Banco Nacional de Angola

Guia sobre a implementação de um programa de prevenção do branqueamento de capitais e do financiamento do terrorismo

Documento destinado às instituições financeiras sob a supervisão do Banco Nacional de Angola

1 Introdução

1.1 Objectivo do documento

Este documento visa clarificar o que é esperado das instituições financeiras relativamente à prevenção do branqueamento de capitais (BC) e do financiamento do terrorismo (FT) e a proliferação de armas de destruição em massa, nos termos do disposto na Lei n.º 05/20, de 27 de Janeiro, não possuindo um carácter vinculativo.

As instituições financeiras possuem discricionariedade na implementação das políticas e respectivos processos.

Os principais objectivos deste documento são:

- Interpretar os requisitos legais e regulamentares e fornecer indicações gerais sobre a implementação dos mesmos;
- Indicar exemplos gerais e específicos relativos aos vários processos de prevenção de BC, FT e PA mediante a implementação de uma abordagem baseada no risco, adequada à dimensão e natureza do negócio;
- Auxiliar as instituições financeiras no que diz respeito à implementação dos controlos necessários para mitigar o risco de envolvimento em práticas criminosas.

1.2 Destinatários

Este documento destina-se às instituições financeiras sob a supervisão do Banco Nacional de Angola, nos termos do disposto no artigo 2.º e 9.º da Lei n.º 14/21, de 19 de Maio - Lei do Regime Geral das Instituições Financeiras, assumindo especial incidência relativamente às instituições financeiras bancárias.

1.3 Definição de BC e FT

O branqueamento de capitais e o financiamento do terrorismo encontram-se criminalizados nos artigos 82.º e 83.º da Lei n.º 05/20, de 27 de Janeiro.

O crime de branqueamento de capitais corresponde ao processo de ocultação da existência, origem ilegal ou a utilização de bens provenientes de actividades criminosas, de modo a fazer com que estes bens pareçam legítimos.

Para efeitos de branqueamento de capitais, de acordo com 82.º da Lei n.º 05/20, de 27 de Janeiro, são actividades criminosas relevantes todos os factos ilícitos típicos puníveis com pena de prisão de 2 (dois) a 8 (oito) anos em conformidade com disposto no Código Penal em vigor e legislação criminal avulsa.

Em consonância com as exigências estabelecidas nas Recomendações do GAFI/FATF (40 Recomendações e 9 Recomendações Especiais) e nas Convenções das Nações Unidas, nomeadamente na Convenção contra a Criminalidade Organizada Transnacional (Convenção de Palermo), Convenção sobre o Tráfico Ilícito de Estupefacientes e Substâncias Psicotrópicas (Convenção de Viena) e Convenção para a Supressão do Financiamento do Terrorismo, existe um conjunto de crimes cujo produto apresenta maior susceptibilidade de ser objecto de branqueamento de capitais como o tráfico de estupefacientes, contrabando, fraude ou extorsão (neste sentido vide **o Anexo I** do presente documento).

Geralmente, o processo de branqueamento de capitais consiste em três fases distintas:

- Colocação: a introdução dos bens provenientes da actividade criminosa (ex. furto) no sistema financeiro através do depósito, transferências electrónicas ou outros meios. Um exemplo de colocação poderá ser o depósito de vários montantes em numerário numa conta bancária.
- Ocultação: a execução de transacções (múltiplas) de modo a separar os bens ganhos ilicitamente, da sua fonte. Um exemplo de ocultação poderá ser a conversão de numerário em cheques de viagem, ordens de pagamento, etc.
- Integração: a colocação dos bens ilícitos, novamente, na economia formal, de modo a criar a percepção de legitimidade. Um exemplo de integração poderá ser o pagamento de empréstimos (falsos), comissões ou salários.

O financiamento do terrorismo pode ser definido como o fornecimento ou recolha de fundos, por qualquer meio, directa ou indirectamente, com a intenção de os utilizar ou tenha conhecimento que de que possam vir a ser utilizados, total ou parcialmente no planeamento, preparação ou prática de um crime de organização terrorista, terrorismo ou terrorismo internacional.

A maior diferença entre o branqueamento de capitais e o financiamento do terrorismo assenta no facto do branqueamento de capitais envolver sempre bens provenientes de actividade ilícita. Por outro lado, os fundos utilizados para financiamento do terrorismo podem ser de carácter legal, não obstante, a finalidade para a qual são utilizados ser ilegítima.

Note-se que, apesar da origem dos fundos utilizados para financiamento do terrorismo poder ser legítima, as organizações terroristas continuam a possuir a necessidade de dissimular o rasto dos fundos, de modo a esconder a ligação entre os investidores e a organização terrorista ou as actividades terroristas.

1.4 Outros crimes financeiros

O risco de branqueamento de capitais e de financiamento do terrorismo estão directamente relacionados aos riscos associados a outros crimes financeiros, como a utilização abusiva de informação privilegiada, manipulação do mercado, fraude ou desvio de fundos (neste sentido *vide* **Anexo I** do presente documento para outros exemplos de crimes financeiros);

Estas orientações não são dirigidas à detecção de actividades relacionadas com fraude ou abuso de mercado, enquanto crimes autónomos, mas estes crimes devem ser tidos em consideração durante a leitura deste documento, dado que são infracções subjacentes ao branqueamento de capitais.

As instituições financeiras podem associar a fraude e o branqueamento de capitais como parte de uma estratégia global para combater o crime financeiro, considerando os procedimentos já existentes contra a fraude e o abuso de mercado.

2 Enquadramento legal e regulamentar

2.1 Legislação e regulamentação aplicável

Legislação

Lei n.º 05/20, de 27 de Janeiro, Lei de prevenção e repressão do branqueamento de capitais e do financiamento do terrorismo e da proliferação de armas de destruição em massa, que revogou a Lei n.º 12/10, de 9 de Julho
Decreto Presidencial n.º 02/18, de 11 de Janeiro, que estabeleceu a organização e funcionamento da Unidade de Informação Financeira
Lei n.º 1/12, de 12 de Janeiro, Lei da designação e aplicação de actos internacionais

Regulamentação

Aviso n.º 14/2020, de 22 de Junho, destinado às instituições financeiras bancárias e não bancárias
Instrutivo n.º 20/2020, de 09 de Dezembro - Relatório de Prevenção ao Branqueamento de Capitais, Financiamento do Terrorismo e da Proliferação - Avaliação do Risco - Ferramentas e Aplicativos Informáticos
Instrutivo n.º 02/12, de 20 de Abril, destinado às casas de câmbio
Directiva n.º 01/DSI/12, de 10 de Abril, sobre a comunicação de operações suspeitas à Unidade de Informação Financeira
Directiva n.º 03/DSI/2012, de 24 de Julho, sobre a comunicação de pessoas, grupos ou entidades designadas
Directiva n.º 04/DSI/2012 de 24 de Julho, sobre o congelamento de fundos e recursos económicos de Pessoas, Grupos ou Entidades Designadas

2.2 Obrigações das instituições financeiras em sede de BC e FT

O branqueamento de capitais e o financiamento do terrorismo foram criminalizados através Lei n.º 05/20, de 27 de Janeiro.

Esta Lei implementou novas medidas de prevenção do branqueamento de capitais e financiamento do terrorismo no início e durante a relação de negócio e/ou no estabelecimento de uma transacção ocasional.

Neste sentido, foram determinadas as seguintes obrigações gerais, a saber:

- Obrigação de Identificação e verificação da identidade do cliente e, caso aplicável, dos seus representantes e do beneficiário efectivo;
- Obrigação de identificação e diligência, incluindo diligência reforçada;
- Obrigação de recusa de estabelecimento de relação de negócio ou execução de transacção ocasional, em caso de impossibilidade de cumprimento das obrigações de identificação e diligência;
- Obrigação de conservação de registos referentes ao cliente e a transacções, no mínimo por um período de até 10 (dez) anos;

- Obrigação de comunicação das informações legalmente devidas à Unidade de Informação Financeira;
- Obrigação de abstenção da realização de operações quando se constate que uma determinada operação que evidencia fundada suspeita de constituir prática de crime;
- Obrigação de cooperação e prestação de informação das instituições financeiras com as autoridades competentes, nomeadamente autoridades de supervisão autoridades governamentais;
- Obrigação de sigilo das instituições financeiras face aos clientes ou a terceiros relativamente à comunicação de informações legalmente devidas ou que se encontrem sob investigação criminal;
- Obrigação de estabelecer políticas e processos em matérias de controlo interno, em particular gestão do risco e auditoria, bem como os processos adequados para assegurar critérios exigentes de contratação de empregados, de forma a permitir-lhes que, em qualquer altura, estejam aptos a cumprir as obrigações preconizadas pela Lei n.º 05/20, de 27 de Janeiro;
- Obrigação de garantir a formação adequada aos seus empregados e gestores, visando o cumprimento das obrigações impostas pela Lei n.º 05/20, de 27 de Janeiro, e regulamentação em matéria de prevenção e repressão do branqueamento de capitais e do financiamento do terrorismo.

