Sexta-feira, 30 de Agosto de 2024 I SÉRIE — Número 170

BOLETIM DA REPÚBLICA

PUBLICAÇÃO OFICIAL DA REPÚBLICA DE MOÇAMBIQUE

IMPRENSA NACIONAL DE MOÇAMBIQUE, E.P.

AVISO

A matéria a publicar no «Boletim da República» deve ser remetida em cópia devidamente autenticada, uma por cada assunto, donde conste, além das indicações necessárias para esse efeito, o averbamento seguinte, assinado e autenticado: **Para publicação no «Boletim da República».**

SUMÁRIO

BANCO DE MOÇAMBIQUE

Aviso n.º 10/GBM/2024

de 30 de Agosto

A Lei n.º 14/2023, de 28 de Agosto estabelece o novo regime de Prevenção e Combate ao Branqueamento de Capitais, Financiamento do Terrorismo e Financiamento da Proliferação de Armas de Destruição em Massa em Moçambique.

Mostrando-se necessário orientar a actuação das instituições financeiras que, nos termos da referida Lei, se encontram sob sua alçada de supervisão e monitorização, o Banco de Moçambique, no uso das competências que lhe são atribuídas pelas disposições conjugadas das alíneas *d*) e *e*) do n.º 2 do artigo 56 da referida Lei, determina:

1. São aprovadas as Directrizes sobre Prevenção e Combate ao Branqueamento de Capitais, Financiamento do Terrorismo e Financiamento da Proliferação de Armas de Destruição em Massa, em anexo ao presente Aviso, e que dele faz parte integrante.

2. O incumprimento das normas do presente Aviso constitui contravenção punível nos termos da Lei n.º 14/2023, de 28 de Agosto.

3. É revogado o Aviso n.º 5/GBM/2022, de 17 de Novembro, Directrizes sobre Prevenção e Combate ao Branqueamento de Capitais e Financiamento do Terrorismo.

4. O presente Aviso entra imediatamente em vigor.

5. As dúvidas na interpretação e aplicação do presente Aviso são submetidas ao Departamento de Regulamentação e Licenciamento do Banco de Moçambique.

Banco de Moçambique, em Maputo, 23 de Agosto de 2024. O Governador, — *Rogério Lucas Zandamela*.

Directrizes Sobre Prevenção e Combate ao Branqueamento de Capitais, Financiamento do Terrorismo e Financiamento da Proliferação de Armas de Destruição em Massa

CAPÍTULO I

Disposições Gerais

ARTIGO 1

(Objecto)

As presentes Directrizes estabelecem os procedimentos e medidas de prevenção e combate ao branqueamento de capitais, financiamento do terrorismo e financiamento da proliferação de armas de destruição em massa.

ARTIGO 2

(Âmbito de aplicação)

As presentes Directrizes aplicam-se a todas as instituições financeiras que, ao abrigo das alíneas *a*), *b*), *c*), *d*) e *f*) do artigo 4 da Lei n.º 14/2023, de 28 de Agosto, se encontram sob supervisão e monitorização do Banco de Moçambique.

CAPÍTULO II

Políticas de gestão de risco

ARTIGO 3

(Responsabilidades do conselho de administração ou equiparado)

1. O conselho de administração ou órgão equiparado das instituições financeiras deve documentar e aprovar as políticas sobre identificação, avaliação e gestão de risco e medidas de controlo interno que permitam gerir e mitigar eficazmente os riscos de branqueamento de capitais, financiamento do terrorismo e financiamento da proliferação de armas de destruição em massa identificados e submeter ao Banco de Moçambique.

2. Para efeitos do número anterior, o conselho de administração ou órgão equiparado deve privilegiar uma abordagem baseada no risco.

3. O conselho de administração ou órgão equiparado deve aprovar, anualmente, a política de avaliação de risco da instituição, determinar o nível de risco que a mesma está disposta a aceitar e propor medidas adequadas de mitigação de risco.

4. O conselho de administração ou órgão equiparado deve, pelo menos, anualmente:

a) comunicar formalmente as estratégias de tolerância ao risco e aceitação de risco a todos os funcionários da instituição; e

b) divulgar as recomendações sobre a implementação da política de prevenção e combate ao branqueamento de capitais, financiamento do terrorismo e financiamento da proliferação de armas de destruição em massa.

5. O conselho de administração ou órgão equiparado deve garantir que o processo de controlo e os procedimentos adoptados são eficazes, efectivos e contribuem para a redução do risco de a instituição ser usada para fins de branqueamento de capitais, financiamento do terrorismo e financiamento da proliferação de armas de destruição em massa.

ARTIGO 4

(Política de gestão de risco)

A política de gestão de risco de branqueamento de capitais, financiamento do terrorismo e financiamento da proliferação de armas de destruição em massa deve conter, no mínimo, informação sobre os seguintes procedimentos:

a) dever de identificação e verificação;

b) avaliação, gestão e monitoria de risco;

c) sigilo relativo às contas que se encontram sob monitoria para determinar transacções suspeitas;

d) reporte de transacções suspeitas e outros tipos de reportes; e

e) conservação de documentos.

ARTIGO 5

(Avaliação de risco)

1. As instituições financeiras devem elaborar, anualmente, uma avaliação de risco documentada para todos os riscos de branqueamento de capitais, financiamento do terrorismo e financiamento da proliferação de armas de destruição em massa, e a mesma deve ser aprovada pelo conselho de administração ou órgão equiparado.

2. No processo de elaboração da avaliação de risco, a instituição deve atender o disposto na legislação aplicável e recorrer à informações internas, como dados operacionais e transaccionais, bem como informações externas, como relatórios de avaliações de risco nacionais e sectoriais.

3. A avaliação de risco deve ser elaborada com recurso a elementos quantitativos e qualitativos e deve ser actualizada quando se verifique qualquer alteração nos pressupostos utilizados para a sua elaboração que possa ter um impacto material.

4. A avaliação de risco deve ser aprovada formalmente pelo conselho de administração ou órgão equiparado, por meio de acta, devendo abranger, nomeadamente os seguintes elementos:

a) produtos e serviços prestados aos clientes;

b) especificidades das transacções da instituição, incluindo, mas não se limitando à natureza e complexidade;

c) canais de distribuição directos ou indirectos;

d) características dos clientes; e

e) áreas geográficas onde se encontram os seus clientes ou transacções relacionadas.

5. A avaliação de risco deve considerar todas as jurisdições com as quais a instituição tem relação comercial e todos os tipos possíveis de transacções, nomeadamente:

a) créditos documentários;

b) correspondentes bancários; e

c) transferências.

ARTIGO 6

(Implementação das medidas de mitigação de risco)

Em cumprimento do dever de avaliação do risco, o conselho de administração ou órgão equiparado deve assegurar a implementação das medidas de mitigação aprovadas no âmbito da avaliação de risco.

ARTIGO 7

(Procedimentos relativos à confidencialidade)

1. Os procedimentos das instituições financeiras sobre sigilo devem conter disposições relativas à confidencialidade da existência, conteúdo e acompanhamento da comunicação de operações suspeitas, para evitar delações (*tipping-off*).

2. O *tipping-off* constitui uma infracção penal, nos termos do artigo 206 da Lei n.º 20/2020, de 31 de Dezembro.

CAPÍTULO III

Oficial de comunicação de operações suspeitas

ARTIGO 8

(Nomeação do Oficial de Comunicação de Operações Suspeitas)

1. O conselho de administração ou órgão equiparado deve nomear para sede, agências, sucursais e outras formas de representação da instituição um Oficial de Comunicação de Operações Suspeitas (OCOS) e assegurar recursos suficientes para o seu funcionamento, nomeadamente recursos humanos, materiais e tecnológicos.

2. O OCOS deve ser escolhido de entre os funcionários de nível de gestão da instituição, devendo, no mínimo, ser dotado de alto grau de responsabilidade e independência.

3. O nível dos recursos referidos no n.º 1 do presente artigo deve reflectir a dimensão, complexidade, número de clientes e produtos oferecidos pela instituição.

ARTIGO 9

(Responsabilidades do OCOS)

1. O OCOS suporta e orienta a gestão do risco de branqueamento de capitais, financiamento do terrorismo e financiamento da proliferação de armas de destruição em massa na instituição financeira.

2. Sem prejuízo do estabelecido na legislação aplicável, são responsabilidades do OCOS, nomeadamente:

a) rever, com regularidade, a adequação do sistema de controlos sobre a prevenção e combate ao branqueamento de capitais, financiamento do terrorismo e financiamento da proliferação de armas de destruição em massa, nomeadamente:

i. fiscalizando a implementação das políticas e procedimentos para a prevenção e combate ao branqueamento de capitais, financiamento do terrorismo e financiamento da proliferação de armas de destruição em massa;

ii. assegurando um processo de monitoria apropriado; e

iii. participando de forma activa na escolha da aplicação informática (*software*) para monitorar os clientes e suas transacções.

b) garantir que toda a informação relevante seja transmitida aos trabalhadores, fiscalizando o cumprimento das políticas sobre a formação e capacitação aprovada pela instituição e assegurando que o seu conteúdo seja adequado, actual e se encontre alinhado com as boas práticas e as tendências do fenómeno de branqueamento de capitais, financiamento do

terrorismo e financiamento da proliferação de armas de destruição em massa.

ARTIGO 10

(Confidencialidade)

1. Os OCOS estão sujeitos à obrigação de confidencialidade relativamente a todos os alertas individuais, transacções e operações suspeitas que tenham de tratar no exercício das suas funções.

2. A troca de informações dentro da instituição só pode ser feita com pessoas da organização sujeitas à mesma obrigação de confidencialidade em casos de branqueamento de capitais, financiamento do terrorismo e financiamento da proliferação de armas de destruição em massa e com base na regra de necessidade de conhecimento (*"need to know"*) definida nos procedimentos da instituição financeira.

ARTIGO 11

(Coordenação centralizada)

1. As instituições financeiras devem nomear um OCOS coordenador, com a função de coordenar e centralizar as informações recebidas dos demais OCOS e analisar as transacções incomuns detectadas.

2. O OCOS coordenador tem, em especial, a responsabilidade de:

a) monitorar a aplicação efectiva das políticas, dos procedimentos e controlos adequados à gestão eficaz dos riscos de branqueamento de capitais, financiamento do terrorismo e financiamento da proliferação de armas de destruição em massa a que a instituição financeira esteja ou venha a estar exposta;

b) promover o cumprimento pela instituição financeira das normas legais e regulamentares em matéria de prevenção do branqueamento de capitais, financiamento do terrorismo e financiamento da proliferação de armas de destruição em massa;

c) garantir o envio de reportes de transacções suspeitas ao Gabinete de Informação Financeira de Moçambique (GIFiM), com toda a informação relevante sobre a transacção e o cliente;

d) garantir o envio imediato de toda a informação adicional solicitada pelas autoridades competentes, no âmbito de casos suspeitos de branqueamento de capitais, financiamento do terrorismo e financiamento da proliferação de armas de destruição em massa; e

e) assegurar a coordenação centralizada com as várias partes interessadas, nomeadamente os auditores internos, os auditores externos, o Banco de Moçambique, o GIFiM e as autoridades judiciais e administrativas.

ARTIGO 12

(Substituição)

1. Em caso de necessidade de substituição do OCOS, por ausência ou outro motivo, a instituição financeira deve garantir que o substituto reúna os requisitos relevantes.

2. De modo a evitar conflitos de interesses, em nenhuma situação, o OCOS pode ser substituído por um membro da auditoria interna.

ARTIGO 13

(Conflitos de interesse)

O conselho de administração ou órgão equiparado deve adoptar disposições sobre a prevenção de conflitos de interesse para os OCOS, incluindo a proibição de concessão de incentivos que possam constituir obstáculo para a identificação e comunicação atempada de transacções suspeitas às autoridades competentes.

CAPÍTULO IV

Auditoria interna

ARTIGO 14

(Responsabilidades da auditoria interna)

A auditoria interna é responsável pela realização de uma avaliação independente e pela eficácia e eficiência do sistema de prevenção ao branqueamento de capitais, financiamento do terrorismo e financiamento da proliferação de armas de destruição em massa, devendo, nomeadamente:

a) verificar a adequação das políticas;

b) adoptar procedimentos e sistema de suporte para detectar potenciais operações suspeitas de branqueamento de capitais, financiamento do terrorismo e financiamento da proliferação de armas de destruição em massa;

c) avaliar se cada linha de defesa desempenha adequadamente as tarefas e funções atribuídas; e

d) rever o funcionamento do sistema para garantir um desempenho adequado.

ARTIGO 15

(Independência)

A auditoria interna deve ser sempre independente e reportar directamente ao conselho de administração ou órgão equiparado.

ARTIGO 16

(Programa e relatório de auditoria interna)

1. O programa de auditoria interna deve estar alinhado com a avaliação do risco efectuado pela instituição financeira.

2. O relatório de auditoria interna deve ser remetido, em tempo útil, ao conselho de administração ou órgão equiparado e ao comité de auditoria, existindo.

ARTIGO 17

(Escopo e metodologia)

O conselho de administração ou órgão equiparado deve assegurar que o escopo e a metodologia da auditoria interna são adequados ao perfil de risco da instituição financeira e que a frequência das auditorias seja baseada no risco.

ARTIGO 18

(Constatações)

Quaisquer constatações adversas da auditoria interna devem ser devidamente encaminhadas ao conselho de administração ou órgão equiparado, de acordo com a estrutura formal de governação corporativa.

ARTIGO 19

(Deveres da auditoria interna)

1. A auditoria interna deve assegurar o cumprimento dos procedimentos de prevenção de branqueamento de capitais, financiamento do terrorismo e financiamento da proliferação de armas de destruição em massa em todas as agências e sucursais da instituição financeira.

2. O dever referido no número anterior deve abranger terceiros e agentes que actuam em nome da instituição financeira, para garantir a sua conformidade com as políticas e procedimentos da instituição financeira.

3. A auditoria interna deve, em particular, rever os processos de *due diligence* e de "Conheça o seu Cliente" (*Know Your Costumer*) realizados para clientes, produtos, serviços ou canais de distribuição identificados como de alto risco.

4. A auditoria interna deve verificar o tratamento diligente dos alertas de branqueamento de capitais, financiamento do terrorismo e financiamento da proliferação de armas de destruição em massa, e se os alertas gerados são prontamente encerrados com uma avaliação de risco adequada.

ARTIGO 20

(Periodicidade)

As auditorias internas devem ser realizadas em todo ou parte do sistema de prevenção ao branqueamento de capitais, financiamento do terrorismo e financiamento da proliferação de armas de destruição em massa da instituição financeira, pelo menos, anualmente.

CAPÍTULO V

Terceirização e organização de grupos

ARTIGO 21

(Terceirização)

1. As instituições financeiras podem subcontratar processos, serviços ou actividades no âmbito do cumprimento dos deveres previstos na legislação atinente ao branqueamento de capitais, financiamento ao terrorismo e financiamento da proliferação de armas de destruição em massa.

2. Sempre que as instituições financeiras subcontratem processos, serviços ou actividades, as mesmas são responsáveis, em exclusivo, pelo cumprimento do disposto na legislação referida no número anterior.

3. Não podem ser objecto de subcontratação os processos, serviços ou actividades cuja subcontratação seja susceptível de prejudicar a qualidade das medidas e procedimentos adoptados para dar cumprimento aos requisitos da legislação atinente ao branqueamento de capitais, financiamento ao terrorismo e financiamento da proliferação de armas de destruição em massa.

4. As instituições financeiras estão vedadas de recorrer a prestadores de serviços estabelecidos em países com regimes legais que prevejam proibições ou restrições que impedem ou limitem o cumprimento das normas legais e regulamentares em matéria de prevenção do branqueamento de capitais, financiamento do terrorismo e financiamento da proliferação de armas de destruição em massa, incluindo ao nível da prestação e circulação de informação.

ARTIGO 22

(Relação de grupo)

1. Se a instituição financeira pertencer a um grupo ou for a empresa-mãe de um grupo financeiro, os procedimentos internos devem permitir a partilha de informação dentro do grupo, para efeitos de organização e vigilância de prevenção de branqueamento de capitais, financiamento do terrorismo e financiamento da proliferação de armas de destruição em massa, incluindo o encaminhamento de informação à empresa-mãe do grupo.

2. Os procedimentos de partilha de informação devem estar em conformidade com o disposto na legislação relevante sobre a matéria.

ARTIGO 23

(Princípio de equivalência)

Se a instituição financeira for a empresa-mãe de um grupo financeiro, o OCOS responsável pela implementação da política de gestão de risco de branqueamento de capitais, financiamento do terrorismo e financiamento da proliferação de armas de destruição em massa do grupo deve verificar se as medidas aplicadas em entidades no estrangeiro são, no mínimo, equivalentes às vigentes em Moçambique e se as sucursais localizadas em outros Estados cumprem disposições semelhantes às de Moçambique.

ARTIGO 24

(Comunicações)

Se a instituição financeira for a empresa-mãe de um grupo financeiro, o OCOS responsável pela implementação do sistema de grupo deve ser informado da existência de comunicações de operações suspeitas feitas a uma Unidade de Informação Financeira por qualquer entidade do grupo.

ARTIGO 25

Sucursais

Caso a instituição financeira detenha sucursais, o OCOS responsável pela implementação do sistema do grupo deve verificar se a legislação local aplicável não impede o acesso rápido aos documentos ou detalhes da transacção.

CAPÍTULO VI

Dever de identificação e verificação

SECÇÃO I

Políticas e classificação de clientes

ARTIGO 26

(Conheça o seu cliente)

1. As instituições financeiras devem adoptar políticas sobre a identificação e verificação dos seus clientes, independentemente do montante de transacções individuais.

2. A política do "Conheça o Seu Cliente" das instituições financeiras deve incorporar, entre outros, os seguintes elementos:

a) política de aceitação de clientes;
b) os procedimentos de identificação e verificação do cliente;
c) monitoria de operações; e
d) gestão de riscos.

ARTIGO 27

(Política de aceitação de clientes)

As instituições financeiras devem elaborar uma política clara sobre a aceitação de clientes, incluindo medidas aplicáveis para cada categoria de clientes.

ARTIGO 28

(Conteúdo da política de aceitação de clientes)

1. A política de aceitação de clientes deve ter em conta os riscos associados ao cliente, ao país ou à região geográfica, e riscos associados ao canal de entrega do produto, ao serviço ou à operação, conforme exemplos apresentados no Anexo I destas Directrizes.

2. No essencial, a política de aceitação de clientes deve integrar, sem limitar, o seguinte:

a) proibição de abertura de contas anónimas ou fictícias;
b) proibição de abertura de contas numeradas;

c) categorização do cliente consoante a avaliação de risco efectuada;
d) documentação necessária, informações adicionais a serem exigidas e medidas aplicáveis para cada categoria de cliente, tendo por base a avaliação de risco efectuada;
e) medidas de diligência reforçadas para aceitação de clientes de alto risco, conforme exemplos, meramente exemplificativos, constantes do Anexo II;
f) proibição de abertura ou encerramento de conta quando a instituição financeira seja incapaz de aplicar as medidas de diligências;
g) as circunstâncias nas quais ao cliente seja permitido agir em nome de outrem, seja pessoa física ou jurídica, de acordo com a legislação em vigor;
h) medidas de identificação dos beneficiários efectivos;
i) procedimentos de abertura de contas de forma não presencial;
j) procedimentos para a aprovação superior nos casos de abertura de contas por pessoas politicamente expostas bem como os demais clientes de alto risco; e
k) tipo de averiguações necessárias, antes de abertura da conta, de modo a verificar se o cliente não possui antecedentes criminais, não se encontra na lista de terroristas ou organizações terroristas.

ARTIGO 29

(Classificação de risco)

1. As instituições financeiras devem ter uma política de classificação de risco de seus clientes.

2. A classificação de risco dos clientes deve ser actualizada, pelo menos, uma vez por ano.

3. A frequência de classificação de risco deve ser aumentada para os casos de clientes de alto risco.

ARTIGO 30

(Sistema de gestão de activadores)

As instituições financeiras devem ter um sistema de gestão de activadores (*triggers*) adequado que permita realizar o necessário exame do processo de aceitação do cliente à luz de quaisquer eventos que ocorram ao cliente e que possam implicar uma revisão da respectiva classificação de risco.

SECÇÃO II

Procedimentos de identificação e verificação de clientes

ARTIGO 31

(Dever de identificação)

As instituições financeiras devem identificar os seus clientes nos termos e situações previstas na na legislação sobre o branqueamento de capitais, financiamento do terrorismo e financiamento de armas de destruição em massa e sempre que careçam de informações suficientes e actuais sobre o cliente.

ARTIGO 32

(Dever de verificação)

1. As instituições financeiras devem identificar e verificar a identidade e o endereço actual dos seus clientes e perceber a natureza dos negócios do cliente, as suas fontes de rendimento, situação financeira e a qualidade com que pretendam estabelecer a relação de negócio com a instituição.

2. As instituições financeiras devem assegurar, tanto quanto possível, que estão a lidar com uma pessoa idónea e verificar a identidade da pessoa em causa, em conformidade com as disposições do presente Capítulo.

ARTIGO 33

(Intermediários)

1. Se os fundos a serem depositados ou transferidos estiverem a ser fornecidos por uma terceira pessoa, a instituição deve proceder à identificação e verificação dessa pessoa.

2. Se a instituição não for capaz de determinar se o requerente, no negócio, está a agir por conta própria ou a mando de um terceiro deve considerar a apresentação de comunicação de operação suspeita ao GIFiM, mesmo que eventualmente a conta não seja aberta ou a transacção não seja processada.

ARTIGO 34

(Medidas de vigilância)

As instituições financeiras devem exigir que os clientes forneçam, por escrito, a identidade e informações da(s) pessoa(s) física(s) beneficiária(s) efectiva(s) da relação de negócio ou transacção, como parte de medidas de vigilância para identificar e verificar a identidade do(s) mesmo(s).

ARTIGO 35

(Confirmação da identidade)

1. As instituições financeiras devem obter todas as informações necessárias para confirmar a identidade do cliente e verificar a informação por este prestada.

2. Para o efeito do disposto no número anterior, as instituições financeiras podem usar informações públicas nacionais e internacionais disponíveis, cruzar informações com outros elementos de prova, nomeadamente factura de fornecimento de serviços de água, energia, telefone, listas telefónicas, centrais de registo de crédito, registos criminais e manter tais elementos em seus arquivos.

ARTIGO 36

(Identidade do beneficiário efectivo)

1. Caso o cliente não seja o beneficiário da relação de negócio, a instituição financeira deve adoptar medidas razoáveis para verificar a identidade do beneficiário efectivo, usando informações ou dados relevantes obtidos a partir de uma fonte que considere idónea para a confortar.

