Fraude: O concorrente que a sua organização desconhece

Global Economic Crime and Fraud Survey 2018 - Perspectiva sobre Angola

27%
das organizações em Angola afirmam ter sido vítimas de fraude ou crime económico

55%
das organizações em Angola não realizaram uma avaliação geral do risco de fraude

62%
das empresas que foram vítimas de fraude em Angola sofreram uma apropriação indevida de activos

64%
dos inquiridos em Angola afirmam que os agentes internos são os principais responsáveis por cometer fraude.

pwc

www.pwc.com/ao/gecs

Sumário Executivo

Patrique Fernandes
Partner da PwC Angola
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 Angola, apenas 27% 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 Angola com 95 participantes, com o propósito de realçar alguns dos desafios estratégicos que as organizações enfrentam actualmente 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 efectuado relativamente a esta matéria. Que acções podem ser tomadas para que o combate à fraude e ao crime económico seja efectuado de forma eficaz?

Combater a fraude

Reconhecer a fraude quando a vemos

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

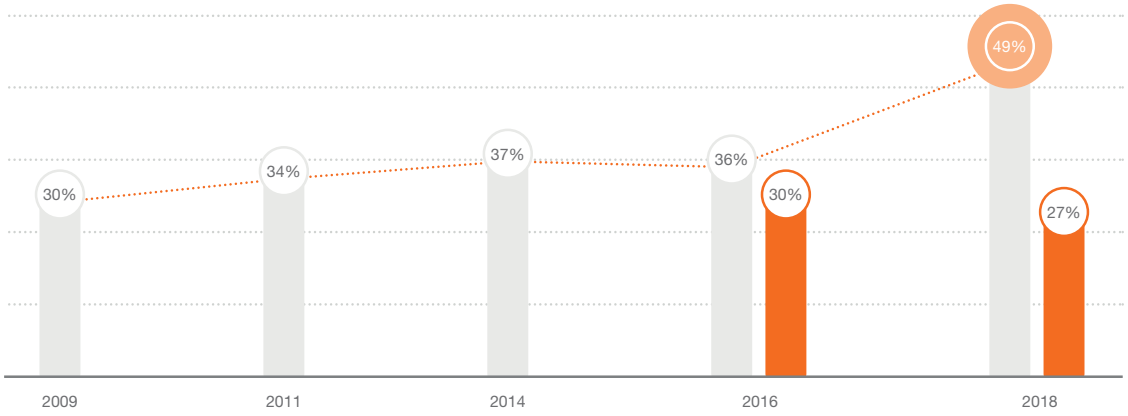
Este ano, 49% dos inquiridos do *Global Economic Crime and Fraud Survey* disseram que as suas organizações tinham sido vítimas de fraude ou crime económico, o que contrasta com os 36% obtidos em 2016. Em Angola, 27% das organizações afirmam que foram vítimas de fraude, o que representa aproximadamente o mesmo índice face ao *Survey* anterior (30% em 2016). Parece-nos pouco provável que a incidência de fraude e crime económico em Angola seja tão mais baixa que a nível global.

Este diminuição pode ser explicada por uma combinação de factores:

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

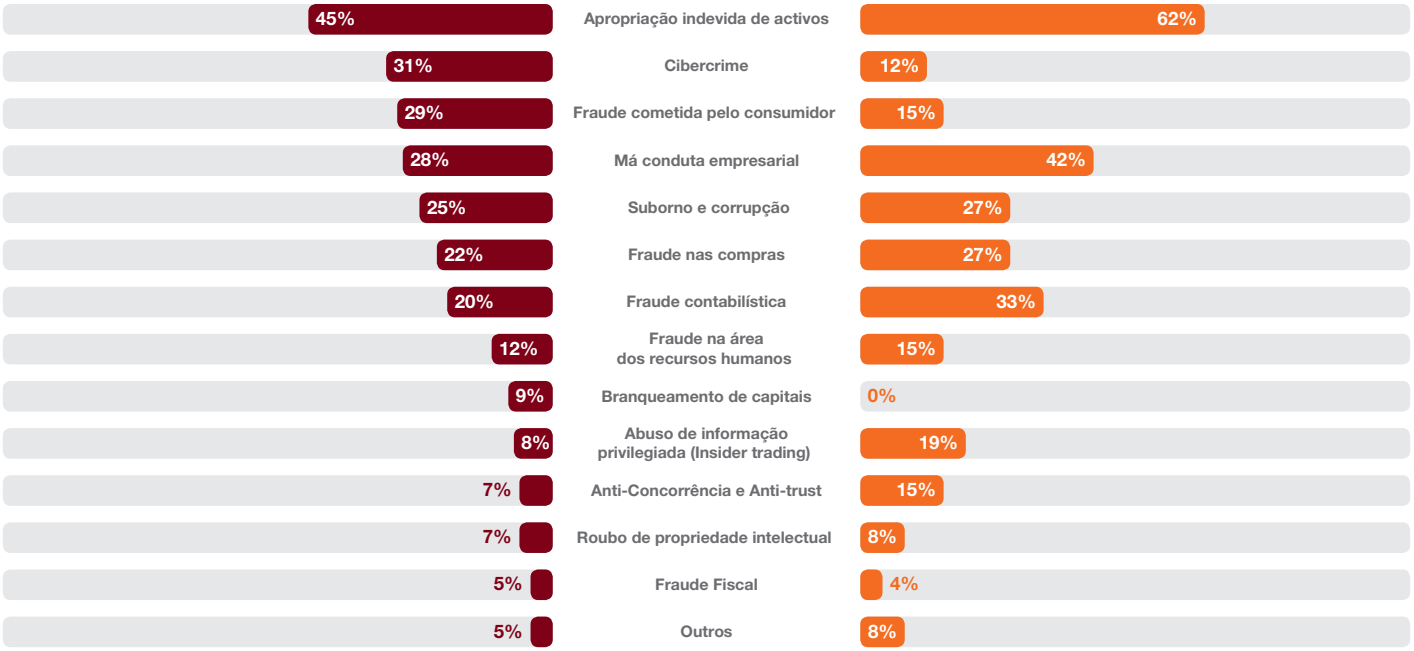
Mas toda a organização, por mais atenta que seja, é vulnerável a "ângulos mortos". E como esses "ângulos mortos" geralmente só se tornam visíveis depois da fraude ocorrer, é necessário aumentar os esforços de combate à fraude através de procedimentos de identificação desses mesmos "ângulos mortos".

Figura 1: Em Angola, o índice de fraude e crimes económicos permanece aproximadamente no mesmo patamar que há dois anos atrás



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

Apropriação indevida de activos é 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 a nível global, o mesmo sucedeu com o montante que as empresas estão a gastar para combater a fraude:

- 43% dos inquiridos em Angola, 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).