O Banco Nacional de Angola emitiu o Aviso n.º 14/2020, de 22 de Junho (doravante designado por Aviso) e o Instrutivo n.º 02/12, de 20 de Abril, que contêm normas específicas destinadas às instituições financeiras bancárias e não bancárias no âmbito da prevenção de branqueamento de capitais e ao financiamento do terrorismo.

3 Abordagem ao programa de prevenção de BC e de FT

As instituições financeiras devem implementar um programa de prevenção do branqueamento de capitais e de financiamento do terrorismo de forma a conseguir identificar, monitorizar e impedir actividades de natureza criminosa, nos termos do disposto na Lei de prevenção e combate do branqueamento de capitais e financiamento do terrorismo e a proliferação de armas de destruição em massa - Lei n.º 05/20, de 27 de Janeiro.

O programa de prevenção de branqueamento de capitais e de financiamento do terrorismo assenta numa abordagem baseada no risco, ou seja, a instituição financeira deve identificar as áreas potencialmente vulneráveis a serem utilizadas para o branqueamento de capitais e o financiamento do terrorismo.

Uma abordagem baseada no risco deve incluir a identificação e avaliação dos riscos associados ao branqueamento de capitais e financiamento do terrorismo e, consequentemente, a definição dos controlos a serem estabelecidos para os diferentes riscos identificados.

Assim, a instituição financeira deve identificar e avaliar os clientes, entidades, produtos, serviços e localizações geográficas que representam um maior risco de BC e FT (relativamente a todas as linhas de negócio). Cabe a cada instituição financeira definir a abordagem mais apropriada considerando a sua vulnerabilidade aos factores enunciados.

Importa referir que, naturalmente, uma abordagem baseada no risco não deve ser concebida de forma a impossibilitar a realização de negócios pelas instituições financeiras e, por si só, não garante que o branqueamento de capitais e financiamento do terrorismo não aconteça ou que seja efectivamente detectado.

No final, e independentemente da estratégia adoptada, devem estar cumpridas as obrigações previstas legalmente, ou seja, a instituição financeira deve conhecer adequadamente os seus clientes e se estes são susceptíveis de estarem envolvidos em actividades criminosas.

3.1 Risco de BC e de FT

O branqueamento de capitais e o financiamento do terrorismo determinam a existência de vários riscos para a instituição financeira. Existem áreas de risco a considerar como associadas ao branqueamento de capitais e financiamento do terrorismo, como o risco de *compliance* ou o *risco reputacional.*

Estes riscos não são exclusivos e, encontram-se frequentemente, interligados exercendo uma influência directa entre si. A gestão efectiva do risco de branqueamento de capitais e financiamento do terrorismo é crucial para a estabilidade da instituição financeira e do sistema financeiro.

O risco de *compliance* será o risco proveniente de violações ou incumprimento de leis, regras, regulações, contratos, práticas prescritas ou *standards* éticos. Neste sentido a instituição financeira está sujeita a um risco acrescido quando viola a legislação ou regulação existente no âmbito do branqueamento de capitais e financiamento do terrorismo, ficando sujeita a sanções, responsabilidade civil, etc.

O risco de *compliance* pode ter impacto na imagem das instituições financeiras por parte de clientes, contrapartes, accionistas, investidores, supervisores e opinião pública em geral (risco de reputação). Quando uma instituição financeira não coloca em prática programas efectivos de prevenção de BC/FT pode ficar associada a este tipo de actividades e, por conseguinte, aumenta o seu risco reputacional.

3.2 Factores do risco de BC e FT

De modo a analisar adequadamente o risco de BC e de FT, as instituições financeiras devem identificar os factores que estão na base desse risco. Note-se que não existe uma única metodologia, uma vez que os distintos níveis de risco dependem de diferentes factores característicos de cada instituição financeira, incluindo a sua estrutura, actividades (inter) nacionais, produtos e serviços, base de clientes, etc.

Por exemplo, os riscos para uma instituição financeira internacional com diversas unidades de negócio serão diferentes dos riscos inerentes a uma instituição financeira que apenas presta serviços no mercado local.

3.2.1 Identificação dos factores de risco

De acordo com as práticas internacionais[1] em vigor, podem ser tidos em consideração os seguintes factores gerais:

- ► Cliente / Transacções;
- ► Produto;
- ► Serviço;
- ► Canal de distribuição;
- ► Localização geográfica.

3.2.1.1 Cliente

Nos termos do disposto nos artigos 9.º e 10.º da Lei n.º 05/20, de 27 de Janeiro, as instituições financeiras devem adoptar um sistema de gestão de risco de BC e de FT associado aos clientes, tanto em relação a novos clientes como a clientes já existentes, de modo a garantir que as medidas de identificação e diligência sejam adaptadas ao perfil de risco identificado, com vista à prevenção de branqueamento de capitais e do financiamento do terrorismo.

---

[1] Financial Action Task Force, '*Guidance on the Risk Based Approach to Combating Money Laundering and Terrorist Financing',* Junho 2007

Todos os clientes (existentes ou potenciais) podem ser considerados como susceptíveis de estarem relacionados com o BC e FT, contudo determinados clientes e entidades podem assumir um risco acrescido devido a determinadas características, que incluem, entre outras:

- Natureza do cliente (natureza jurídica, estrutura da propriedade, etc);
- Natureza da actividade do cliente;
- Complexidade, volume e natureza das transacções (a serem) efectuadas pelo cliente;
- Origem dos fundos do cliente;
- Histórico do cliente;
- Relacionamento do cliente com outros clientes (mesmo que estes últimos não sejam intervenientes nas respectivas relações de negócio estabelecidas com a instituição financeira).

As seguintes categorias de clientes podem representar um maior risco de branqueamento de capitais e financiamento do terrorismo:

- Clientes cujas actividades sejam conhecidas por estarem associadas a corrupção (por exemplo: negociantes de armas);
- Clientes que sejam pessoas politicamente expostas;
- Clientes cuja origem dos fundos seja difícil de apurar;
- Clientes com estruturas complexas ou pouco transparentes, que impeçam a identificação dos beneficiários efectivos;
- Clientes cujas actividades estejam relacionadas com negócios de grande liquidez, tais como:
  - Actividades relacionadas com serviços de pagamento (por exemplo: prestadores de remessas de valores, casas de câmbio, agentes que executam transferências de fundos ou outros negócios que visem a transferência de fundos);
  - Actividades relacionadas com a indústria do Jogo (por exemplo: casinos);
  - Negociantes de bens de valor elevado (por exemplo: negociantes de jóias, metais e pedras preciosas, negociantes de arte e antiquários, leiloeiras, agentes e corretores imobiliários);
  - Outros negócios que gerem montantes substanciais de dinheiro (por exemplo: negociantes de automóveis e agências de turismo).
- Clientes que realizem as seguintes transacções:
  - Movimentos frequentes e injustificados de contas para outras instituições financeiras;
  - Movimentos frequentes e injustificados de fundos entre instituições financeiras diferentes;
  - Movimentos frequentes e injustificados entre diferentes jurisdições;
  - Transacções avultadas e de cariz complexo que não encaixam no perfil do cliente;
  - Clientes que solicitam produtos e serviços que não estão em conformidade com o conhecimento que a instituição financeira tem do cliente, isto é, que não se enquadram com o seu perfil.

As instituições financeiras devem ter presente que as categorias mencionadas contêm características que poderão indicar envolvimento em actividades associadas ao BC ou ao FT, contudo, tal não significa que exista,

necessariamente, uma suspeita de tais actividades; por exemplo, se a transacção encaixa no perfil esperado do cliente e haja uma explicação lógica em termos de negócio para essa transacção ou a relação de negócio ser legítima. Caso aplicável, o histórico da relação de negócio deve ser revisto para determinar se existe um racional (comercial) para que o cliente adquira o produto ou serviço em questão ou realize determinada transacção.

