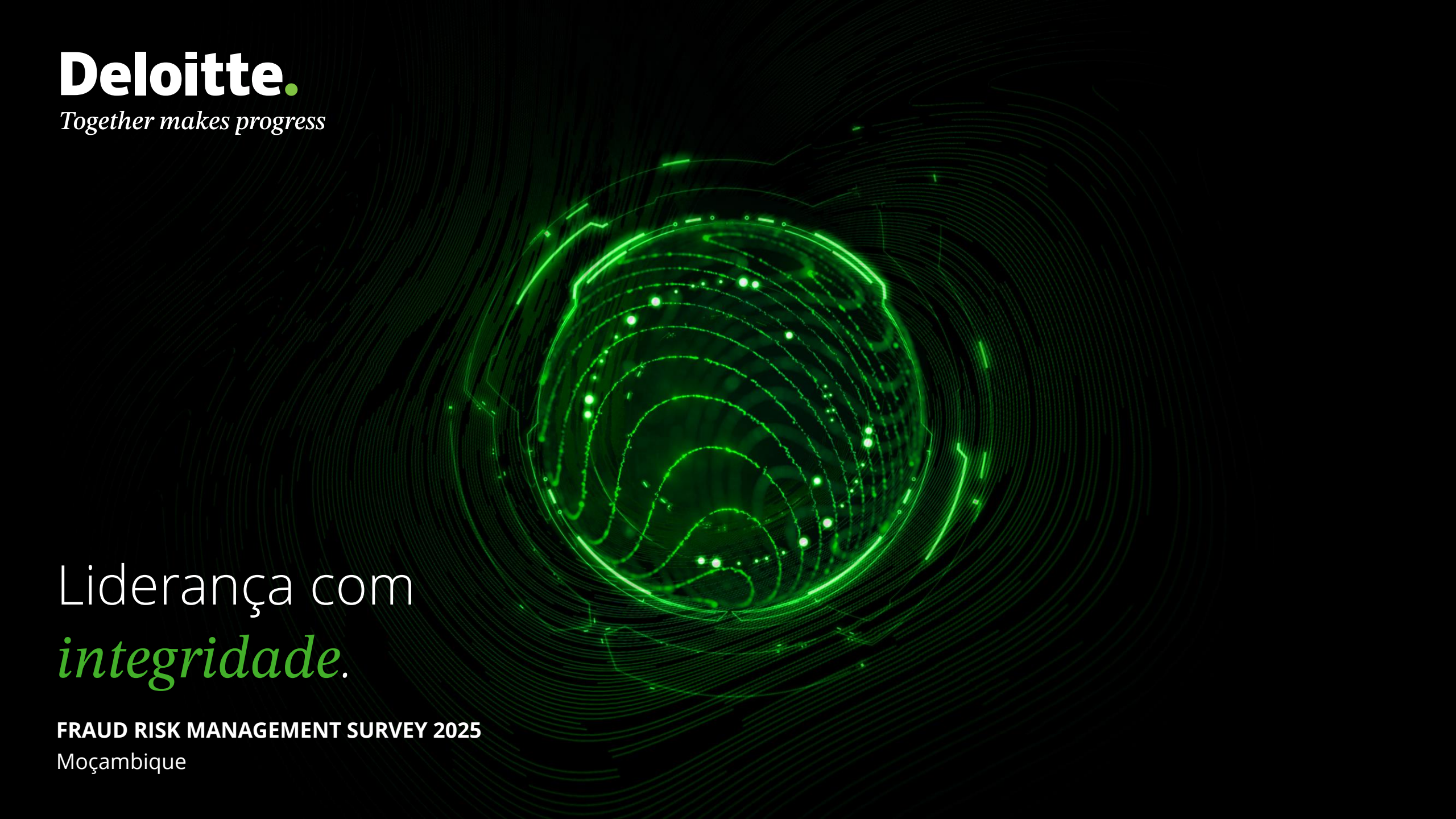
Deloitte.

Together makes progress



Liderança com *integridade*.

FRAUD RISK MANAGEMENT SURVEY 2025

Moçambique

Editorial

Bem-vindos,

É com grande satisfação que apresentamos a **primeira edição** do ***Fraud Risk Management Survey* 2025 em Moçambique**, o mais recente estudo realizado pela Deloitte Moçambique, através de um inquérito dirigido a empresas do mercado moçambicano, focado em ética, integridade e gestão do risco de fraude.

A ética e a integridade corporativa têm vindo a ganhar cada vez mais atenção, num contexto de crescente escrutínio social e regulamentar. A tolerância face a situações irregulares é cada vez menor, e a rápida transformação digital do ambiente empresarial reforça a importância de os líderes definirem estratégias claras e eficazes para promover uma cultura organizacional íntegra e resiliente.

As repercussões associadas à ocorrência de irregularidades tendem a causar impactos significativos do ponto de vista reputacional, financeiro, operacional ou legal. Torna-se, por isso, importante conhecer aprofundadamente as situações de fraude e outras irregularidades, os riscos e as consequências que delas advêm para as organizações, e a forma como são mitigadas, incluindo os mecanismos e as ferramentas mais utilizadas na prevenção, detecção e remediação da fraude e irregularidades conexas.

Com esta edição do ***Fraud Risk Management Survey* 2025 em Moçambique**, procuramos contribuir para uma maior consciencialização sobre a importância de uma abordagem preventiva, detectiva e remediadora face ao risco de fraude.