2. Para o cumprimento do previsto no número anterior, as instituições financeiras devem ainda observar as disposições legais da Lei n.º 14/2023, de 28 de Agosto e do respectivo Regulamento aplicáveis à matéria.

3. No caso de pessoas colectivas de natureza não societária, fundações, centros de interesses colectivos sem personalidade jurídica, fundos fiduciários e entidades similares, as instituições financeiras devem, conforme aplicável, identificar e verificar a identidade do:

a) fundador;
b) administrador;
c) curador ou protector;
d) beneficiários ou, se os mesmos não estiverem determinados, pessoas em cujo interesse principal a entidade foi constituída ou exerce a respectiva actividade;
e) pessoas que exercem o efectivo controlo; e
f) pessoas em situações equivalentes ou similares às mencionadas anteriormente.

4. A identificação dos curadores de um fundo fiduciário (trust) deve ser entendida como incluindo o protector e qualquer outra pessoa singular que exerça, em última instância, o seu controlo efectivo.

ARTIGO 37

(Encerramento de contas)

1. Quando um cliente encerrar uma conta e solicitar a abertura de outra na mesma instituição financeira, não fica dispensado o dever de identificação e verificação e, neste caso, os detalhes sobre o arquivo do cliente devem ser reconfirmados.

2. Os detalhes das contas e as diligências efectuadas nos termos do número anterior, para verificar a identidade e os registos efectuados, devem ser transferidos para os registos da nova conta.

ARTIGO 38

(Alteração de elementos de identificação)

1. Qualquer alteração posterior do nome do cliente, endereço ou da informação sobre a sua situação laboral de que a instituição tenha conhecimento deve ser registada e devidamente fundamentada por prova documental, como parte do processo de medidas de diligências.

2. A informação relativa ao cliente e ao beneficiário efectivo deve ser conservada em arquivo.

ARTIGO 39

(Transferência do saldo de contas)

1. Caso um cliente proceda à transferência do saldo de uma conta que ele tenha mantido com uma instituição financeira para uma outra, a instituição receptora deve considerar a possibilidade de o gestor de contas anterior possuir suspeitas sobre as actividades do cliente.

2. Se a instituição receptora tiver qualquer razão para suspeitar que o cliente tenha sido rejeitado por outra instituição financeira, deve aplicar procedimentos de diligência reforçada antes de o aceitar.

ARTIGO 40

(Confirmação da identidade por meio de entrevista)

1. As instituições financeiras devem, no caso de contas individuais, assegurar que as provas de identidade sejam obtidas durante o curso de uma entrevista com o cliente, de modo a certificar se o cliente é realmente a pessoa que ele afirma ser e apurar a semelhança entre a pessoa e a fotografia que conste do documento de identidade.

2. No caso de contas conjuntas, as instituições financeiras devem verificar os nomes e endereços de todos os titulares das contas.

3. Os procedimentos de verificação necessários para estabelecer a identidade do cliente devem ser os mesmos, qualquer que seja o tipo de conta, seja conta corrente, de depósito, entre outras.

ARTIGO 41

(Identificação dos funcionários)

O nome do funcionário da instituição que conduziu o processo de abertura da conta e do responsável superior que o autorizou devem constar do arquivo do cliente.

ARTIGO 42

(Controlo de negócios e bens)

As instituições financeiras devem proceder à identificação e verificação das pessoas ou entidades que detenham o controlo sobre os negócios e bens dos clientes.

ARTIGO 43

(Apresentadores de terceiros)

Quando recorram a um ou mais agentes ou apresentadores de terceiros (*third-party introducers*) para estabelecer relações comerciais com clientes, as instituições financeiras são as únicas entidades responsáveis por concluir o *due diligence* para os clientes apresentados.

ARTIGO 44

(Dever de recusa)

1. Sempre que uma instituição financeira não possa obter todas as informações relativas às medidas de diligências necessárias, não deve abrir a conta, iniciar relações comerciais ou realizar a transacção.

2. Nos casos previstos no número anterior, a instituição financeira deve considerar o envio da comunicação de operação suspeita ao GIFiM.

SECÇÃO III

Abertura de contas

Subsecção I

Clientes individuais

ARTIGO 45

(Abertura de conta de clientes individuais)

Nos casos em que o cliente seja uma pessoa singular, a identificação deve ser comprovada pela apresentação de um dos documentos oficiais referidos no Decreto n.º 53/2023, de 31 de Agosto, tendo em atenção a categoria de risco do mesmo.

ARTIGO 46

(Abertura de conta de forma presencial por clientes individuais)

1. A identificação de um cliente individual deve, entre outros elementos referidos no n.º 1 do artigo 10 do Decreto n.º 53/2023, de 31 de Agosto, abranger:

a) o nome;
b) a data de nascimento;
c) o endereço físico;
d) a natureza do negócio;
e) a fonte de rendimento;
f) o nível de conhecimento sobre as transacções financeiras normais; e
g) qualquer relação de representação.

2. O nome de clientes individuais deve ser verificado, através de um documento válido, no decorrer de uma entrevista com o mesmo.

ARTIGO 47

(Confirmação do domicílio)

Para efeitos da alínea *a*) do n.º 1 do artigo 12 do Decreto n.º 53/2023, de 31 de Agosto, consideram-se elementos idóneos para confirmação do domicílio, entre outros, os seguintes:

a) facturas emitidas pelos serviços de fornecimento de energia, água, telefone, *internet*;
b) informação que conste da lista telefónica;
c) extracto recente do cartão de crédito ou débito de uma outra instituição financeira;
d) referência bancária recente; e
e) qualquer outro documento que individualmente ou cumulativamente comprove o endereço do requerente para o negócio, nomeadamente a declaração do bairro e da entidade patronal.

ARTIGO 48

(Formulários para abertura de conta de clientes individuais)

1. O formulário de abertura de conta para cliente individual deve, no mínimo, conter a seguinte informação:

a) nome;
b) endereço permanente actual;
c) endereço para correspondência;
d) número de telefone e fax;
e) endereço electrónico, existindo;
f) data e local de nascimento;
g) nacionalidade;
h) ocupação e nome do empregador (se trabalhador por conta própria, a natureza do auto-emprego e a respectiva confirmação);
i) Número Único de Identificação Tributária (NUIT);
j) Código de Classificador de Actividades Económicas (CAE), tratando-se de empresários;
k) assinatura(s); e
l) autorização para a instituição financeira averiguar e obter referências sobre o cliente.

2. Ao formulário, devidamente preenchido, devem ser anexas cópias legíveis dos documentos usados para efeitos de prova das situações acima referidas.

ARTIGO 49

(Verificação da identidade nos casos de abertura de conta na forma não presencial)

Antes de aceitar a relação de negócios com cliente não presencial, as instituições financeiras devem:

a) adoptar procedimentos de identificação de clientes aplicáveis aos clientes presenciais e, logo que possível, criar condições para a entrevista;
b) adoptar medidas de diligência reforçadas para mitigar o risco inerente ao cliente não presencial; e
c) considerar não realizar operações de débito antes da entrevista.

ARTIGO 50

(Abertura de conta por clientes individuais não residentes)

1. Os clientes individuais não residentes que solicitem a abertura de conta a partir do exterior devem preencher um formulário de candidatura que, no mínimo, contenha a seguinte informação:

a) nome;
b) endereço permanente;
c) endereço actual;
d) número de telefone e número de fax;
e) endereço electrónico, existindo;
f) data e local de nascimento;
g) nacionalidade(s);
h) ocupação e nome do empregador (se trabalhador por conta própria, a natureza do auto-emprego);
i) número, data de emissão e data de validade do passaporte;
j) assinatura(s);
k) carta abonatória da instituição bancária na qual é cliente no país de residência actual;
l) autorização para que a instituição financeira possa averiguar referências sobre o potencial cliente; e
m) autorização da autoridade cambial para abertura da conta no estrangeiro, quando aplicável.

2. O formulário de inscrição, devidamente preenchido, deve ser acompanhado da cópia de passaporte válido e da informação sobre o endereço, confirmado através de original ou cópia autenticada de factura emitida por entidades prestadoras de serviços de terceiros, nomeadamente fornecedores de serviços de energia, água, telefone, *internet*, etc.

3. As instituições financeiras podem, ainda, solicitar, como medidas adicionais relacionadas com a verificação de endereço, a consulta à lista telefónica ou averiguações junto a instituições financeiras ou outras entidades no país de residência do cliente ou ainda consultas à fontes nacionais ou internacionais que a instituição requerida considere idónea.

Subsecção II

Pessoas colectivas

ARTIGO 51

(Abertura de conta por pessoas colectivas)

1. No processo de abertura de conta de pessoas colectivas, as instituições financeiras devem verificar:

a) a identificação dos sócios ou accionistas que detenham o controlo de negócios e activos da empresa;
b) a identificação dos beneficiários efectivos;
c) a identificação dos seus gestores seniores;
d) a identificação de todos os detentores de participação qualificada;
e) a identificação de todos os detentores de participações e direitos de voto de valor igual ou superior a 10%;
f) a identificação das pessoas autorizadas a representar a empresa e os respectivos poderes;
g) o Número Único de Identificação Tributária (NUIT);
h) o Código de Classificador de Actividades Económicas (CAE); e
i) as provas sobre a existência legal da empresa.

2. No processo de identificação e verificação devem ser apresentados os elementos indicados na alínea *b*) do n.º 2 do artigo 11 do Decreto n.º 53/2023, de 31 de Agosto.

3. No caso de associações agropecuárias, os elementos de identificação estipulados no inciso i. da alínea *b*) do n.º 2 do artigo 11 do Decreto n.º 53/2023, de 31 de Agosto são substituíveis por certidão de reconhecimento emitida pelo administrador do distrito ou chefe do posto administrativo da sua sede, nos termos do Decreto-Lei n.º 2/2006, de 3 de Maio.

ARTIGO 52

(Visitas às pessoas colectivas)

Nos cenários de risco elevado, a verificação e as consultas devem ser efectuadas mediante visita às pessoas colectivas, de modo a apurar a sua existência, bem como a inexistência de qualquer processo de dissolução ou liquidação, e confirmar a finalidade económica, nos termos do alvará ou junto da entidade de tutela.

ARTIGO 53

(Procedimentos de monitorização)

1. A diligência do "Conheça o Seu Cliente" nas contas de pessoas colectivas deve ser um processo contínuo à semelhança das contas de clientes individuais.

2. Se houver mudanças na estrutura da pessoa colectiva ou se as suspeitas forem despertadas por uma mudança na natureza do negócio ou no perfil de pagamentos ou recebimentos na conta da pessoa colectiva, outras verificações devem ser efectuadas para determinar a razão das referidas alterações.

ARTIGO 54

(Abertura de conta por pessoas colectivas não residentes)

O processo de identificação e verificação referido nos artigos 51 a 53 deve ser igualmente aplicável, com as necessárias adaptações, às pessoas colectivas não residentes que pretendam abrir conta a partir do exterior.

ARTIGO 55

(Informação de natureza fiscal)

1. As instituições financeiras devem, no momento da abertura de uma conta de depósito bancário, obter informação sobre o Número Único de Identificação Tributária (NUIT) de cada um dos respectivos titulares.

2. O NUIT pode ser comprovado mediante a apresentação do original ou de cópia de documento onde conste aquele número, ou através da recolha e verificação desse elemento de informação junto das entidades responsáveis pela sua gestão.

ARTIGO 56

(Consórcios e sociedades irregulares)

1. Nos casos de empresas constituídas sob a forma de consórcios ou de empresa sem personalidade jurídica, a identificação e verificação das pessoas que detenham o controlo, dos sócios ou accionistas com participação qualificada e dos seus mandatários deve, igualmente, obedecer, com as necessárias adaptações, ao estabelecido nos artigos 45 a 50.

2. As instituições financeiras devem proceder a averiguações para confirmar a verdadeira natureza das actividades de negócio e para verificar se as actividades empresariais em causa possuem um propósito legítimo.

ARTIGO 57

(Clubes e instituições de caridade)

Antes de procederem à abertura de contas para clubes ou instituições de caridade, as instituições financeiras devem:

a) certificar a finalidade legítima da organização;
b) solicitar uma cópia autenticada da constituição do clube ou instituição de caridade; e
c) em caso de dúvida, efectuar uma visita às suas instalações, para conhecer a verdadeira natureza das suas actividades.

ARTIGO 58

(Identificação e verificação de pessoas que detenham o controlo do clube ou da instituição de caridade)

1. A identidade e a verificação das pessoas que detenham o controlo do clube ou da instituição de caridade devem ser determinadas de acordo com os procedimentos necessários para os clientes individuais.

2. As mudanças ocorridas no seio do clube ou da instituição de caridade implicam a realização de novas diligências de identificação e verificação.

ARTIGO 59

(Fundações e associações)

A identificação e verificação de uma fundação ou associação abrange, entre outros, os seguintes elementos:

a) nome;
b) certidão de registo;
c) data e o país de constituição, no caso de entidades estrangeiras;
d) domicílio profissional; e
e) principal local de negócios e operações, se diferente do domicílio profissional.

ARTIGO 60

(Procedimentos de verificação da fundação ou associação)

1. A diligência para a verificação da fundação ou associação é efectuada, nomeadamente, mediante a apresentação de:

a) certidão de registo emitida pela entidade competente;
b) demonstrações financeiras dos últimos dois anos;
c) outras informações adicionais julgadas pertinentes.

2. A identificação das pessoas que dirigem a fundação ou associação abrange os membros da gestão ou de órgão equiparado, especialmente aqueles que tenham autoridade para realizar um negócio ou para dar instruções sobre o uso ou a transferência de fundos ou bens, o fundador, o executor, o protector, o beneficiário e o administrador.

3. Se a fundação ou associação tiver fins de caridade, são-lhe aplicáveis as normas relativas à identificação de clubes e instituições de caridade.

SECÇÃO IV

Pessoas e instituições financeiras estrangeiras

ARTIGO 61

(Bancos correspondentes)

1. Nas relações de negócio com bancos correspondentes, as instituições financeiras devem:

a) reunir informações suficientes sobre os seus correspondentes, para entender a natureza dos seus negócios;
b) determinar, a partir de informações públicas disponíveis, a reputação e a qualidade de regulação e supervisão da instituição, inclusive se ela foi alvo de alguma investigação ou acção relacionada com o branqueamento de capitais, financiamento do terrorismo ou financiamento da proliferação de armas de destruição em massa;
c) avaliar os sistemas de controlo sobre a prevenção de branqueamento de capitais, financiamento do terrorismo ou financiamento da proliferação de armas de destruição em massa e verificar se os mesmos são adequados e eficazes;
d) obter autorização do competente órgão de gestão sénior da instituição, antes de estabelecer novas relações de correspondência; e
e) documentar as responsabilidades de cada instituição, entre outras, em matéria de prevenção ao branqueamento de capitais, financiamento do terrorismo ou financiamento da proliferação de armas de destruição em massa.

2. Para efeitos do disposto na aliena *a*) do n.º 1 do presente artigo, devem ser considerados os seguintes factores:

a) informações sobre a gestão do correspondente;
b) principais actividades de negócios;
c) localização;
d) regime de prevenção e combate ao branqueamento de capitais, financiamento do terrorismo e financiamento da proliferação de armas de destruição em massa; e
e) identificação de terceiros que utilizem os serviços correspondentes.

3. A violação do estabelecido nos números anteriores implica a cessação imediata da relação de negócio.

ARTIGO 62

(Correspondentes de transferência)

No caso de contas correspondentes de transferência (*payable-through accounts*), as instituições financeiras devem assegurar que o banco cliente aplicou as medidas de diligência contínua relativamente ao cliente que tenha acesso directo às contas do banco correspondente e que aquele banco se encontra habilitado a fornecer dados adequados sobre a identificação dos seus clientes, quando tal lhe for solicitado pelo banco correspondente.

ARTIGO 63

(Bancos de fachada)

As instituições financeiras devem, em especial, recusar-se a iniciar ou manter uma relação com o correspondente quando este não tenha presença física e não se integre num grupo financeiro regulamentado (bancos de fachada).

ARTIGO 64

(Países não cooperantes)

1. As instituições financeiras devem aplicar medidas de diligência reforçadas nos casos de uma relação de negócio ou transacções com pessoas colectivas e instituições financeiras de países considerados pelo Grupo de Acção Financeira (GAFI) como não cooperantes, cabendo ao Banco de Moçambique a divulgação, por circular, da referida lista.

2. No âmbito da abordagem baseada no risco, as instituições financeiras devem aplicar medidas reforçadas de vigilância nos casos de relações comerciais ou transacções com pessoas colectivas e instituições financeiras de países identificados como de alto risco na sua avaliação anual de risco ou por outras fontes, como a Avaliação Nacional de Riscos, avaliações sectoriais de riscos, etc.

SECÇÃO V

Pessoas politicamente expostas

ARTIGO 65

(Deveres das instituições financeiras)

Sem prejuízo das disposições constantes em outra legislação, as instituições financeiras devem:

a) adoptar sistemas de gestão de risco adequados para determinar se um potencial cliente, um cliente existente ou o beneficiário efectivo é ou não uma Pessoa Politicamente Exposta (PPE);

b) desenvolver uma política clara, procedimentos de controlos internos adequados e manter-se especialmente vigilantes em relação a relações de negócio com as PPE, com pessoas e empresas que estejam claramente relacionadas ou associadas a eles ou outros clientes de alto risco;

c) adoptar medidas razoáveis para determinar as fontes de riqueza e de recursos do cliente e beneficiários identificados como PPE;

d) obter aprovação da direcção de topo antes de estabelecer uma relação comercial com uma PPE;

e) elaborar uma lista das PPE que gozem de má reputação e actualizá-la regularmente, sempre que necessário, com base em fontes de informação fidedignas, como meios de comunicação/notícias, etc.;

f) publicar na página de *internet* oficial informações sobre as medidas de diligências reforçadas aplicáveis em seus negócios; e

g) identificar as PPE no país em causa e determinar se o cliente possui ou não ligação familiar ou comercial com essas pessoas, sempre que tenham relação de negócios com clientes de países cujas informações públicas e idóneas os retratem como sendo vulneráveis a corrupção.

ARTIGO 66

(Monitoria contínua)

1. As instituições financeiras devem proceder à monitoria contínua, tendo em atenção o facto de os clientes poderem estabelecer conexões com as PPE após a criação da relação comercial.

2. Considerando o facto de que as PPE podem não ser inicialmente identificadas como tal e considerando ainda que os clientes existentes podem, posteriormente, adquirir a qualidade de PPE, a instituição deve proceder a revisões regulares dos seus clientes, com a periodicidade não superior a doze meses.

SECÇÃO VI

Transferências electrónicas

ARTIGO 67

(Transferências electrónicas internacionais)

1. Para garantir que o sistema de transferência electrónica não seja usado para fins ilícitos, sem prejuízo da demais legislação aplicável, as instituições financeiras devem assegurar a existência de informações exactas do ordenante, bem como informações exigidas sobre o beneficiário.

2. As instituições financeiras devem, ainda, incluir, em todas as transferências de fundos, as mensagens relacionadas.

3. As mensagens referidas no número anterior devem permanecer na cadeia da transferência de pagamento até ao seu destino final.

4. A informação que acompanha todas as transferências electrónicas deve incluir:

a) nome do ordenante;

b) número da conta do ordenante, se a conta foi usada para o processamento da operação;

c) endereço do ordenante;

d) número do documento de identificação nacional ou número de identificação de cliente;

e) data e local de nascimento;

f) nome do beneficiário;

g) número de conta do beneficiário, se essa conta for utilizada para o processamento da operação;

h) instituição bancária beneficiária; e

i) valor da transacção.

5. Nos casos de ausência de uma conta, deverá ser incluído o número de referência único da operação que permita sua rastreabilidade.

ARTIGO 68

(Transferências processadas por um intermediário)

1. Sempre que as transferências de fundos sejam processadas por um intermediário e nos montantes definidos na alínea *c*) do n.º 4 do artigo 49 do Decreto n.º 53/2023, de 31 de Agosto, a instituição financeira que actue como intermediária na cadeia de transferências electrónicas deve assegurar que toda a informação sobre o ordenante e o beneficiário que acompanha a transferência seja conservada e, sempre que possível, incluída na mensagem gerada.

2. Caso existam limitações de ordem técnica que impeçam que a informação necessária sobre o ordenante ou o beneficiário que acompanha uma transferência electrónica internacional seja transmitida com a transferência electrónica doméstica correspondente, a instituição financeira intermediária que as recebe deve manter, durante pelo menos dez anos, um registo de toda a informação recebida da instituição financeira ordenante ou de outra instituição financeira intermediária.

ARTIGO 69

(Medidas de controlo)

1. A instituição financeira intermediária deve adoptar medidas de controlo razoáveis para identificar as transferências electrónicas internacionais cuja informação necessária sobre o ordenante ou o beneficiário se encontre omissa.

2. As medidas referidas no número anterior podem incluir o acompanhamento posterior ou em tempo real, sempre que possível.

ARTIGO 70

(Políticas e procedimentos baseados no risco)

A instituição financeira intermediária deve dispor de políticas e procedimentos eficazes baseados no risco para determinar:

a) quando deve executar, rejeitar ou suspender uma transferência electrónica, cuja informação necessária sobre o ordenante ou o beneficiário se encontre omissa; e

b) as actividades adequadas de acompanhamento.

ARTIGO 71

(Comunicação ao Gabinete de Informação Financeira de Moçambique)

A falta de informações completas do ordenante pode ser considerada factor de suspeita e, por consequência, a instituição financeira intermediária deve considerar a possibilidade de comunicação ao GIFiM.

ARTIGO 72

(Restrição ou cessação da relação de negócios)

A instituição financeira beneficiária deve considerar restringir ou até mesmo cessar a sua relação de negócios com instituições financeiras que não cumpram os requisitos referidos nos artigos anteriores.

ARTIGO 73

(Transferências electrónicas nacionais)

1. As transferências electrónicas nacionais devem incluir informação do ordenante, tal como indicado nas transferências electrónicas internacionais, salvo se a informação puder ser disponibilizada pela instituição financeira beneficiária às autoridades competentes, nomeadamente, o GIFiM e autoridades judiciárias.

2. Nos casos referidos no número anterior, a instituição financeira ordenante necessita apenas de incluir o número de conta ou o número de referência único da operação, desde que esse número permita identificar que a operação está associada ao ordenante ou ao beneficiário.