Caso se confirme que não existe nenhuma razão aparente para este comportamento, a instituição financeira deve considerar a possibilidade de envolvimento em BC ou FT, e recusar estabelecer qualquer relação de negócio, assim como deve reportar essa situação à Unidade de Informação Financeira.

3.2.1.2 Produto/ serviço / canal de distribuição

Existem produtos e serviços disponibilizados ao cliente susceptíveis de serem utilizados para branqueamento de capitais ou financiamento de terrorismo. As instituições financeiras devem, no âmbito da avaliação de risco, questionar se as características de determinado produto/serviço podem ser utilizadas para realizar actividades relacionadas com o BC, FT ou qualquer outro crime, por exemplo, a possibilidade de executar pagamentos a terceiros, a complexidade e transparência do produto ou serviço.

Tendo em conta que as instituições financeiras disponibilizam produtos/serviços com características diferentes, não é possível estabelecer um padrão para a classificação de risco dos produtos/serviços, não obstante, os serviços de correspondência bancária, serviços de "*private banking*" e serviços relacionados com depósitos ou pagamentos em numerário serem geralmente considerados de risco elevado para as instituições financeiras.

Existem vários exemplos de como o canal de distribuição de um serviço ou produto pode aumentar o risco da transacção porque não existe uma relação presencial com o cliente que permita aferir a veracidade dos elementos disponibilizados, nomeadamente, quando um cliente deseja abrir uma conta através da *internet*, ou quando não se encontra presente na mesma jurisdição da instituição financeira.

3.2.1.3 Localização geográfica

Alguns países/jurisdições são potencialmente mais susceptíveis ao BC/FT que outros, tais como, países sem legislação apropriada de combate a estes crimes.

Este factor de risco implica que as instituições financeiras realizem a avaliação da localização:

- ► País/jurisdição de residência do cliente;
- ► País/jurisdição de residência da empresa-mãe, subsidiárias e/ou beneficiário efectivo último;
- ► País/jurisdição onde a maioria das actividades de negócio são desempenhadas;
- ► País/jurisdição onde estão localizados os parceiros comerciais.

As seguintes categorias, entre outras, podem ser consideradas pela instituição financeira como possuindo um risco mais elevado associado à localização geográfica:

- ► Países/jurisdições sujeitos a sanções, embargos ou outras medidas semelhantes emitidas pelas Nações Unidas ou por organizações internacionais semelhantes;
- ► País/jurisdição sujeito a qualquer tipo de sanção aplicada pelo Governo de Angola;
- ► Países identificados, por fontes credíveis, como países com ausência de leis, regulações e outras medidas de combate ao branqueamento de capitais e financiamento de terrorismo;
- ► Países identificados, por fontes credíveis, como países que apoiam actividades terroristas;

► Países identificados, por fontes credíveis, como países onde existam níveis significativos de corrupção, ou de outras actividades criminosas.

Não existem critérios gerais e independentes para a classificação de países relativamente à sua susceptibilidade para o branqueamento de capitais e financiamento do terrorismo. Não obstante, as instituições financeiras podem desenvolver o seu próprio modelo de classificação do risco de um país, usando fontes credíveis independentes, nomeadamente:

► Publicações emitidas pelo Grupo de Acção Financeira Internacional (GAFI);

► Publicações emitidas pelas Nações Unidas;

► Publicações emitidas pelo Banco Mundial;

► Publicações emitidas pela Transparência Internacional (TI);

► Publicações emitidas pelas autoridades governamentais Angolanas.

3.2.2 Análise e revisão dos factores de risco

A combinação dos factores de risco associados ao cliente, ao produto, serviço, canal de distribuição e localização geográfica determinam o risco geral de uma relação de negócio ou transacção ocasional, e consequentemente, as medidas de diligência aplicáveis.

De uma forma geral, a título ilustrativo, após a análise realizada dos factores de risco os seguintes perfis de risco podem ser estabelecidos ao nível da sua base de clientes, produto, serviço, canal, localização geográfica:

► Baixo:

► Normal;

► Elevado;

► Inaceitável.

As instituições financeiras poderão desenvolver uma matriz de risco na qual os diferentes possíveis indicadores e categorias de risco são combinados numa categoria de risco final que será materializada nas políticas da instituição financeira.

A matriz de risco das instituições financeiras deve ser adaptada aos indicadores e categorias de risco identificados pela instituição, desde que justificáveis e em linha com a sua politica de gestão de risco (a título de exemplo *vide* a matriz ilustrativa constante no **Anexo 1)**.

A instituição financeira deve rever periodicamente a adequação da análise dos factores de risco de BC e FT. A gestão do risco é um processo dinâmico dado que a vulnerabilidade dos produtos/transacções a actividades relacionadas com o BC e FT variam também em função da percepção externa da sua vulnerabilidade.

É recomendável, no mínimo, a revisão anual de avaliação do risco, e mais frequentemente quando a instituição financeira introduz novos produtos ou serviços, aceita ou rejeita novas relações de negócio ou transacções com clientes de risco elevado ou foi objecto de fusões ou cisões com outras instituições financeiras ou entidades.

3.3 Programa de prevenção do BC e FT

As instituições financeiras devem mitigar e gerir internamente o risco de BC e FT identificado, de acordo com o disposto nas secções anteriores, através da definição e implementação de um programa transversal a toda a organização, incluindo, caso necessário, todo o grupo financeiro ou económico, consubstanciado em políticas e processos, e respectivo modelo orgânico e funcional, de forma a assegurar que os riscos assumidos se mantenham ao nível previamente definido pelo Órgão de Gestão e que não afectem, significativamente, a situação financeira da instituição ou do grupo.

Este programa tem de ser adequado às operações das instituições financeiras e à sua dimensão permitindo um conhecimento suficiente dos seus clientes e das relações de negócio, de modo a reconhecer atempadamente os riscos relacionados com branqueamento de capitais e financiamento do terrorismo e tomar as medidas de diligência necessárias para os mitigar.

O programa de prevenção de BC e FT é constituído por políticas e processos, assente numa estrutura organizacional adequada assegurando o cumprimento dos requisitos legais e regulamentares em sede de prevenção de branqueamento de capitais e do financiamento do terrorismo, assim como dos parâmetros de risco assumidos pela instituição financeira relativamente a BC e FT.

Destacam-se, no mínimo, quatro componentes essenciais inerentes a qualquer programa de prevenção de BC e FT:

- ► Políticas;
- ► Modelo orgânico e funcional;
- ► Programa de formação e sensibilização;
- ► Processos de prevenção do BC e do FT.

A politica de prevenção do BC e do FT da instituição financeira pode incluir, entre outros elementos:

- Declaração da cultura e valores a serem adoptados pela instituição relativamente à prevenção das actividades criminosas no sistema financeiro
- Obrigação de conhecer a "identidade" do cliente tanto no início como durante a relação de negócio através da realização de medidas que permitam verificar a identidade e negócio do clientes
- Obrigação de formar os respectivos colaboradores relativamente às obrigações legais em sede de BC e FT
- Abordagem sumária da instituição financeira relativamente À avaliação e gestão do risco de BC e FT
- Alocação de responsabilidades em sede de BC e FT a pessoas ou funções específicas

Fonte: JMLSG, Prevention of money laundering

3.3.1 Políticas

A instituição financeira deve elaborar políticas, incluindo se risco de branqueamento de capitais e financiamento do terrorismo previamente realizada.

As políticas devem estabelecer os padrões mínimos de cumprimento dos requisitos legalmente exigidos, de forma transversal a toda a organização.

Nos termos do disposto no Aviso n.º 14/2020, de 22 de Junho, a definição das políticas da instituição financeira devem ser da responsabilidade do *Compliance Officer de ABC/CFT*, aprovadas pelo Órgão de Gestão e disponibilizadas a todos os colaboradores da instituição financeira.

Adicionalmente, deve ser implementado um processo que garanta a revisão periódica das referidas políticas e a respectiva aprovação pelo Órgão competente.