Esperamos que as organizações utilizem este estudo para fortalecer a sua capacidade de **prevenção**, **detecção e gestão de riscos**, promovendo práticas de governança mais robustas e uma cultura de integridade duradoura.

João Machado
Country Managing Partner
Deloitte

Índice

Fraud Risk Management Survey 2025

1

Integridade

A percepção das empresas em Moçambique quanto à sua actual exposição ao risco da ocorrência de situações de conduta imprópria de um ponto de vista de ética e integridade.

2

Crime Financeiro

Tipologias de crime financeiro a que as empresas em Moçambique estão expostas e as medidas implementadas para prevenir e mitigar estas ocorrências.

3

Fraude interna e externa nas empresas

A presença de situações de fraude nas empresas e que mecanismos são utilizados para prevenir e detectar actividades fraudulentas.

4

Tecnologia

A adopção de ferramentas tecnológicas pelas empresas moçambicanas para prevenção e detecção de irregularidades relacionadas com ética e integridade, assim como os principais obstáculos à implementação de novas soluções.

Sumário executivo (1/2)

A primeira edição do *Fraud Risk Management Survey* 2025 em Moçambique analisou o panorama da fraude, ética e integridade nas empresas do país, destacando desafios, práticas de prevenção e oportunidades de inovação tecnológica.

Dois terços dos inquiridos experienciaram eventos de fraude

60%

dos inquiridos relataram ter conhecimento de casos de fraude interna nos últimos 24 meses.

O conluio em esquemas de fraude em meios de pagamento foi identificado como a prática mais comum, referida por 88% dos participantes. Seguem-se o uso indevido de recursos da empresa (44%), o roubo de bens (24%) e a manipulação de registos financeiros (20%).

Entre as causas principais estão a falta de valores éticos (33%), sistemas de controlo ineficientes (28%) e nível remuneratório reduzido (23%).

No plano externo, as empresas identificam fraude promovida por clientes ou fornecedores (35%), fraude cibernética (19%) e falsificação de documentos (19%) como os riscos mais significativos.

Riscos de crime financeiro

Entre os mecanismos de prevenção mais utilizados destacam-se auditorias regulares (81%), sensibilização contínua dos colaboradores (60%) e políticas de prevenção e avaliação do risco de crime financeiro (42%).

Por outro lado, os principais desafios que as empresas enfrentam na implementação das recomendações do Grupo de Acção Financeira (GAFI) no que respeita a prevenção de temas de branqueamento de capitais, destacam-se a utilização de tecnologia inadequada (49%), a falta de conhecimento técnico dos colaboradores (42%) e a cultura organizacional existente (40%).

35%

das empresas foram vítimas de um incidente recente de crime financeiro.

A importância dos canais de denúncias e da cultura organizacional

70%

das empresas dispõem de um canal formal de denúncia anónima, mas a relutância em denunciar devido ao receio de retaliação continua a ser o principal obstáculo (56%).

Foram destacados os seguintes obstáculos à adopção mais efectiva de uma cultura de ética e integridade nas empresas: desinteresse por parte dos órgãos de gestão (65%), falta de consciencialização para estas matérias (60%), e falta de conhecimento técnico sobre a temática (21%).

Sumário executivo (2/2)

A primeira edição do *Fraud Risk Management Survey* 2025 em Moçambique analisou o panorama da fraude, ética e integridade nas empresas do país, destacando desafios, práticas de prevenção e oportunidades de inovação tecnológica.

Inovação e avanços tecnológicos

A adopção de *Big Data, GenAI e Machine Learning* permite identificar padrões anómalos, antecipar riscos e melhorar a eficiência operacional, reforçando os sistemas de controlo interno e *compliance.* Apesar das oportunidades oferecidas – maior eficiência operacional (60%), automatização de processos (47%), melhoria da transparência (37%) e reforço da segurança da informação (28%) – a implementação destas tecnologias enfrenta desafios, como custos elevados (51%), resistência cultural (37%).

33%

das empresas afirmaram desconhecer as soluções disponíveis de *Big Data, GenAI e Machine Learning*.

Riscos de crime financeiro

49%

das empresas planeiam investir, nos próximos 24 meses, em sistemas de monitorização de transacções em tempo real.

Entre os outros investimentos, destacam–se sistemas de monitorização de actividades e os respectivos acessos de colaboradores aos mesmos (28%), bem como sistemas baseados em regras e *Machine Learning* para branqueamento de capitais (26%).

1 | Integridade

À medida que o ambiente empresarial continua a evoluir rapidamente, novos desafios surgem na gestão do risco de conduta imprópria. A complexidade crescente dos mercados, nomeadamente, o moçambicano, aliada a factores como transformação tecnológica e instabilidade económica, exige que as organizações desenvolvam uma cultura mais sólida de integridade e adoptem abordagens mais sofisticadas e flexíveis para a prevenção e detecção de eventos de conduta imprópria. Este contexto dinâmico reforça a importância de estratégias inovadoras e proactivas para enfrentar eficazmente ameaças internas e externas.