- 49% dos inquiridos em Angola, 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 proactivas relativamente à fraude e à corrupção? Ou são apenas uma reacção, 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.

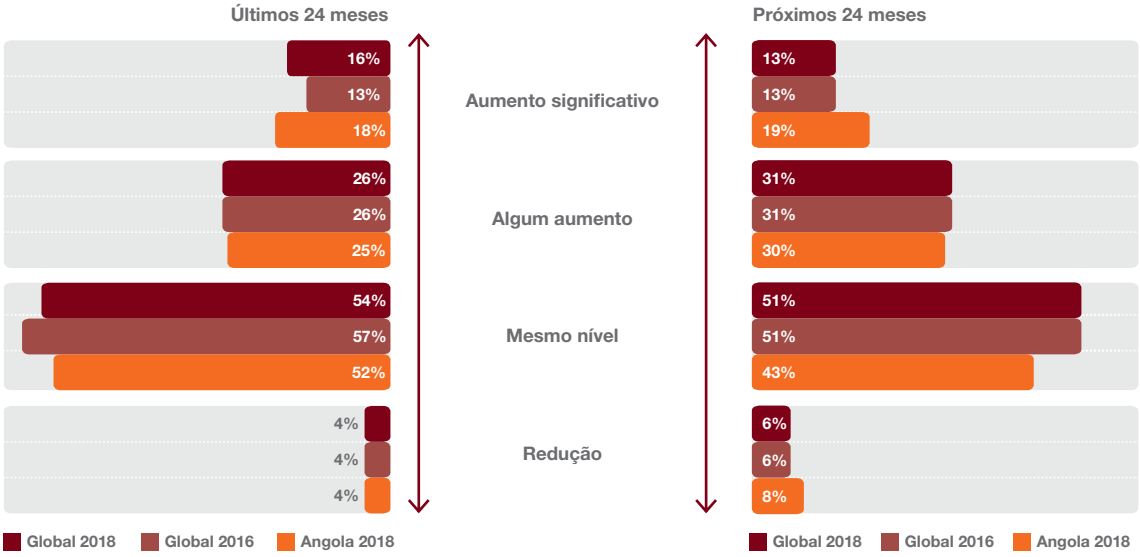
43%

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

49%

das organizações inquiridas em Angola 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, 55% dos inquiridos em Angola não tenham realizado uma avaliação geral do risco de fraude, analisando os principais riscos que enfrentam os seus negócios ou actividades.

Na nossa perspectiva, uma avaliação do risco de fraude, ponderada, objectiva e focalizada, constitui o pilar para o desenho das restantes actividades antifraude. A ausência de uma avaliação de risco de fraude, significa que os processos de negócios e antifraude implementados pela organização podem ser mal direccionados 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 (35%), combate ao suborno e corrupção (31%), prevenção do branqueamento de capitais (24%), obrigações regulamentares específicas da indústria (22%) e plano de resposta cibernético (21%).

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

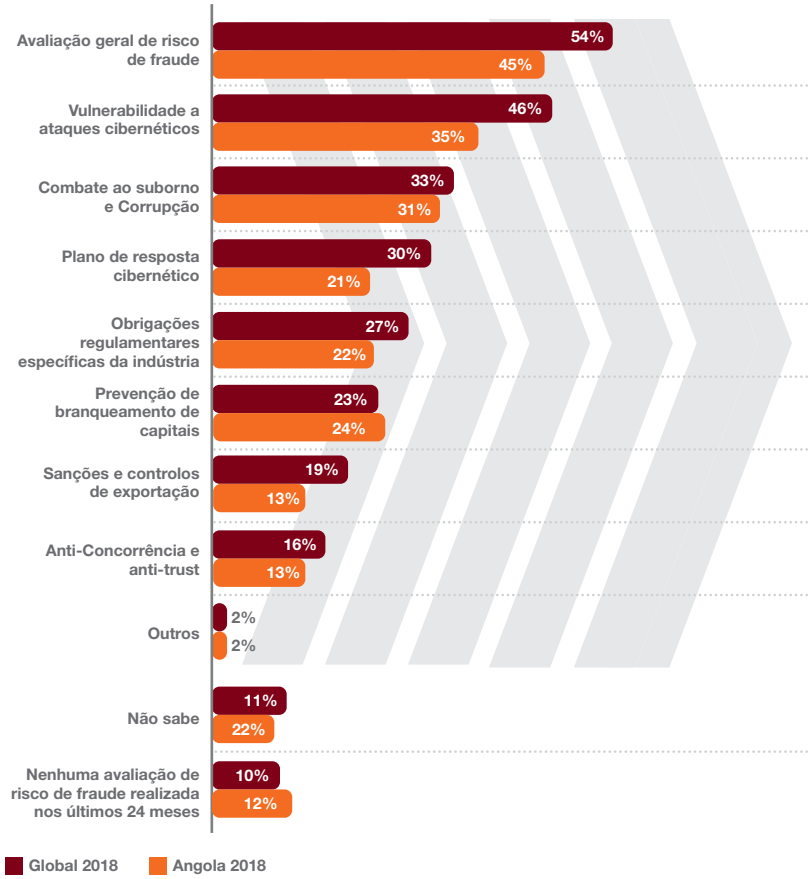
Da nossa experiência, são poucas as organizações que implementaram processos para identificar grandes alterações ao perfil de risco do negócio ou partes do negócio. As avaliações de risco de fraude, quando existentes, são frequentemente documentos estáticos, reflectindo um momento no tempo, em vez de 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 actividades, operações, pessoas e estruturas do negócio, o que torna fundamental que as avaliações de risco sejam actualizadas regularmente para garantir que as ameaças sejam devidamente tratadas. A ausência de actualizações regulares é uma preocupação significativa.

55%

das organizações em Angola não realizaram uma avaliação geral do risco de fraude.

Figura 4: Menos de metade das organizações realizaram avaliações de risco "direccionadas" 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*

Adoptar uma abordagem proactiva no combate à fraude

A responsabilidade da administração

O nosso *Survey* refere que o custo directo da fraude e as suas consequências podem ser significativos. Mas quando os custos indirectos (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 indirectos.

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

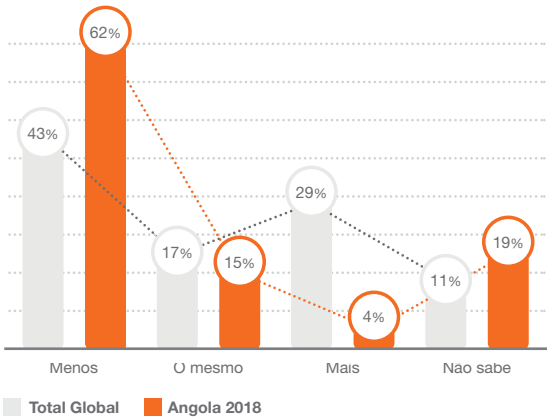
Um administrador é cada vez mais visto como a personificação de uma organização. Assim, quando se verificam falhas ao nível ético ou ao nível do *compliance*, esses indivíduos são muitas vezes responsabilizados individualmente - tanto pelos media e opinião pública, como pelos reguladores e tribunais. Se é merecido ou não, uma coisa é certa: os principais directores 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, 20% dos inquiridos angolanos 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.