A instituição financeira deve definir e elaborar políticas, entre outras, que visem implementar processos e procedimentos sobre:

- ► Prevenção do BC e FT;
- ► Sanções financeiras;
- ► Aceitação de clientes;
- ► Diligência, incluindo diligência reforçada;

- ► Pessoas politicamente expostas;
- ► Comunicação de operações suspeitas;
- ► Conservação de registos.

Complementarmente, e caso aplicável, podem ser elaboradas políticas relativas a linhas de negócio especificas para assegurar o cumprimento dos requisitos específicos das linhas de negócio em sede de prevenção do branqueamento de capitais e financiamento do terrorismo.

3.3.1.1 Políticas de sanções financeiras

Sanções financeiras são medidas restritivas de natureza financeira implementadas por organizações internacionais ou por países (a título individual) aplicáveis a jurisdições, pessoas ou entidades com o propósito de combater o terrorismo e manter ou restaurar a paz e a segurança internacional.

De entre os países ou organizações internacionais que mantêm listas de pessoas, grupos ou entidades designadas destaca-se, entre outros o Office for Foreign Assets and Control (OFAC), Her Magesty's Treasury (HMT), o European Union's Common Foreign and Security Policy (CFSP) e o Comité de Sanções de acordo com as diferentes Resoluções do Conselho de Segurança das Nações Unidas (CSNU).

De acordo com a Directiva 03/DSI/12, de 24 de Julho, emitida pelo Banco Nacional de Angola, são «pessoas, grupos ou entidades designadas» as pessoas, grupos ou entidades designadas:

- ► Pelo Comité de Sanções das Nações conforme a Resolução do Conselho de Segurança das Nações Unidas n.º 1267, mediante a Lista actualizada pelo referido Comité de Sanções;
- ► Pelo Comité de Sanções conforme a Resolução do Conselho de Segurança das Nações Unidas n.º 1988, que mantém uma Lista actualizada de pessoas, grupos e entidades associados com os Talibã, que constituam uma ameaça para a paz, estabilidade e segurança do Afeganistão;
- ► Por qualquer outro Comité de Sanções criado pela Organização das Nações Unidas ou outro organismo da Organização das Nações Unidas que mantenha listas de pessoas, grupos ou entidades associadas ao terrorismo, incluindo o financiamento do terrorismo, a terroristas ou a organizações terroristas, com vista à aplicação de medidas restritivas de natureza financeira; e
- ► Pela autoridade nacional competente pela designação nacional e aplicação de medidas restritivas, mediante Lista nacional, conforme a Lei n.º 1/12, de 12 de Janeiro - Lei sobre a Designação e Execução de Actos Jurídicos Internacionais, sempre que a designação for relativa a pessoas, grupos ou entidades associadas ao terrorismo, incluindo o financiamento do terrorismo, a terroristas ou a organizações terroristas, com vista à aplicação de medidas restritivas de natureza financeira.

No mínimo, a politica de sanções financeiras a implementar pela instituição financeira deve compreender os seguintes temas:

- ► Definição de sanção financeira;
- ► Definição de «pessoa*, grupo ou entidade designada*» que abranja no mínimo, a definição acima mencionada, sem prejuízo da instituição ter a liberdade de alargar a definição a outras Listas de pessoas, grupos ou entidades designadas por outros países ou organizações internacionais; e,
- ► Princípios gerais e procedimentos a aplicar pela instituição financeira quando uma transacção envolve uma jurisdição sancionada ou identifique uma pessoa, grupo ou entidade sancionada envolvida numa relação de negócio ou transacção.

Não obstante, as instituições financeiras devem estar atentas a outras medidas restritivas de natureza não financeira, nomeadamente medidas comerciais, diplomáticas ou outras que visam a modificação das actividades aplicáveis a jurisdições, pessoas ou entidades, implementadas por organizações internacionais ou por países (a título individual) que possam impactar directa ou indirectamente a sua actividade.

3.3.2 Modelo orgânico e funcional (*Governance*) em sede de prevenção de BC/FT

A instituição financeira deve definir intervenientes e respectivas atribuições e responsabilidades de forma transversal a toda a organização relativamente à aprovação, implementação e monitorização do programa de prevenção de BC e FT.

Destacam-se:

- **Órgão de Gestão**, que será responsável pela prevenção e detecção de actividades ou operações suspeitas de branqueamento de capitais e de financiamento do terrorismo mediante a implementação de um sistema de controlo interno.

  O Órgão de Gestão é, em princípio, o conjunto de pessoas, eleitas pelos sócios ou accionistas, incumbidos de representar a sociedade, deliberar sobre todos os assuntos e praticar todos os actos para realização do seu objecto social. Engloba, designadamente, os gerentes das sociedades por quotas previstos no artigo 282.º e os elementos do conselho de administração previstos no artigo 425.º, ambos da Lei n.º1/04, Lei das Sociedades Comerciais.

  Compete ao Órgão de Gestão:

  - Aprovar as políticas da instituição;
  - Designar o *Compliance Officer;*
  - Definir, implementar e aprovar os processos relacionados com as principais funções do *Compliance Officer*;
  - Supervisionar a estratégia de prevenção de branqueamento de capitais e do financiamento ao terrorismo;

- ***Compliance Officer (para efeitos de ABC/CFT)***: é o responsável pela implementação do programa de prevenção de BC e do FT, sendo igualmente responsável pela centralização de informação e comunicação de operações susceptíveis de branqueamento de capitais e financiamento do terrorismo à Unidade de Informação Financeira e outras autoridades competentes[2].

  Compete ao *Compliance Officer*, designadamente:

  - Obter a aprovação do programa de prevenção de BC e FT;
  - Monitorizar o cumprimento de políticas e processos definidos no âmbito do sistema de prevenção de branqueamento de capitais e de financiamento do terrorismo implementados pela instituição financeira;
  - Gerir e monitorizar a implementação de controlos relativos à prevenção de branqueamento de capitais e do financiamento do terrorismo;
  - Centralizar e analisar as comunicações recebidas internamente;

[2] Artigo 17.º n.º1 do Aviso n.º 14/2020, de 22 de Junho

- Comunicar as operações susceptíveis de configurar a prática do crime de branqueamento de capitais e de financiamento do terrorismo à Unidade de Informação Financeira e outras entidades competentes;
- Receber pedidos de informação da Unidade de Informação Financeira ou de qualquer outra entidade competente, bem como facultar, caso aplicável, a informação solicitada;
- Elaborar um relatório anual relativo à avaliação do risco realizada pela instituição financeira e da eficácia da implementação de medidas no âmbito da prevenção do branqueamento de capitais e do financiamento do terrorismo, destinado ao Órgão de Gestão.

Note-se que, caso aplicável, dada a escala e complexidade do negócio da instituição financeira, poderá ser designado um responsável pela prevenção do BC e FT, por linha de negócio, dentro da instituição financeira que reportará ao *Compliance Officer*.

Estes serão os *Compliance Officers* locais que serão consultados antes de se reportar determinada actividade ao *Chief Compliance Officer*, dado que estas pessoas têm conhecimento das operações, produtos, serviços e clientes das linhas de negócio específicas da organização.

- **Áreas de negócio e operativas**: cada área responsável para realizar controlos enquanto parte da sua actividade normal, por exemplo, aceitação de clientes, realização de transacções, definição de novos produtos. Os controlos devem ser estabelecidos pelo responsável designado pela instituição de acordo com a política de prevenção de BC/FT.

A formação e a sensibilização dada pela instituição financeira pode incluir, entre outros, os seguintes tópicos:

- Definição de branqueamento de capitais e financiamento do terrorismo;
- Enquadramento jurídico do branqueamento de capitais e financiamento do terrorismo;
- Políticas e processos internos;
- Definição de actividade suspeita e como pode ser detectada;
- Como proceder em caso de actividade suspeita;
- Comunicação de actividade ou transacção suspeita entre outras comunicações legalmente devidas;
- Deveres e responsabilização dos colaboradores, nomeadamente o de *não violação da obrigação de sigilo;*

Fonte: World Bank, Preventing Money Laundering and Terrorist Financing - A Practical Guide for Bank Supervisors

Sempre que existam responsabilidades estabelecidas para diferentes áreas de negócio, existe a necessidade de ser criada uma interligação entre os responsáveis dentro da instituição, com o objectivo de gerir estas diferentes áreas de risco e reportar informação exigida, de acordo com as políticas da instituição, ao Órgão de Gestão.

- **Função de auditoria interna**: responsável pela monitorização do programa de prevenção doe FT definido.