No que diz respeito às condutas não éticas mais frequentes no meio empresarial moçambicano, os inquiridos identificaram o suborno e a corrupção como a prática mais comum, referida por 84% dos participantes. Seguem-se as fraudes em processos de *procurement* (60%), o conflito de interesses (44%) e o branqueamento de capitais (37%). Outras práticas menos frequentes incluem o desvio de fundos ou apropriação indevida de activos (30%) e a fraude fiscal (14%). Estes resultados evidenciam áreas críticas onde as organizações devem concentrar esforços de prevenção, monitorização e formação, de modo a reduzir a exposição a riscos éticos e financeiros.

Relativamente às áreas em que as organizações pretendem concentrar investimentos futuros para fortalecer a prevenção e detecção de fraude, as empresas inquiridas identificam três principais medidas: A formação regular dos colaboradores, apontada por 40% dos inquiridos, seguida da implementação de um código de ética (30%) e do desenvolvimento de um *framework* de avaliação de gestão de risco em matéria de integridade (21%).

Os inquiridos consideram que os principais obstáculos à adopção de uma cultura de ética e integridade nas empresas em Moçambique são o desinteresse por parte dos órgãos de gestão, percepcionado como o factor mais relevante (65%), seguido da falta de consciencialização para estas matérias (60%) e da falta de conhecimento técnico sobre a temática (21%). Estes resultados evidenciam que a consolidação de uma cultura ética depende, em grande medida, do compromisso da liderança e da sensibilização contínua dos colaboradores.

84%

dos participantes referiu práticas de suborno e corrupção como o tipo de condutas não éticas mais comum no meio empresarial moçambicano.

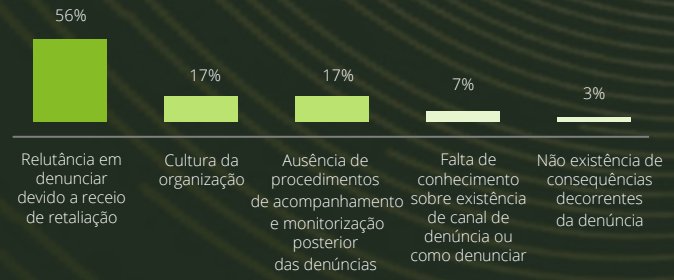
65%

das empresas referiu o desinteresse por parte dos órgãos de gestão como o principal obstáculo à adopção de uma cultura de ética e integridade.

1 | Integridade

Existe algum canal específico (denúncia) na sua empresa para reportar de forma anónima situações de carácter irregular e potencialmente não éticas?

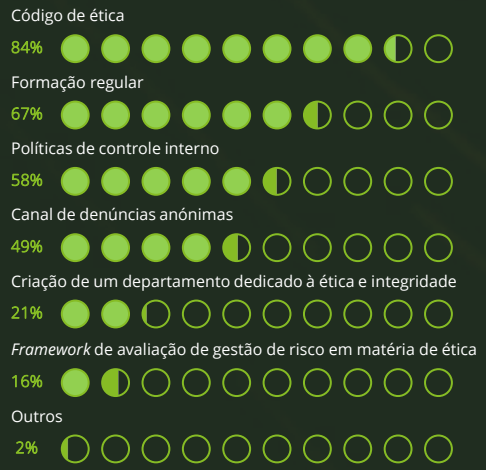
Caso exista, qual dos seguintes é o desafio mais significativo para o funcionamento eficaz desse canal na empresa?



Na sua opinião, quais das seguintes condutas não éticas são as mais frequentes no meio empresarial moçambicano?

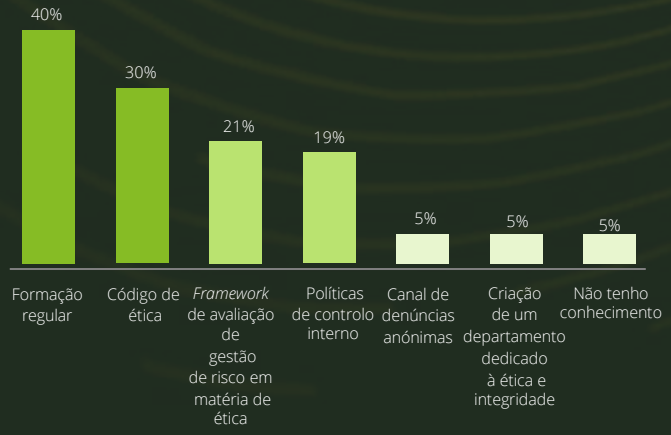
Nota: Esta é uma pergunta com resposta múltipla pelo que o total não perfaz os 100%.

Que políticas ou práticas específicas da sua empresa promovem a integridade?



Nota: Esta é uma pergunta com resposta múltipla pelo que o total não perfaz os 100%.

E onde pretende investir nos próximos 24 meses em termos de governança?



Nota: Esta é uma pergunta com resposta múltipla pelo que o total não perfaz os 100%.

Na sua opinião, quais são os principais obstáculos que podem impedir a adopção mais efectiva de uma cultura de ética e integridade nas empresas em Moçambique?

Desinteresse por parte dos órgãos de gestão	**65%**
Falta de consciencialização para estas matérias	**60%**
Falta de conhecimento técnico sobre a temática	**21%**
Falta de recursos financeiros	12%
Outros	5%

Nota: Esta é uma pergunta com resposta múltipla pelo que o total não perfaz os 100%.

1 | Práticas e soluções de referência no mercado

Canal de Denúncias

Os canais formais de denúncia constituem um pilar essencial dos sistemas de governança, ética e *compliance* nas organizações.