20%

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

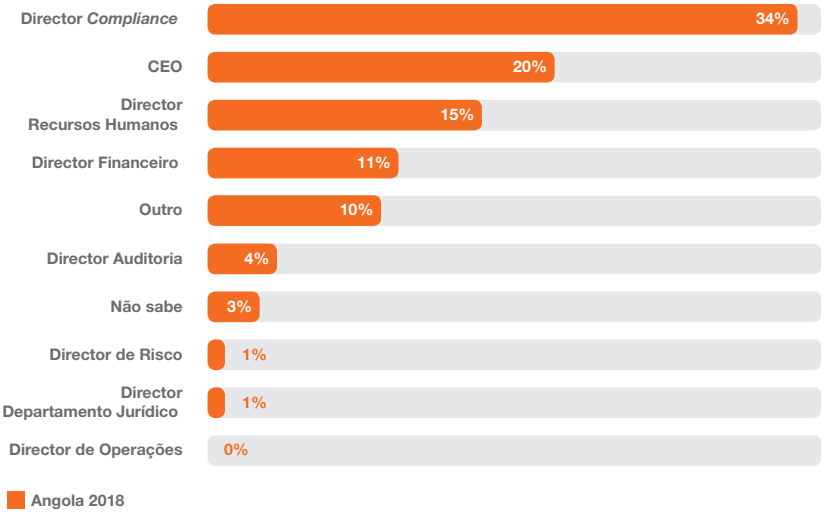
Figura 5: O valor gasto em investigações e outras intervenções como resultado de fraude, a nível global, é significativo



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 mundoolha para a fraude e para a corrupção tem ocorrido nos últimos anos. Os dados do nosso *Survey* reflectem essa mesma realidade, tanto por parte dos media e opinião pública como por parte dos reguladores, no sector 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 Angola, 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 expectativas 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 a moral dos trabalhadores no topo dos impactos negativos oriundos de crimes económicos, e ainda com a percepção pública (reputação, relações comerciais) a ter o maior impacto.

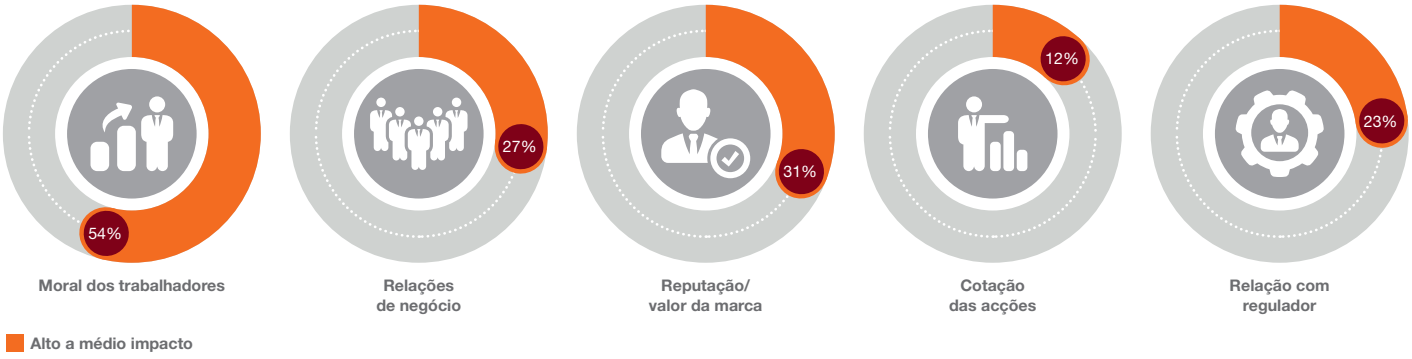
O *compliance* continua a ser um factor crítico com uma importância nunca vista. Verifica-se adicionalmente que as exigências regulatórias e de reporte, incluindo em matéria de comportamento ético e legal, continuam a aumentar.

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

43%

dos inquiridos em Angola 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 Angola



Q. Qual foi o nível de impacto do crime económico mais diruptivo sofrido sobre os seguintes aspectos 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.

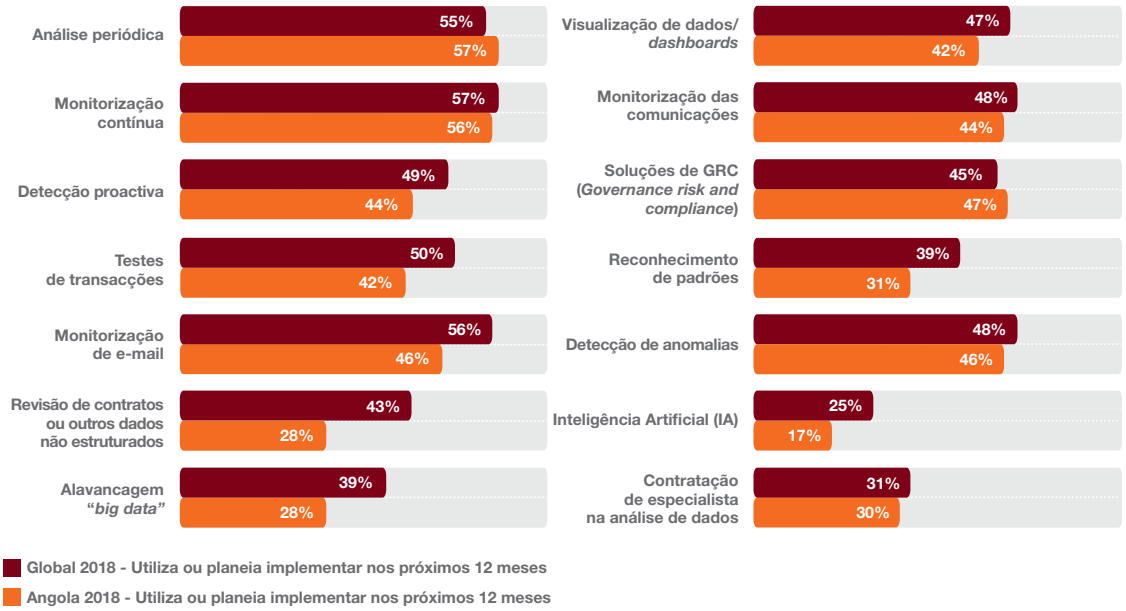
Muitas dessas tecnologias podem ser aproveitadas para combater a fraude e actuar como linhas adicionais de defesa para as organizações.