3. A informação referida nos números anteriores deve ser disponibilizada pela instituição financeira ordenante num prazo de três dias úteis, após a recepção do pedido da instituição beneficiária ou das autoridades igualmente referidas no n.º 1.

SECÇÃO VII

Moeda electrónica

ARTIGO 74

(Procedimentos de identificação e verificação)

1. Os procedimentos de identificação de usuários de moedas electrónicas devem prever a verificação da identidade do cliente, independentemente do valor convertido em moeda electrónica com recurso à notas e moeda em circulação (moeda física).

2. Os procedimentos devem ainda prever a implementação de medidas de vigilância reforçadas durante o reembolso ou levantamento de moeda electrónica acima de um limite relevante definido pelo Banco de Moçambique.

ARTIGO 75

(Recolha e armazenamento de informações e dados)

1. Os procedimentos de conversão de moeda electrónica devem incluir a recolha e armazenamento de informações e dados técnicos relativos à activação, carregamento e utilização do dinheiro electrónico por meio de suporte físico, para efeitos da sua rastreabilidade.

2. A instituição financeira deve conservar as informações sobre identificação de clientes e transacções por um prazo mínimo de dez anos, contado da data da cessação da relação de negócio.

SECÇÃO VIII

Monitoria da conta e de transacções

ARTIGO 76

(Monitoria contínua)

A monitoria contínua, como um aspecto essencial para a gestão do risco de branqueamento de capitais, financiamento do terrorismo e financiamento da proliferação de armas de destruição em massa, deve incluir o exame das transacções realizadas no decurso da relação com o cliente para garantir que as mesmas são consentâneas com o conhecimento que a instituição financeira possui do cliente, nomeadamente perfil de negócios e risco.

ARTIGO 77

(Reconstituição das transacções)

1. Para permitir a reconstituição das transacções, as instituições financeiras devem assegurar que os documentos apresentados ou as informações recolhidas, no âmbito das medidas de diligências, são conservados de forma actualizada e são relevantes.

2. O apuramento da relevância é efectuado através da realização de revisões dos registos existentes e da análise das transacções, especialmente para as categorias de clientes ou relações comerciais de risco mais elevado.

ARTIGO 78

(Avaliação do risco)

1. A monitoria deve estar em concordância com a avaliação de risco, devendo, para todas as contas, ter sistemas para detectar padrões complexos, incomuns ou transacções suspeitas.

2. As instituições financeiras devem, no âmbito da avaliação de risco, considerar que alguns tipos de transacções e actividades podem alertá-las sobre a possibilidade de actos de branqueamento de capitais, financiamento do terrorismo e financiamento da proliferação de armas de destruição em massa.

3. Os exemplos de transacções e actividades suspeitas podem ser aprofundados através da consulta às avaliações nacionais e sectoriais de risco, às tipologias de branqueamento de capitais,

financiamento do terrorismo ou financiamento da proliferação de armas de destruição em massa publicados pelo GIFiM, Grupo de Acção Financeira (FATF/GAFI) em http://www.fatf-·gafi.org, organizações regionais do tipo FATF/GAFI e ao Anexo III destas Directrizes.

ARTIGO 79

(Contas de risco elevado)

As instituições financeiras devem intensificar a monitoria das contas de risco elevado, devendo estabelecer indicadores-chave para essas contas, tomando por base a informação conhecida do cliente, como por exemplo:

a) país de origem;
b) fonte(s) de recursos;
c) tipo de transacções envolvidas; e
d) outros factores de risco.

ARTIGO 80

(Sistemas de informação de gestão)

As instituições financeiras devem dispor de sistemas de informação de gestão adequados para fornecer aos gestores e OCOS informações actualizadas necessárias para identificar, analisar e monitorar as contas.

ARTIGO 81

(Procedimentos para a distinção entre transacções ocasionais e relações de negócio)

1. As instituições financeiras devem dotar os seus sistemas de controlo interno de meios e procedimentos para distinguirem os clientes de transacções ocasionais dos demais com quem estabelecem relações de negócio.

2. Nos casos em que, independentemente de qualquer limiar ou relação, o número de operações efectuadas por um cliente evidenciar um padrão de frequência e habitualidade, as instituições financeiras devem considerar estar perante um relacionamento tendencialmente estável e duradouro, qualificando-o, como uma efectiva relação de negócio, para efeitos da adopção dos procedimentos de identificação e diligência devidos, nos termos da legislação atinente à prevenção e combate ao branqueamento de capitais, financiamento ao terrorismo e financiamento de proliferação de armas de destruição em massa.

ARTIGO 82

(Registo centralizado relativos a transacções ocasionais)

1. As instituições financeiras devem dotar os seus sistemas de controlo interno de meios e procedimentos para verificarem a existência de operações aparentemente relacionadas entre si.

2. Na definição dos meios e procedimentos previstos no número anterior, as instituições financeiras devem considerar os seguintes critérios indiciadores da existência de operações relacionadas entre si:

a) os intervenientes envolvidos e a aparente existência de relações entre si;
b) o lapso temporal decorrido entre as operações;
c) a segmentação dos montantes envolvidos;
d) tipo e número de operações efectuadas; e
e) outros critérios que se mostrem adequados à mitigação dos riscos específicos identificados e avaliados pela instituição financeira.

3. Por forma a garantir o efectivo controlo dos limites previstos na legislação atinente ao branqueamento de capitais, financiamento do terrorismo e financiamento da proliferação de armas de destruição em massa, as instituições financeiras devem implementar um registo informatizado e centralizado de todas as transacções ocasionais efectuadas, independentemente do respectivo montante, de modo a identificarem o fraccionamento de operações.

4. As instituições financeiras devem assegurar que o registo referido no número anterior:

a) contém, pelo menos, a data, o valor da operação, o nome ou a denominação completos e o tipo e o número do documento de identificação do cliente;
b) é actualizado sempre que efectuem uma transacção ocasional; e
c) está permanentemente disponível para toda a estrutura organizativa, bem como para os seus agentes, distribuidores e terceiros com funções operacionais.

ARTIGO 83

(Operações próprias)

1. As instituições financeiras devem cumprir os deveres preventivos previstos na legislação atinente ao branqueamento de capitais, financiamento do terrorismo e financiamento da proliferação de armas de destruição em massa relativamente às operações, e respectivas contrapartes, que efectuem:

a) por conta própria; e
b) por conta de terceiros que não revistam a qualidade de cliente.

2. Incluem-se no disposto no número anterior quaisquer operações, por conta própria ou não, entre a instituição financeira e quaisquer outras entidades que integrem o mesmo grupo, fora do âmbito de uma relação de clientela.

3. As instituições financeiras devem definir e adoptar, relativamente às suas relações com as contrapartes, procedimentos de prevenção do branqueamento de capitais, financiamento do terrorismo e da proliferação de armas de destruição em massa que devem assegurar, no mínimo:

a) que não praticam actos de que possa resultar o seu envolvimento em qualquer operação de branqueamento de capitais, de financiamento do terrorismo e de armas de destruição em massa, adoptando todas as medidas adequadas para prevenir tal envolvimento;
b) a obtenção, junto da contraparte, dos elementos necessários a uma adequada gestão do risco de branqueamento de capitais, financiamento do terrorismo e financiamento da proliferação de armas de destruição em massa, podendo ser adoptadas medidas simplificadas, desde que reunidas as condições legais; e
c) a adopção das demais medidas de acompanhamento da contraparte e das operações que se mostrem proporcionais ao risco concretamente identificado.

4. Para efeitos do disposto na alínea *b*) do número anterior, configuram situações indicativas de risco potencialmente reduzido, entre outras que venham a ser identificadas pelas próprias instituições financeiras ou pelo Banco de Moçambique, as seguintes:

a) relações estabelecidas com entidades habilitadas à prática de serviços financeiros com sede ou estabelecimento em países nos quais exista um quadro normativo e de supervisão compatível com o de Moçambique;
b) operações em mercado com garantias adequadas de transparência quanto às informações relativas aos beneficiários efectivos e à titularidade formal das contrapartes;
c) operações entre entidades que integrem o mesmo grupo, quando não existam restrições à circulação de informação e a mesma possa ser obtida para dar resposta aos pedidos recebidos pelas autoridades competentes; e

d) operações estabelecidas com contrapartes que não estejam relacionadas com a prestação de serviços financeiros, incluindo as relações de subcontratação (*outsourcing*).

5. Sempre que as instituições financeiras tomem conhecimento de que uma pessoa singular ou colectiva pretende nela deter uma participação qualificada, na acepção prevista na Lei das Instituições de Crédito e Sociedades Financeiras, previamente à entrada de capital, aquelas devem:

a) obter informações comprovadas sobre a origem dos fundos; e

b) identificar os beneficiários efectivos dos propostos adquirentes.

CAPÍTULO VII

Inovações financeiras

ARTIGO 84

(Políticas e medidas de prevenção)

1. As instituições financeiras devem adoptar as políticas ou medidas necessárias para prevenir o uso indevido de desenvolvimentos tecnológicos em esquemas de branqueamento de capitais, financiamento do terrorismo e de financiamento da proliferação de armas de destruição em massa.

2. As instituições financeiras devem identificar, avaliar e compreender os riscos de branqueamento de capitais, financiamento do terrorismo e de financiamento da proliferação de armas de destruição em massa associados a todos os produtos novos ou pré-existentes, serviços e canais de distribuição e da utilização de novas tecnologias.

ARTIGO 85

Avaliação de risco

As instituições financeiras devem realizar a avaliação de risco antes da introdução de novos produtos, serviços, canais de entrega e tecnologias e devem aplicar as medidas necessárias para gerir eficazmente os riscos de branqueamento de capitais, financiamento do terrorismo e de financiamento da proliferação de armas de destruição em massa associados.

CAPÍTULO VIII

Conservação de documentos

ARTIGO 86

(Registos de identidade)

Toda a documentação exigida pelas instituições financeiras, nos termos das presentes Directrizes e demais legislação aplicável, para verificar a identidade dos clientes e dos beneficiários efectivos deve ser conservada por um período não inferior a dez anos após o encerramento da conta ou cessação da relação de negócio com o cliente em questão.

ARTIGO 87

(Terceirização)

Se a instituição financeira optar pelos serviços de um terceiro para realizar a verificação de procedimentos de identificação ou para confirmar a identidade de clientes, a conservação de documentos deve ser efectuada nos termos do número anterior.

ARTIGO 88

(Registos de transacções)

Os registos de transacções, independentemente da forma como são utilizados, devem ser conservados por um período não inferior a dez anos após a conclusão das operações em causa, de forma a auxiliar na investigação de casos de suspeita de branqueamento de capitais, financiamento do terrorismo, financiamento da proliferação de armas de destruição em massa e devem incluir o seguinte:

a) volume de negócio efectuado através da conta;

b) origem dos fundos, incluindo todos os detalhes do cliente;

c) a forma em que os fundos foram creditados ou debitados da conta;

d) identidade da pessoa que efectua a operação e a identidade do beneficiário efectivo;

e) detalhes da contraparte;

f) destino dos fundos;

g) a forma de instrução;

h) data da transacção;

i) tipo e o número de identificação de qualquer conta envolvida na transacção; e

j) qualquer outra informação que possibilite a reconstituição da transacção.

ARTIGO 89

(Período de conservação de documentos)

O relatório interno sobre a prevenção do branqueamento de capitais, financiamento do terrorismo e financiamento da proliferação de armas de destruição em massa, as comunicações de operações suspeitas, as transacções em numerário, as transacções electrónicas de fundos e em cheque remetidas ao GIFiM devem ser conservados por um período não inferior a dez anos após a data da respectiva elaboração.

ARTIGO 90

(Conservação das constatações)

Sem prejuízo do disposto no artigo anterior, todas as conclusões relativas às transacções complexas, não comuns, suspeitas ou outras que, não tendo aquelas características, façam parte das transacções a serem comunicadas ao GIFiM, devem ser mantidas, por um período não inferior a dez anos, contados da data da respectiva constatação.

ARTIGO 91

(Conservação da informação relativa às investigações em curso)

1. Os registos relacionados com investigações em curso devem ser mantidos até que seja confirmado pelas autoridades competentes que o caso foi encerrado.

2. A confirmação de casos encerrados pelas autoridades deve ser mantida para registo e deve incluir a documentação que informe o motivo do encerramento.

3. As políticas e procedimentos devem delinear critérios e protocolos utilizados para o encerramento dos casos e indicar os registos que podem deixar de ser mantidos.

ARTIGO 92

Conservação das transacções efectuadas por meios electrónicos

Os registos de pagamentos electrónicos e respectivas mensagens devem ser tratados nos termos referidos nos artigos anteriores.

CAPÍTULO IX

Reconhecimento e comunicação de operações suspeitas

ARTIGO 93

(Reconhecimento de operações suspeitas)

1. Os funcionários das instituições financeiras devem receber capacitação e orientação suficientes para reconhecer as operações suspeitas, nos termos estabelecidos no Capítulo X.

2. As questões a serem consideradas para determinar se uma transacção é suspeita, podem ser, exemplificativamente, as seguintes:

a) o volume, quantidade ou frequência das transacções é consistente com as actividades regulares ou antecedentes, padrão e propósito do cliente;
b) a operação é razoável ou justificada no contexto de negócios ou actividades pessoais do cliente;
c) o valor da transacção é compatível com a ocupação profissional e a situação financeira declarada pelo cliente;
d) o padrão de actuação do cliente mudou materialmente em relação ao histórico ou perfil de negócios do cliente;
e) o grau de complexidade e risco da operação é compatível com a qualificação técnica do cliente;
f) quando a transacção é internacional, existe uma razão óbvia para o cliente fazer negócios com o país envolvido; e
g) a transacção faz sentido económica e legalmente, ou aparenta ter apenas a finalidade de ocultar ou tornar obscura outra transacção separada.

ARTIGO 94

(Actualização dos procedimentos internos)

No processo de actualização dos procedimentos internos, a instituição financeira deve sempre considerar os factos e circunstâncias que deram origem a relatórios de transacções suspeitas.

ARTIGO 95

(Tipologias de transacções com alto nível de risco)

As instituições financeiras devem implementar procedimentos adaptados de triagem, identificação e investigação que permitam detectar as tipologias de transacções com alto nível de risco de branqueamento de capitais, financiamento do terrorismo e financiamento da proliferação de armas de destruição em massa constantes do Anexo II do Decreto n.º 53/2023, de 31 de Agosto e Anexo IV das presentes Directrizes.

ARTIGO 96

(Reporte de transacções suspeitas)

Todas as instituições financeiras devem assegurar que:

a) os funcionários, nos seus postos de trabalho, sabem a quem reportar as transacções suspeitas;
b) a cadeia de comunicação é clara, com menor número possível de intervenientes, de modo que as suspeitas sejam repassadas de forma directa e imediata ao OCOS;
c) os procedimentos prevejam que os funcionários que denunciem riscos ou problemas em operações suspeitas estejam totalmente protegidos, isentos de responsabilidade e imunes a quaisquer repercussões; e
d) seja possível a reconstituição da transacção.

ARTIGO 97

(Relatório de comunicação de operações suspeitas)

As instituições financeiras devem ser registadas no sistema informático do GIFiM, passando a ter um número de registo e uma senha de acesso ao formulário, a serem atribuídos ao OCOS.

ARTIGO 98

(Conteúdo da comunicação de transacção suspeita)

Sem prejuízo do estabelecido na legislação sobre prevenção e combate ao branqueamento de capitais, financiamento ao terrorismo e financiamento de proliferação de armas de destruição em massa, cada comunicação de transacção suspeita enviada ao GIFiM, através do formulário, manual ou electrónico, deve ter o seguinte conteúdo:

a) instituição financeira que envia a comunicação;
b) número da conta bancária envolvida na transacção;
c) titular da conta;
d) executor da transacção;
e) valor monetário da transacção;
f) descrição resumida da natureza da transacção e todas as circunstâncias que motivaram a suspeita;
g) relação de negócio entre o suspeito e a instituição financeira;
h) quando o suspeito seja cliente interno da instituição financeira (funcionário), referência a esta qualidade;
i) qualquer declaração voluntária sobre a origem, fonte ou destino dos recursos;
j) impacto da actividade suspeita na credibilidade da instituição ou pessoa que comunica; e
k) nome e assinatura do oficial de comunicação de operação suspeita.

ARTIGO 99

(Responsabilidade do OCOS)

1. O OCOS é responsável por determinar se a informação ou outros assuntos contidos no relatório de transacção que recebeu geram suspeitas razoáveis de que um cliente possa estar envolvido em actos de branqueamento de capitais, financiamento do terrorismo e financiamento da proliferação de armas de destruição em massa.

2. Na avaliação, o OCOS deve considerar todas as informações relevantes disponíveis sobre a pessoa singular ou colectiva a quem o relatório inicial faz referência.

3. O referido no número anterior pode incluir a necessidade de se proceder à revisão de outros padrões de transacções e dos volumes, através dos seguintes elementos:

a) conta ou contas no mesmo nome;
b) duração da relação de negócio; e
c) registos de identificação efectuados.

4. Se, depois de concluir a revisão, decidir que existem factos suspeitos, o OCOS deve imediatamente comunicar ao GIFiM.

5. No reporte de transacções suspeitas e no exercício de toda a sua função, o OCOS deve agir de forma honesta e racional e deve formular o seu juízo na base de boa-fé.

ARTIGO 100

(Procedimento de relatórios internos)

1. Para garantir a rapidez e sigilo, o canal de comunicação de transacções suspeitas deve ser o mais curto possível, com um número mínimo de intervenientes entre o funcionário que detecta a suspeita e o OCOS.

2. O funcionário que detecta a suspeita pode primeiro discutir com o OCOS e, em seguida, preparar o relatório inicial e enviá-lo, devendo aquele acusar a sua recepção.

3. O relatório deve incluir detalhes completos do cliente, o seu perfil, extractos de contas, se necessário, e o relato completo quanto possível dos motivos que deram origem à suspeita.

4. Todas as transacções suspeitas comunicadas ao OCOS devem ser documentadas.

ARTIGO 101

(Investigações)

1. Todas as investigações internas feitas em relação ao relatório, bem assim a razão que determinou o seu envio ou não ao GIFiM, devem ser documentadas.

2. A informação referida no número anterior pode ser necessária para completar o relatório inicial ou como evidência de boas práticas, se, em algum momento futuro, houver uma investigação sobre um caso que o OCOS tenha optado por não comunicar, vindo posteriormente as suspeitas a confirmar-se.

ARTIGO 102

(Formato)

O formato padrão de comunicação de operações suspeitas é concebido e definido pelo GIFiM, devendo todas as instituições financeiras agir nos termos determinado por este.

CAPÍTULO X

Selecção e formação de funcionários e agentes

SECÇÃO I

Selecção

ARTIGO 103

(Selecção de funcionários)

1. As instituições financeiras devem, na sua política de contratação, adoptar procedimentos de verificação, de modo a garantir um elevado padrão na contratação de funcionários.

2. No momento do recrutamento, as instituições financeiras devem procurar obter referências apropriadas.

ARTIGO 104

(Recrutamento de agentes)

1. Caso as instituições financeiras contratem agentes ou distribuidores para alguns dos seus produtos e serviços, eles devem ser submetidos a procedimentos de triagem para avaliar seu carácter e idoneidade (*fit and proper*).

2. Para efeitos do estabelecido no número anterior, as instituições de moeda electrónica devem submeter, numa base anual, os super-agentes aos referidos procedimentos de triagem.

SECÇÃO II

Formação de funcionários

ARTIGO 105

(Programa de formação contínua)

As instituições financeiras devem implementar um programa de formação contínua para os seus funcionários, no que concerne a programas e práticas de gestão de risco.

ARTIGO 106

(Requisitos para diferentes categorias de funcionários)

1. Todos os funcionários devem receber formação sobre a prevenção e combate ao branqueamento de capitais, financiamento do terrorismo e financiamento da proliferação de armas de destruição em massa, relativa ao quadro legal e regulamentar vigente em Moçambique, aos normativos internacionais que regulem a matéria e sobre as tendências e os desenvolvimentos no que respeita às práticas inerentes.

2. Todos os funcionários devem ainda receber formação sobre a avaliação e gestão de risco.

3. Os funcionários com responsabilidade de abertura de conta e aceitação de novos clientes devem receber formação no que diz respeito à identificação e aos procedimentos de verificação da identidade dos clientes.

4. Os funcionários devem, igualmente, estar familiarizados com o reconhecimento e manuseio de transacções suspeitas, assim como com os procedimentos de comunicação de operações suspeitas internas.

ARTIGO 107

Formação de membros do conselho de administração)

1. Os membros de conselhos de administração, órgãos equiparados e demais gestores das instituições financeiras devem receber formação sobre todos os aspectos do processo de prevenção ao branqueamento de capitais, financiamento do terrorismo e financiamento da proliferação de armas de destruição em massa.

2. Entre outros conteúdos, a formação dos membros de conselhos de administração, órgãos equiparados e demais gestores das instituições financeiras deve incluir:

a) políticas de gestão de risco;
b) sanções decorrentes da Lei nos casos de falta de comunicação;
c) exclusão de responsabilidades em casos de reporte;
d) procedimentos de comunicação interna;
e) requisitos para a verificação da identidade;
f) manutenção de registos;
g) alocação de recursos para prevenção; e
h) consulta das Listas Designadas.

ARTIGO 108

(Formação do oficial de comunicação de operações suspeitas)

Para além da capacitação geral sobre a prevenção do branqueamento de capitais, financiamento do terrorismo e financiamento da proliferação de armas de destruição em massa, o OCOS deve beneficiar de formação que inclua:

a) todos os aspectos da inteligência financeira;
b) políticas internas aplicáveis em suas instituições;
c) reconhecimento de transacções suspeitas;
d) instrução inicial e contínua sobre a validação e comunicação de operações suspeitas;
e) regime de retorno da informação suspeita encaminhada;
f) novas tipologias e tendências do tipo legal de crime.

ARTIGO 109

(Funcionários recém-admitidos)

1. Os funcionários recém-admitidos devem, logo que possível, beneficiar de formação geral sobre a prevenção ao branqueamento de capitais, financiamento do terrorismo e financiamento da proliferação de armas de destruição em massa e sobre os procedimentos internos adoptados para o reporte de operações suspeitas.

2. Os funcionários referidos no número anterior devem, igualmente, ter acesso a toda a legislação e às políticas e procedimentos da instituição sobre a prevenção do branqueamento de capitais, financiamento do terrorismo e financiamento da proliferação de armas de destruição em massa.