Em situações de subcontratação dos serviços de auditoria interna esta deve ser realizada por entidades ou pessoas devidamente habilitadas para esse exercício.

3.3.3 Programa de formação e sensibilização

O programa de formação e sensibilização é um componente essencial para assegurar a eficácia de qualquer programa de prevenção de BC e FT.

A instituição financeira deve familiarizar todos os seus colaboradores, incluindo o Órgão de Gestão, relativamente ao enquadramento legislativo e regulamentar existente no âmbito da prevenção do branqueamento de capitais e do financiamento do terrorismo, bem como quanto às políticas e processos da instituição financeira. A formação deve permitir que os colaboradores identifiquem comportamentos e/ou operações suspeitas, devendo ensinar quais os passos subsequentes à identificação de uma operação suspeita.

O primeiro passo no estabelecimento de um programa de formação eficaz será identificar a audiência-alvo, pois a formação dada deve ser adequada aos tópicos e assuntos relevantes à função de cada colaborador não sendo necessário que todos os colaboradores tenham o mesmo nível de formação. Por este motivo, as instituições

financeiras devem determinar qual o tipo de formação relevante para cada colaborador. Neste sentido, será especialmente relevante a formação dada ao *Compliance Officer* que deve ser apropriada à função que desempenha.

O conteúdo da formação deve variar entre instituições financeiras dependendo da base de clientes, produtos, serviços oferecidos, bem como a periodicidade e o formato da mesma que também deve atender à natureza e dimensão de cada instituição.

Nos termos da Lei n.º 05/20, de 27 de Janeiro a formação deve ser dada periodicamente (e.g. pelo uma vez por ano) e de preferência em sessões formadas por pequenos grupos, de forma a ser possível debater opiniões e expor as principais dúvidas relacionadas com o tema em questão.

Note-se que podem ser incluídas na formação dilemas e cenários hipotéticos para estimular o debate, sendo preferível a inclusão de casos de branqueamento de capitais e financiamento de terrorismo criados a partir de situações reais que tenham ocorrido na instituição ou em instituições financeiras similares.

O tipo de formação depende dos tópicos e da audiência. De facto, existem métodos e abordagens de formação que poderão ser mais adequadas, tais como sessões de formação através de programas de aprendizagem *Web-based*, sessões de grupo, entre outras.

Quando ocorrem eventos importantes na área da prevenção e combate do branqueamento de capitais e do financiamento do terrorismo, as instituições devem informar atempadamente os seus colaboradores, fornecendo-lhes informação sobre as implicações que estes eventos terão na sua actividade.

A instituição financeira deve conservar os detalhes da formação, incluindo o número e nome dos colaboradores presentes. As instituições financeiras devem decidir quais as consequências para a ausência do colaborador sem motivo válido.

3.3.4 Processos

As políticas definidas e aprovadas pelo Órgão de Gestão, nos termos do disposto no ponto 3.3.1, irão manifestar-se na actividade normal da instituição financeira através da implementação de processos.

Na Lei n.º 05/20, de 27 de Janeiro e nos Avisos n.º 14/2020, de 22 de Junho, encontra-se estabelecida a obrigatoriedade de implementar processos, como a realização de medidas de diligência, que incluirão, entre outros, procedimentos de identificação e verificação da identidade de clientes, conservação de documentos, comunicação, não obstante a legislação e regulação actualmente em vigor não especificar como devem executar estes controlos, pelo que cabe às instituições financeiras a operacionalização dos mesmos.

4 Medidas de diligência

A política de diligência aprovada pelo Órgão de Gestão deve explicitar claramente o processo de identificação de clientes a ser executado nas diferentes etapas que constituem as medidas de diligência, nos temos do disposto no artigo 11.º da Lei n.º 05/20, de 27 de Janeiro:

- Identificação de clientes, e caso aplicável do beneficiário efectivo ou representante;
- Verificação da identidade do cliente, e caso aplicável, do beneficiário efectivo ou representante;
- Obtenção de informação sobre o objecto e natureza da relação de negócio;
- Obtenção de informação sobre a origem e o destino dos fundos;
- Actualização da informação do cliente;
- Monitorização contínua da relação de negócio.

A implementação de medidas de diligência traduz-se num conjunto de processos que permitem às instituições financeiras obterem um conhecimento razoável sobre a identidade de um cliente, assim como obter e conservar a informação necessária para compreender a natureza do seu negócio, a sua actividade e o seu perfil de risco.

4.1 Identificação do cliente

A "*Identificação*" do cliente significa o acto pela qual a instituição financeira determina o nome e outras informações relevantes sobre um potencial cliente, pessoa singular ou colectiva.

O artigo 9.º da Lei n.º 05/20, de 27 de Janeiro, assim como os Avisos em vigor exigem o estabelecimento de controlos, entre os quais se destaca o estabelecimento de procedimentos de identificação de cliente, nas seguintes situações:

- Quando se estabelece uma relação de negócio, ou;
- Quando ocorra uma transacção ocasional, se acima de um certo limite, ou;
- Exista a suspeita de envolvimento em actividades associadas ao branqueamento de capitais e financiamento de terrorismo, ou;
- Quando existem dúvidas quanto à autenticidade ou fiabilidade dos dados de identificação dos clientes.

A Lei n.º 05/20, de 27 de Janeiro e o Aviso em vigor determinam que género de informação, no mínimo, deve ser recolhida pelas instituições financeiras quando estabeleçam uma relação de negócio ou efectuem uma transacção ocasional.

O artigo 7.º do Aviso n.º 14/2020, de 22 de Junho, indicam os elementos que, no mínimo, devem ser solicitados aos potenciais clientes no inicio da relação de negócio.

4.1.1 Identificação de um novo cliente

Quando um novo cliente solicita um produto ou serviço, este deve ser identificado antes do início da relação de negócio ou antes de ocorrer uma transacção ocasional.

4.1.1.1 Estabelecimento da relação de negócio

Note-se que o estabelecimento da relação de negócio não deve estar condicionado à apresentação de todos os elementos solicitados no artigo 7.º do Aviso n.º 14/2020, de 22 de Junho, no entanto, caso ocorra esta situação, o cliente deve fornecer a informação disponível.

Nos termos do disposto no n.º 37 do artigo 3.º da Lei n.º 05/20, de 27 de Janeiro, para efeitos do disposto na referida Lei uma relação de negócio caracteriza-se por uma "*relação de natureza comercial ou profissional entre as entidades sujeitas e os seus clientes que, no momento em que esta, efectivamente, se estabelece, se prevê que venha a ser, ou seja duradoura*" como, a título de exemplo, a abertura de uma conta poupança ou a realização de um contrato de *leasing*.

No mínimo, no momento do estabelecimento da relação de negócio, o Gestor do Cliente ou outro responsável pela relação de negócio deve assegurar o preenchimento e assinatura de um documento semelhante a uma "Ficha do Cliente", que deve estar em conformidade com as regras "*Know Your Customer (KYC)*" (doravante designados por "documentos").

Estes documentos contêm informação essencial relativa ao cliente e ao beneficiário efectivo. Pode ser considerada informação essencial do cliente o seu estado civil, situação profissional, identificação da entidade empregadora quando aplicável, situação financeira, origem dos fundos depositados no banco e via utilizada para o efeito, e toda e qualquer outra informação que permita ao banco aferir da real situação financeira do cliente.

Não obstante, as instituições financeiras podem, discricionariamente, recolher informação adicional que lhes permita aumentar o conhecimento que detêm do cliente e da relação de negócio e, consequentemente, auxiliar na

avaliação do nível de risco associado ao cliente, podendo solicitar, por exemplo, informação sobre a identidade dos directores ou administradores com poderes de gestão corrente relativamente ao cliente.

4.1.1.2 Realização de uma transacção ocasional

Adicionalmente, existe a obrigação de identificação quando:

- Ocorre uma transacção ocasional, realizada por uma pessoa ou entidade e;
- A transacção ocasional possui um montante igual ou superior a USD 15.000 (quinze mil dólares dos Estados Unidos da América), independentemente de a transacção ser realizada através de uma única operação ou de várias operações que aparentem estar relacionadas entre si. Caso o montante total da transacção não seja conhecido no momento do início da operação, a instituição financeira, deve exigir a identificação, a partir do momento que conheça o valor em causa, e este for de montante igual ou superior a USD 15.000,00 (quinze mil dólares dos Estados Unidos da América).