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

Apenas 17%

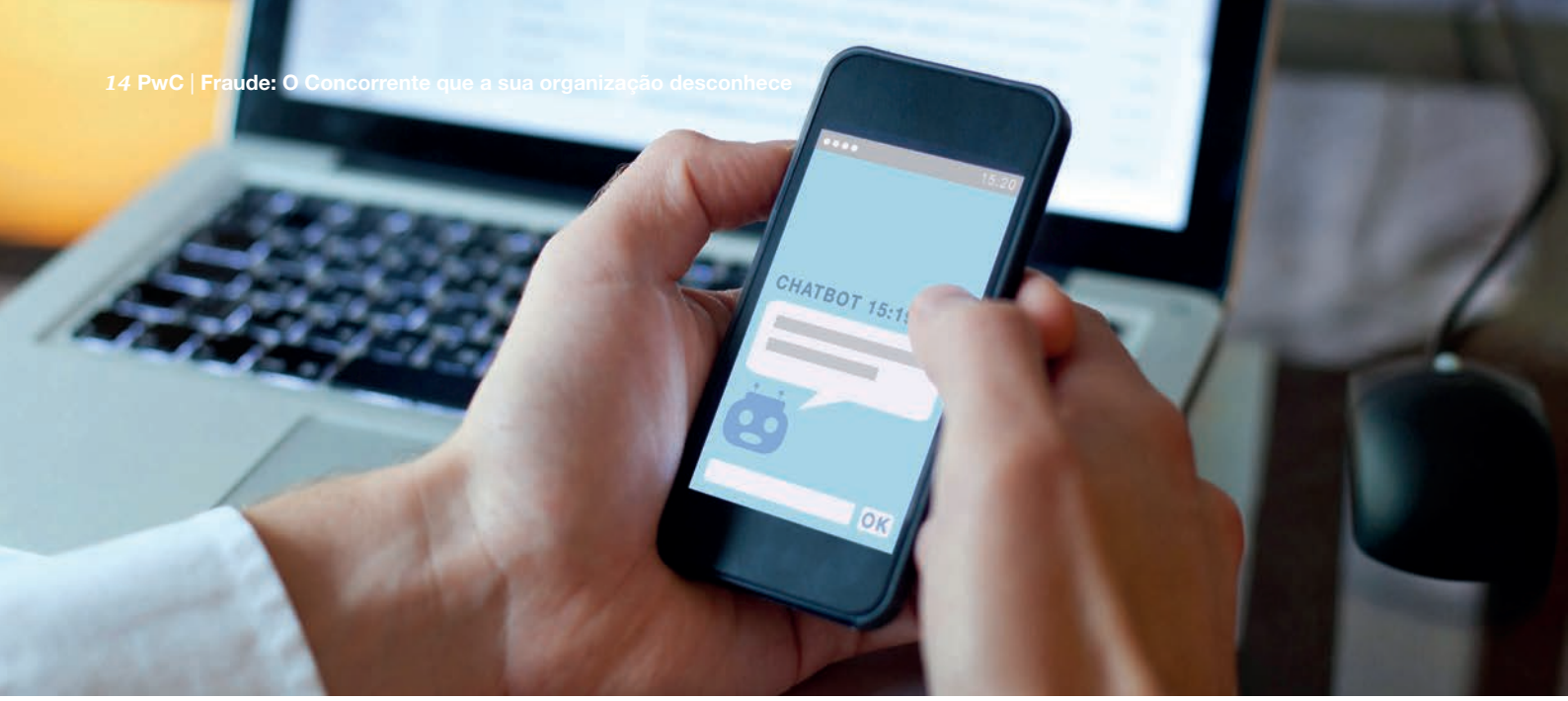
dos inquiridos em Angola afirmam que têm implementado ou tencionam implementar inteligência artificial (IA) nos próximos 12 meses para ajudar a combater fraudes e crimes económicos

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



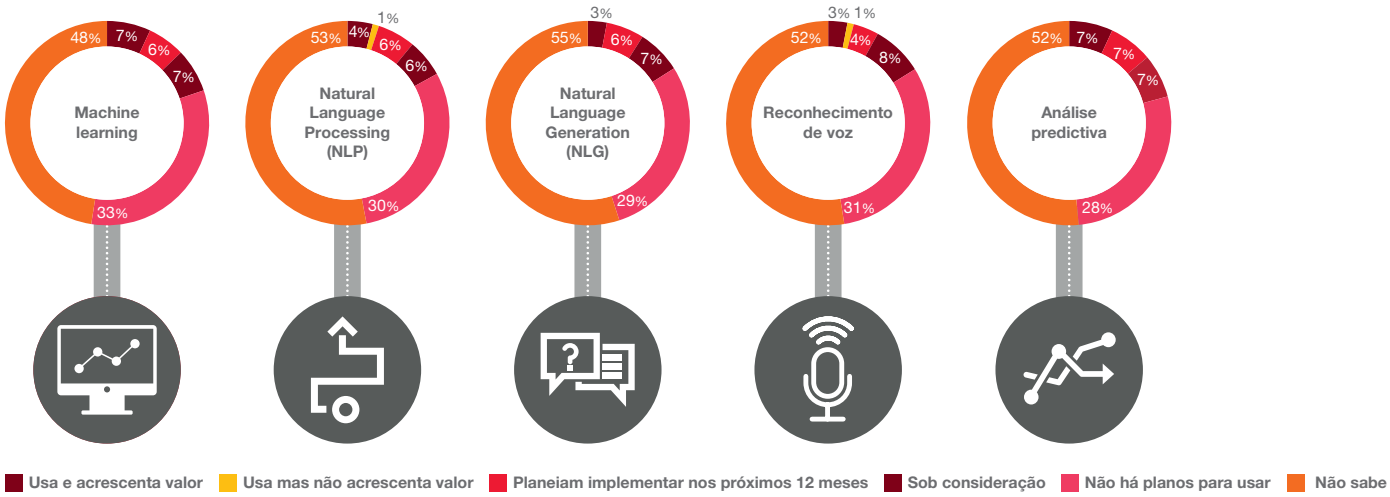
Q. Em que medida é que a sua organização utiliza, ou tem em conta, as seguintes tecnologias alternativas e técnicas disruptivas no seu ambiente para combater a fraude e/ou o crime económico?

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 reparada 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 angolanas não estão a usar toda a sua extensão - ou, pior, nem sequer a usam. Os resultados de Angola do nosso *Survey* indicam que apenas 17% 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 angolanos 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 perspectiva sobre a natureza multifacetada das ameaças cibernéticas e das fraudes que as acompanham.

