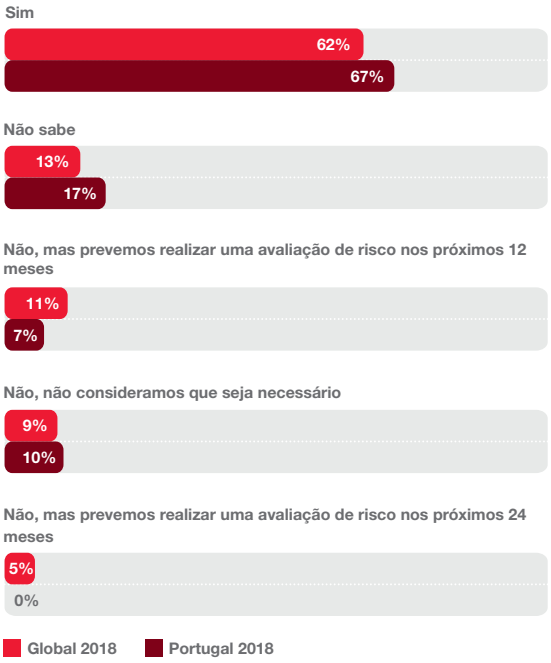
A Lei da Prevenção do Branqueamento de Capitais e Combate ao Financiamento do Terrorismo, é umas das poucas leis em que o regulador transfere e/ou partilha uma parte significativa da obrigação de controlo para as entidades obrigadas, o que também demonstra bem a pressão e a vontade para combater este tipo de crime.

Todos estes fatores têm contribuído para uma também crescente preocupação por parte das entidades nas relações de negócio que estabelecem com terceiros, uma vez que os danos reputacionais que podem decorrer deste tipo de crime são significativos, podendo muitas vezes colocar em causa a própria continuidade operativa das mesmas.

Há, por esta razão, um número cada vez maior de entidades com negócios internacionais que, antes e durante as suas relações de negócio, procura garantir que as suas contrapartes acompanham a evolução regulatória e sobretudo cumprem com as bases comuns da mesma.

Os métodos de branqueamento de capitais continuam a evoluir e, com o aumento de produtos e serviços que facilitam o pagamento anónimo, como por exemplo as moedas digitais, as entidades devem cada vez mais avaliar os riscos e a forma como responderão e garantirão o devido nível de diligência dos procedimentos de avaliação dos seus clientes e das transações.

Figura 15: A avaliação de risco em PBC/CFT



Q: A sua organização efetuou uma avaliação de risco PBC/CFT transversal a toda a organização e suas áreas geográficas nos últimos 24 meses?

Fonte: PwC's 2018 Global Economic Crime and Fraud Survey

17%

dos inquiridos em Portugal sujeitos a regras de PBC/CFT indicaram que não efetuaram uma avaliação de risco PBC/CFT nos últimos dois anos

Aplicação regulatória

No nosso *Survey*, 30% dos inquiridos, em Portugal, sujeitos a regras de PBC/CFT indicaram que tinham sido abordados pelo regulador ou sujeitos a uma inspeção regulatória de PBC/CFT nos últimos dois anos (significativamente menos do que os 55% a nível global). Mais de metade (53%) acredita que as recentes mudanças no ambiente regulatório e geopolítico terão um impacto acrescido nas suas organizações nos próximos dois anos.

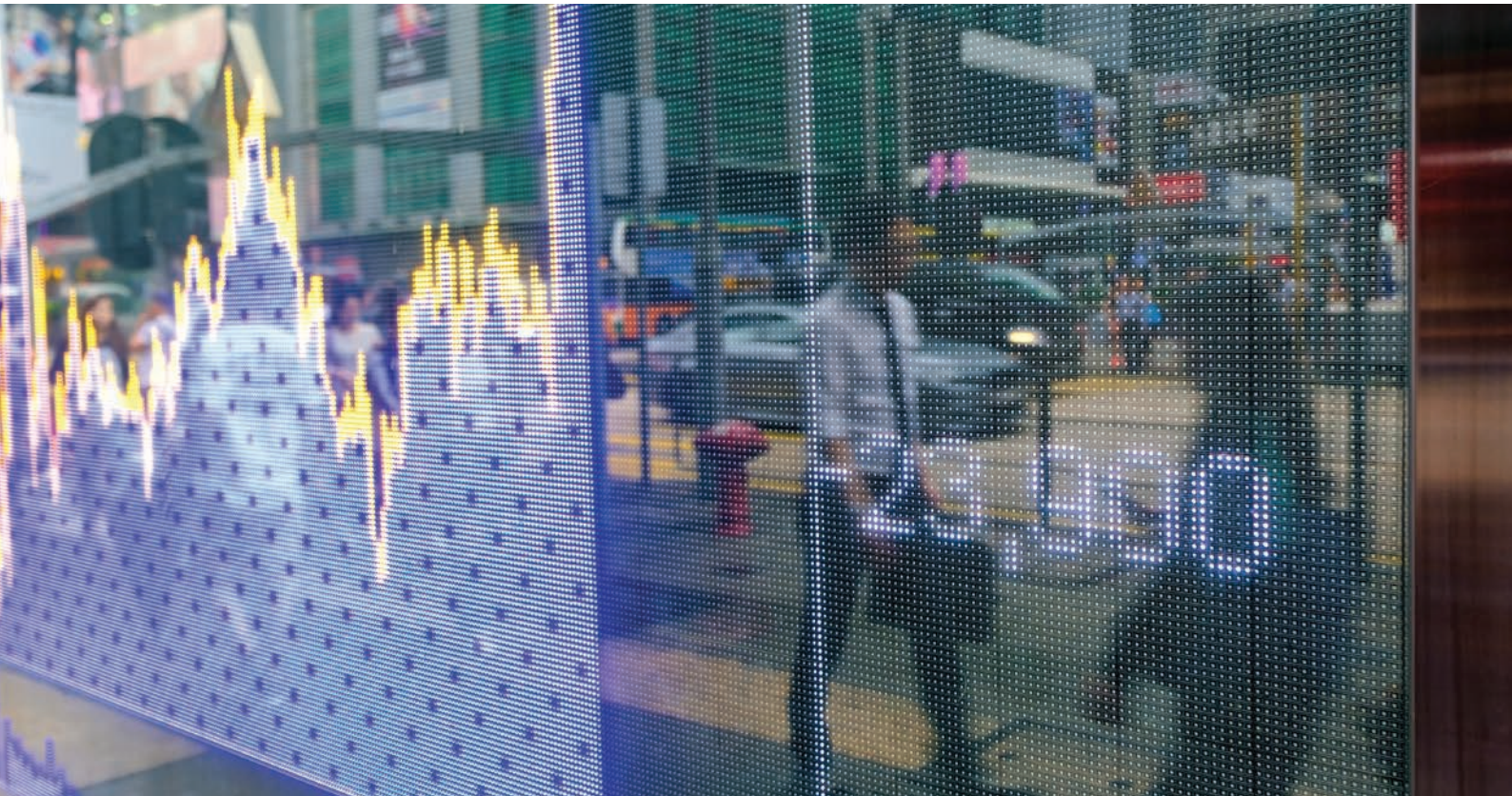
O *compliance* deixa de ser um exercício de *tick in the box* para ser uma tarefa que tem de ser levada a sério. Neste contexto, as entidades deverão munir-se de bons sistemas, robustecer processos e procedimentos, implementar politicas formativas efetivas para que se garanta o cumprimento da legislação da PBC/CFT.