Nos termos do disposto no n.º 39 do artigo 3.º da Lei n.º 05/20, de 27 de Janeiro, são transacções ocasionais "*qualquer transacção efectuada pelas entidades sujeitas fora do âmbito de uma relação de negócio já estabelecida*", ou seja, uma transacção pontual que não se consubstancia no conceito de relação comercial duradoura que normalmente existe entre uma instituição financeira e um cliente.

Neste caso, o cliente é um cliente "*ocasional*" que solicita uma única transacção em moeda estrangeira ou uma instrução isolada de compra de acções[3], acima do limiar referido, não existindo, à partida um carácter duradouro associado a esta relação

As instituições financeiras devem ter em consideração a existência de determinados factores que podem ligar transacções ocasionais, e avaliar se existe um carácter de habitualidade ou repetição inerente às transacções com o fim de determinar se a transacção possui um montante igual ou superior ao acima referido, por exemplo, os pagamentos são feitos para a mesma pessoa a partir de uma ou mais fontes num curto período de tempo, ou um cliente que regularmente transfere fundos para uma ou mais fontes.

Adicionalmente, a habitualidade ou frequência das transacções podem alterar o estatuto da relação ocasional conferindo-lhe uma natureza duradoura.

Em princípio, e no caso de situações que apresentem um baixo risco de BC/FT e que à partida não dão origem ao estabelecimento de uma relação de negócio, as instituições podem estabelecer um período de três meses para "*ligar*" transacções.

No mínimo, antes da realização da transacção ocasional devem ser solicitados os elementos constantes no artigo 7.º do Aviso n.º 14/2020, de 22 de Junho, nomeadamente o nome completo e assinatura, nacionalidade, data de nascimento, nome do documento de identificação utilizado, número de identificação, data de expiração e entidade emissora.

4.1.2 Identificação de um cliente existente

A Lei n.º 05/20, de 27 de Janeiro, não requer, somente, às instituições financeiras que identifiquem os seus novos clientes, mas também define algumas situações em que os clientes existentes devem ser identificados.

Estas situações ocorrem quando a instituição financeira tem a suspeita de envolvimento em branqueamento de capitais e financiamento do terrorismo ou dúvidas relativamente à autenticidade ou fiabilidade das informações prestadas pelo cliente.

A última situação pode ocorrer, por exemplo, quando acontecer a revisão da informação do cliente.

[3] Na legislação anglo-saxónica as transacções ocasionais também são referidas como"One-off transactions"

Suspeitas que poderão justificar repetição do processo de identificação:

- atribuição de procuração a pessoa que não mantenha qualquer relacionamento com o titular da relação de negócio;
- inconsistência aparente do número de operações ou do montante de activos depositados na conta com a situação financeira conhecida do titular de relação de negócio, ou
- mudança dos procuradores de uma "sociedade domiciliada", sem que o banco tenha obtido confirmação escrita que o beneficiário efectivo se mantém o mesmo.

Por outro lado, e de acordo com o disposto no artigo 7.º do Aviso n.º 14/2020, de 22 de Junho, a obrigação de identificação e verificação da identidade é expressamente aplicada a clientes existentes, ou seja, a clientes cuja relação de negócio se estabeleceu anteriormente à entrada em vigor do Aviso.

De acordo com o disposto no Aviso supracitado, a obrigação de identificação acima mencionada aplica-se a clientes já existentes, em função da avaliação de risco de branqueamento de capitais e do financiamento do terrorismo associado aos mesmos.

Neste caso a instituição financeira deve garantir que possui informação suficiente (no mínimo a informação exigida legalmente) para realizar a avaliação de risco de BC/FT de forma adequada e decidir se pretende continuar essa relação com o cliente.

Caso a informação não esteja disponível, a instituição financeira deve recolhê-la junto do cliente, pois podem existir situações de risco elevado onde a actualização da informação do cliente é necessária.

valiação de risco relativamente a clientes existentes, a instituição pode exemplo, sempre que este realiza um novo negócio (i.e., o cliente pede um novo produto ou serviço) ou em situações com um risco identificado como elevado (i.e., realização de um volume elevado de operações em numerário) ou quando a transacção não está de acordo com o perfil do cliente.

Independentemente, da abordagem utilizada, a instituição deve documentar os critérios utilizados para alterar ou incluir novas informações sobre os clientes existentes.

De forma a minimizar o impacto associado à falta de informações relativamente a clientes cuja relação de negócio se estabeleceu anteriormente à obrigatoriedade de recolha de informações sobre a identificação e diligência nos termos do disposto no Aviso n.º 14/2020, de 22 de Junho, a instituição pode implementar programas de correcção da informação ou de obtenção de informação adicional.

4.1.3 Identificação do beneficiário efectivo do cliente

Quando o cliente é uma pessoa colectiva, as instituições financeiras devem identificar o beneficiário efectivo desse cliente. O beneficiário efectivo é a pessoa singular, que em última instância detém, controla o cliente, ou em nome de quem é realizada uma determinada transacção. No caso de o cliente ser uma pessoa colectiva, de forma a determinar a identidade do beneficiário efectivo, devem ser identificadas:

- As pessoas singulares que detêm a propriedade ou o controlo, directo ou indirecto, igual ou superior a 20% do capital social da sociedade ou dos direitos de voto da pessoa colectiva; e
- As pessoas singulares que, de qualquer outro modo, exerçam o controlo da gestão da pessoa colectiva.

No caso de o cliente ser uma entidade sem personalidade jurídica, tais como centros de interesses colectivos sem personalidade jurídica que administram e distribuem fundos *(trusts)*, de forma a determinar a identidade do beneficiário efectivo, devem ser identificadas:

- As pessoas singulares beneficiárias de pelo menos 20% do seu património, quando os futuros beneficiários já tiverem sido determinados;

- ► As pessoas singulares em cujo interesse principal a pessoa colectiva foi constituída ou exerce a sua actividade, quando os futuros beneficiários não tiverem sido ainda determinados; e
- ► As pessoas singulares que exerçam controlo igual ou superior a 20% do património da pessoa colectiva.

O artigo 11.º da Lei n.º 05/20, de 27 de Janeiro, exige que as instituições financeiras obtenham informação específica sobre a estrutura de accionista/quotas, propriedade e de controlo do cliente, pois, através do conhecimento destes elementos, a instituição financeira pode identificar o beneficiário efectivo.

Estruturas de propriedade complexas podem exigir, das instituições financeiras, medidas adicionais para que fiquem razoavelmente satisfeitas quanto ao conhecimento que possuem do cliente.

Por outro lado, e mediante o risco associado à relação de negócio ou à transacção ocasional, a instituição financeira pode utilizar, por exemplo, relatórios anuais, organigramas da empresa, memorandos, ou contratos, que permitam conhecer e compreender a estrutura de propriedade e controlo.

As instituições financeiras podem solicitar ao cliente que forneça a identidade do beneficiário efectivo e, caso haja mais do que um beneficiário efectivo, a identidade de todos eles deve ser facultada

O controlo sobre pessoas colectivas pode ser exercido de diferentes formas e depende de vários factores, nomeadamente, a forma societária e o sector de negócio.

No entanto, durante o processo de identificação do beneficiário efectivo a instituição financeira pode verificar que o controlo da propriedade é tão diversificado que não existe uma pessoa singular que efectivamente exerça controlo sobre a pessoa colectiva.

Neste caso, a instituição deve demonstrar que realizou todas as medidas necessárias para averiguar a identidade do beneficiário efectivo que exerça o controlo sobre a instituição. Se após a realização das medidas referidas não forem identificados quaisquer beneficiários, as instituições devem procurar realizar as medidas necessárias para identificar a pessoa que detém poderes de gestão sobre a pessoa colectiva.

4.1.4 Identificação dos beneficiários de seguros de vida

As instituições financeiras bancárias que possuam produtos como seguros de vida, entre outros tipos de investimentos na actividade seguradora, devem realizar, além de medidas de diligência para identificar o cliente e o respectivo beneficiário efectivo, as seguintes medidas relativas ao beneficiário do seguro de vida ou de outras apólices de seguro, no momento em que o(s) beneficiário(s) sejam identificados/designados pelo tomador do seguro:

- ► Recolher o nome da pessoa - beneficiários que sejam identificados como pessoas singulares ou colectivas ou entidades sem personalidade jurídica;
- ► Obter informações suficientes a respeito do beneficiário da apólice de seguro para que a instituição financeira esteja satisfeita que poderá determinar a identidade do beneficiário no momento do pagamento - beneficiários que sejam designados por características ou por classe (por exemplo, cônjuge ou filhos no momento em que ocorra o incidente segurado) ou por outros meios (por exemplo, através de testamento).