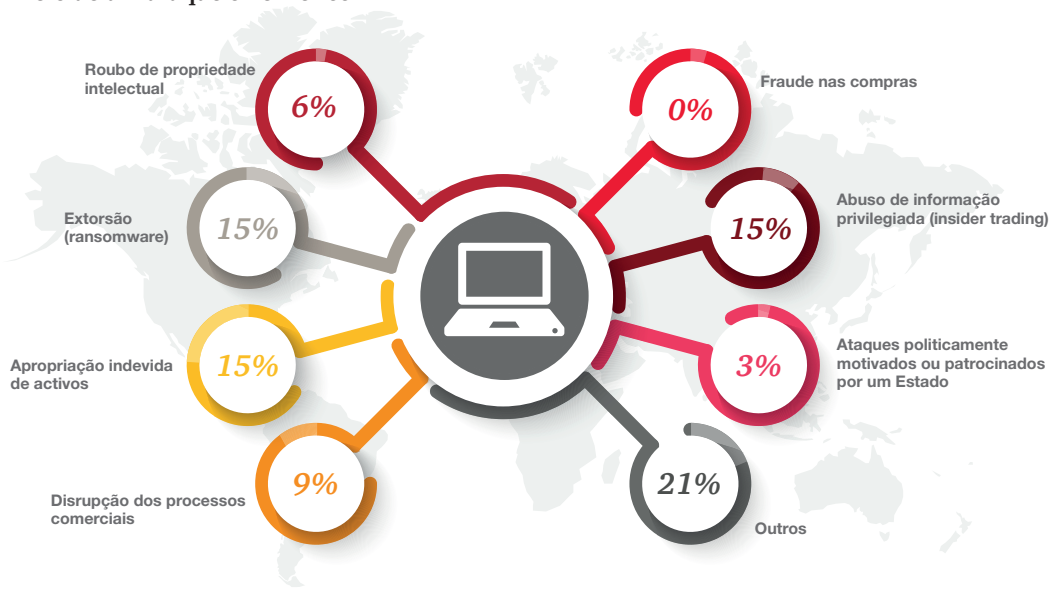
Normalmente, o primeiro sinal para uma organização perceber que algo sistémico está a acontecer é quando detecta um possível ciber-ataque, como por exemplo o *phishing* ou o *malware*. A crescente frequência, sofisticação e magnitude desses ataques está a levar as organizações a implementar medidas preventivas.

Esta abordagem permite um maior enfoque na prevenção de fraudes. 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.

10%

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

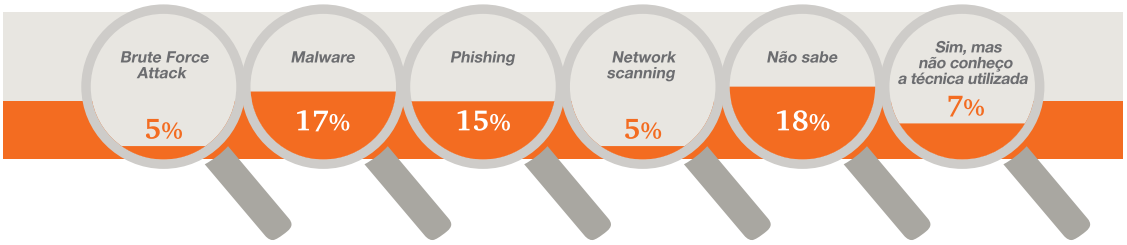
Figura 10: Os tipos de fraude de que as organizações foram vítimas, em Angola, por meio de um ataque cibernético



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*

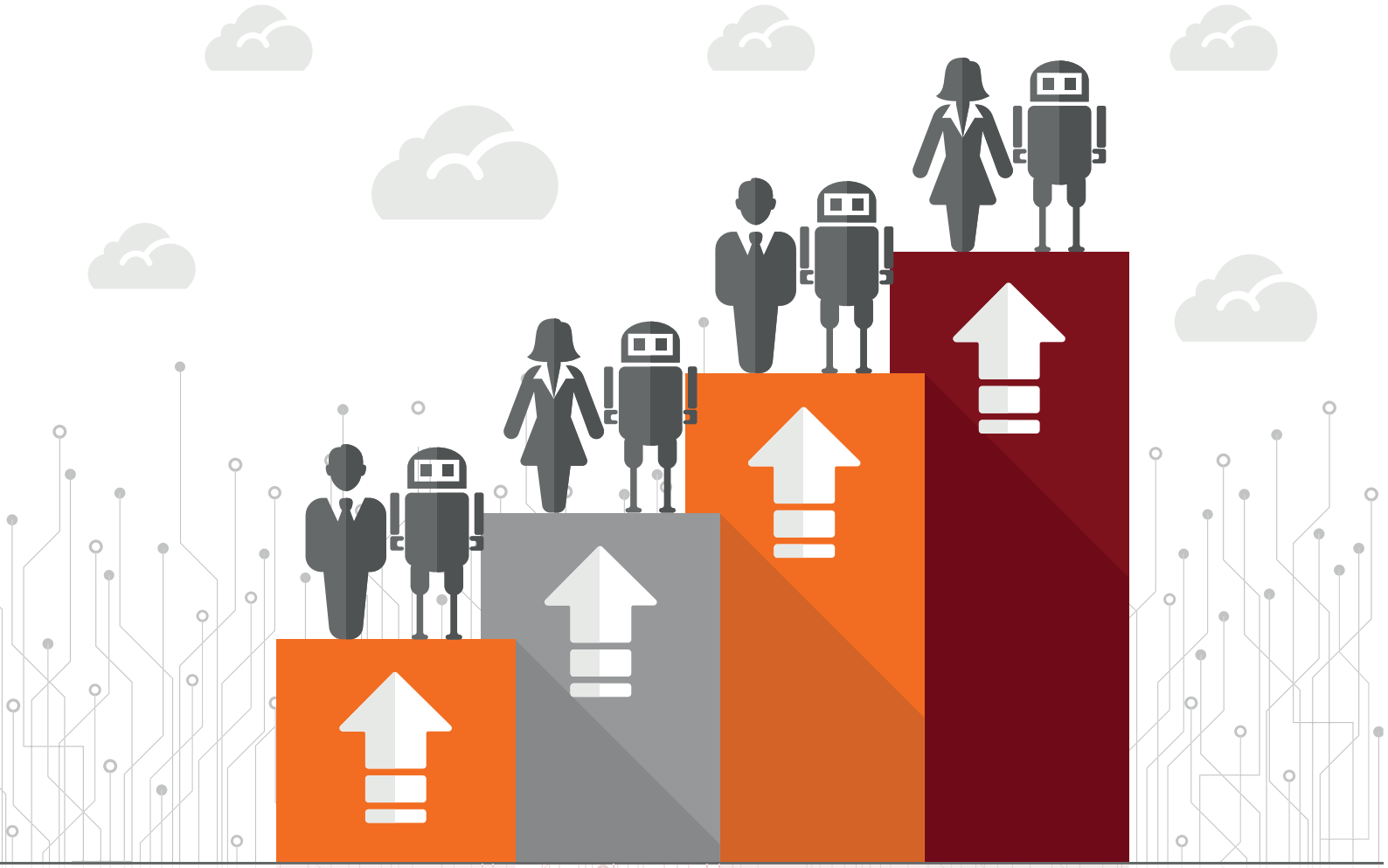
Figura 11: Técnicas de ciber-crime usadas contra as organizações a nível global



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 factor mais crítico na decisão de cometer fraude é, em última instância, o comportamento humano - e isso oferece a melhor oportunidade para combatê-lo.