Quando devidamente estruturados, permitem que colaboradores, fornecedores e outros *stakeholders* reportem de forma confidencial e segura situações de irregularidade, fraude ou conduta antiética, contribuindo assim para a detecção precoce de riscos e para a promoção de uma cultura de integridade.

A implementação eficaz destes canais assume particular relevância face aos desafios associados à transparência e à confiança organizacional. A existência de mecanismos anónimos e protegidos de denúncia pode reduzir significativamente o receio de retaliação e encorajar a comunicação de comportamentos impróprios que, de outra forma, permaneceriam ocultos.

53%

das situações de fraude são reportadas através de canais de denúncias.

Princípios-chave de prevenção em matéria de ética e integridade

As organizações devem seguir um conjunto de princípios-chave de prevenção e detecção em matéria de ética e integridade.

Conforme defendido pelo *Committee of Sponsoring Organizations of the Treadway Commission* (COSO), estes passam pela promoção de um modelo de governo de gestão de risco de ética e integridade robusto e uma cultura baseada na ética, da avaliação regular do risco, definição de actividades de controlo, gestão da comunicação, investigação e aplicação de medidas correctivas e da implementação de actividades de monitorização.

Ao adoptar estes princípios, as empresas reduzem significativamente o risco de ocorrência de situações impróprias, protegendo a sua reputação e a confiança junto de clientes, fornecedores, reguladores e outros agentes internos e externos.

67%

dos colaboradores que reportaram situações tinham formação sobre fraude.

De acordo com o relatório às nações de 2024 da ACFE (*Association of Certified Fraude Examiners*).

2 | Crime Financeiro

No contexto actual, o crime financeiro continua a ser um dos principais fenómenos globais, comprometendo a confiança nas instituições e a estabilidade dos mercados, sendo por isso fundamental que as organizações adoptem mecanismos robustos de prevenção e detecção de práticas não éticas, de modo a garantir a conformidade com as exigências regulatórias e a promover uma cultura de integridade.

Dos inquiridos no *Fraud Risk Management Survey* 2025, 35% experienciaram algum tipo de incidente de crime financeiro durante o último ano. Entre aqueles que registaram incidentes, o impacto financeiro foi o mais frequente (87%), seguido do impacto reputacional (33%) e do impacto legal (20%).

No que respeita às medidas de prevenção de crimes financeiros adoptadas, a grande maioria das empresas reportou a implementação de auditorias regulares (81%) e acções de sensibilização contínua dos colaboradores (60%).

Outras medidas frequentemente adoptadas incluem a existência de políticas de prevenção e avaliação do risco de crime financeiro (42%), a aplicação de um código de conduta empresarial (42%) e a utilização de sistemas de monitorização e análise de dados (37%). Apesar do avanço na digitalização, a utilização de ferramentas baseadas em inteligência artificial generativa (*GenAI*) para detecção de padrões anómalos ainda é pouco expressiva (7%).

As empresas participantes consideram que as políticas de *KYC (Know Your Customer*) (44%) e as funções de *compliance* e auditorias internas (40%) são os que têm maior impacto na mitigação do risco de branqueamento de capitais, reforçando a importância de processos robustos de verificação e controlo interno.

Na implementação das Recomendações do GAFI (Grupo de Acção Financeira Internacional) quanto aos riscos de branqueamento de capitais, os principais desafios identificados pelas empresas prendem-se com a tecnologia inadequada (49%), a falta de conhecimento dos colaboradores (42%) e a cultura organizacional (40%).

35%

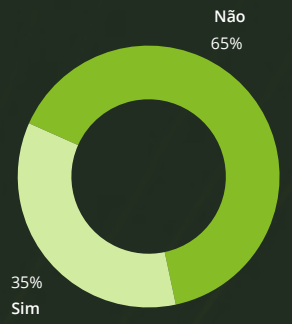
das empresas foi vítima de pelo menos um incidente de crime financeiro.

81%

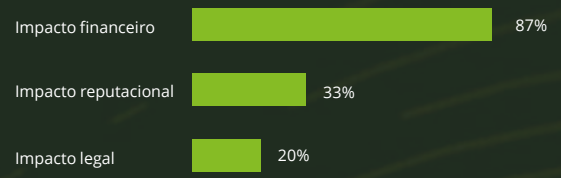
das empresas indicou a implementação de auditorias regulares como uma das suas medidas de prevenção de crimes financeiros.

2 | Crime Financeiro

A sua empresa teve recentemente algum incidente de crime financeiro?



Se sim, que impacto organizacional teve?



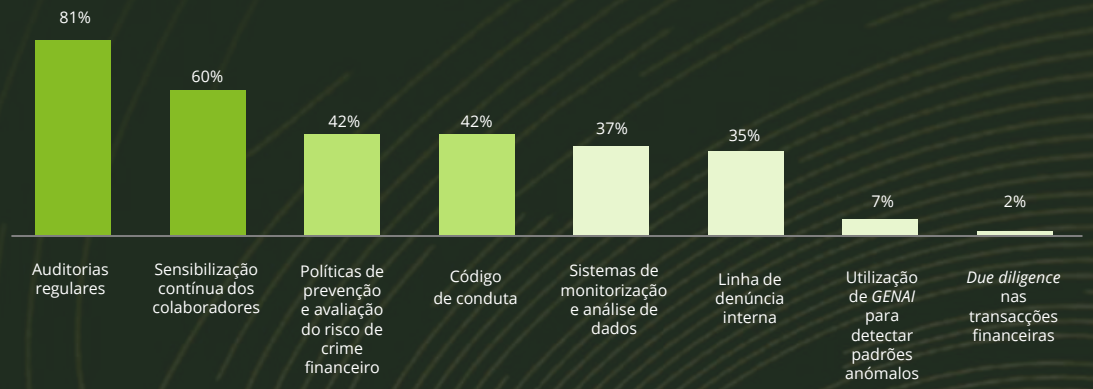
Nota: Esta é uma pergunta com resposta múltipla pelo que o total não perfaz os 100%.