As informações acima mencionadas devem ser registadas e conservadas de acordo com os procedimentos constantes na **secção 4.3 e 4.4**, sendo que a verificação da identidade do beneficiário da apólice apenas deve ocorrer no momento do pagamento.

Note-se que o beneficiário de uma apólice de seguro pode ser tido em consideração como um factor de risco relevante, na determinação da aplicabilidade de medidas de diligência reforçada. De facto, se a instituição financeira determinar, por exemplo que um beneficiário do seguro de vida é uma pessoa colectiva ou uma entidade sem personalidade jurídica pode considerar que este representa um risco mais elevado, pelo que a instituição pode

determinar a exigibilidade da identificação e verificação da identidade do beneficiário efectivo da pessoa colectiva ou entidade sem personalidade jurídica, no momento do pagamento.

4.1.5 Identificação dos representantes legais

Para além da identificação do cliente e do beneficiário efectivo, a Lei n.º 05/20, de 27 de Janeiro, refere-se especificamente à identificação e verificação dos poderes dos representantes que se encontram legalmente incumbidos da representação do cliente.

O representante da pessoa colectiva, dependendo dos respectivos estatutos, pode ser um administrador ou gerente da pessoa colectiva.

Por outro lado, uma pessoa que actua em nome de outrem é, a título ilustrativo, a pessoa que deseja abrir uma conta em nome de outra pessoa que se apresenta impossibilitada de o fazer presencialmente, por exemplo, por motivos de comprovada doença.

Note-se que, em todas estas situações, deverá existir uma procuração (devidamente autenticada pelo notário) que o autorize a agir por conta do cliente e que deve ser apresentada à instituição financeira.

Se a instituição financeira suspeitar que um cliente não está a agir em seu próprio nome, deve tentar obter informações relativamente à identidade da pessoa que está a representar, pois, tanto a pessoa que se apresenta à instituição financeira como sendo o cliente, como a pessoa em cujo nome está a agir, necessitam de ser identificados.

As seguintes circunstâncias que poderão sugerir que um cliente não está a agir em seu próprio nome (entre outras):

- A forma como o cliente utiliza o produto e/ou serviço levam a supor que o cliente é controlado por outras pessoas para além do representante;
- O cliente aparenta receber instruções de terceiros, por exemplo, directamente ou por telemóvel;
- Incerteza relativamente à origem dos fundos, características do produto, ou ao objectivo da operação pretendida;
- O cliente tem uma estrutura de propriedade complexa que é muito difícil de esclarecer;
- As operações financeiras do cliente subitamente mudaram, sem qualquer alteração formal na sua estrutura de gestão ou proprietária.

4.1.6 Identificação de "*trusts*"

A Lei n.º 05/20, de 27 de Janeiro, exige a identificação dos centros de interesses colectivos sem personalidade jurídica (*trusts*) ou instrumentos legais semelhantes sem personalidade jurídica, pelo que as instituições financeiras devem, no mínimo, obter o nome dos administradores (*trustees*), fundadores (*settlor*) e beneficiários.

Como corolário das regras "KYC", deve ser obtida uma declaração de beneficiário efectivo, nomeadamente, quando o cliente seja ou actue por conta de outrem, por exemplo, uma sociedade *off-shore* ou um *trust*. Adicionalmente, as instituições financeiras podem recolher informação sobre as pessoas autorizadas a movimentar a conta e os respectivos beneficiários. Caso existam curadores ou "*protectors*", a referência aos mesmos pode também constar desta declaração.

4.1.7 Identificação realizada por terceiros

A execução dos procedimentos de identificação e de diligência pode ser um processo demorado e, por vezes, causar inconvenientes aos clientes que solicitem um novo produto ou serviço. Desta forma, é possível usar informações sobre o cliente, obtidas através de procedimentos de diligência realizados por outras instituições financeiras autorizadas.

O artigo 14.º da Lei n.º 05/20, de 27 de Janeiro, permite às instituições financeiras, excluindo casas de câmbio e instituições financeiras de pagamento, a permitir a execução das obrigações de identificação e de diligência em relação aos clientes previstas na referida Lei, numa entidade terceira nos termos a regulamentar pela respectiva autoridade de supervisão.

Esta disposição legal significa que o processo de identificação, verificação e diligência (ou outros processos relacionados) será realizado por terceiros em nome da instituição financeira que oferece determinado produto ou serviço ao cliente. Note-se que tais contratos não libertam a instituição financeira das obrigações a que estão sujeitas nos termos da lei e regulação em vigor.

O artigo 7.º do Aviso n.º 14/2020, de 22 de Junho, estabelece o procedimentos de execução das obrigações de identificação e de diligência em relação aos clientes por intermediários ou terceiros para dar cumprimento aos requisitos da Lei n.º 05/20, de 27 de Janeiro, ou para captar negócio, desde que cumpridos os seguintes requisitos:

- Obtenção imediata de informações sobre os requisitos previstos nos artigos 13.º e 14.º da Lei n.º 05/20, de 27 de Janeiro, bem como do artigo 7.º do Aviso.
- Tomada de medidas adequadas para assegurar que as cópias da documentação relativa aos requisitos de identificação e diligência previstos nos artigos 13.º e 14.º da Lei n.º 05/20, de 27 de Janeiro, bem como do Avisos são tempestivamente disponibilizadas;
- Realização e redução a escrito das medidas tomadas para assegurar que o terceiro é uma entidade regulada e supervisionada em matéria de prevenção do branqueamento de capitais e do financiamento do terrorismo;
- Redução a escrito dos resultados da verificação efectuada ao terceiro, relativamente às medidas implementadas para cumprir efectivamente as obrigações previstas no artigo 11.º da Lei n.º 05/20, de 27 de Janeiro.

Note-se que nos termos da regulamentação em vigor apenas se considera terceiro a instituição financeira (excepto casas de câmbio e prestadores de serviços de pagamento) que não se encontre sediada em países que não aplicam ou aplicam de forma insuficiente os requisitos internacionais em matéria de branqueamento de capitais e de financiamento do terrorismo, por exemplo países indicados pelo GAFI como não cooperantes ou que não revelam progressos significativos nesta matéria.

A instituição financeira será responsável pelo correcto cumprimento da obrigação de identificação e diligência dos seus clientes, pelo que deverá ter acesso directo à informação obtida através dos processos de identificação e de diligência realizados. A instituição financeira deve também ter um programa de monitorização que garanta que os procedimentos estão de acordo com os requisitos legais.

As instituições financeiras são obrigadas a elaborar um acordo escrito relativamente aos requisitos de identificação e diligência a realizar por terceiros. Este documento deve conter os detalhes dos procedimentos de diligência, bem como a responsabilidade da própria instituição financeira no cumprimento destas obrigações e garantir o seu acesso imediato à informação recolhida pelo terceiro.

A presente disposição legal não se aplica a contratos de diligência ou externalização de serviços (outsourcing).

4.2 Verificação

4.2.1 Verificação de pessoas singulares e colectivas

A verificação da identidade indica que há provas, através do uso de documentação válida, de que uma pessoa singular ou colectiva é quem afirma ser.

O n.º 1 do artigo 5.º do Aviso n.º 14/2020, de 22 de Junho, estabelece os documentos a apresentar para fins de verificação da identidade.

Em algumas circunstâncias, a verificação deve ser efectuada tendo por base o factor de risco associado ao cliente, de forma a assegurar um maior conhecimento nos casos de risco elevado, mas também com o fim de prevenir esforços desnecessários em casos de risco baixo ou normal.

Os pontos seguintes determinam quais os documentos que podem ser usados neste processo, como devem ser avaliados, bem como o momento da verificação.

A verificação de identidade, incluindo a identidade de clientes, representantes legais e beneficiários efectivos, pode basear-se em vários documentos.

Nos termos da Lei n.º 05/20, de 27 de Janeiro a identidade de qualquer pessoa singular deve ser verificada mediante a apresentação de documento comprovativo válido.