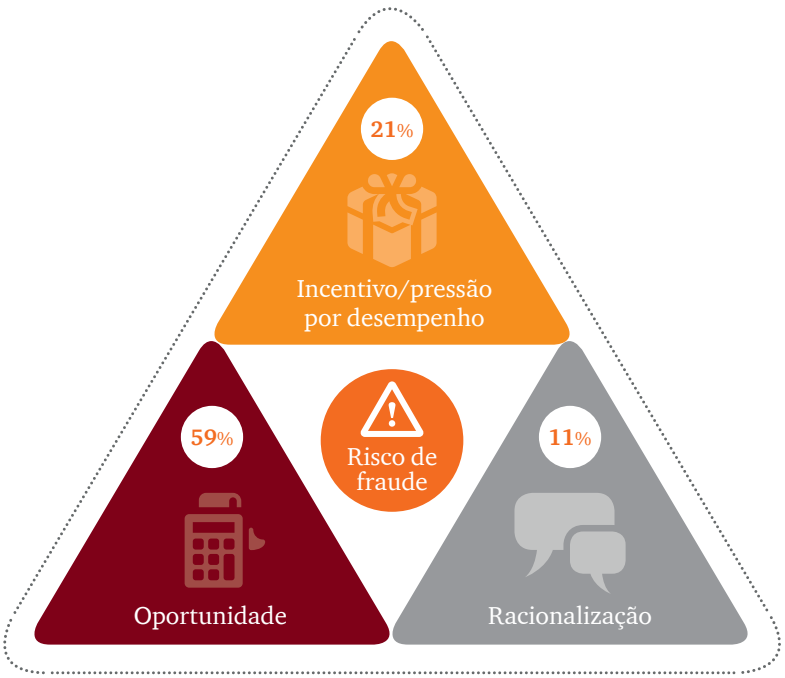
Existe um método poderoso para entender e prevenir os três principais factores da fraude interna - o triângulo da fraude. Um dos vértices do triângulo da fraude é o incentivo (geralmente uma pressão para actuar dentro da organização). Os restantes vértices são a oportunidade e o processo de racionalização interna. Como todos esses três factores devem estar presentes para que um acto 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 actos 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: O Triângulo da fraude: o que leva um funcionário a cometer fraude?



Q. Em que medida é que cada um dos seguintes factores contribuiu para o incidente de fraude e/ou crime económico cometido por agentes internos? (% dos inquiridos, a nível global, que classificaram o agente interno como o principal responsável pela fraude)
Fonte: *PwC's 2018 Global Economic Crime and Fraud Survey*

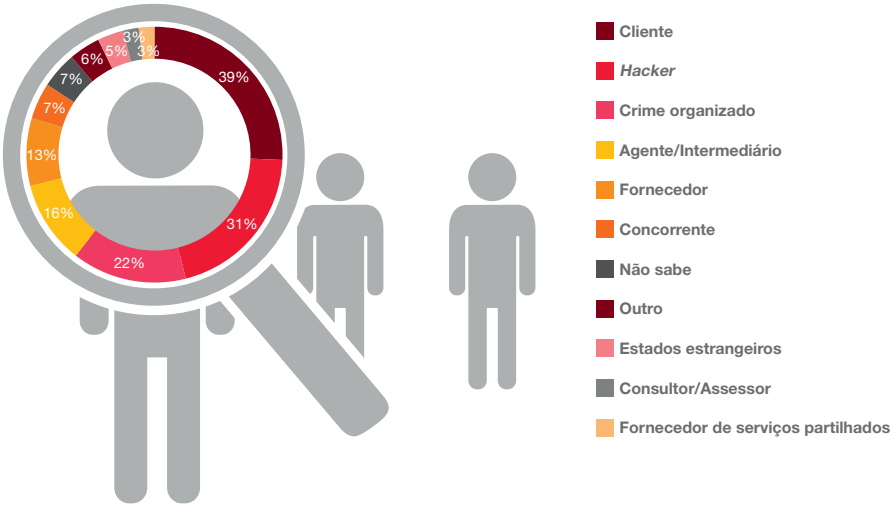
Procurar a fraude nos lugares certos

O *Survey* em Angola revelou um aumento significativo na parcela de crimes económicos cometidos por agentes internos (de 33% em 2016 para 64% em 2018).

De acordo com os nossos inquiridos, em Angola, a fraude interna supera a fraude externa como se verifica a nível global. Em Angola são os agentes internos os principais responsáveis por cometer fraude.

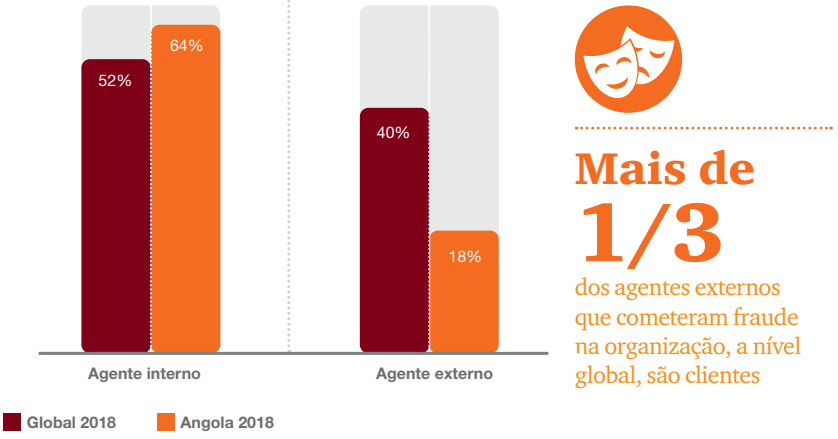
64%
dos autores da fraude são agentes internos à organização