ARTIGO 110

(Front-office)

1. Os funcionários do *front-office* devem receber formação adicional para conhecer a verdadeira identidade do cliente e para obter informação suficiente sobre o tipo de actividades comerciais esperadas do cliente, para que estejam atentos a qualquer mudança no padrão das suas transacções ou a circunstâncias que possam constituir conduta criminosa.

2. Os funcionários do *front-office* devem, igualmente, receber formação sobre o reconhecimento e manuseio de operações suspeitas e sobre os procedimentos a adoptar quando uma transacção é considerada suspeita.

ARTIGO 111

(Transferências electrónicas)

Os funcionários que procedam a transferências electrónicas devem receber formação adicional sobre os riscos de branqueamento de capitais, financiamento do terrorismo e financiamento da proliferação de armas de destruição em massa inerentes à actividade e sobre as medidas preventivas a estas aplicáveis.

ARTIGO 112

(Formação de agentes e distribuidores)

1. Os agentes e distribuidores devem beneficiar de uma formação e informação regular sobre prevenção do branqueamento de capitais, financiamento do terrorismo e financiamento da proliferação de armas de destruição em massa adaptada às suas actividades.

2. Todos os agentes, distribuidores e outras pessoas que actuem em nome e por conta da instituição financeira, em contacto com os clientes, devem ser rastreados, monitorados, informados e formados, no mínimo anualmente, para factores de risco específicos de branqueamento de capitais, financiamento do terrorismo e financiamento da proliferação de armas de destruição em massa, incluindo procedimentos operacionais para as actividades inerentes à sua função.

ARTIGO 113

(Curso de reciclagem)

Numa base anual, as instituições financeiras devem garantir formação para que os seus funcionários e agentes não se esqueçam das suas responsabilidades.

ARTIGO 114

(Registos)

As instituições financeiras devem manter o registo de todas as formações concedidas aos seus funcionários e agentes, incluindo:

a) data de realização;
b) entidade formadora;
c) duração (em horas);
d) natureza (formação interna ou externa);
e) ambiente (formação presencial ou à distância);
f) o conteúdo e material didático de suporte;
g) nome e função dos formandos (internos e externos); e
h) avaliação final dos formandos, quando exista.

ARTIGO 115

(Auditoria interna)

A auditoria interna deve testar a eficácia da formação anual em matéria de prevenção do branqueamento de capitais, financiamento do terrorismo e financiamento da proliferação de armas de destruição em massa de todo o pessoal relevante da instituição financeira, incluindo os membros do conselho de administração ou órgão equiparado.

CAPÍTULO XI

Supervisão baseada no risco e medidas restritivas

ARTIGO 116

(Comunicações)

1. Para a condução da supervisão baseada no risco de branqueamento de capitais, financiamento do terrorismo e financiamento da proliferação de armas de destruição em massa, as instituições financeiras devem reportar anualmente, ao Banco de Moçambique, até ao dia trinta e um de Janeiro seguinte ao ano a que diz respeito, informações relativas aos dados quantitativos e qualitativos.

2. Sem prejuízo do referido no número anterior, em função de perfil de risco de cada instituição, bem como outros factores ponderados, o Banco de Moçambique pode determinar prazos mais curtos ou longos para a prestação da informação exigida.

3. Os dados referidos no n.º 1 do presente artigo devem ser transmitidos em formato Excel, nos termos do Anexo V.

ARTIGO 117

(Listas designadas)

1. Para cumprimento do disposto na legislação atinente ao branqueamento de capitais, financiamento do terrorismo e financiamento de armas de destruição em massa, as instituições financeiras devem dispor de mecanismos permanentes, rápidos e seguros que garantam uma execução imediata, plena e eficaz das medidas restritivas e permitam, pelo menos:

a) a detecção de quaisquer pessoas ou entidades identificadas em medidas restritivas;
b) o bloqueio ou a suspensão da realização de operações ou conjunto de operações, quando a instituição financeira deva dar cumprimento às obrigações de congelamento decorrentes das sanções financeiras; e
c) a existência de canais de comunicação e procedimentos fiáveis, seguros e eficazes, que garantam a adequada execução do dever de comunicação e assegurem a existência de uma estreita cooperação com as autoridades competentes nacionais.

2. As instituições financeiras devem monitorar, através de avaliações periódicas e independentes, o correcto funcionamento dos meios e mecanismos implementados, destinados a assegurar o cumprimento das medidas restritivas.

3. Compete ao OCOS:

a) garantir o conhecimento imediato e pleno e a actualização permanente das listas de pessoas e entidades, emitidas ou actualizadas ao abrigo das medidas restritivas;
b) acompanhar, em permanência, a adequação, a suficiência e a actualidade dos meios e mecanismos destinados a assegurar o cumprimento das medidas restritivas;
c) cumprir as obrigações de notificar previamente, de comunicar e de realizar pedidos prévios de autorização para a execução de transferências de fundos;
d) monitorar à execução das medidas de congelamento e o registo das mesmas;
e) cumprir o dever de comunicação;
f) denunciar as situações que configurem violação; e
g) desempenhar o papel de interlocutor com as autoridades competentes nacionais, assegurando o cumprimento do dever de colaboração.

4. O cumprimento dos deveres previstos nas alíneas *c*) a *f*) do número anterior deve constar de documento ou registo escrito e estão sujeitas ao dever de conservação.

5. Sempre que as instituições financeiras decidam não proceder à execução das medidas restritivas, devem fazer constar de documento ou registo escrito, em conformidade com o disposto no número anterior:

a) os fundamentos da decisão de não execução; e
b) a referência a quaisquer eventuais contactos informais que, no processo de tomada de decisão, tenham sido estabelecidos com as autoridades competentes, com indicação das respetivas datas e meios de comunicação utilizados.

CAPÍTULO XII

Disposições específicas aplicáveis às instituições de transferência de fundos e instituições de moeda electrónica

SECÇÃO I

Disposições iniciais

ARTIGO 118

(Âmbito)

Sem prejuízo do disposto nos capítulos anteriores, o presente Capítulo estabelece as disposições especialmente aplicáveis às instituições de transferência de fundos e instituições de moeda electrónica e às respectivas actividades, qualquer que seja o modo de transmissão utilizado, constituindo medidas de diligência adicional.

ARTIGO 119

(Nomeação de representantes em Moçambique)

As instituições de transferência de fundos que operam em Moçambique a partir de jurisdição estrangeira devem nomear um representante em Moçambique encarregado, nomeadamente, de responder aos pedidos das autoridades de supervisão e das autoridades responsáveis pelo combate ao branqueamento de capitais, financiamento do terrorismo e financiamento da proliferação de armas de destruição em massa.

ARTIGO 120

(Sistema de mapeamento e monitoria de riscos)

1. As instituições de transferência de fundos devem:

a) estabelecer um mapeamento de risco específico para as suas operações em, de e para Moçambique e implementar métodos adaptados para identificar as transacções potencialmente suspeitas; e

b) colocar em prática uma monitoria consolidada, incluindo todas as transacções em, de e para Moçambique, independentemente da rede de agências bancárias, agentes ou jurisdições por onde essas transacções passam.

2. As características do sistema de mapeamento e monitoria de riscos devem ser objecto de relatório enviado anualmente ao Banco de Moçambique.

3. O relatório referido no número anterior deve, nomeadamente:

a) descrever as características do mapeamento de risco e do sistema de detecção de transacções suspeitas;

b) indicar os resultados da monitorização, em termos de alertas, transacções analisadas, transacções comunicadas às redes bancárias ou aos agentes; e

c) indicar as operações comunicadas às autoridades responsáveis pelo combate ao branqueamento de capitais, financiamento do terrorismo e financiamento da proliferação de armas de destruição em massa.

SECÇÃO II

Agentes

ARTIGO 121

(Idoneidade dos agentes)

1. As instituições de transferência de fundos e instituições de moeda electrónica que operem em Moçambique, devem assegurar, permanentemente, a idoneidade dos agentes através dos quais operam em Moçambique.

2. Para efeitos do disposto no número anterior, as instituições referidas devem:

a) avaliar anualmente o modelo de negócio baseado em agentes;

b) estabelecer os critérios que podem eventualmente conduzir à suspensão ou cessação da relação de negócios com os agentes; e

c) implementar um sistema de controlo interno e auditoria interna adequados.

3. A suspensão e a cessação da relação de negócio com os agentes devem ser comunicadas ao GIFiM.

ARTIGO 122

(Treinamento)

1. As instituições de transferência de fundos e instituições de moeda electrónica devem assegurar a formação dos seus agentes.

2. As instituições de transferência de fundos e instituições de moeda electrónica devem rescindir os contratos de todos agentes que não tenham efectuado formações em matéria de branqueamento de capitais, financiamento do terrorismo e financiamento da proliferação de armas de destruição em massa por mais de um ano.

ARTIGO 123

(Operações anómalas)

As instituições de transferência de fundos e instituições de moeda electrónica devem assegurar que todos os agentes cujo saldo entre as operações enviadas e as operações recebidas apresentem anomalias, no que diz respeito à tipologia geral das operações de transferência de fundos, prestem o devido esclarecimento e, se necessário, devem suspendê-los ou rescindir os contratos se os esclarecimentos não forem prestados atempadamente ou não forem satisfatórios.

ARTIGO 124

(Lista actualizada de agentes)

As instituições de transferência de fundos e instituições de moeda electrónica devem manter actualizada uma lista dos seus agentes e redes dentro ou fora de Moçambique, existindo, e, em caso de pedido, fornecer acesso completo e imediato às listas as autoridades competentes.

ARTIGO 125

(Agentes estrangeiros)

1. Caso uma instituição de transferência de fundos possua redes ou agentes estrangeiros, é obrigada a garantir que aqueles apliquem as medidas relevantes de forma consistente com os requisitos de prevenção e combate ao branqueamento de capitais, financiamento do terrorismo e financiamento da proliferação de armas de destruição em massa estabelecidos nas leis moçambicanas e nas regras e regulamentos emitidos ao abrigo dessas leis.

2. Quando os requisitos mínimos de prevenção e combate ao branqueamento de capitais, financiamento do terrorismo e financiamento da proliferação de armas de destruição em massa de uma jurisdição estrangeira forem menos rigorosos que os de Moçambique, ou em caso de ausência dos mesmos, a instituição de transferência de fundos deve aplicar os requisitos da jurisdição moçambicana.

ARTIGO 126

(Responsabilidade)

As instituições de transferência de fundos e as instituições de moeda electrónica são responsáveis por todas as transacções processadas pelos agentes por si contratadas.

SECÇÃO III

Redes bancárias

ARTIGO 127

(Coordenação interinstitucional)

As instituições de transferência de fundos e as instituições de moeda electrónica que operam em Moçambique através de redes bancárias devem assegurar uma coordenação adequada do seu mapeamento de risco e do seu quadro de monitorização ao branqueamento de capitais, financiamento do terrorismo e financiamento da proliferação de armas de destruição em massa com o desenvolvido pelas suas contrapartes bancárias para as suas próprias operações.

ARTIGO 128

(Critérios de busca e identificação de transacções suspeitas)

As instituições de transferência de fundos e as instituições de moeda electrónica devem garantir que os critérios de busca e identificação de transacções suspeitas sejam consistentes e abranjam todas as tipologias de branqueamento de capitais, financiamento do terrorismo e financiamento da proliferação de armas de destruição em massa.

ARTIGO 129

(Comunicação ao gabinete de informação financeira de Moçambique)

1. As instituições de transferência de fundos e as instituições de moeda electrónica devem comunicar ao GIFiM quaisquer transacções em dinheiro ou transferências electrónicas de fundos de montante superior ao estabelecido no n.º 3 do artigo 44 da Lei n.º 14/2023, de 28 de Agosto, ou o seu equivalente em qualquer outra moeda estrangeira.

2. O valor referido no número anterior pode ser referente a uma única transacção ou ao valor agregado de várias transacções efectuadas por uma pessoa, no prazo de um mês.

3. No caso de moeda electrónica, o valor referido no número anterior pode consistir no agregado da utilização de uma ou mais contas de moeda electrónica registadas com o nome e ou endereço da mesma pessoa.

ARTIGO 130

(Contas de moeda electrónica)

1. As instituições de moeda electrónica devem ser capazes de identificar o número de contas de moeda electrónica tituladas por cada cliente, as respectivas particularidades e os detalhes de registo ou inscrição.

2. As instituições de moeda electrónica podem vincular as contas tituladas pelos clientes ao valor total das transacções realizadas em qualquer período.

ARTIGO 131

(Fornecimento de informação)

1. As instituições de transferência de fundos devem fornecer ao Banco de Moçambique informação sobre:

a) a estrutura de propriedade e gestão, quando inclui qualquer envolvimento de PPE;

b) a natureza da sua base de clientes e dos seus agentes; e

c) as áreas geográficas em que opera.

2. A informações referidas no número anterior devem fazer parte de um relatório de actividade e de risco enviado anualmente ao Banco de Moçambique, até ao dia 31 de Janeiro.

ARTIGO 132

(Sistema de informação de gestão)

1. As instituições de transferência de fundos devem dispor de um Sistema de Informação de Gestão (SIG) electrónico adequado.

2. Para efeitos das presentes Directrizes, o SIG é um sistema de informação utilizado para tomada de decisões, processamento de transacções, escrituração, coordenação, controlo interno, auditoria e visualização de informações e toda a organização para complementar o processo de identificação e verificação de clientes.

3. O SIG deve fornecer regularmente informação atempada, de modo a permitir às instituições de transferência de fundos que reportem e detectem qualquer irregularidade nas operações ou qualquer actividade suspeita.

ARTIGO 133

(Avaliação de risco)

Sem prejuízo das disposições do Capítulo IX, as instituições de transferência de fundos devem implementar uma avaliação de risco adequada, mapeamento de risco e quadro de monitoria para mitigar os riscos específicos das suas actividades.

CAPÍTULO XIII

Disposições específicas aplicáveis aos operadores de microfinanças

ARTIGO 134

(Âmbito)

Sem prejuízo das disposições constantes dos Capítulos I a XI, o presente Capítulo é aplicável às cooperativas de crédito, organizações de poupança e empréstimo e operadores de microcrédito e às respectivas actividades.

ARTIGO 135

(Isenções)

As instituições de microfinanças podem beneficiar de isenções de aplicação de determinadas disposições das presentes Directrizes quando:

a) tenham efectuado uma avaliação dos riscos de branqueamento de capitais, financiamento do terrorismo e financiamento da proliferação de armas de destruição em massa, de acordo com as condições estabelecidas no artigo 134, e constatado um baixo nível de risco;

b) a sua actividade consista na prestação de produtos ou serviços financeiros adequadamente definidos e limitados a clientes de baixo risco, de forma a aumentar o índice de inclusão financeira, tais como a conta básica ou simplificada; e

c) obtenham autorização do Banco de Moçambique para aplicar um regime de diligência simplificado aos clientes de baixo risco, sendo aos restantes aplicáveis as medidas de diligência normais.

ARTIGO 136

(Avaliação de risco)

1. A avaliação de risco deve basear-se numa abordagem holística e considerar vários elementos, incluindo, principalmente, os riscos inerentes aos produtos e o perfil das pessoas de baixa renda, sem acesso aos serviços financeiros ou com acesso muito restrito.

2. Os operadores de microfinanças não podem classificar seus clientes como de menor risco apenas pelo facto de serem pessoas singulares de baixa renda, que estão prestes a ser ou foram recentemente integradas ao sistema financeiro regulado ou que estão excluídas financeiramente.

3. Para os riscos associados à natureza digital de um determinado produto ou serviço, incluindo produtos envolvendo novas tecnologias ou canais de distribuição por meio de novas tecnologias e serviços, entre os quais a banca *online*, a avaliação de risco tem que considerar, entre outros, os seguintes factores:

a) a não presença de relações presenciais, tendo em conta as salvaguardas aplicadas;
b) a abrangência geográfica;
c) as formas de financiamento e o acesso ao numerário; e
d) a segmentação de serviços entre várias partes para a execução de pagamentos.

ARTIGO 137

(Medidas de diligências simplificadas)

1. Os operadores de microcrédito e Organizações de Poupança e Empréstimo que sejam autorizados pelo Banco de Moçambique podem aplicar um regime de diligência simplificado aos clientes cuja actividade não seja superior, mensalmente, ao limite de 30.000,00 MT e, anualmente, ao limite de 240.000,00 MT.

2. No caso de titulares de contas, os operadores de microfinanças acima referidos apenas podem aplicar o regime de diligência simplificado se a conta nele aberta for a única que o cliente possui no sistema financeiro.

3. As cooperativas de crédito podem aplicar um regime de diligência simplificado aos clientes que sejam titulares de conta bancária básica, nos termos dispostos em legislação específica.

4. Todos os outros clientes que não se enquadrem no previsto nos números anteriores estão sujeitos à aplicação de medidas de diligências normais.

ARTIGO 138

(Regime simplificado de identificação e verificação)

1. O regime simplificado de diligência consiste em:

a) recolher o nome completo do cliente;
b) recolher o tipo e o número do documento de identificação do cliente; e
c) utilizar, para o registo do cliente, o Número Único de Identificação Bancária (NUIB).

2. Durante o prazo referido no n.º 2 do artigo 139, o processo de identificação dos clientes pode consistir na recolha de duas testemunhas idóneas e outras possíveis provas da identidade dos clientes, previamente comunicadas ao Banco de Moçambique.

3. Em relação à concessão de créditos, o operador de microfinanças deve tomar todas as medidas razoáveis para verificar se as garantias apresentadas não resultam de um produto de crime.

ARTIGO 139

(Casos excepcionais)

1. Os operadores de microfinanças podem aplicar um regime simplificado de diligência a indivíduos formalmente reconhecidos como refugiados e requerentes de asilo em Moçambique.

2. Os clientes que, comprovativamente, não possuem qualquer documento de identificação podem estabelecer relações de negócios com os operadores de microfinanças para abertura de contas temporárias que não podem ser mantidas por mais de três meses.

3. As contas referidas no número anterior aplica-se com as necessárias adaptações o disposto no n.º 13 do artigo 15 da Lei n.º 14/2023, de 28 de Agosto.

4. Nos casos referidos no número anterior, os operadores de microfinanças devem adoptar e implementar um processo apropriado de identificação com base em testemunhos de pessoas idóneas ou outras evidências.

ARTIGO 140

Beneficiário efectivo

1. Se o cliente individual ou um membro da sua família estreitamente relacionado não aparentar ser o beneficiário efectivo, aquele não deve ser tratado como de menor risco.

2. Nos casos referidos no número anterior, os operadores de microfinanças devem aplicar medidas de diligências normais ou reforçadas, de acordo com a avaliação do risco associado ao caso particular.

ARTIGO 141

(Excepções)

1. Os operadores de microfinanças que sejam autorizados pelo Banco de Moçambique a aplicar o regime simplificado de diligência podem:

a) em derrogação ao artigo 29, abster-se de estabelecer um *rating* dos clientes particulares;
b) como excepção ao artigo 30, abster-se de implementar um sistema de gestão de *triggers* para avaliar a aceitação do cliente;
c) como excepção ao artigo 35, abster-se de solicitar provas para confirmação e verificação de identidade;
d) como excepção ao artigo 46, abster-se de recolher informações sobre a fonte de rendimento de seus clientes natureza do negócio;
e) em derrogação ao artigo 47, abster-se de solicitar comprovativos como factura de água, energia ou referência bancária, etc.;
f) como excepção ao artigo 48, abster-se de solicitar comprovativo de telefone, empregador, actividade económica, etc.; e
g) como excepção ao artigo 95, abster-se de implementar ferramentas automatizadas de perfil e filtragem de Tecnologia de Informação para detectar transacções potencialmente suspeitas.

2. O disposto no número anterior não afasta o dever de os operadores de microfinanças:

a) formarem todo o seu pessoal; e
b) estabelecerem procedimentos adaptados de rastreio, identificação e investigação por forma a detectar as tipologias de operações de elevado risco de branqueamento de capitais, financiamento do terrorismo e financiamento da proliferação de armas de destruição em massa, nos termos das presentes Directrizes.

CAPÍTULO XIV

Disposições específicas aplicáveis aos prestadores de serviços de activos virtuais

ARTIGO 142

(Âmbito de aplicação)

Sem prejuízo das disposições constantes dos Capítulos I a XI das presentes Directrizes, o presente Capítulo aplica-se, em especial, aos prestadores de serviços de activos virtuais.

ARTIGO 143

(Nomeação de representantes)

Os prestadores de serviços de activos virtuais que operam em Moçambique, a partir de uma jurisdição estrangeira, devem nomear um representante em Moçambique, encarregado, nomeadamente, de responder aos pedidos das autoridades de supervisão e das autoridades responsáveis pelo combate ao branqueamento de capitais, financiamento do terrorismo e financiamento da proliferação de armas de destruição em massa.

ARTIGO 144

(Mapeamento e monitoria de riscos)

1. Os prestadores de serviços de activos virtuais devem estabelecer um mapeamento de risco específico para as suas operações em, de e para Moçambique e implementar métodos adequados para identificar as transacções potencialmente suspeitas.

2. O mapeamento de risco e as características da estrutura de monitoria referidos no número anterior devem ser comunicados ao Banco de Moçambique por via de um relatório anual, na forma e prazos estabelecidos por Circular do Banco de Moçambique.

ARTIGO 145

(Agentes)

1. Os prestadores de serviços de activos virtuais que operam em Moçambique, devem assegurar, permanentemente, a idoneidade dos seus agentes.

2. Os prestadores de serviços de activos virtuais são responsáveis por todas as transacções processadas pelos seus agentes.

ARTIGO 146

(Formação de agentes)

Os prestadores de serviços de activos virtuais devem assegurar a formação dos seus agentes em matéria de prevenção e combate ao branqueamento de capitais, financiamento do terrorismo e financiamento da proliferação de armas de destruição em massa.

ARTIGO 147

(Rescisão de contratos)

1. Os prestadores de serviços de activos virtuais devem rescindir os contratos de todos agentes que não tenham efectuado formações em matéria de branqueamento de capitais, financiamento do terrorismo e financiamento da proliferação de armas de destruição em massa por um período superior a um ano.

2. Os prestadores de serviços de activos virtuais devem estabelecer os critérios que conduzam à rescisão dos contratos dos agentes.

ARTIGO 148

(Programas e sistemas)

1. Os prestadores de serviços de activos virtuais devem possuir e manter programas e sistemas de prevenção e combate ao branqueamento de capitais, financiamento do terrorismo e financiamento da proliferação de armas de destruição em massa adequados para gerir e mitigar os seus riscos.