Quais os 2 mecanismos que considera que mais impacto têm no reforço da mitigação do risco de branqueamento de capitais?

Políticas de *KYC* (*Know Your Customer*)	**44%**
***Compliance* e auditorias internas**	**40%**
Formação contínua	**35%**
Sistema de monitorização e alerta	35%
Relatórios de transacções suspeitas	33%

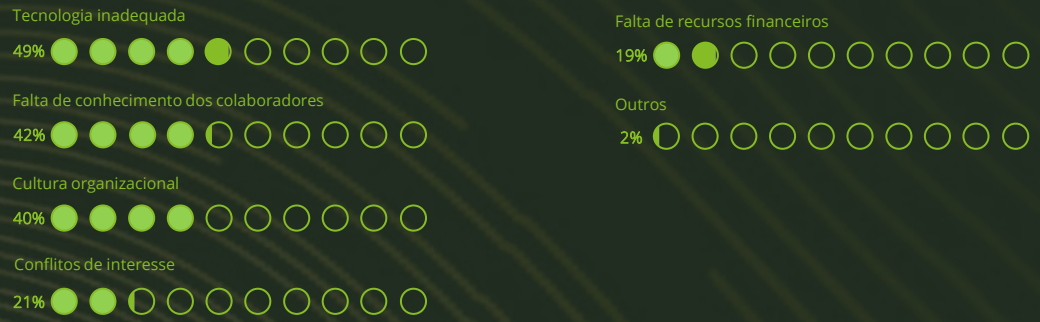
Nota: Esta é uma pergunta com resposta múltipla pelo que o total não perfaz os 100%.

Que medidas de prevenção de crimes financeiros existem na sua empresa?



Nota: Esta é uma pergunta com resposta múltipla pelo que o total não perfaz os 100%.

Quais são os principais desafios que a sua empresa enfrenta na implementação das Recomendações do GAFI no que respeita a prevenção de temas de branqueamento de capitais?



Nota: Esta é uma pergunta com resposta múltipla pelo que o total não perfaz os 100%.

2 | Práticas e soluções de referência no mercado

O benefício do investimento anti-fraude

O investimento em *compliance* e mecanismos antifraude é justificado pela poupança financeira directa e indirecta associada.

Por um lado, uma estrutura de *compliance* bem definida permite aumentar a eficiência dos processos nas organizações (e.g., via uma segregação de funções clara).
Por outro lado, a adopção das melhores práticas nesta temática aumentam a atractividade e reputação das organizações, sendo um aspecto cada vez mais valorizado por terceiros.

Finalmente, evitar custos de não *compliance* traduz-se num benefício financeiro directo. A título de exemplo, um estudo da *ACFE* em 2024, indica uma mediana de perda financeira anual de USD 145.000 nas organizações em casos de fraude e corrupção. O mesmo estudo indica que, em média, as empresas só conseguem reaver a totalidade dos fundos em 13% dos casos.

18%

Dos profissionais dedicados à prevenção e detecção de fraude usam *GenAI* e *Machine Learning*.

Relevância do *GenAI* na prevenção e do combate ao branqueamento de capitais

A utilização da inteligência artificial generativa (*GenAI*) pode ser um recurso estratégico na prevenção e detecção de actividades de branqueamento de capitais.

A tecnologia permite analisar grandes volumes de transacções financeiras, identificando padrões complexos que possam indicar comportamentos suspeitos ou tentativas de ocultar fundos. Pode também cruzar informações de múltiplas fontes, como registos de clientes, transacções internacionais e dados de terceiros, para gerar alertas antecipados sobre possíveis riscos.

Além disso, o *GenAI* pode apoiar a aplicação de políticas de *KYC (Know Your Customer*), monitorizando continuamente o perfil dos clientes e identificando mudanças que mereçam investigação. Ao automatizar a detecção de sinais de risco e fornecer relatórios detalhados às equipas de compliance, esta tecnologia torna os processos de controlo mais eficientes, permitindo respostas mais rápidas e informadas.

83%

Das empresas planeiam implementar estes métodos nos próximos 2 anos.

De acordo com o relatório às nações de 2024 da ACFE (*Association of Certified Fraude Examiners*).

3 | Fraude interna e externa nas empresas

A fraude constitui um dos principais desafios à integridade e à sustentabilidade das organizações, quer através de práticas internas, quer de ameaças externas.

De acordo com os resultados do *Fraud Risk Management Survey* 2025, 60% dos inquiridos afirmaram ter testemunhado ou tido conhecimento de casos de fraude interna nas suas empresas nos últimos 24 meses. Os tipos de fraude interna com maior frequência foram o conluio em esquemas de fraude em meios de pagamento (88%), o uso indevido de recursos da empresa (44%), o roubo de bens (24%) e a manipulação de registos financeiros (20%).