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



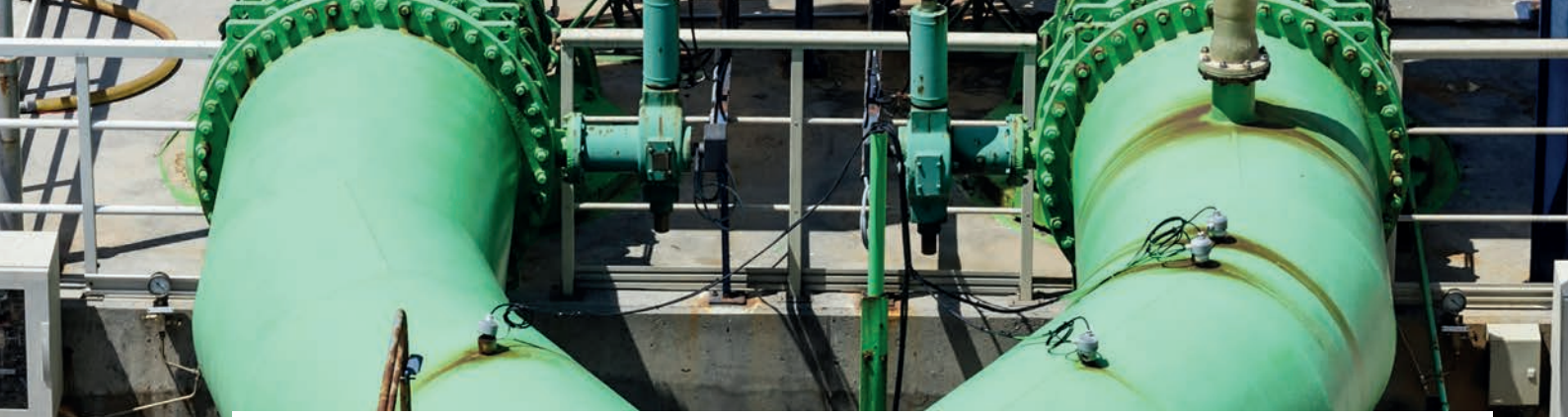
Q. Quem foram os autores da fraude externa contra a sua organização?
Fonte: *PwC's 2018 Global Economic Crime and Fraud Survey*

Figura 14: Em Angola, os agentes internos são os principais responsáveis por cometer fraude

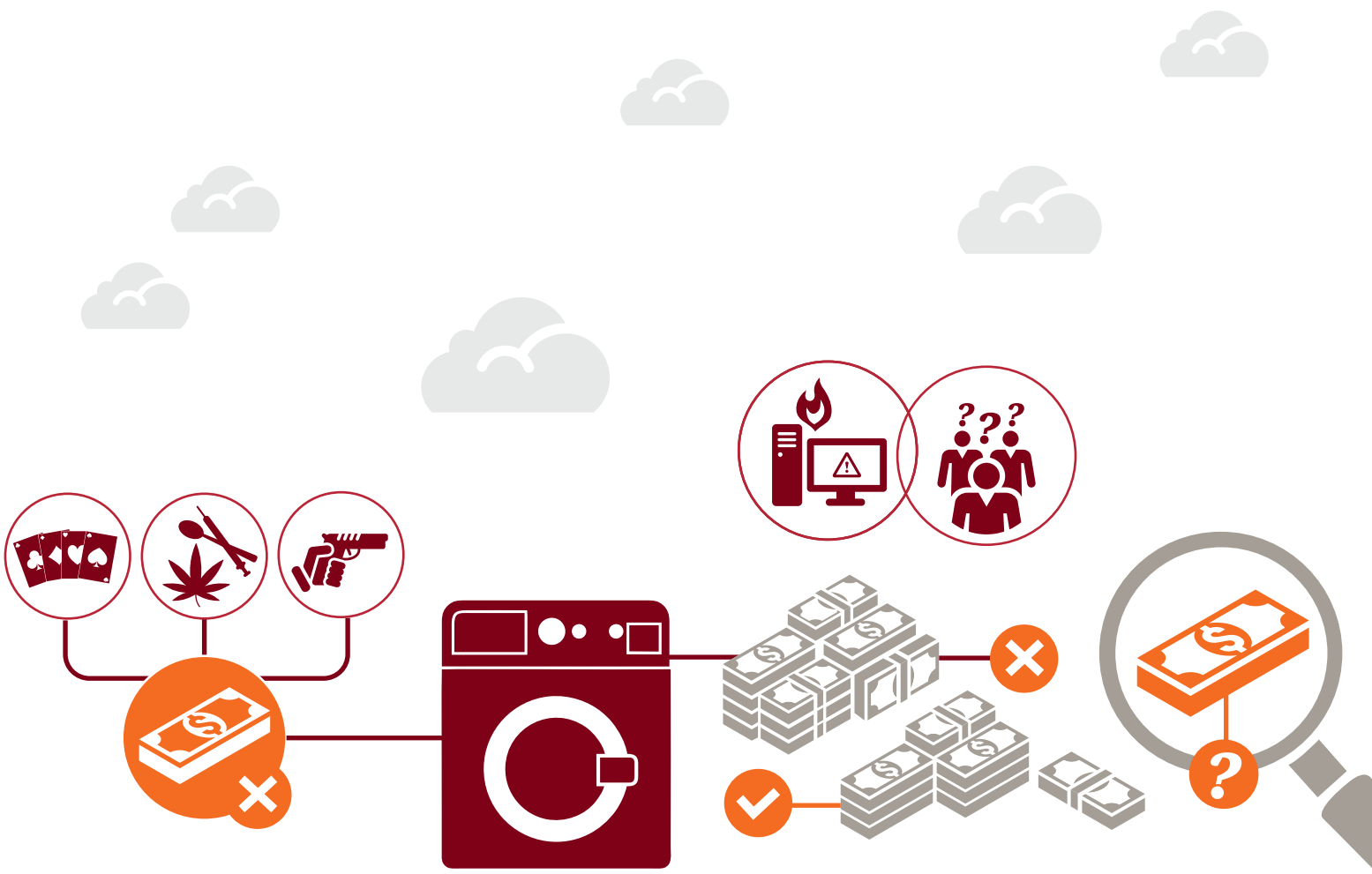


Mais de 1/3
dos agentes externos que cometeram fraude na organização, a nível global, são clientes

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



Branqueamento de capitais: Uma longa caminhada pela frente



O que já foi feito

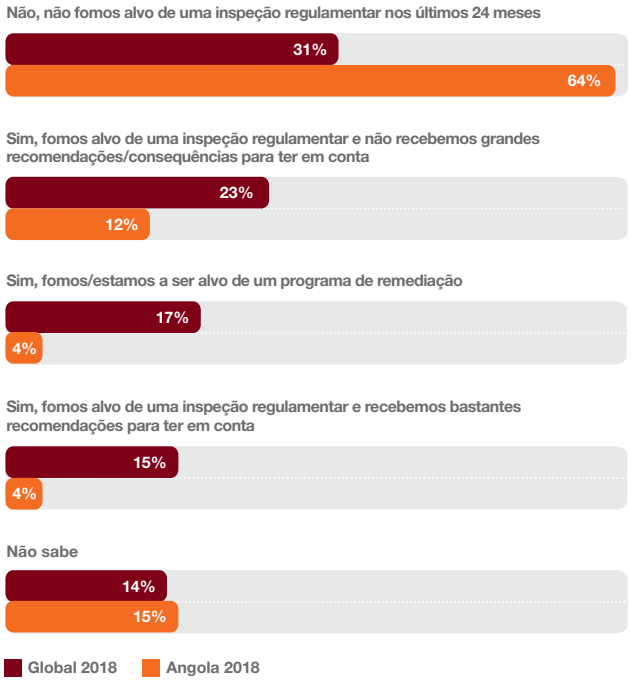
O nível de maturidade do sistema financeiro em Angola tem melhorado nos últimos anos, mas continua longe dos exigentes padrões internacionais.