2. Os prestadores de serviços de activos virtuais devem possuir sistemas com capacidade de assinalar, para análise, quaisquer movimentos incomuns ou suspeitos de fundos, transacções ou actividades que sejam indicativos de potencial envolvimento em actividade ilícita, independentemente das transacções ou actividades serem de natureza fiduciária, virtual para virtual, fiduciária para virtual ou vice-versa.

ARTIGO 149

(Sistema de informação de gestão)

Os prestadores de serviços de activos virtuais devem dispor de um SIG electrónico adequado, nos termos previstos no artigo 129 das presentes Directrizes.

ARTIGO 150

(Controlo interno)

Os prestadores de serviços de activos virtuais devem possuir sistemas de controlo interno que incluam regras de governação corporativa apropriadas que permitam:

a) reforçar os requisitos de controlo para situações ou actividades de maior risco envolvendo activos virtuais;

b) aplicar medidas de diligência reforçadas, quando necessárias;

c) identificar, compreender e avaliar os riscos de branqueamento de capitais, financiamento do terrorismo e financiamento da proliferação de armas de destruição em massa existentes em relação aos activos virtuais;

d) identificar, compreender e avaliar os riscos de branqueamento de capitais, financiamento do terrorismo e financiamento da proliferação de armas de destruição em massa relacionados com as actividades ou operações financeiras de activos virtuais e dos prestadores de serviços de activos virtuais, com foco para activos virtuais potencialmente de maior risco; e

e) adoptar medidas destinadas a mitigar efectivamente os riscos referidos nas alíneas *c*) e *d*) do presente artigo.

ARTIGO 151

(Avaliação e mapeamento de risco)

1. A avaliação de risco pelos prestadores de serviços de activos virtuais é obrigatória e tem em conta todos os factores de risco que aquelas instituições financeiras e as autoridades competentes considerem relevantes, incluindo:

a) tipos de serviços, produtos ou transacções;

b) produtos, serviços ou operações que envolvam a utilização de numerário ou outros meios não rastreáveis;

c) natureza e escopo de cada canal de distribuição utilizado, incluindo quando se trate de circuito "aberto" ("*open-loop*") ou "fechado" (*closed-loop*);

d) risco do cliente;

e) emitente de cada activo virtual disponibilizado;

f) valor total dos activos virtuais disponibilizados;

g) número e valor de operações com activos virtuais;

h) execução de transferências de activos virtuais com origem em, ou destino a endereços auto-alojados (*self-hosted addresses*);

i) factores geográficos;

j) tipos de activos virtuais a serem disponibilizados e as características principais de cada um, incluindo se os mesmos são de algum modo susceptíveis de ofuscar a identidade, bem como os protocolos utilizados e a susceptibilidade de estes serem alterados a serem disponibilizados e as características principais de cada um;

k) se e em que medida os canais de distribuição dos produtos e serviços com activos virtuais interagem com, ou estão ligados a canais de distribuição de produtos e serviços em moeda fiduciária;

l) robustez do programa de *compliance* dos prestadores de serviços de activos virtuais; e

m) recurso a outros prestadores de serviços para disponibilização de produtos, serviços e operações.

2. Ao determinar o nível de risco, nos termos do número anterior, os prestadores de serviços de activos virtuais devem ter em consideração a extensão em que os usuários podem usar activos virtuais ou recorrer a prestadores de serviços de activos virtuais globalmente, para fazer pagamentos ou transferência de fundos.

3. Sem prejuízo das disposições do Capítulo IX das presentes Directrizes, para além da realização de uma avaliação de risco adequada, os prestadores de serviços de activos virtuais devem implementar um mapeamento de risco e um quadro de monitoria para seguir os riscos específicos das suas actividades, em particular, de entre outros potenciais, os identificados no Anexo VII das presentes Directrizes.

ARTIGO 152

(Dever de identificação e verificação)

1. Os prestadores de serviços de activos virtuais devem adoptar medidas de diligência sempre que efectuem uma transacção ocasional, em conformidade com os requisitos do Capítulo VI das presentes Directrizes.

2. Quando não for possível aplicar o nível adequado de diligência, o prestador de serviços de activos virtuais não deve estabelecer uma relação de negócio ou realizar a transacção ocasional e deve cessar a relação de negócio existente e comunicar a transacção suspeita ao GIFiM.

ARTIGO 153

(Informações adicionais)

Os prestadores de serviços de activos virtuais devem recolher informações adicionais sobre seus clientes, específicas da actividade, para além das medidas de diligência exigidas nos termos do Capítulo VI das presentes Directrizes, nomeadamente:

a) endereço IP (Internet Protocol) com carimbo temporal associado;
b) dados de geo-localização;
c) identificadores de dispositivos; e
d) endereços da carteira de activos virtuais.

ARTIGO 154

(Medidas de diligência reforçada)

1. As medidas de diligência reforçada devem ser aplicadas sempre que uma transacção seja considerada de alto risco.

2. Nos termos do número anterior, podem ser considerados indicadores de alto risco, de entre outros, os seguintes:

a) países ou áreas geográficas identificadas por fontes credíveis como financiadores ou apoiantes de actividades terroristas ou que neles operam organizações terroristas;
b) países identificados por fontes credíveis como tendo índices significativos de crime organizado, corrupção ou outras actividades criminosas, incluindo países de origem ou trânsito de drogas ilegais, tráfico de seres humanos, contrabando e jogos de fortuna e azar ilegais;
c) países sujeitos a sanções, embargos ou medidas similares emitidas por organizações internacionais, como a Organização das Nações Unidas; e
d) países identificados por fontes credíveis como tendo regimes de governação, aplicação da lei e regulamentação fracos, incluindo países identificados pelas declarações do Grupo de Acção Financeira (GAFI) como tendo regimes de prevenção e combate ao branqueamento de capitais, financiamento do terrorismo e financiamento da proliferação de armas de destruição em massa fracos e para os quais as instituições financeiras devem prestar atenção especial às relações e transacções comerciais.

3. As medidas de diligência reforçada devem incluir:
a) confirmar as informações de identidade recebidas do cliente, como número de identidade nacional, com informações em bancos de dados de terceiros ou outras fontes credíveis;
b) rastrear o endereço IP do cliente;
c) pesquisar na internet as informações disponíveis sobre o cliente;
d) obter informações adicionais do cliente sobre a natureza pretendida da relação comercial;
e) obter informações sobre a origem dos fundos do cliente; e
f) obter informações sobre os motivos das transacções pretendidas ou realizadas.

ANEXO I

Avaliação de risco

O presente anexo tem como objectivo apresentar alguns exemplos sobre a avaliação de risco. Contudo, apesar de recomendada, a sua aplicação não é obrigatória, cabendo a cada instituição financeira aferir a utilidade deste instrumento no contexto da sua política e dos seus procedimentos de gestão de risco.

I. **Circunstâncias exemplificativas para avaliação de risco de branqueamento de capitais, financiamento do terrorismo e financiamento da proliferação de armas de destruição em massa:**

1. Os riscos de branqueamento de capitais, de financiamento do terrorismo e de financiamento da proliferação de armas de destruição em massa podem ser, de entre outros, os seguintes:

a) risco cliente;
b) risco país ou geográfico; e
c) risco associado ao produto, aos serviços, à operação ou ao canal de pagamento.

2. As categorias de risco de branqueamento de capitais, financiamento do terrorismo e de financiamento da proliferação de armas de destruição em massa podem ser, de entre outros, as seguintes:

a) risco baixo;
b) risco moderado; e
c) risco elevado.

II. Exemplo de diferentes categorias de riscos

1. Cliente de risco elevado:

a) a relação de negócios decorre de forma invulgar (exemplo: uma significativa e inexplicada distância geográfica entre a instituição e o cliente);
b) clientes não residentes;
c) pessoa Politicamente Exposta;
d) pessoas colectivas ou entidades sem personalidade jurídica que sejam estruturadas de detenção de activos pessoais;
e) sociedade com accionistas por conta de outra pessoa ou acções ao portador;
f) actividades que tenham necessidade de fontes de financiamento consideráveis; e
g) a estrutura da propriedade da sociedade parece ser invulgar ou excessivamente complexa, dada a natureza da actividade da sociedade.

2. Cliente de risco baixo:

a) instituições financeiras que implementam eficazmente as obrigações de prevenção e combate ao branqueamento de capitais, financiamento do terrorismo e financiamento da proliferação de armas de destruição em massa;

b) sociedades comerciais cotadas num mercado bolsista e sujeitas a deveres de informação que visam garantir transparência adequada aos beneficiários efectivos; e

c) administrações ou empresas públicas.

Observação:

As entidades referidas na alínea *c*) não devem sempre ser consideradas de risco baixo.

Dependendo das jurisdições de origem, as administrações ou empresas públicas podem ser de risco elevado. Por exemplo, as empresas estatais com origem ou que operem num país considerado como de altos índices de corrupção.

3. Risco país ou geográfico elevado:

a) os países identificados por fontes idóneas como não dispondo de sistemas adequados de prevenção e combate ao branqueamento de capitais, financiamento do terrorismo e financiamento da proliferação de armas de destruição em massa. Por exemplo: os relatórios de avaliação mútua, de avaliação pormenorizada ou relatórios de acompanhamento publicados;

b) países sujeitos a sanções, embargos ou medidas análogas impostas pela Organização das Nações Unidas - ONU (sanção por parte do Conselho de Segurança) ou outras organizações internacionais;

c) países identificados por fontes idóneas como sendo caracterizados por níveis consideráveis de corrupção ou outra actividade criminal; e

d) países ou zonas geográficas identificados por fontes idóneas como financiadores ou apoiadores de actividades terroristas ou nos quais operem organizações terroristas designadas.

4. Risco país ou geográfico baixo:

a) os países identificados por fontes idóneas como dispondo de sistemas eficazes de branqueamento de capitais, financiamento do terrorismo e financiamento da proliferação de armas de destruição em massa. Por exemplo: os relatórios publicados de avaliação mútua, pormenorizada, ou de acompanhamento; e

b) países identificados por fontes idóneas como sendo caracterizados por níveis reduzidos de corrupção ou outra actividade criminal.

5. Risco elevado associado ao produto, serviço, operação ou canal de distribuição:

a) banca privada (serviços *corporate*, banca à distância);

b) relações de negócios ou operações sem a presença física do cliente; e

c) pagamento recebido de terceiros desconhecidos ou não associados.

6. Risco baixo associado ao produto, serviço, operação ou canal de distribuição:

Produtos ou serviços financeiros que proporcionem serviços limitados e definidos de modo pertinente, com vista a aumentar o acesso a determinados tipos de clientes para fins de inclusão financeira.

ANEXO II

Medidas de diligência contínua

1. As instituições financeiras podem implementar, consoante a categoria de risco envolvida, os seguintes tipos de medidas de diligência:

a) **medidas de diligência simplificadas**: medidas de diligências menos rigorosas comparativamente às medidas de diligência básicas, que apenas podem ser aplicadas quando o grau de risco seja reduzido.

As medidas de diligências simplificadas devem ser proporcionais aos factores de baixo risco.

Observação: as medidas simplificadas não devem ser aplicáveis quando exista suspeita de actos de branqueamento de capitais, de financiamento do terrorismo e financiamento da proliferação de armas de destruição em massa.

b) **medidas de diligência reforçadas:** quaisquer medidas de diligência adicionais empreendidas para além das diligências básicas.

Observação: as medidas de diligência reforçadas são realizadas para todos os clientes de alto risco.

2. Exemplos de medidas de diligência simplificadas:

a) verificação da identidade do cliente e do beneficiário efectivo após o estabelecimento da relação de negócio;

b) redução da frequência das actualizações dos elementos de identificação do cliente;

c) redução da intensidade da vigilância contínua e da profundidade do exame e das operações; e

d) não recolher informações específicas nem implementar medidas específicas que permitam compreender o objecto e a natureza da relação de negócio, mas inferir o objecto e a natureza do tipo de transacção efectuada ou relação de negócio estabelecida.

3. Exemplo de medidas de diligências reforçadas:

a) obtenção de informações adicionais sobre o cliente, tais como: profissão, bens, informações disponíveis em bases de dados nacionais, ou internacional, na *internet*, etc.;

b) actualização regular, no intervalo máximo de 12 meses, da informação de identificação do cliente e do beneficiário efectivo;

c) obtenção de informações adicionais sobre a natureza da relação de negócio;

d) obtenção de informação sobre os motivos das operações pretendidas ou realizadas;

e) obtenção de autorização do conselho de administração ou órgão equiparado para iniciar ou continuar a realização de negócio;

f) aumento da frequência de controlos e selecção do tipo de operações que necessitem de um exame mais profundo; e

g) obrigação de efectuar o primeiro pagamento, através de uma conta aberta em nome do cliente, a partir de uma outra instituição financeira sujeito a normas de diligência semelhante.

ANEXO III

Exemplos de transacções suspeitas referentes a actos de branqueamento de capitais, financiamento do terrorismo e financiamento de armas de destruição em massa

Observações:

A. Nenhum dos factores a seguir exemplificados, de forma isolada, significa necessariamente que um cliente ou terceiro está envolvido em actos de branqueamento de capitais, financiamento do terrorismo ou financiamento da proliferação de armas de destruição em massa.

B. No entanto, na maioria dos casos uma combinação dos factores abaixo pode despertar suspeitas.

C. Em qualquer caso, o que poderá ou não dar origem a uma suspeita dependerá de circunstâncias particulares.

1. Exemplos de transacções suspeitas branqueamento de capitais

1.1 Branqueamento de capitais, através de transacções em numerário

a) depósitos à vista em montantes elevados feitos por um indivíduo ou empresa que, pelo tipo de negócio ou actividades que desenvolva, normalmente, seriam efectuados por cheques ou outros instrumentos;

b) aumentos substanciais nos depósitos em numerário de qualquer pessoa ou empresa, sem causa aparente, especialmente se tais depósitos são posteriormente transferidos dentro de um curto período para outra conta e/ou para um destino que normalmente não tem ligação com o cliente;

c) cliente que efectua vários depósitos em numerário em montantes considerados normais (abaixo do limite estabelecido nas alíneas *a*) e *b*) do n.º 3 do artigo 44 da Lei n. º 14/2023, de 28 de Agosto), mas que no final totalizam montantes significativos;

d) contas de empresas cujas operações, depósitos e levantamentos, sejam em numerário em vez de nas formas de movimentos normalmente associados às operações comerciais de uma empresa (por exemplo, cheques, cartas de crédito, letras de câmbio, etc.);

e) cliente que constantemente pague ou deposite dinheiro paro cobrir pedidos de transferências bancárias, conta corrente ou outros instrumentos monetários negociáveis e facilmente comercializáveis;

f) cliente que constantemente solicite a troca de grandes quantidades de notas de baixa denominação para as de maior denominação;

g) troca (compra) frequente de dinheiro em outras moedas; e

h) agências/Filiais com muitas mais transacções em numerário do que o habitual.

1.2 Branqueamento de capitais usando contas bancárias

a) cliente que deseje manter e administrar um número de contas não compatível com o seu tipo de negócio ou transacções;

b) cliente que possua inúmeras contas bancárias e em cada uma delas, quantias em dinheiro consideradas normais para o seu perfil. mas cujo saldo total o saldo extravase o seu perfil financeiro;

c) qualquer pessoa ou empresa cuja conta bancária aponte para um perfil normal de negócio, mas seja usada para receber ou desembolsar grandes somas sem finalidade óbvia nem relação com o titular da conta e/ou com o seu negócio;

d) solicitação de pagamento de cheques de terceiros em grandes montantes, endossados a favor do cliente;

e) levantamento em numerário de uma conta previamente dormente/inactiva, ou a partir de uma conta que acabe de receber um elevado crédito do exterior;

f) cliente que use várias agências para realizar transacções em numerário e operações cambiais;

g) uso frequente de representantes, evitando o contacto com a instituição financeira;

h) aumentos substanciais nos depósitos em numerário ou instrumentos negociáveis por uma empresa, usando contas de clientes ou de empresa, especialmente se os depósitos forem prontamente transferidos para outro cliente ou empresa;

i) cliente que recuse fornecer informações que, em circunstâncias normais, seriam úteis para a sua elegibilidade a crédito ou outros serviços bancários;

j) uso insuficiente das facilidades bancárias normais (por exemplo, recusas de oferta de altas taxas de juros em razão do montante do saldo existente); e

k) pagamentos efectuados por um grande número de indivíduos na mesma conta, sem uma explicação adequada.

1.3 Branqueamento de capitais através de uma actividade internacional *offshore*

a) uso de cartas de crédito e outros métodos de financiamento ao comércio exterior para movimentar dinheiro entre os países onde esse comércio não é compatível com o negócio habitual do cliente;

b) clientes que façam pagamentos regulares e em montantes elevados, incluindo transferências electrónicas, não claramente identificados como transacções de boa-fé, ou clientes que recebam pagamentos regulares em montantes elevados provenientes de países que são comummente associados com a produção, transformação ou comercialização de drogas, organizações terroristas ou prática de qualquer um dos crimes precedentes referidos no artigo 7 da Lei n.º 14/2023, de 28 de Agosto;

c) existência de grandes saldos não consistentes com o conhecimento do volume de negócios do cliente e posterior realização de transferências para conta (s) no exterior;

d) transferências electrónicas de fundos inexplicáveis por parte dos clientes, usando os serviços de transferência de dinheiro ou similares; e

e) pagamentos frequentes de emissão de cheques de viagem, saques em moeda estrangeira ou outros instrumentos negociáveis.

1.4 Branqueamento de capitais envolvendo funcionários de instituições financeiras

a) alterações nas características dos empregados (por exemplo, estilos de vida luxuosos);

b) mudanças no desempenho do funcionário ou agente (por exemplo, vendedor de produtos com aumento notável ou inesperado no seu desempenho);

c) efectivação de transacções sem que se revele a identidade do beneficiário efectivo; e

d) esquemas de sobrefacturação, em que os materiais encomendados para uma compra são de baixa qualidade e os preços maiores que o estipulado, sem que tal se reflicta no contrato negociado.

1.5 Branqueamento de capitais com recurso a financiamentos garantidos e não garantidos

a) clientes que reembolsem empréstimos de forma inesperada;

b) pedido de financiamento contra activos detidos pela instituição ou por um terceiro, onde a origem dos bens não seja razoavelmente conhecida ou os bens sejam incompatíveis com a posição do cliente; e

c) pedido de financiamento cuja fonte de recursos para o reembolso nos termos do acordo não esteja clara.

1.6 Relação negocial

a) clientes que sem nenhuma razão discernível usem os serviços da empresa, por exemplo, clientes com endereços distantes que poderiam encontrar o mesmo serviço mais próximo das suas residências;

b) clientes cujos requisitos não estejam no padrão normal dos negócios da empresa, que poderiam ser mais facilmente atendidos em outro lugar;

c) um investidor introduzido por uma instituição financeira sedeada no exterior, baseados em países com conotação de produção de drogas, tráfico de drogas, ou outro crime precedente referido no artigo 7 da Lei n. º 14/2023, de 28 de Agosto; e

d) qualquer transacção em que a contraparte da operação seja desconhecida.

1.7 Intermediários

Qualquer uso aparentemente desnecessário de um intermediário numa transacção deve dar origem a um inquérito complementar.

1.8 Recurso ao sigilo como fundamento para ocultar alguma informação pode despertar suspeitas:

a) zelo excessivo ou desnecessário do potencial cliente;

b) concessão desnecessária de amplos poderes na procuração;

c) falta de vontade de divulgar as fontes de recursos; e

d) atraso e/ou falta de vontade de revelar a identidade dos beneficiários efectivos.

1.9 Factores de suspeitas na actuação de empresas:

a) as empresas que mantenham a continuidade da sua actividade mesmo com perdas substanciais;

b) as estruturas de grupo complexas. sem uma causa aparente;

c) a rotatividade frequente de accionistas, directores ou administradores, sem causa aparente;

d) estrutura de grupo rentável para efeitos fiscais;

e) uso de contas bancárias em várias moedas, sem motivo aparente;

f) a existência de transferências inexplicáveis de grandes somas de dinheiro, através de várias contas bancárias; e

g) administração ou gestão fraudulenta; em prejuízo dos interesses da própria empresa.

2. Exemplos de operações suspeitas – financiamento do terrorismo

2.1 Contas

a) conta inactiva com saldo mínimo, mas que, de repente, recebe um depósito ou uma série de depósitos, seguidos de levantamentos diários até ao limite do montante depositado;

b) ao abrir uma conta, o cliente furta-se a prestar as informações requeridas pela instituição financeira, ou presta declarações falsas ou de difícil verificação;

c) conta sobre a qual, várias pessoas possuam poderes para assinar, aparentando tais pessoas, no entanto, não ter qualquer relação entre si (qualquer vínculo familiar ou relacionamento de negócios); e

d) conta aberta em nome de uma pessoa jurídica, uma associação ou fundação, que pode estar ligada a uma organização terrorista e que apresente os movimentos de saldo acima do nível declarado.

2.2. Depósitos e levantamentos

a) conta de empresa a partir da qual sejam normalmente privilegiados levantamentos em numerário em detrimento de outros meios de pagamentos;

b) depósito de elevados montantes efectuado em numerário para a conta de uma pessoa física ou jurídica, quando a actividade empresarial aparente do indivíduo ou entidade seria normalmente, realizada em cheque ou outros instrumentos de pagamento;

c) mistura de depósitos em numerário e instrumentos monetários numa conta em que tais operações não pareçam ter qualquer relação com o uso normal da conta;

d) várias transacções realizadas no mesmo dia, ou em dias consecutivos, em várias agências da instituição financeira, que indiciem uma tentativa de despiste; e

e) depósitos ou levantamentos em numerário de forma consecutiva e em quantias que se encontrem abaixo do limite de reporte ao GIFiM.

2.3 Transferências electrónicas

a) transferência bancárias ordenadas em pequenos montantes, em dias consecutivos ou intercalados, estando evidente um aparente esforço para evitar a submissão de relatórios ao GIFiM;

b) transferência bancária em ausência de informações sobre o remetente ou a pessoa em nome da qual a transacção é realizada, quando a inclusão de tais informações seria de se esperar;

c) uso de várias contas, nomeadamente pessoal, de empresa, de organismos ou instituições de caridade para recolher fundos e remeter imediatamente ou após um curto penado de tempo para um pequeno número de beneficiários estrangeiros; e

d) operações cambiais realizadas em nome de um cliente por um terceiro, seguidas de transferências electrónicas de fundos para locais que não tenham relação comercial aparente com o cliente ou para países considerados não cooperantes.