Entre as causas mais apontadas para a ocorrência deste tipo de fraude destacam-se a falta de valores éticos (33%), os sistemas de controlo ineficientes (28%) e o nível remuneratório reduzido (23%), seguidos dos conflitos de interesse (16%). Estes resultados sugerem que factores de natureza comportamental e organizacional continuam a ter um peso significativo na origem de incidentes de fraude interna.

No que respeita à fraude externa, as empresas participantes consideram que estão mais expostas à fraude promovida por clientes ou fornecedores (35%), à fraude cibernética (19%) e à falsificação de documentos (19%). Outras tipologias referidas incluem a fraude com cartões (16%), esquemas com recurso a *GenAI* (7%) e, em menor grau, a apropriação indevida de dados (4%), reflectindo o surgimento de novas ameaças associadas à tecnologia e à digitalização dos processos de negócio.

Em relação aos mecanismos de prevenção actualmente instituídos, as práticas mais comuns são a existência de uma política de gestão de risco de fraude alinhada com disposições de um referencial internacional (44%) e a análise periódica de indicadores de impacto financeiro de eventos de fraude (40%).

Outras medidas implementadas incluem a formação periódica direccionada (30%), o canal de denúncia e ferramenta de gestão e monitorização de denúncias (30%), a verificação de antecedentes e referências dos colaboradores (26%) e o uso de soluções de tecnologia antifraude com integração de meios analíticos (23%). A avaliação de terceiros, como fornecedores e prestadores de serviços, é menos comum, sendo referida por 7% dos inquiridos.

60%

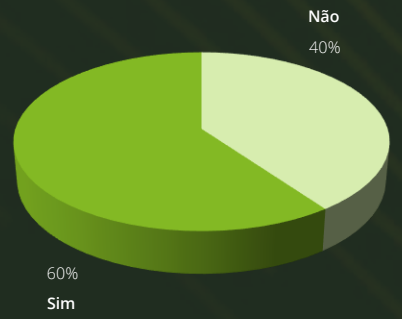
das empresas afirmaram ter sido vítimas de fraude interna.

33%

das empresas considera que a principal causa para a ocorrência de eventos de fraude interna é a falta de valores éticos.

3 | Fraude interna e externa nas empresas

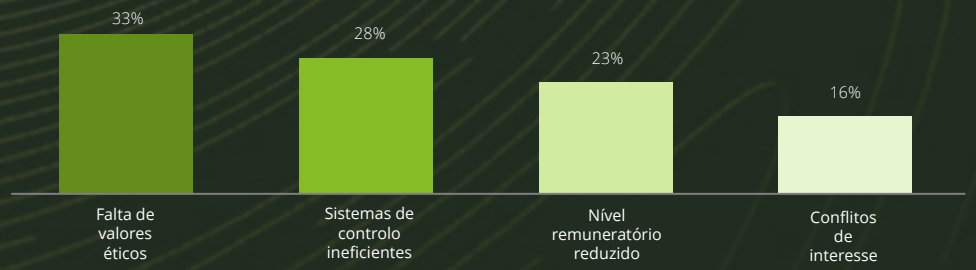
Nos últimos 24 meses testemunhou ou teve conhecimentos de casos de fraude interna na sua empresa?



E se sim, quais?

Conluio em esquemas de fraude em meios de pagamento	**88%**
Uso indevido de recursos da empresa	**44%**
Roubo de bens	24%
Manipulação de registos financeiros	20%
Suborno	8%
Branqueamento de capitais	4%

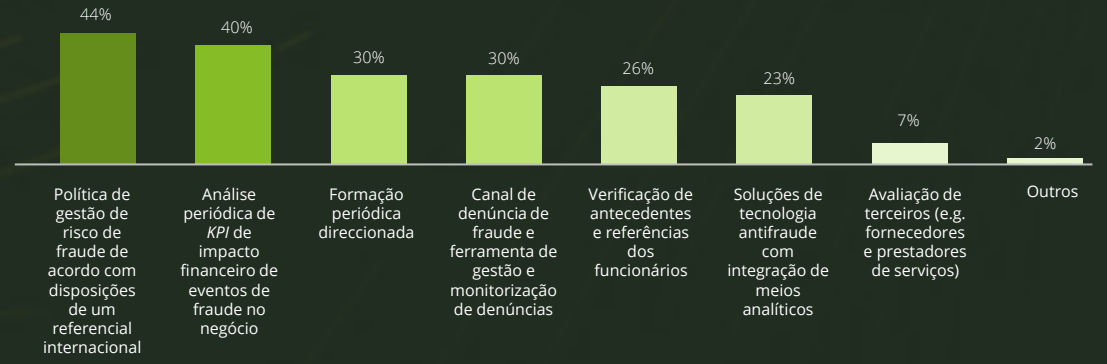
Qual considera ser o principal motivo para a ocorrência de fraude interna nas empresas em Moçambique?



Qual considera ser a principal tipologia de fraude externa a que a sua empresa se encontra mais exposta?

Fraude promovida por clientes/fornecedores	**35%**
Fraude cibernética	**19%**
Falsificação de documentos	19%
Fraude com cartões	16%
Esquemas com a utilização de *GENAI*	7%
Apropriação indevida de dados	4%

Que mecanismos de prevenção de ocorrências de eventos de fraude estão actualmente instituídos na sua empresa?