As organizações devem adotar programas de *compliance* alinhados com os seus objetivos estratégicos, sendo fundamental olhar para o *compliance* não como um custo, mas como um investimento, que não só lhes trará estabilidade interna, como lhes poderá garantir a continuidade das relações de negócio com as organizações internacionais.

Figura 16: O número de inspeções regulatórias está a aumentar

Q: A sua Organização foi alvo de sanções regulamentares/ inspeção em matéria de PBC/CFT nos últimos 24 meses?

Fonte: PwC's 2018 Global Economic Crime and Fraud Survey



Conclusão

Esteja preparado e seja firme

O nosso *Survey* demonstra que, embora muito esteja a ser feito no que diz respeito à fraude e crime económico, continua a haver muito por fazer. O nível de preparação de muitas organizações é ainda insuficiente.

Desenvolver uma visão partilhada sobre aqueles que são os principais riscos de fraude e incorporar nos processos e sistemas de negócio uma cultura de combate à fraude são dois dos elementos essenciais de uma estratégia de combate à fraude bem sucedida. A cultura da organização e a forma como se tratam as pessoas é muito mais importante do que se pode pensar na prevenção da fraude.

O grau de preparação de uma organização para lidar com um incidente de fraude é determinante para a eficácia de atuação, no que diz respeito à rapidez com que se deteta, mas também na forma como se atua para remediar a fraude e ainda a forma como se gere o impacto mediático e reputacional.

A ameaça do crime económico continua a intensificar as regras e as expectativas de todos os *stakeholders* - incluindo reguladores, acionistas, o público, especialmente através das redes sociais, e os colaboradores - aumentaram e continuarão a aumentar.

A transparência e a aderência ao cumprimento da lei são mais críticas do que nunca e a forma como se reage quando uma questão de fraude ou *compliance* surge é tão importante quanto o próprio evento.

Tomar ações deliberadas para planear, prevenir, detetar e remediar é fundamental. Seja para cumprir requisitos legais, com um serviço de denúncias ou cumprir as obrigações de PBC/CFT, desenvolver uma estrutura abrangente de controlo de fraude em toda a organização ou estratégia de cibercrime, a adoção de uma estratégia de combate à fraude irá permitir proteger a empresa de riscos finaceiros e reputacionais.

Gerir ativamente os riscos de crime económico darão uma vantagem competitiva num mercado cada vez mais exigente, procurando organizações com fortes estruturas éticas e de transparência.

O que se segue?

Se quiser saber mais sobre qualquer um dos temas discutidos acima, seja risco de fraude ou suborno, cibercrime, tecnologia forense, PBC/CFT ou *due diligence* de parceiros de negócio, entre em contacto com um dos nossos especialistas.

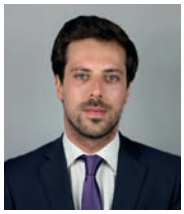
Contactos

Quer saber mais sobre o que pode fazer na luta contra a fraude?
Entre em contacto com um dos nossos especialistas.

Patrique Fernandes
Partner
patrique.fernandes@pwc.com
+351 21 359 93 14

Carolina Simões Costa
Director
carolina.simoes.costa@pwc.com
+351 21 359 93 14

Miguel Sepúlveda
Senior Manager
miguel.padeira.sepulveda@pwc.com
+351 21 359 93 14



Gonçalo Magalhães Almeida
Manager
goncalo.magalhaes.almeida@pwc.com
+351 21 359 93 14

Sobre o Survey

O Global Economic Crime and Fraud Survey reuniu dados valiosos de mais de 7.200 participantes em 123 países, incluindo Portugal com 86 participantes. Do número total de participantes 52% representam senior executives das respectivas organizações, 42% representam empresas cotadas e 55% representam organizações com mais de 1.000 funcionários.

pwc

Visite-nos nas redes sociais