2.4 Características do cliente ou da actividade

a) partilha de endereço por indivíduos envolvidos em transacções em numerário, especialmente quando o endereço seja também um local de negócios e/ou não pareça corresponder à ocupação declarada (por exemplo, estudantes, desempregados, trabalhadores por conta própria, etc.);

b) ocupação declarada pelo cliente não compatível com o nível ou tipo de transacção (por exemplo, um estudante ou um indivíduo desempregado que recebe ou envia um grande número de transferências bancárias, ou que faz levantamentos máximos de caixa diários em várias agências);

c) transacções efectuadas por organizações sem fins lucrativos ou de caridade, nas quais não pareça haver finalidade económica ou lógica, e não pareça haver relação entre a actividade declarada da organização e as outras partes envolvidas na transacção; e

d) inconsistências inexplicáveis detectadas no processo de identificação ou verificação do cliente (por exemplo, em relação ao país de residência anterior ou actual, ao país de emissão do passaporte, a países visitados, de acordo com o registo do passaporte, e em documentos fornecidos para confirmar o nome, o endereço e a data de nascimento).

2.5 Transacções ligadas as zonas geográficas ou países ou identificados por fontes idóneas como proporcionando fundos ou apoio a actividades terroristas

a) as operações envolvendo trocas de moeda estrangeira consecutivas dentro de um curto espaço de tempo, por transferências electrónicas para locais identificados por fontes idóneas como jurisdições não cooperantes;

b) depósitos consecutivos, dentro de um curto espaço de tempo, de transferências electrónicas de fundos, especialmente para ou através de locais considerados por fontes idóneas como jurisdições não cooperantes;

c) a conta bancária que receba ou ordene um grande número de transferências electrónicas, em relação às quais pareça não haver nenhuma lógica de negócio ou outra finalidade económica, principalmente quando estas transferências se destinem ou provenham de jurisdições consideradas não cooperantes;

d) uso de várias contas para colectar e canalizar fundos para um pequeno número de beneficiários estrangeiros, pessoas físicas e empresas, particularmente quando estes estejam em jurisdições não cooperantes;

e) cliente que obtenha um instrumento de crédito ou se envolva em transacções financeiras comerciais com o movimento de fundos para ou a partir de jurisdições não cooperantes, quando não pareça haver razões lógicas de negócios para lidar com esses locais;

f) abertura de contas de instituições financeiras a partir de locais de jurisdições não cooperantes; e

g) enviar ou receber fundos, através de transferências internacionais de e/ou para locais ou jurisdições não cooperantes.

ANEXO IV

Tipologias de transacções com alto nível de risco de branqueamento de capitais, financiamento do terrorismo e financiamento da proliferação de armas de destruição em massa

A. Operações de caixa desproporcionais ao perfil do cliente

1. Depósitos em dinheiro extraordinariamente grandes e depósitos em dinheiro recorrentes desproporcionais à actividade do cliente;
2. Depósitos recorrentes em dinheiro por diferentes pessoas ou entidades em contas de um determinado cliente para fins pouco claros e sem relação entre essas pessoas ou entidades e o cliente.

B. Operações de caixa com características incomuns ou anormais

1. Grandes depósitos em dinheiro transferidos, dentro de um curto período de tempo, para um terceiro que não está intimamente relacionado à actividade do cliente que transferiu;
2. Depósitos recorrentes em dinheiro em várias agências da mesma instituição financeira num curto período, seja pelo mesmo titular da conta ou por outras pessoas;
3. Saques repetidos de fundos logo após o depósito sem justificativa clara.

C. Operações em dinheiro com uso anormal de caixas electrónicos

1. Grandes depósitos ou saques feitos em caixas electrónicos para evitar o contacto directo com os funcionários da instituição financeira, especialmente se esses depósitos ou saques não estiverem de acordo com a natureza da actividade do cliente;
2. Cliente usando vários caixas electrónicos para transacções simultâneas em dinheiro na mesma conta.

D. Trocas de dinheiro anormais

1. Pessoas que pretendam trocar grandes quantidades de notas pequenas por notas de grandes denominações sem justificação clara;
2. Pessoas que pretendam trocar grandes quantidades de notas danificadas por notas válidas sem justificação clara.

E. Uso anormal de contas

1. Clientes que usam várias contas para depositar grandes quantias em dinheiro num curto período;
2. Múltiplas transacções realizadas das contas do cliente na instituição financeira para contas em outra instituição financeira, após o que os fundos retornam à instituição financeira em que as transacções começaram;
3. Movimentos de dinheiro de débito e crédito feitos na mesma conta dentro de um curto período sem justificativa clara;
4. Uso do cliente de sua conta como uma conta intermediária entre outras partes ou contas.

F. Uso anormal de contas inactivas

1. Grandes depósitos e saques em dinheiro de contas inactivas;
2. Contas que recebem vários depósitos ou transferências em dinheiro e são fechadas após um curto período ou ficam estagnadas;
3. Grandes transferências do exterior para contas inactivas.

G. Uso incomum de transferências

1. Transferências de grandes quantias, especialmente aquelas acompanhadas de instruções para pagamento em dinheiro que não sejam proporcionais à actividade do cliente;
2. Transferências recorrentes de diferentes partes que não têm relação clara com o cliente ou aquelas enviadas do cliente para essas partes;
3. Grandes transferências provenientes regularmente de áreas conhecidas por determinados crimes, como tráfico ou cultivo de drogas, ou de estados que não possuem sistemas de prevenção e combate ao branqueamento de capitais, financiamento do terrorismo e financiamento da proliferação de armas de destruição em massa eficazes;
4. Acções tomadas para evitar proibições de sanções aplicáveis, como remoção, ou a resubmissão e/ou mascaramento de sanções em transacções transfronteiriças.

H. Reserva incomum de linhas de crédito

1. Se a instituição financeira estiver oferecendo crédito documentário, importação ou exportação de bens cujo tipo ou valor não corresponda à natureza ou ao tamanho da actividade do cliente ou ao valor dos bens constantes da carta de crédito ou dos documentos de cobrança é significativamente diferente do seu valor real;
2. Solicitação do cliente, sem justificativa clara, para alteração do nome do beneficiário da carta de crédito ou documentos de cobrança antes do pagamento;
3. Abertura de várias cartas de crédito ou negociação através de documentos de cobrança ou contragarantias financeiras de forma não compatível com a actividade do cliente;
4. Pedidos de empréstimo por garantia de activos de propriedade de terceiros, ou a prestação de garantias adicionais de propriedade de terceiros pelos mutuários, sem vínculo claro com eles;
5. Registo de linhas de crédito contragarantias de uma instituição financeira que opera fora do país sem motivo aparente;
6. Solicitações de um cliente mutuário para transferir rapidamente o valor do empréstimo para outras instituições financeiras, sem objectivo claro.

I. Reserva incomum de garantias

1. Emissão múltipla de cartas de fiança desproporcionais à natureza e tamanho da actividade do cliente;
2. Cartas de fiança contragarantias financeiras que não são compatíveis com o tamanho da actividade do cliente ou suas transacções anteriores com a instituição financeira.

J. Reembolso incomum de linhas de crédito

1. Condições de pagamento incomuns ou pagamento a terceiros que não tenham relação aparente com a carta de crédito ou os documentos de cobrança;
2. Pagamento antecipado inesperado de dívidas pelo cliente ou outras partes, especialmente para clientes inadimplentes.

K. Liquidações incomuns de garantias

Pedido do beneficiário, sem justificativa clara, para liquidar cartas de fiança logo após sua emissão pela instituição financeira.

L. Actividades incomuns do cartão

Saques repetidos com frequência no exterior do máximo de dinheiro diário disponível para o cartão.

M. Transacções incomuns em moeda estrangeira

Para transacções de câmbio e cheques de viagem, compra ou venda de moedas estrangeiras por grandes quantias que não são proporcionais à actividade do cliente.

N. Nenhuma outra transacção incomum

Para além do processo de filtragem e identificação das tipologias acima referidas cuja implementação nas ferramentas automatizadas de vigilância das instituições financeiras é obrigatória, as instituições financeiras devem implementar métodos e ferramentas de vigilância adaptados às operações de alto risco identificadas no risco anual avaliação.

ANEXO V

Relatório anual sobre o risco de branqueamento de capitais, financiamento do terrorismo e financiamento da proliferação de armas de destruição em massa

Observação:

Os seguintes dados e respostas aos questionários anuais devem ser reportados com referência à 31 de Janeiro do ano seguinte a que dizem respeito, devendo ser remetidos ao Banco de Moçambique, em ficheiro Excel disponibilizado pelo Banco de Moçambique.

A. Dados quantitativos

Nome da instituição: ----------
Dados referentes aos últimos 12 meses terminando em : ----------

As devoluções são aprovadas por: (Administrador Delegado ou equiparado)----------	
Nome da pessoa responsável: ----------	Número de telefone:----------
E-mail:----------	
Data de envio ao Banco de Moçambique :-------	

1. Ficheiro institucional

Informações relacionadas à instituição financeira		
1. Se for parte de um grupo: (a) Nome do grupo: ----------(b) País de origem:----------		
2. Número de funcionários		
2.a. Número de funcionários responsáveis pelo monitoria da AMLCFT		
2.b. Número de funcionários treinados em AMLCFT durante o ano passado		
3. Número de agências:		
4. Número de subsidiárias /filiais:		
5. Activos totais – em milhões de meticais		

2. Análise dos riscos de produtos e serviços seleccionados

2.1. Operações sensíveis	Número de clientes	Número de operações	Valores em meticais
a. Cheques pagos em dinheiro - emitidos pelo governo ou fundos pensões		Nos últimos 12 meses	O valor total das transacções referentes aos últimos 12 meses
b. Cheques pagos em dinheiro - outros		Nos últimos 12 meses	O valor total das transacções referentes aos últimos 12 meses
c. Transacções para o exterior (cheques, créditos documentários, transferências, etc.)		Nos últimos 12 meses	Total de remessas emitidas nos últimos 12 meses
d. Transacções de países estrangeiros (cheques, créditos documentários, transferências, etc.)		Nos últimos 12 meses	Total de remessas recebidas nos últimos 12 meses

2.2 Serviços de financiamento	Número de clientes	Valor em MT
A. Linhas de crédito garantidas por dinheiro, ouro ou pelo governo Total das facilidades é ..... Número de clientes ..... Total de facilidades	Número de clientes de acordo com	Total de facilidades está conforme
B. Linhas de crédito garantidas por outras garantias Número de cliente	Número de clientes de acordo com	Total de facilidades
C. Linhas de crédito / parcelas pagas em dinheiro antes do vencimento	Número de clientes de acordo com	Total de facilidades
D. Linhas de crédito / prestações pagas em espécie antes da data de vencimento	Número de clientes de acordo com	Total de facilidades

2.3. Banca privada (*Private banking*)	**Número total de clientes**	**Depósitos**		**Facilidades de crédito**		**Exposições fora do balanço/ *Off-balance-sheet exposures***	
		Número de clientes	**Valor em MT**	**Número de clientes**	**Valor em MT**	**Número de clientes**	**Valor em MT**
Serviços de banca privada		Número de clientes	Depósitos totais em	Número de clientes	Total de facilidades	Número de clientes	Exposições totais em

2.4. Serviços de cartão bancários	**Número de cartões**	**Número de clientes**	**Volume de usuários em milhões de MT**
A. Cartões emitidos com valor pré-pago	O número de cartões emitidos é	O número de clientes de acordo com	O valor total das transacções nos últimos 12 meses
B. Outros diferentes de cartões de crédito e débito	O número de cartões emitidos é	O número de clientes de acordo com	O valor total das transacções nos últimos 12 meses

2.5. Outros		Número de clientes	Número de transacções	Valor em MT
A. Serviços em dinheiro / Cash services	**A.** Depósitos em dinheiro	Número de clientes para os quais o serviço foi prestado nos últimos 12 meses……	Número de depósitos em dinheiro efectuado nos últimos 12 meses ……	Valor total dos depósitos em dinheiro nos últimos 12 meses……...
	B. Levantamentos em dinheiro	Número de clientes para os quais o serviço foi prestado nos últimos 12meses……	Número de saques em dinheiro nos últimos 12 meses …	O valor total de saques em dinheiro nos últimos 12 meses
B. Serviços de banca electrónica	**A.** *Internet banking*	Número de clientes para os quais o serviço foi prestado nos últimos 12 meses……	Número de transacções que ocorreram nos últimos 12 meses…….	Valor total das transacções nos últimos 12 meses….....
	B. *Phone banking*	Número de clientes para os quais o serviço foi prestado nos últimos 12 meses……	Número de transacções que ocorreram nos últimos 12 meses…….....	Valor total das transacções nos últimos 12 meses……
C. *Wireless transfers*	**A.** Transferências emitidas (*Outgoing transfers*)	Número de clientes para os quais o serviço foi prestado nos últimos 12 meses……..	Número de transferências emitidas/processadas nos últimos 12 meses……...	Valor total das transferências nos últimos 12 meses……
	B. Transferências recebidas (*Incoming transfers*)	Número de clientes para os quais o serviço foi prestado nos últimos 12 meses……	Número de transferências recebidas nos últimos 12 meses……..	Valor total das transferências recebidas nos últimos 12 meses……
D. Transacções/operações cambiais	**A.** Compra de moeda estrangeira	Número de clientes para os quais o serviço foi prestado nos últimos 12 meses……	Número de transacções ocorridas nos últimos 12 meses…….	Valor total das compras feitas pela instituição financeira nos últimos 12 meses……...
	B. Venda de moedas estrangeira	Número de clientes para os quais o serviço foi prestado nos últimos de 12 meses……	Número de transacções que ocorreram nos últimos 12 meses……..	Valor total das transacções de vendas realizadas pela instituição financeira nos últimos 12 meses……
E. Financiamento ao comércio externo (créditos documentários... etc.)		Número de clientes para os quais o serviço foi prestado nos últimos 12 meses……	Número de transacções que ocorreram nos últimos 12 meses……..	O valor total das transacções nos últimos 12 meses……

3. Análise de risco do cliente

3.1. Serviços prestados aos titulares das contas (é necessário indicar o saldo no final do período)	**Número total de clientes**	**Média das transacções em MT**
Na data do relatório		
Total de clientes com contas		
A. Clientes residentes individuais		
B. Pessoas jurídicas residentes		
C. Clientes não residentes individuais		
D. Pessoas jurídicas não residentes		

3.2. Análise dos riscos de cliente (Saldo exigido no final do período)	Número total de clientes	Média de transacções em MT
1. Entidades e organizações sem fins lucrativos		
a. Local		
b. Estrangeiro		
2. Pessoas políticas que representam um risco		
a. Local		
b. Estrangeiro		
c. Organizações internacionais		
3. Clientes banca privada		
4. Clientes que lidam com caixa de forma intensiva (entradas ou saídas de caixa > 500.000 MZN/mês)		
5. Pessoas jurídicas / o verdadeiro beneficiário é desconhecido		
6. Instituições de Transferência de Fundos		
7. Casas de câmbios		
8. Negócios imobiliários (inclui agentes)		
9. Negociantes de gemas e metais preciosas		
10. Proprietários de negócios e profissões não financeiras (advogados, contabilistas e intermediários que trabalham em benefício de outros)		
11. Pessoas jurídicas		
a. Local		
b. Estrangeiro		
12. Vendedores e revendedores de veículos, casinos e entidades exploradoras de jogos sociais e de diversão, entidades de microfinanças		

3.3. Análise de Risco Geoespacial - Análise Baseada na Residência do Cliente

Cláusula	Número de ATMs	Depósito		Transferências					
				Recebidas			Enviadas		
		Número de Clientes	Depósito em MT	Número de Transacções	Número de Clientes	Valores em MT	Número de Transacções	Número de Clientes	Valores em MT
1. Local									
A. Zonas fronteiriças, zonas de conflito e de mineração		Número de clientes de acordo com	Saldo total de acordo com	Número total de remessas de fundos nos últimos 12 meses	Número de clientes para os quais o serviço foi prestado nos últimos 12 meses	Valor total das remessas internas nos últimos 12 meses	Número total de remessas enviadas nos últimos 12 meses	Número de clientes para os quais o serviço foi prestado nos últimos 12 meses	Valor total das remessas internas nos últimos 12 meses
B. Outras regiões de Moçambique		Número de clientes.....	Saldo total.....	Número total de remessas de fundos nos últimos 12 meses	Número de clientes para os quais o serviço foi prestado nos últimos 12 meses	Valor total das remessas internas nos últimos 12 meses	Número total de remessas enviadas nos últimos 12 meses	Número de clientes para os quais o serviço foi prestado nos últimos 12 meses	Valor total das remessas internas nos últimos 12 meses
2. Estrangeiro									
A. Países classificados pelo GAFI como países de alto risco		Número de clientes de acordo com	Saldo total de acordo com	Número total de remessas de fundos nos últimos 12 meses	Número de clientes para os quais o serviço foi prestado nos últimos 12 meses	Valor total das remessas internas nos últimos 12 meses	Número total de remessas enviadas nos últimos 12 meses	Número de clientes para os quais o serviço foi prestado nos últimos 12 meses	Valor total das remessas internas nos últimos 12 meses
B. Outros países que foram identificados como tendo elevados riscos de branqueamento de capitais e financiamento do terrorismo		Número de clientes de acordo com	Saldo total de acordo com	Número total de remessas de fundos nos últimos 6 meses	Número de clientes para os quais o serviço foi prestado nos últimos 6 meses	Valor total das remessas internas nos últimos 12 meses	Número total de remessas enviadas nos últimos 12 meses	Número de clientes para os quais o serviço foi prestado nos últimos 12 meses	Valor total das remessas internas nos últimos 12 meses
C. Outros países		Número de clientes de acordo com	Saldo total de acordo com	Número total de remessas de fundos nos últimos 12 meses	Número de clientes para os quais o serviço foi prestado nos últimos 12 meses	Valor total das remessas internas nos últimos 12 meses	Número total de remessas enviadas nos últimos 12 meses	Número de clientes para os quais o serviço foi prestado nos últimos 12 meses	Valor total das remessas internas nos últimos 12 meses

Relatórios de operações suspeitas inusitadas

Cláusula	Número (nos últimos 12 meses)
Número de operações pouco usuais / suspeitas detectadas	
Número de transacções suspeitas comunicadas ao GIFiM	
Número de operações castradas (abortadas)	

Questionários qualitativos

Perguntas sobre avaliação e perfil de risco
1. A instituição concluiu, durante o último ano, uma avaliação de risco formalizada e documentada para todos os riscos de branqueamento de capitais, financiamento do terrorismo e financiamento da proliferação de armas de destruição em massa?
2. Se solicitado pelas autoridades competentes, a instituição está em condições de apresentar uma avaliação de risco formalmente documentada e demonstrar a base sobre a qual as avaliações de risco foram construídas?
3. Ao construir a avaliação de risco, a metodologia de avaliação de risco exige que a instituição utilize informações internas, tais como dados operacionais e transaccionais, bem como informações externas, tais como relatórios de avaliações de risco nacionais?
4. A instituição garante que a avaliação de risco da instituição é construída utilizando tanto elementos quantitativos como qualitativos e é sempre mantida até à data?
5. A avaliação de risco abrange todos os produtos e serviços fornecidos e prestados aos clientes?
6. A avaliação de risco tem em consideração as especificidades de todas as transacções da instituição (natureza, complexidade, etc.)?
7. A avaliação de risco tem em consideração todos os canais de distribuição directos e indirectos?
8. A avaliação de risco tem em consideração as características dos seus clientes?
9. A avaliação de risco tem em consideração as áreas geográficas dos seus clientes ou transacções relacionadas?
10. A avaliação de risco tem em consideração todas as jurisdições com as quais a instituição trabalha, através de todos os tipos de transacções possíveis: créditos documentais, bancos correspondentes, transferências, etc.?
11. A instituição integrou os factores ou riscos de financiamento do terrorismo e financiamento da proliferação de armas de destruição em massa na sua avaliação de risco?
12. Algum evento interno ou externo durante o último ano desencadeou uma modificação ou revisão da exposição da instituição aos riscos de branqueamento de capitais, financiamento do terrorismo e financiamento da proliferação de armas de destruição em massa e, subsequentemente, esteve na origem de uma revisão da classificação de riscos da instituição ou da avaliação de riscos? *Os eventos desencadeantes podem incluir, mas não se limitam a mudanças na Avaliação Nacional de Riscos, mudanças na estrutura accionista da instituição, mudanças na estrutura de controlo chave, riscos negativos para os meios de comunicação social ou reputacionais, grandes mudanças nas actividades actuais e acompanhamento das auditorias de branqueamento de capitais, financiamento do terrorismo e financiamento da proliferação de armas de destruição em massa.*

Perguntas sobre avaliação e perfil de risco
13. Alguma missão de auditoria realizada por auditores internos ou externos durante o último ano destacou a relevância do perfil de risco branqueamento de capitais, financiamento do terrorismo e financiamento da proliferação de armas de destruição em massa da instituição e a ausência de necessidade de o actualizar ou modificar?
14. O conselho de administração ou órgão equiparado aprovou, durante o último ano, a avaliação de risco do a instituição e determinou o nível de risco de branqueamento de capitais, financiamento do terrorismo e financiamento da proliferação de armas de destruição em massa que a instituição está pronto a aceitar?
15. O conselho de administração ou órgão equiparado aprovou formalmente o exercício de avaliação de risco e as medidas de mitigação adaptadas ao nível de risco acima mencionado?
16. O conselho de administração ou órgão equiparado assegura o acompanhamento da implementação das medidas de mitigação aprovadas no contexto do exercício de avaliação de risco?
17. A instituição identifica e avalia os riscos de branqueamento de capitais, financiamento do terrorismo e financiamento da proliferação de armas de destruição em massa que podem surgir em relação ao desenvolvimento de novos produtos e novas práticas comerciais, incluindo novos mecanismos de entrega, a utilização de novas tecnologias ou em desenvolvimento tanto para produtos novos como para produtos pré-existentes?