Nota: Esta é uma pergunta com resposta múltipla pelo que o total não perfaz os 100%.

3 | Práticas e soluções de referência no mercado

Relevância da prevenção do risco de fraude contra terceiros

Em Moçambique, as organizações enfrentam desafios significativos na gestão da fraude externa, incluindo riscos associados a fornecedores, prestadores de serviços e parceiros comerciais. Entre os exemplos mais comuns destacam-se a fraude promovida por clientes ou fornecedores, a falsificação de documentos, a fraude cibernética e a fraude com cartões, que podem afectar tanto o desempenho financeiro como a reputação das empresas.

A implementação de medidas de prevenção, como *due diligence* de terceiros, *scoring* de clientes e monitorização contínua das relações comerciais, permite identificar riscos de forma antecipada e reduzir a probabilidade de incidentes. Estas práticas são essenciais para fortalecer a governança corporativa, promover a transparência e garantir a conformidade com normas internacionais de ética e integridade.

35%

das empresas afirmaram que a fraude externa mais comum é levada a cabo por clientes ou fornecedores.

A relevância da cultura de prevenção de gestão de risco de fraude

A criação e manutenção de uma cultura organizacional focada na prevenção e gestão do risco de fraude é um dos pilares para assegurar a integridade e a resiliência das empresas. Uma cultura sólida promove comportamentos éticos, reforça a consciencialização dos colaboradores e garante que todos os níveis da organização compreendam a importância de seguir políticas e procedimentos de controlo interno.

Investir numa cultura preventiva permite reduzir vulnerabilidades internas, incentivar a denúncia de condutas irregulares e fortalecer a reputação institucional.

A cultura de prevenção actua assim como uma base estratégica, complementando mecanismos formais de gestão do risco de fraude.

44%

das empresas afirmaram que dispõem de uma política de gestão de risco de fraude.

4 | Tecnologia

Os resultados do *Fraud Risk Management Survey* 2025 revelam que as organizações em Moçambique enfrentam diversos desafios na adopção de tecnologia para reforçar as práticas de governança. Entre os principais desafios, destacam-se os custos elevados de *software e hardware* (51%), a resistência cultural à utilização de novas tecnologias (37%) e o desconhecimento sobre as soluções disponíveis no mercado (33%). Também são apontados obstáculos como, a necessidade de adaptação e integração de sistemas internos (23%), a dificuldade em reter colaboradores com competências técnicas especializadas (23%) e as exigências formativas de colaboradores (16%).

Apesar destes desafios, as empresas reconhecem um potencial significativo na utilização da tecnologia para fortalecer a sua governança. As principais oportunidades identificadas incluem a melhoria da eficiência operacional (60%), a automatização de processos (47%), o reforço da transparência (37%), e o aumento da segurança da informação (28%), reflectindo uma crescente percepção do papel estratégico da transformação digital na gestão corporativa.

No que respeita às ferramentas tecnológicas disponíveis para a detecção de crimes financeiros, observa-se uma presença relevante de soluções que combinam regras de negócio com modelos analíticos (28%) e de ferramentas de *analytics* suportadas por regras de detecção de irregularidades (27%). Já os procedimentos especializados em *eDiscovery* (18%) e as ferramentas de inteligência artificial generativa para detecção de padrões de crime financeiro (16%) revelam uma adopção mais limitada.

Relativamente aos instrumentos de prevenção e detecção nos quais as organizações prevêem investir nos próximos 24 meses, destaca-se o reforço dos sistemas de monitorização de transacções em tempo real (49%) e de monitorização de actividades de colaboradores (28%), bem como o desenvolvimento de sistemas baseados em regras e *Machine learning* orientados para o risco de branqueamento de capitais (26%). Outras áreas de investimento incluem aplicação de regras sobre soluções para outros riscos de crime financeiro (23%), *scoring* de risco de clientes (21%) e soluções de verificação de identidade (19%), evidenciando um movimento gradual para a digitalização e automação dos mecanismos de controlo interno e *compliance.*

49%

das empresas planeia investir no reforço de sistemas de monitorização de transações em tempo real.

9%

das empresas considera investir em soluções de *outsourcing* de capacidades de deteção ou investigação.

4 | Tecnologia

Quais considera serem os dois principais desafios relacionados com tecnologia nas práticas de governança em Moçambique?

Custos elevados de *software e hardware*	**51%**
Desafios culturais e resistência à utilizações destas tecnologias	**37%**
Desconhecimento sobre as soluções de mercado	33%
Necessidade de alteração e integração dos sistemas internos existentes	23%
Manutenção de colaboradores com *skills* de uso e análise deste tipo de ferramentas	23%

Nota: Esta é uma pergunta com resposta múltipla pelo que o total não perfaz os 100%.

Que oportunidades considera que a tecnologia pode trazer para melhorar as práticas de governação na sua empresa?

Nota: Esta é uma pergunta com resposta múltipla pelo que o total não perfaz os 100%.

Das seguintes ferramentas tecnológicas para a detecção de eventos de crime financeiro, quais é que a sua empresa dispõe?