Desde que o GAFI (Gabinete de Ação Financeira) identificou deficiências estratégicas em matérias de Prevenção de Branqueamento de Capitais e Combate ao Financiamento do Terrorismo (PCF/CFT) em Junho de 2010 e Fevereiro de 2013, o Estado angolano e o BNA têm feito progressos significativos, adoptando várias medidas legislativas e regulamentares no sentido de aproximar o regime legal angolano das recomendações do GAFI. Finalmente, em Fevereiro de 2016, Angola deixou de estar sujeita ao processo de monitorização permanente por parte do GAFI. A Lei do Combate ao Branqueamento de Capitais e Financiamento do Terrorismo (Lei 34/2011) foi um passo fundamental neste percurso, na medida em que o Estado transferiu e/ou partilhou uma parte significativa da obrigação de controlo para as entidades obrigadas, incluindo os bancos.

No sector financeiro, o BNA tem dado passos significativos e ao longo dos anos tem reforçado as exigências regulamentares, nomeadamente os Avisos n.º 21/2012 e n.º 22/2012, assim como a Directiva n.º 03/DSI/2012 no âmbito das sanções económicas. Adicionalmente, o guia sobre PBC/CFT apresentado na Directiva n.º 02/DRO/DSI/15, ainda que apenas com um carácter orientador, apresenta uma direcção mais alinhada com as boas práticas internacionais que o regulador pretende que as Instituições Financeiras sigam. Contudo, importa salientar que as obrigações emanadas pelo regulador assentam em tecnologias e processos que os bancos ainda não têm. Assim, tem-se assistido por parte das instituições financeiras a uma vontade de cumprir, mas com muito poucos meios para o fazer. Neste contexto, e por forma a evitar coimas, assiste-se a um desenvolvimento de medidas "ad hoc" que se vêm mostrado relativamente ineficazes por não fazerem parte de uma estratégia de desenvolvimento integrada e robusta.

No que diz respeito aos bancos que operam em Angola, muito tem sido já feito no sentido de tornar mais robustos os seus processos de compliance: foram constituídos departamentos de compliance, muitas instituições implementaram ferramentas informáticas de KYC (*know your customer*) e KYT (*know your transaction*).

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*

O que ainda falta fazer

No entanto muito há ainda por fazer. A eficácia das medidas legislativas e regulamentares demora naturalmente algum tempo até que a eficácia pretendida seja atingida. Sentimos que falta ainda vencer o desafio da capacitação dos recursos humanos afectos à área do compliance, através de formação cada vez mais avançada. Por outro lado, embora se deva reconhecer a crescente autonomia dos gabinetes de compliance, existem ainda instituições em que a independência com que o compliance actua não parece ser total. Mudar isto requer uma alteração no modo de funcionamento dos órgãos de governo societário e a atribuição de um *empowerment* adequado à função de compliance. Em paralelo, é importante que os sistemas informáticos sejam parametrizados e testados, por forma a minimizar os alertas falsos negativos (melhorando a eficácia dos processos de PBC/CFT & Sanções) e também os falsos positivos (melhorando a eficiência e reduzindo custos).

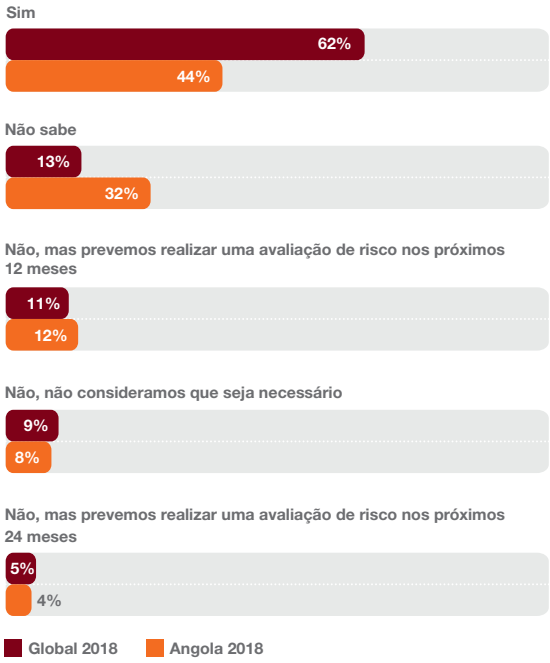
Só quando todos estes factores estiverem devidamente tratados será possível a Angola dar o passo final no reestabelecimento da sua reputação internacional no domínio da PBC/CFT e assistir-se com naturalidade ao estabelecimento de relações de correspondência com instituições bancárias dos EUA.

De acordo com o nosso survey, 24% dos inquiridos em Angola, sujeitos a regras de PBC/CFT, reconheceram não ter efectuado uma avaliação de risco de PBC/CFT nos últimos 24 meses. Há de facto aqui uma oportunidade de melhoria, mas é importante que as organizações que estão agora a iniciar uma avaliação de PBC/CFT reconheçam que esta é uma tarefa demorada, dispendiosa e stressante, especialmente se for deixada para o último minuto.

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 transacções.

Apesar dos esforços realizados, ainda existe um longo caminho pela frente. Várias instituições ainda não têm um sistema informático de PBC/CFT & Sanções e não têm definidos procedimentos que permitam mitigar os riscos a que as instituições se encontram expostas. Adicionalmente, a instituições que realizaram investiram em sistemas informáticos de PBC/CFT não o têm devidamente parametrizado nem adequado à sua realidade operativa (regras não adequadas aos clientes, aos produtos e às transacções realizadas) o que muitas vezes em vez de criar soluções cria novos problemas (backlogs de alertas). Neste contexto, é importante que os passos sejam dados de forma calculada, assegurando boas bases, para que a evolução seja efectivamente um potenciador de eficácia e não um capitalizador de problemas.

Figura 16: A avaliação de risco em PBC/CFT



Q: A sua organização efectuou 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*

24%

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

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 actuação, no que diz respeito à rapidez com que se detecta, mas também na forma como se actua 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, accionistas, 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 acções deliberadas para planear, prevenir, detectar 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 adopção 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.

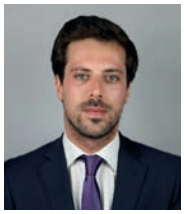
Contactos

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 Angola com 95 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