Questões sobre a organização do quadro de branqueamento de capitais, financiamento do terrorismo e financiamento da proliferação de armas de destruição em massa	
1.	A instituição organizou uma coordenação centralizada para a análise das transacções não habituais detectadas?
2.	A instituição organizou uma coordenação centralizada para a elaboração de relatórios de transacções suspeitas para transacções para as quais existem razões para suspeitar que são de origem ilegal?
3.	A instituição organizou uma coordenação centralizada para a elaboração de relatórios de transacções suspeitas relacionadas com o financiamento do terrorismo?
4.	A instituição organizou uma coordenação centralizada de respostas a requisições judiciais ou administrativas, bem como aos deveres de comunicação ao GIFiM?
5.	A instituição implementou ferramentas automatizadas, em tempo real, e procedimentos baseados no risco para determinar se deve transferir, rejeitar ou suspender transacções que não sejam acompanhadas das informações necessárias sobre o ordenante e o beneficiário?
6.	Se recorre ao *outsourcing* com prestadores de serviços para actividades operacionais que incluem ou que estão ligadas às obrigações de branqueamento de capitais, financiamento do terrorismo e financiamento da proliferação de armas de destruição em massa, e especialmente se estas estão localizadas no estrangeiro, a instituição verifica se os seus procedimentos são realmente implementados pelo prestador de serviços?
7.	Se a instituição pertence a um grupo ou é a empresa-mãe de um grupo financeiro, os procedimentos de grupo permitem e facilitam a partilha de informações dentro do grupo para efeitos de organização da vigilância de branqueamento de capitais, financiamento do terrorismo e financiamento da proliferação de armas de destruição em massa, incluindo a partilha de informações para a empresa-mãe do grupo?
8.	Se a instituição é a empresa-mãe de um grupo financeiro, a pessoa responsável pela implementação das políticas de branqueamento de capitais, financiamento do terrorismo e financiamento da proliferação de armas de destruição em massa ao nível grupo assegura que as medidas aplicadas em entidades no estrangeiro são, pelo menos, equivalentes às medidas em vigor em Moçambique?
9.	Se a instituição é a empresa-mãe de um grupo financeiro, a pessoa responsável pela implementação do quadro legal de branqueamento de capitais, financiamento do terrorismo e financiamento da proliferação de armas de destruição em massa do grupo assegura que as filiais e sucursais localizadas em outro Estado cumprem as disposições aplicáveis nesse Estado?
10.	Se a instituição é a empresa-mãe de um grupo financeiro, a pessoa responsável pela implementação do sistema de grupo é mantida informada da existência de relatórios de transacções suspeitas feitos a uma Unidade de Informação Financeira por uma entidade do seu grupo?
11.	A instituição tem agências ou filiais no estrangeiro cuja lei aplicável localmente impede a empresa-mãe do dispositivo do grupo de ter acesso aos documentos ou aos detalhes da transacção?

Questões sobre as diligências devidas pelos clientes
1. A instituição assegura a identificação e verificação da identidade do cliente ou, se aplicável, a identificação e verificação da identidade do proprietário beneficiário, independentemente do montante de cada transacção individual?
2. O processo de "*Customer Due Diligence*" (CDD) da instituição assegura a recolha e retenção da seguinte informação: a) Estrutura de propriedade; b) Identificação do cliente; c) Actividades antecipadas; d) Natureza do negócio/emprego; e) Produtos solicitados; f) Finalidade da conta/ relação de negócios; g) Fontes dos fundos; h) Fontes de riqueza; i) Beneficiários efectivos; j) Exposição geográfica, k) Tipo de negócio / indústria; l) Produtos utilizados; m) Tipo de entidade jurídica; n) Informação sobre a situação profissional, económica e financeira dos clientes?
3. No caso da verificação da identidade do cliente e, quando aplicável, do beneficiário efectivo, ou a recolha de informações sobre o objecto e a natureza da relação comercial se revelar impossível ou limitada, a instituição abstém-se de celebrar a relação comercial?
4. No caso de a verificação da identidade do cliente e, quando aplicável, do beneficiário efectivo, ou a recolha de informações sobre o objecto e a natureza da relação comercial se revelar impossível ou limitada, a instituição abstém-se de celebrar a relação comercial?
5. A instituição tem em funcionamento um sistema de computação de perfis e monitorização da relação comercial?
6. A instituição tem procedimentos internos que impõem a verificação de que qualquer pessoa que pretenda agir em nome do cliente está autorizada a fazê-lo, e identificar e verificar a identidade dessa pessoa?
7. Os procedimentos permitem que a instituição detecte Pessoas Politicamente Expostas (PPE) ou pessoas/entidades a elas ligadas ou agir como seus associados ao iniciar uma relação comercial e durante a relação comercial e a sua organização investiga a origem dos fundos e as fontes de riqueza dos PPE ou pessoas/entidades a eles ligadas ou age como seus associados?
8. Os seus procedimentos preveem vigilância adicional / medidas reforçadas a serem implementadas quando a relação comercial, o produto ou a operação têm uma classificação de "alto risco"?
9. Se a instituição utiliza um ou mais terceiros para estabelecer relações comerciais com clientes, continua a ser a única responsável por completar as diligências devidas pelos clientes apresentados pelo apresentador terceiro?

Questões sobre as diligências devidas pelos clientes
10. A instituição tem uma política de actualização da informação dos clientes, pelo menos uma vez por ano, para todos os clientes, independentemente da sua classificação de risco?
11. A instituição tem uma política de actualização da informação dos clientes pelo menos uma vez por ano para todos os clientes, independentemente da sua classificação de risco?
12. A instituição tem um sistema adequado de gestão de limiares que permite a instituição realizar as revisões CDD necessárias à luz de qualquer evento de disparo que ocorra ao cliente e que possa implicar uma revisão da classificação de risco deste cliente?
13. Todos os clientes que constam dos registos da instituição têm uma classificação de risco adequada?
14. A instituição conduz acções terroristas/sanções, notícias negativas e rastreio PPE a bordo do cliente e, posteriormente, com frequência, com potenciais jogos que são prontamente revistos e escalados.
15. As políticas e procedimentos da instituição explicam claramente quais os clientes e partes relacionadas que devem ser rastreados e como este processo deve ser levado a cabo?

Questões sobre o acompanhamento contínuo
1. A instituição dispõe de ferramentas automatizadas para detectar transacções atípicas ou suspeitas?
2. A instituição define critérios de importância para detectar transacções atípicas e suspeitas, através de soluções de monitorização de transacções ou por outros meios, tais como referências de empregados?
3. Se o cliente não fornecer uma justificação sobre os detalhes de qualquer transacção ou actividade bancária específica, as políticas e procedimentos da instituição obrigam ao registo, à apresentação de relatórios à GIFiM e/ou à restrição ou cessação de relações comerciais com esses clientes?
4. Os procedimentos internos preveem que as transferências de fundos emitidas sejam acompanhadas das informações necessárias sobre o ordenante e o beneficiário?
5. A instituição implementou um processo de detecção automática de informações em falta sobre o ordenador ou o beneficiário e procedimentos baseados no risco para determinar se deve transferir, rejeitar ou suspender transacções que não sejam acompanhadas das informações necessárias sobre o ordenador e o beneficiário?
6. A instituição utiliza agentes e/ou distribuidores para alguns dos seus produtos, eles beneficiam de uma formação e informação regular sobre branqueamento de capitais, financiamento do terrorismo e financiamento da proliferação de armas de destruição em massa e adaptada às suas actividades?
7. As políticas e procedimentos internos da instituição garantem que o(s) agente(s) e/ou o(s) distribuidor(es) estejam sujeitos a CDD e que estão em conformidade com o seu quadro de branqueamento de capitais, financiamento do terrorismo e financiamento da proliferação de armas de destruição em massa?
8. Se a instituição utiliza ou está a realizar uma actividade de correspondente bancário transfronteiriço, tomou todas as medidas necessárias para assegurar um controlo contínuo reforçado deste tipo de transacções?
9. A instituição implementa medidas adicionais de monitorização contínua para clientes ou transacções identificadas como de "alto risco"?
10. Para o caso de moeda electrónica, os procedimentos da instituição preveem a verificação da identidade do cliente, independentemente do montante quando carregam a conta com recurso ao dinheiro físico?
11. Para o caso de moeda electrónica, o sistema da instituição prevê a implementação de medidas de vigilância durante o reembolso e/ou levantamento de moeda electrónica acima de um limiar relevante definido nos seus procedimentos?
12. Para o caso de moeda electrónica, os procedimentos da instituição incluem a recolha e armazenamento de informações e dados técnicos relativos à activação, carregamento e utilização da moeda electrónica através de um meio físico para efeitos da sua rastreabilidade?

Questões sobre o relatório ao GIFiM
1. A instituição compromete-se a comunicar ao GIFiM, relatórios de actividades suspeitas ou potencialmente suspeitas, no âmbito de um processo consistente de investigação, documentação, comunicação de actividades suspeitas e, ao mesmo tempo, obedecendo aos mais elevados padrões de exactidão, exaustividade e tendo os relatórios concluídos dentro dos prazos legais?
2. A instituição tem políticas, procedimentos e processos de monitorização baseados no risco para a identificação e notificação de actividades invulgares ou suspeitas?
3. O sistema da instituição prevê que os relatórios de transacções suspeitas incluam os elementos de análise que levaram à comunicação das transacções/actividades e sejam acompanhados de qualquer documento útil à sua exploração?
4. Os procedimentos da instituição contêm disposições relativas à confidencialidade da existência, conteúdo e acompanhamento das transacções suspeitas para evitar "*dicas*"?
5. As políticas e procedimentos da instituição obrigam a que todas as actividades determinadas a serem suspeitas e escaladas pelos vários meios sejam revistas por um colaborador sénior e comunicadas atempadamente ao GIFiM?

Questões sobre a auditoria interna e o controlo
1. A instituição tem uma função de auditoria interna e uma função de controlo interno ou outro terceiro independente, para avaliar os riscos de branqueamento de capitais, financiamento do terrorismo e financiamento da proliferação de armas de destruição em massa e as políticas e práticas relacionadas numa base regular?
2. O conselho de administração da instituição garante que o âmbito e a metodologia da auditoria são adequados ao perfil de risco da instituição e que a frequência de tais auditorias se baseia também no risco?
3. Todas as constatações adversas da auditoria interna e externa são devidamente escaladas para a gestão sénior dentro do quadro formal de governação?
4. A função de auditoria e/ou de controlo interno assegura que o cumprimento dos procedimentos de branqueamento de capitais, financiamento do terrorismo e financiamento da proliferação de armas de destruição em massa são devidamente implementados em todas as sucursais e filiais da instituição?
5. A auditoria independente e/ou o controlo abrange terceiros e agentes que actuam em nome da organização para assegurar a sua conformidade com as políticas e procedimentos de branqueamento de capitais, financiamento do terrorismo e financiamento da proliferação de armas de destruição em massa da instituição?
6. Em particular, a auditoria independente e/ou o controlo revê o CDD, o processo de "*due diligence*" melhorado e o processo " Conheca o seu Cliente " realizado para as relações comerciais, em particular as identificadas como de alto risco pela sua organização?

Questões sobre a auditoria interna e o controlo
7. A auditoria e/ou controlo independente verifica, em particular, a diligência reforçada realizada para os produtos, serviços ou canais de distribuição, em particular os classificados como de alto risco?
8. Em particular, a auditoria e/ou controlo independente verifica o reforço da diligência devida para as actividades realizadas com pessoas estabelecidas em Estados ou territórios classificados como de alto risco ou aqueles que se sabe terem deficiências estratégicas de branqueamento de capitais, financiamento do terrorismo e financiamento da proliferação de armas de destruição em massa?
9. A auditoria e/ou controlo independente verifica a actualização regular dos elementos de conhecimento (CDD) da relação comercial de acordo com a frequência definida nos procedimentos e adaptada aos riscos?
10. A auditoria e/ou controlo independente verifica o tratamento diligente dos alertas de branqueamento de capitais, financiamento do terrorismo e financiamento da proliferação de armas de destruição em massa, e se os alertas gerados são tratados prontamente e encerrados com uma avaliação de risco adequada?
11. A auditoria interna verifica, em particular, a relevância da classificação dos riscos de branqueamento de capitais e de financiamento do terrorismo e financiamento da proliferação de armas de destruição em massa desenvolvida pela instituição?
12. A auditoria interna e/ou controlo verifica a adequação das políticas e procedimentos de prevenção e combate ao branqueamento de capitais, financiamento do terrorismo e financiamento da proliferação de armas de destruição em massa da instituição na abordagem dos riscos identificados?
13. A auditoria interna e/ou controlo verifica, em particular, a eficácia do pessoal da instituição na implementação das políticas e procedimentos da instituição; em particular do sistema de detecção e análise das operações de branqueamento de capitais, financiamento do terrorismo e financiamento da proliferação de armas de destruição em massa?
14. A auditoria interna e/ou o controlo testa a eficácia da formação em matéria de branqueamento de capitais, financiamento do terrorismo e financiamento da proliferação de armas de destruição em massa do pessoal relevante da instituição?
15. A data da última missão de auditoria realizada pela auditoria interna na totalidade ou em parte do sistema de prevenção e combate ao branqueamento de capitais, financiamento do terrorismo e financiamento da proliferação de armas de destruição em massa da instituição é inferior a um ano?
16. A auditoria interna efectua controlos aos parâmetros dos sistemas de prevenção e combate ao branqueamento de capitais, financiamento do terrorismo e financiamento da proliferação de armas de destruição em massa, aos cenários e à suficiência dos cenários implantados?
17. As funções independentes de auditoria/controlo analisam as práticas de congelamento de bens para assegurar a implementação, após a sua entrada em vigor, de medidas de congelamento de fundos ou de recursos económicos?
18. A auditoria independente / funções de controlo revê as práticas relacionadas com o rastreio do nome a bordo, o rastreio do nome durante a relação e na revisão do CDD, o rastreio das transacções e a gestão das listas de sanções?

Questões sobre o acompanhamento contínuo
1. O conselho de administração ou órgão equiparado e a gestão de topo estão activamente envolvidos na implementação de um quadro sólido de *compliance* que proteja a instituição contra quaisquer riscos de branqueamento de capitais, financiamento do terrorismo e financiamento da proliferação de armas de destruição em massa ou sanções?
2. A gestão de risco está integrada em três linhas de defesa em que a segunda linha de defesa inclui o chefe de operações responsável pela prevenção e combate branqueamento de capitais, financiamento do terrorismo e financiamento da proliferação de armas de destruição em massa, bem como a função de conformidade e a terceira linha de defesa é assegurada pela função de auditoria interna?
3. A administração e a direcção comunicam formalmente a tolerância ao risco e as estratégias de aceitação de risco da instituição a todos os funcionários da instituição?
4. O conselho de administração ou órgão equiparado divulgou à todo o pessoal da instituição recomendações sobre a implementação da política de prevenção e combate branqueamento de capitais, financiamento do terrorismo e financiamento da proliferação de armas de destruição em massa durante o último ano?
5. Existe algum funcionário devidamente qualificado nomeado pelo conselho de administração que possui a responsabilidade geral pela função prevenção e combate branqueamento de capitais, financiamento do terrorismo e financiamento da proliferação de armas de destruição em massa?
6. A instituição implementou uma estrutura formal de governação, onde os comités e sub-comités de gestão de topo são responsáveis pelo cumprimento de prevenção e combate branqueamento de capitais, financiamento do terrorismo e financiamento da proliferação de armas de destruição em massa que também recebem relatórios sobre todas as principais questões de do cumprimento da medidas de mitigação?
7. A informação adequada é transmitida regularmente aos comités e sub-comités? 7.1. As agendas dos comités devem normalmente abordar questões de risco de branqueamento de capitais, financiamento do terrorismo e financiamento da proliferação de armas de destruição em massa e sanções, planos de atenuação de prazos para encerramentos, incluindo controlos provisórios; 7.2. Os comités devem também supervisionar as tipologias de branqueamento de capitais, financiamento do terrorismo e financiamento da proliferação de armas de destruição em massa, novas tendências de risco, estatísticas e quaisquer preocupações regulamentares.
8. O conselho de administração ou órgão equiparado recomendou que se cesse ou se evite estabelecer relações comerciais com clientes para os quais a devida diligência não tenha dado toda a garantia de legitimidade?
9. O conselho de administração aprovou um processo de escalonamento para examinar directamente casos específicos de clientes cuja relação comercial possa incluir questões de branqueamento de capitais, financiamento do terrorismo e financiamento da proliferação de armas de destruição em massa?

Questões sobre *compliance*
1. A instituição tem procedimentos / planos para aumentar a sensibilização do pessoal para os riscos de branqueamento de capitais, financiamento do terrorismo e financiamento da proliferação de armas de destruição em massa?
2. É a formação obrigatória em matéria de prevenção e combate ao branqueamento de capitais, financiamento do terrorismo e financiamento da proliferação de armas de destruição em massa que cobre todos os riscos ministradas ao conselho de administração, aos membros de direcção, à primeira, segunda e terceira linhas de defesa e terceiros para os quais foram externalizadas actividades específicas?
3. A instituição promove formação em matéria de prevenção e combate ao branqueamento de capitais, financiamento do terrorismo e financiamento da proliferação de armas de destruição em massa obrigatória quando o pessoal é contratado e à todo o pessoal numa base anual?
4. Todo o pessoal é obrigado a passar um teste no final da formação com uma nota mínima de conclusão?
5. Existem medidas de acompanhamento nos casos em que um empregado não cumpra o teste, que estão claramente documentadas nas políticas e procedimentos da instituição?
6. Todos os agentes e pessoas agindo em nome e por conta da instituição, em contacto com os clientes, são informados e formados, pelo menos anualmente, sobre factores de risco específicos para o branqueamento de capitais, financiamento do terrorismo e financiamento da proliferação de armas de destruição em massa, incluindo procedimentos operacionais para a realização das tarefas da sua função?
7. Todos os agentes e pessoas agindo em nome e por conta da sua organização, em contacto com os clientes, são informados e formados pelo menos anualmente sobre factores de risco específicos para o financiamento do terrorismo, incluindo procedimentos operacionais para a realização das tarefas da sua função?
8. São realizadas diligências específicas sobre os agentes encarregados da função de prevenção e combate ao branqueamento de capitais, financiamento do terrorismo e financiamento da proliferação de armas de destruição em massa, a fim de assegurar a sua aptidão e propensão?
9. O conselho de administração ou órgão equiparado decidiu sobre disposições específicas relativas à prevenção de conflitos de interesse para o pessoal encarregado das funções de prevenção e combate ao branqueamento de capitais, financiamento do terrorismo e financiamento da proliferação de armas de destruição em massa?
10. O conselho organizou a função de prevenção e combate ao branqueamento de capitais, financiamento do terrorismo e financiamento da proliferação de armas de destruição em massa com todas as disposições relevantes para assegurar a sua independência (remuneração, posicionamento no organigrama, relatórios hierárquicos, etc.)?

Questões sobre assuntos específicos
1. A instituição permite detectar, após a entrada em vigor de uma nova medida nacional ou sanções da Organização das Nações Unidas (ONU), como o congelamento de bens, qualquer soma ou transacção que possa estar em causa?
2. A sua organização permite detectar, após a entrada em vigor de uma nova medida nacional ou sanções da ONU (como o congelamento de bens), fundos e recursos económicos que não pertencem a uma pessoa ou entidade sujeita a um congelamento de bens, mas controlada por ela?
3. No caso da instituição possuir uma ferramenta de filtragem informática automatizada, considera as variações ortográficas dos nomes e apelidos ou nomes destas pessoas ou entidades que não corresponderiam exactamente aos registados nas listas de sanções nacionais e das ONU?
4. O sistema de monitorização da instituição permite detectar operações de caixa desproporcionadas em relação ao perfil do cliente: a) Depósitos em numerário excepcionalmente grandes e depósitos em numerário recorrentes desproporcionados em relação à actividade do cliente; b) Depósitos recorrentes em numerário efectuados por diferentes pessoas ou entidades em contas de um determinado cliente para fins pouco claros e sem qualquer relação entre essas pessoas ou entidades e o cliente.
5. O seu sistema de monitorização permite detectar operações de caixa com características anormais ou anormais: a) Grandes depósitos em numerário que são transferidos, num curto espaço de tempo, para um terceiro que não está intimamente relacionado com a actividade do cliente que transfere; b) Depósitos recorrentes em numerário em várias agências da mesma instituição num curto espaço de tempo, quer pelo mesmo titular da conta, quer por outras pessoas retiradas repetidas de fundos pouco depois do depósito, sem justificação clara.
6. O sistema de controlo interno da instituição permite detectar operações em numerário com utilização anormal de caixas ATMs: a) Grandes depósitos ou levantamentos efectuados através de caixas automáticas para evitar o contacto directo com os funcionários da instituição especialmente se tais depósitos ou levantamentos não estiverem de acordo com a natureza da actividade do cliente; b) Cliente que utiliza vários ATMs para transacções simultâneas em numerário na mesma conta.
7. O sistema da instituição de monitorização permite detectar trocas anormais de dinheiro: a) Pessoas que procuram trocar grandes quantidades de notas de pequeno valor facial por notas de grande valor facial sem justificação clara; b) Pessoas que procuram trocar grandes quantidades de notas danificadas por notas válidas sem justificação clara.
8. O sistema de controlo da instituição permite detectar o uso anormal das contas: a) Clientes que utilizam múltiplas contas para depositar grandes quantias em dinheiro num curto espaço de tempo; b) Múltiplas transacções efectuadas das contas do cliente na instituição para contas em outra instituição, sendo que os fundos

Questões sobre assuntos específicos
retornam à instituição em que as transacções começam; c) Movimentos de débito e crédito de numerário efectuados na mesma conta num curto espaço de tempo, sem justificação clara; d) Utilização pelo cliente da sua conta como conta intermediária entre outras partes ou contas.
9. O sistema de monitorização da instituição permite detectar o uso anormal de contas inactivas: a) Grandes depósitos e levantamentos em numerário de contas inactivas; b) Contas que recebem múltiplos depósitos ou transferências em numerário e são depois encerradas após um curto período ou deixadas estagnadas; c) Grandes transferências do estrangeiro para contas inactivas.
10. O sistema de monitorização da instituição permite detectar a utilização invulgar de transferências: a) Transferências em grandes montantes, especialmente as acompanhadas de instruções de pagamento em dinheiro que não são proporcionais à actividade do cliente; b) Transferências recorrentes de diferentes partes que não têm uma relação clara com o cliente ou as que são enviadas pelo cliente para essas partes; c) Grandes transferências provenientes regularmente de áreas conhecidas por certos crimes, tais como tráfico ou cultivo de droga, ou de estados que não possuem sistemas de prevenção e combate branqueamento de capitais, financiamento do terrorismo e financiamento da proliferação de armas de destruição em massa eficazes; d) Medidas tomadas para se subtrair às proibições de sanções aplicáveis, tais como a remoção, ou a reapresentação e/ou mascaramento de informações relevantes em transacções transfronteiriças.
11. O sistema de monitorização permite detectar reservas de facilidades de crédito pouco usuais: a) Se a instituição oferece crédito documentário, importação ou exportação de bens cujo tipo ou valor não corresponde à natureza ou à dimensão da actividade do cliente ou o valor dos bens indicados na carta de crédito ou nos documentos de cobrança é significativamente diferente do seu valor real; b) Pedido do cliente, sem justificação clara, de alteração do nome do beneficiário da carta de crédito ou dos documentos de cobrança antes do pagamento; c) Abertura de múltiplas cartas de crédito ou negociação através de documentos de cobrança ou contragarantias financeiras de uma forma não consentânea com a actividade do cliente; d) Pedidos de empréstimo através da garantia de activos pertencentes a terceiros, ou da prestação de garantias adicionais por parte de mutuários, sem qualquer ligação clara com estes; e) Reserva de facilidades de crédito contragarantias de uma instituição que opera fora do país, sem razão aparente;

Questões sobre assuntos específicos
f) Pedidos de um cliente mutuário para transferir rapidamente o montante do empréstimo para outras instituições, sem propósito claro.
12. O sistema de monitorização da instituição permite detectar reservas de garantias pouco usuais, tais como: a) Emissão múltipla de cartas de garantia que são desproporcionadas à natureza e dimensão da actividade do cliente; b) Cartas de garantia, contra garantias financeiras que não sejam proporcionais à dimensão da actividade do cliente ou às suas transacções anteriores com a instituição.
13. O sistema de monitorização da instituição permite detectar o reembolso de facilidades de crédito pouco usuais, tais como: a) Condições de pagamento pouco usuais ou pagamento a terceiros que não têm qualquer relação aparente com a carta de crédito ou os documentos de cobrança; b) Pagamento antecipado inesperado de dívidas pelo cliente ou outras partes, especialmente por clientes em falta.
14. O sistema de monitorização da instituição permite detectar liquidações de garantias pouco usuais como: a) Pedido do beneficiário, sem justificação clara, de liquidar cartas de garantia pouco tempo após a sua emissão pela instituição.
15. O sistema de monitorização da instituição permite detectar actividades invulgares de cartões como: Retirada frequentemente repetida no estrangeiro do máximo de dinheiro diário disponível para o cartão.
16. O sistema de monitorização da instituição permite detectar transacções em moeda estrangeira pouco usuais como: Transacções de divisas e cheques de viagem, compra ou venda de divisas estrangeiras para grandes montantes que não são proporcionais à actividade do cliente.