	Dispõe	Não Dispõe	Solução Interna	Solução Externa	Ambas soluções
Ferramentas que combinam regras de negócio com modelos analíticos de detecção de padrões de irregularidades	**28%**	**72%**	**42%**	**16%**	**42%**
Ferramentas de *analytics* suportadas por uma lista de regras de detecção de irregularidades	**27%**	**73%**	**38%**	**22%**	**40%**
Procedimentos especializados em *eDiscovery*	18%	82%	43%	19%	38%
Inteligência artificial generativa direccionada para a detecção de padrões de crime financeiro	16%	84%	28%	28%	44%
Outros	11%	89%	38%	16%	46%

Nota: Esta é uma pergunta com resposta múltipla pelo que o total não perfaz os 100%.

Dos seguintes instrumentos de prevenção e detecção de crime financeiro, identifique os dois nos quais a sua organização perspectiva investir mais nos próximos 24 meses.

49%
Sistema de monitorização de transacções com identificação de potencial risco de irregularidade em tempo real

28%
Sistema de monitorização de actividades e acessos de colaboradores

26%
Sistema de monitorização de transacções com regras e *Machine Learning* para detecção de *AML*

23%
Conjunto de regras aplicadas sobre soluções para outros riscos de crime financeiro

21%
Sistema de *scoring* de risco de clientes

19%
Soluções de verificação de identidade

9%
Outsourcing de capacidades de detecção ou investigação

Nota: Esta é uma pergunta com resposta múltipla pelo que o total não perfaz os 100%.

4 | Práticas e soluções de referência no mercado

O papel da *GENAI* na prevenção e detecção de situações de fraude

A inteligência artificial generativa é uma ferramenta valiosa na prevenção e combate de situações de conduta imprópria em empresas uma vez que pode identificar padrões e comportamentos suspeitos, ajudando as empresas a detectar e prevenir potenciais irregularidades. Além disso, a inteligência artificial generativa pode ser usada para criar simulações e cenários hipotéticos que podem ajudar a avaliar a eficácia das políticas e procedimentos existentes, permitindo que as empresas ajustem as suas estratégias em conformidade.

Ferramentas que utilizam a inteligência artificial generativa permitem analisar grandes volumes de dados em tempo real e detectar padrões suspeitos. A título de exemplo, esta tecnologia pode ser programada para detectar variações no padrão operativo de clientes numa instituição financeira.

60%

das empresas respondeu que a utilização de novas tecnologias melhora a eficácia operacional.

Relevância de análise de (*Big Data*) na prevenção e detecção de situações de fraude

Os mecanismos de análise de *Big Data* têm um papel importante na prevenção e detecção de situações de conduta imprópria, permitindo a identificação de padrões suspeitos e comportamentos anómalos. Adicionalmente, a sistematização das análise de grandes volumes de dados em planilhas gráficas interactivas (*dashboards)* permite identificar transacções e actividades que possam indiciar condutas impróprias por parte dos colaboradores e/ou terceiros.

De forma a garantir a eficácia dos mecanismos de *Big Data* é fundamental que as organizações capacitem os seus colaboradores para a correcta utilização e interpretação dos resultados, bem como para que consigam garantir o alinhamento das ferramentas.

47%

das empresas referiu que um dos benefícios é a automatização de processos.

Sobre o *Fraud Risk Management Survey* 2025

O *Fraud Risk Management Survey* 2025 foi realizado entre os dias 5 de Agosto e 21 de Setembro de 2025.

O inquérito obteve um total de **43 respostas**[1], sendo esta a base de análise do presente estudo.

Dimensão[2]

74%
Grandes organizações
26%
PME

Sector de actividade[3]

45%
Serviços financeiros
14%
Transporte e Logística
7%
Construção
7%
Consumo

O *Fraud Risk Management Survey 2025* tem como objectivo proporcionar uma perspectiva abrangente e actualizada sobre como os líderes empresariais em Moçambique encaram as questões relacionadas a gestão de risco de fraude, destacando as tendências emergentes no combate ao crime financeiro.

Este estudo é uma ferramenta valiosa para as organizações na identificação e implementação das melhores práticas para a prevenção, detecção, investigação e mitigação de riscos associados à fraude. Neste contexto, são exploradas as principais causas das irregularidades e as estratégias que as organizações estão a adoptar para enfrentar estes desafios e minimizar esses riscos.

[1] Todas as respostas recolhidas são anónimas e confidenciais, sendo apenas analisadas no seu conjunto.
[2] PME: consideraram-se PME as organizações com um número de colaboradores inferior a 100 e grandes organizações aquelas que apresentam um número igual ou superior a 100 colaboradores.
[3] Banca (40%), Seguros (5%), Construção (7%), Energia (2%), Manufactura (2%), Retalho (5%), Transporte e Logística (14%), Tecnologia, Média e Telecomunicações (0%), Consumo (7%) e Outro (19%).

Contactos

Inácio Neves
Associate Partner
ineves@deloitte.co.mz

Vera Pita
Associate Partner
vpita@deloitte.pt

Aniceto Rodrigues
Manager
anicrodrigues@deloitte.co.mz

Deloitte.

MAKING AN IMPACT THAT MATTERS since 1845

bsi ISO 22301 Business Continuity Management CERTIFIED ISO/IEC 27001 Information Security Management CERTIFIED

Tipo: Sociedade por quotas | NUIT: 400016410 | NUEL nº: 101875873 | Capital social: 26.443.395 Meticais
Sede: Rua dos Desportistas nº 833, JAT V-1, 3º andar, Maputo, Moçambique