ANEXO VI

Avaliação de risco específica à actividade das instituições de transferência de fundos e instituições de moeda electrónica

1. Categorias de clientes

***a)* Categorias de agentes cujos negócios ou actividades possam indicar um risco mais elevado**, incluindo, de forma exemplificativa:

i. Agentes representando mais de uma instituição de transferência de fundos;

ii. Agentes localizados numa jurisdição ou país de alto risco ou que servem clientes ou transacções de alto risco;

iii. Agentes realizando um número atípico e alto de transacções com outro local de agente, particularmente com um agente numa área geográfica de alto risco ou clientes ou transacções de corredor;

iv. Volume de transacções do agente é inconsistente com o volume geral ou relativo ao volume típico de transacções anteriores;

v. Padrão de transacção indicando o valor das transacções imediatamente abaixo de qualquer limite de diligências adequadas aplicável;

vi. Agentes que foram objecto de atenção negativa da "mídia" credível ou sanções de autoridades de aplicação da lei;

vii. Agentes que não compareceram ou não concluíram as formações;

viii. Agentes que operam programas de conformidade abaixo do padrão, consistindo em programas que não gerem efectivamente o cumprimento de políticas internas, limites monetários, regulamentação externa, etc.;

ix. Agentes com histórico de não conformidade regulatória e que não estão dispostos a seguir as recomendações de revisão do programa de conformidade e sujeitos à suspensão ou rescisão;

x. Agentes que não forneçam as informações necessárias do originador da transferência, após a solicitação;

xi. Agentes cuja colecta de dados ou manutenção de registos é negligente, desleixada ou inconsistente;

xii. Agentes dispostos a aceitar identificação falsa ou registos de identificação que contenham informações falsas, endereços inexistentes que seriam conhecidos como inexistentes para uma pessoa naquela área ou números de telefones falsos ou inexistentes usados como preenchimento;

xiii. Agentes com relação de envio para recebimento desequilibrada, compatível com outros agentes da localidade, ou cujas transacções e actividades indiquem potencial cumplicidade com actividade criminosa;

xiv. Agentes cuja flutuação sazonal de negócios não seja compatível com seus rendimentos ou com outros agentes no local, ou seja, compatível com padrões de procedimentos criminais; e

xv. Agentes cuja proporção de clientes seja duvidosa ou anómala tendo em conta que não fazem parte de grupos normais para os locais onde operam ou locais comparáveis.

***b)* Categorias de clientes cujos negócios ou actividades podem indicar um risco maior,** incluindo:

i. Cliente ou contraparte seja uma instituição de transferência de fundos ou uma instituição financeira que tenha sido sancionada pela respectiva autoridade nacional competente por não cumprir o regime prevenção e combate ao branqueamento de capitais, financiamento do terrorismo e financiamento da proliferação de armas de destruição em massa aplicável e que não esteja a efectuar remediações para melhorar o seu cumprimento.

***c)* Cliente conduzindo suas relações comerciais ou transacções em circunstâncias incomuns,** como:

i. Cliente que percorre distâncias inexplicáveis até locais distantes para realizar transacções;

ii. Redes de clientes (ou seja, grupos definidos de indivíduos que realizam transacções num ou vários pontos de venda, ou em vários serviços);

iii. Cliente possui ou opera um negócio baseado em dinheiro que parece ser uma empresa fictícia ou de fachada, ou mistura receitas ilícitas e lícitas, conforme determinado a partir de uma revisão de transacções que parecem inconsistentes com a situação financeira ou ocupação;

iv. Pessoas Politicamente Expostas, seus familiares ou associados próximos, e quando o beneficiário efectivo de um cliente for uma Pessoa Politicamente Exposta, conforme previsto na Recomendação 12 da GAFI;

v. Cliente não presencial, onde existam dúvidas sobre a sua identidade;

vi. Cliente que utiliza agentes ou associados onde a natureza da relação ou transacção dificulta a identificação do beneficiário efectivo dos fundos;

vii. Cliente que desconhece na íntegra ou está relutante em divulgar detalhes sobre o beneficiário, tais como endereço, informações de contacto etc.;

viii. Cliente que fornece informações inconsistentes (por exemplo: fornece nomes diferentes);

ix. Cliente envolvido em transacções que não tem vínculos aparentes com o país de destino e sem explicações razoáveis;

x. Cliente que tenha sido alvo de sanções de autoridade de aplicação da lei, relativos a produtos geradores de crimes, conhecido pela instituição de transferência de fundos;

xi. Cliente que fornece identificação falsa ou fraudulenta, quer seja evidenciada apenas pelo documento, pela falta de ligação do documento com o cliente ou pelo contexto do documento com outros documentos (por exemplo: utilização de cartões de identificação ou documentos em nomes diferentes sem explicação razoável); e

xii. Cliente cujas transacções e actividades indicam conexão com potencial envolvimento criminal, tipologias ou "bandeiras vermelhas" fornecidas em relatórios produzidos pelo GAFI ou autoridades nacionais competentes, como, por exemplo, o GIFiM e as autoridades policiais.

d) Suspeita de que o cliente está agindo em nome de um terceiro, mas não divulga essa informação, ou está sendo controlado por outra pessoa (seu manipulador). Por exemplo: o cliente leva uma transferência de

dinheiro e imediatamente a entrega a outra pessoa, ou outra pessoa solicita que o cliente faça uma transferência, mas ele coloca a transacção em seu nome.

2. Para além das situações referidas no número anterior, as instituições de transferência de fundos devem ter em contra outras situações de maior risco relacionadas com a sua actividade, podendo incluir, de forma exemplificativa, transacções enviadas ou tentadas, tendo em atenção de forma exemplificativa as seguintes situações:

***a)* Comportamento do cliente no ponto de origem:**

i. O cliente estrutura a transacção numa aparente tentativa de dividir os valores para ficar abaixo de qualquer limite de diligência aplicável, evitando relatórios ou manutenção de registos;

ii. A transacção é desnecessariamente complexa, sem fins comerciais ou legais aparentes;

iii. O número ou valor das transacções é inconsistente com a situação financeira ou ocupação ou está fora do curso normal dos negócios do cliente à luz das informações por ele fornecidas ao realizar a transacção ou durante o contacto subsequente (como uma entrevista, discussão ou com base nas informações fornecidas às autoridades fiscais e disponibilizadas instituição de transferência de fundos, etc.);

iv. O cliente oferece um suborno ou uma gorjeta que não seja habitual ou está disposto a pagar taxas incomuns para que as transacções sejam realizadas;

v. O cliente tem um conhecimento vago sobre a quantia de dinheiro envolvida na transacção;

vi. O cliente faz perguntas incomuns, ameaça ou tenta convencer a equipa a evitar denúncias;

vii. O cliente envia dinheiro internacionalmente e espera receber uma transferência igual ou vice--versa;

viii. O cliente transfere dinheiro para páginas de internet de jogos de azar online ilegais ou verificação da existência de endereços de e-mail contendo referências de jogos de azar ou transferências para países com um grande número de páginas de internet de jogos de azar na internet;

ix. O cliente transfere dinheiro para jurisdição, país ou corredor de maior risco;

x. O cliente tenta uma transacção, mas como provavelmente estaria sujeito à medidas de diligência em função do valor, cancela a transacção para evitar relatórios ou outros requisitos;

xi. O cliente transfere dinheiro para reivindicar prémios de lotaria ou prémios ou para alguém que conheceu apenas online; e

xii. Transferências para cartão de crédito, para taxa de empréstimo, para oportunidade de emprego ou oportunidade de compra misteriosas, constituem indicadores de potencial fraude do consumidor;

xiii. Os remetentes parecem não ter nenhuma relação familiar com o destinatário e nenhuma explicação para a transferência.

***b)* a actividade detectada durante a monitoria,** em muitos desses cenários, a actividade do cliente pode ser aparente tanto durante a interacção no ponto de venda quanto durante a monitoria de transacções de *back-end*, tais como:

i. Transferências para a mesma pessoa de pessoas diferentes ou para pessoas diferentes da mesma pessoa, sem explicação razoável;

ii. Transferências bancárias agregadas incomumente grandes, de alto volume, ou frequência de transacções sem motivo lógico ou aparente;

iii. O cliente usa alcunhas, pseudónimos ou vários nomes e endereços diferentes;

iv. Clientes cujo índice de concentração de transferências feitas para uma jurisdição é notavelmente superior ao esperado considerando a base global de clientes;

v. Clientes que transferem ou recebem fundos de pessoas envolvidas em actividades criminosas conforme as informações disponíveis;

vi. Rede de clientes que usa informações de contacto compartilhadas, como endereço, telefone ou e-mail, onde tal compartilhamento não é normal ou razoavelmente explicável; e

vii. Transferências para HOSSPs em destinos onde tais transacções são consideradas ilegais pela instituição de transferência de fundos.

***c)* transacções recebidas:**

i. Transacções que não são acompanhadas das informações exigidas do originador ou beneficiário;

ii. Situações em que informações adicionais do cliente ou transaccionais foram solicitadas de uma instituição de transferência de fundos solicitante, mas não foram recebidas; e

iii. Grande número de transacções recebidas de uma só vez, ou durante um determinado período de tempo, que não parecem corresponder ao padrão passado usual do destinatário (por exemplo: durante as temporadas de produção de drogas ilícitas, para contrabando de migrantes, etc.).

ANEXO VII

Riscos específicos às actividades dos prestadores de serviços de activos virtuais

Os prestadores de serviços de activos virtuais devem monitorar os riscos específicos das suas actividades, especificamente, de entre outros potenciais, os seguintes:

1. Volume e frequência das transacções, incluindo:

a) estruturação de operações de activos virtuais em pequenos montantes ou em montantes abaixo dos limites de registo ou reporte;

b) realização de várias transacções de alto valor em curto tempo, num padrão escalonado e regular, sem novas transacções registadas, durante um longo período posterior ou para uma conta recém-criada ou ainda para uma conta anteriormente inactiva;

c) transferência de activos virtuais imediatamente para vários prestadores de serviços de activos virtuais;

d) depósito de activos virtuais numa bolsa e, frequentemente, posterior retirada e imediata conversão em vários tipos de activos virtuais ou retirada dos activos de um prestador de serviços de activos virtuais directamente para uma carteira privada;

e) aceitar fundos suspeitos de serem roubados, furtados ou fraudulentos.

2. Indicadores de bandeira vermelha (*red flag)* relacionados aos padrões de transacção, incluído:

a) transacções que correspondam a grandes depósitos iniciais, referentes aos novos usuários, inconsistentes com o perfil do cliente;

b) transacções, referentes a novos usuários, que correspondam a um grande depósito inicial e financiamento total do depósito durante o primeiro dia e o cliente começa a negociar o valor total ou uma grande parte, durante o mesmo dia ou no dia seguinte ou ainda o cliente retira o valor total no dia seguinte;

c) novo usuário que tenta negociar todo o saldo de activos virtuais; e

d) novo usuário que retira os activos virtuais e tenta enviar todo o saldo para fora da plataforma.

3. Transacções relativas a usuários que possam estar preocupados com o princípio de "nenhuma explicação lógica de negócios", incluindo:

a) uso de vários activos virtuais;

b) uso de várias contas;

c) transferências frequentes num determinado período de tempo, nomeadamente, um dia, uma semana, um mês, etc.;

d) transacções recebidas de várias carteiras não relacionadas, em quantidades relativamente pequenas, com posterior transferência para outra carteira ou troca total por moeda fiduciária;

e) conversão de moeda fiduciária em activos virtuais, com perda potencial;

f) conversão de uma grande quantidade de moeda fiduciária em activos virtuais; e

g) conversão de uma grande quantidade de um tipo de activos virtuais em outros tipos de activos virtuais.

4. Indicadores de bandeira vermelha (*red flag*) relativos ao anonimato, incluindo:

a) mais de um tipo de activo virtual envolvido, apesar das taxas de transacção adicionais, especialmente se fornecerem maior possibilidade de anonimato;

b) movimentação de um activo virtual que opera numa *blockchain* pública e transparente para um serviço de câmbio centralizado e, em seguida, a sua imediata troca por uma "*moeda de privacidade*'' ou Criptomoeda Reforçada para Anonimato (CRA);

c) Clientes que operam como um prestador de serviços de activos virtuais não registado ou licenciado em páginas de internet de troca Ponto a Ponto (P2P);

d) actividade transaccional anormal de activos virtuais levantados em serviços de câmbio de carteiras associadas à plataforma P2P;

e) activos virtuais transferidos de e para carteiras que apresentem padrões anteriores de actividade associados ao uso de prestadores de serviços de activos virtuais que operam serviços mistos ou plataformas P2P;

f) utilização de "*mixing and tumbling services*";

g) fundos depositados ou retirados de um endereço ou carteira de activos virtuais com *links* de exposição directa e indirecta à fontes suspeitas conhecidas;

h) uso de carteiras em *hardware* ou papel, descentralizadas ou não alocadas, para transportar activos virtuais além-fronteiras;

i) usuários da plataforma de prestadores de serviços de activos virtuais que registam seus nomes de domínio na *internet* por meio de proxies ou usando Domain Name System (DNS) que suprimem ou eliminam os proprietários dos nomes de domínio;

j) usuários da plataforma de prestadores de serviços de activos virtuais que utilizam um endereço IP associado a uma *darknet* ou outro *software* similar que permita comunicação anónima;

k) transacções por meios de comunicação criptografados anónimos em detrimento de um prestador de serviços de activos virtuais;

l) existência de um grande número de carteiras de activo virtuais, aparentemente não relacionadas, controladas a partir do mesmo endereço IP ou Endereço de Controlo de Acesso de Media (MAC *Adreess*);

m) utilização de activos virtuais cujo projecto não está devidamente documentado;

n) utilização de activos virtuais vinculados a possíveis fraudes ou esquemas fraudulentos;

o) recepção ou envio de fundos para prestadores de serviços de activos virtuais cujos processos de "Conheça o seu Cliente" sejam fracos ou inexistentes; e

p) utilização de caixas de ATMs ou quiosques digitais de activos virtuais apesar das taxas de transacção serem mais altas, incluindo as comumente usadas por mulas de dinheiro (*money mule*) ou vítimas de fraudes ou golpes, especialmente em locais de alto risco, onde ocorrem maiores actividades criminosas.

Observação: uma única utilização de uma ATM não é necessariamente uma bandeira vermelha, excepto se a ATM estiver numa área de alto risco ou usado para pequenas transacções repetidas ou para outros factores adicionais.

5. Indicadores de bandeira vermelha (*red flag*) sobre remetentes ou destinatários, incluindo:

a) durante a criação da conta:

i. Criação de contas separadas com nomes diferentes;

ii. Transacções iniciadas de endereços IP não confiáveis, endereços IP de jurisdições sancionadas ou endereços IP previamente sinalizados como suspeitos;

iii. Tentativa de abrir uma conta frequentemente no mesmo prestador de serviços de activos virtuais a partir do mesmo endereço IP; e

iv. Comerciantes ou usuários corporativos com registos de domínio da internet numa jurisdição diferente da sua jurisdição de estabelecimento ou em outra com um processo fraco para registo de domínio.

b) durante o processo de diligência reforçada:

i. Informações de "Conheça o Seu Cliente" incompletas ou insuficientes ou ainda clientes que recusam solicitações de documentos relacionados ou consultas sobre a origem dos fundos;

ii. Transacções sem conhecimento do remetente, destinatário ou em que são fornecidas informações imprecisas sobre a transacção, fonte de recursos ou relacionamento com a contraparte; e

iii. Cliente que forneça documentos falsificados ou fotografias editadas como parte do processo de integração.

c) perfil do Cliente:

i. Cliente que forneça dados de identificação ou credenciais de conta partilhadas por outra conta;

ii. Endereços IP associados ao perfil do cliente diferentes dos endereços IP a partir dos quais as transacções são iniciadas;

iii. Endereço virtual (*virtual address*) de um cliente que aparece em fóruns públicos associados a actividades ilegais;

iv. Cliente conhecido por meio de informações publicamente disponíveis devido à associação criminosa anterior; e

v. O perfil do cliente não corresponde à negociação regular de activos virtuais de alto valor.

d) perfil de potencial mula de dinheiro (*money mule*) ou vítima de golpe:

i. Remetente não familiarizado com a tecnologia activos virtuais ou soluções de carteira de custódia online;

ii. Cliente muito mais velho do que a idade média dos usuários da plataforma que abrem uma conta e realizam várias transacções;

iii. Cliente financeiramente vulnerável; e

iv. Cliente que adquire grandes quantias de activos virtuais não comprovada pela riqueza disponível ou inconsistente com seu perfil financeiro histórico.

6. Outros comportamentos incomuns, incluindo:

a) clientes que alterem frequentemente suas informações de identificação, tais como endereços de e-mail, endereços IP, informações financeiras, etc.;

b) clientes que tentam entrar nas plataformas de um ou mais prestadores de serviços de activos virtuais com recurso a diferentes endereços IP com frequência, no mesmo dia;

c) utilização de linguagem nos campos de mensagens de activos virtuais indicativas de transacções de apoio à actividade ilícita ou compra de bens ilícitos; e

d) clientes que realizem repetitivamente transacções com um subconjunto de indivíduos com lucro ou prejuízo significativo.

7. Indicadores de bandeira vermelha (*red flag*) na fonte de fundos ou riqueza, incluindo:

a) transacções com endereços de activos virtuais ou cartões bancários ligados a esquemas conhecidos de fraude, extorsão, ransomware, endereços sancionados, mercados darknet ou outras páginas de internet ilícitos;

b) transacções de activos virtuais originadas ou destinadas aos serviços de jogos de fortuna e azar online;

c) uso de um ou vários cartões de crédito ou de débito vinculados à carteira de activos virtuais para retirar grandes quantias de valores fiduciários;

d) recursos para compra de activos virtuais provenientes de depósitos em dinheiro em cartões de crédito;

e) depósitos em conta ou endereço de activos virtuais significativamente maior que o normal, com origem desconhecida de recursos, seguido de conversão para moeda fiduciária;

f) falta de transparência ou de informação suficiente sobre a origem e titulares dos fundos;

g) transacções recebidas de sistemas de pagamentos online através de cartões de crédito ou pré-pago, seguido de levantamento instantâneo;

h) fundos provenientes directamente de serviços mistos de terceiros ou de carteira;

i) grande parte da fonte de riqueza de um cliente derivada de investimentos em activos virtuais, Initial *Coin Offering* fraudulentas, etc.; e

j) fonte de riqueza do cliente desproporcionalmente extraída de activos virtuais originários de outros prestadores de serviços de activos virtuais que não possuem controlos para a prevenção e combate ao branqueamento de capitais, financiamento do terrorismo e financiamento da proliferação de armas de destruição em massa.

8. Indicadores de bandeira vermelha (*red flag*) relativos a riscos geográficos, incluindo:

a) fundos do cliente que provêm de ou são enviados para uma carteira não registada na jurisdição onde o cliente ou a bolsa está localizada;

b) cliente que usa uma bolsa de activos virtuais ou instituição de transferência de fundos localizado numa jurisdição de alto risco que possuam regulamentos de prevenção e combate ao branqueamento de capitais, financiamento do terrorismo e financiamento da proliferação de armas de destruição em massa inadequados para prestadores de serviços de activos virtuais e medidas inadequadas de diligência ou "Conheça o Seu Cliente";

c) cliente que envie fundos para prestadores de serviços de activos virtuais que operam em jurisdições que não possuam regulamentação de activos virtuais ou que não implementem controlos de prevenção e combate ao branqueamento de capitais, financiamento do terrorismo e financiamento da proliferação de armas de destruição em massa;

d) cliente que instale ou mude de escritórios para jurisdições que não possuam regulamentação ou não implementem regulamentação que rege os activos virtuais; e

e) cliente que estabeleça novos escritórios em jurisdições onde não há uma lógica comercial clara para o fazer.

Aviso n.º 11/GBM/2024

de 30 de Agosto

Havendo necessidade de estabelecer o capital social mínimo das sociedades de garantia mútua e das sociedades gestoras dos fundos de garantia mútua, o Banco de Moçambique, no uso das competências que lhe são conferidas pelo n.º 1 do artigo 81 da Lei n.º 20/2020, de 31 de Dezembro, Lei das Instituições de Crédito e Sociedades Financeiras, determina:

Artigo 1

(Objecto)

O presente Aviso estabelece o capital social mínimo das sociedades de garantia mútua e das sociedades gestoras de fundos de garantia mutuária.

Artigo 2

(Âmbito)

O presente Aviso aplica-se:

a) às sociedades de garantia mútua;