Os Avisos em vigor determinam que caso sejam residentes cambiais, os elementos dos clientes singulares, são verificados através da apresentação de bilhete de identidade ou cartão de residente emitido pelo órgão competente, ou, caso se tratem de não residentes cambiais, através da apresentação do passaporte, ou, se tiverem nacionalidade angolana, através da apresentação de bilhete de identidade.

Após o cliente facultar esta documentação, a instituição financeira deve confirmar que a fotografia, nome, género e a data de nascimento do bilhete de identidade ou do passaporte, corresponde com a informação facultada e com a pessoa que solicita a transacção ou a relação de negócio. O mesmo procedimento aplica-se aos respectivos representantes legais e aos beneficiários efectivos.

As pessoas colectivas, residentes, são identificadas através da apresentação de certificado de registo comercial ou outro documento público (por exemplo uma cópia do Diário da República, que contenha informação relativa aos estatutos da empresa), ou um contrato de constituição da empresa por um notário certificado.

Por outro lado, as pessoas colectivas, não residentes cambiais, devem ser identificadas através da apresentação de certidão de registo comercial ou outro documento público devidamente certificado pelas autoridades competentes do país de residência, e autenticado pelo representante consular angolano no país de residência.

Se o cliente for uma pessoa colectiva, as instituições financeiras devem também verificar a identidade do beneficiário efectivo e obter informação relativamente à estrutura accionista/quotas e de controlo da empresa.

Nos termos do disposto nos Avisos em vigor, a identidade do beneficiário efectivo pode ser verificada através da seguinte documentação:

- Certificado que confirme a identidade do(s) beneficiário(s) efectivo(s);
- Cópia do contrato, de acordos de parceria ou outros documentos equivalentes;
- Acta da Assembleia-geral Constituinte, bem como as actas de alterações à estrutura accionista/quotas;
- Outra informação publicamente disponível que a instituição financeira considere relevante.

4.2.2 Certificação de documentos

A verificação da identidade do cliente poderá ser feita através do uso de documentos originais ou de cópias certificadas de documentos originais de forma a demonstrar a proveniência e veracidade da informação, por exemplo, a verificação da identidade de pessoas colectivas residentes podem ser realizada através da escritura de constituição certificada por um notário.

As instituições financeiras são aconselhadas a ter em conta a reputação da pessoa que certificou a documentação em apreço e podem considerar necessário especificar ao cliente quais os documentos que irão aceitar.

Para certificar os documentos acima referidos são, normalmente, consideradas competentes as seguintes entidades:

- Notários;

► Conservadores de registo;

4.2.3 Documentação apropriada para verificação

O Aviso referido indica que a morada, a profissão e, caso aplicável, o empregador da pessoa singular devem ser confirmados através de um "*documento que comprove a informação prestada*".

A verificação da morada depende da abordagem da instituição financeira. Para verificar a morada da pessoa singular, poderá ser usada, por exemplo, a seguinte documentação original:

► Factura recente de electricidade, ou água;

► Extracto bancário de outra instituição financeira;

► Declaração fiscal recente;

► Contrato de arrendamento;

► Apólice de seguro;

► Atestado de residência;

A documentação usada para verificar a morada deve ser recente de forma a reflectir a actual situação do cliente. Por exemplo, as instituições financeiras podem decidir aceitar documentação cuja emissão não tenha transcorrido, por exemplo, há mais de 3 (três) meses. Desta forma será possível assegurar que a documentação reflecte a situação actual do cliente.

Podem existir situações em que o potencial cliente não consegue apresentar um documento que comprove onde reside, este pode apresentar uma "*Declaração de Confirmação de Morada*" a preencher por um declarante com morada completa. Esta declaração deve, no mínimo, incluir o nome completo do declarante, morada, número do documento de identificação e respectiva data de emissão.

O recurso a esta declaração possui uma natureza excepcional, sendo que neste caso a instituição deve registar por escrito não só os motivos apresentados pelo potencial cliente para a não apresentação de documento comprovativo de morada, bem como a justificação dos motivos apresentados para a instituição.

Adicionalmente, a instituição financeira deve recolher informações sobre o colaborador que tomou a referida decisão.

Para verificar a profissão, a entidade empregadora do cliente (caso existente), a natureza e montante do rendimento, as instituições financeiras podem, por exemplo, usar a seguinte documentação:

► Contrato de trabalho;

► Recibo de vencimento recente.

Adicionalmente, devem ser verificadas as seguintes informações:

► Número de identificação fiscal: através da comparação entre o número facultado e o indicado no cartão de identificação fiscal ou documento equivalente emitido pela Direcção Nacional de Impostos.

► Identidade do representante da pessoa colectiva e confirmação do seu mandato: através de uma declaração escrita emitida pela pessoa colectiva, que contenha os nomes dos membros do conselho de administração, procuradores e representantes.

► Identificar os accionistas/sócios com direito de voto igual ou superior a 20%: através da informação presente na acta da Assembleia-geral Constituinte ou correspondentes actas com alterações de estrutura accionista/quotas.

Caso a instituição financeira tenha dúvidas de que a pessoa colectiva está localizada na morada facultada, poderá fazer uma visita ao local ou obter documentação que confirme que o cliente reside no local indicado.

4.2.4 Momento da verificação

Regra geral, a verificação de informação deve ter lugar antes de ser estabelecida a relação de negócio ou no início da transacção ocasional. Contudo existem excepções a esta regra, quando se inicia a relação de negócio.

Estas excepções são aplicáveis quando:

- O risco de branqueamento de capitais e financiamento de terrorismo é baixo;
- A verificação da identidade ocorra no mais curto espaço de tempo;
- É essencial para não interromper o desenrolar da relação de negócio, nomeadamente:
  - Transacções efectuadas sem a presença física do cliente;
  - Transacções de valores mobiliários.
- Não existe disposição legal e regulamentar em contrário;
- Existem procedimentos de gestão de risco, incluindo a limitação do número, do tipo e/ou do valor das transacções a serem realizadas no momento do seu estabelecimento e da verificação da identidade.

Caso ocorra alguma destas excepções, a verificação pode acontecer após o estabelecimento da relação de negócio, devendo esta ser finalizada com a maior brevidade possível. A instituição financeira deve avaliar, caso a caso, se esta excepção poderá, ou não, ser aplicada.

Os casos em que é permitido às instituições financeiras efectuarem a verificação após o início da relação de negócio são estabelecidos nos avisos e serão objecto de recomendações para cada sector.

4.2.5 Avaliação de documentos

É preciso ter em consideração que os documentos apresentados no momento de verificação podem não ser credíveis, ou mesmo falsificados.

Além disso, se a instituição financeira optar por aceitar documentos redigidos em língua estrangeira, devem ser tomadas medidas de diligência adequadas para que sejam satisfeitos os critérios de identificação e verificação dos clientes.

Os seguintes indicadores podem auxiliar as instituições financeiras a identificar a documentação falsa:

- Letras ou números pouco claros, ou confusos, em especial, nome, data de nascimento e data de validade do documento de identificação;
- Mudanças no tipo de letra usada na impressão de informações relativas à identidade;
- Documentos com textura rugosa ou irregular;
- Pontas rasgadas ou qualquer outra evidência que possa sugerir que a superfície foi laminada e adulterada;
- Ausência de película holográfica, marca de água, ou fotografia;
- Informação fornecida pelo cliente que não corresponda na totalidade ao documento de identificação;
- Qualidade do documento inconsistente com os documentos normais, por exemplo, má qualidade do material usado, espessura anormal do papel, cor do documento diferente dos originais e forma como as bordas são cortadas, entre outros;
- Documentação cujo prazo de validade expirou.

Qualquer um dos pontos acima indicados pode ser um indício de que a documentação apresentada não é genuína. Neste caso, as instituições financeiras devem efectuar averiguações adicionais relativamente ao cliente, solicitando outro documento comprovativo de identificação e verificar se existem inconsistências.

Se a instituição financeira não estiver satisfeita com a verificação da identidade do cliente, não deve estabelecer uma relação de negócio ou efectuar a transacção ocasional.

4.3 Obtenção de informação adicional

4.3.1 Origem dos fundos e origem dos rendimentos

De acordo com o n.º 1 do artigo 13.º da Lei n.º 05/20, de 27 de Janeiro, as instituições financeiras devem obter informação relativa à origem e destino dos fundos. A verificação desta informação e das medidas de diligência, de acordo com o número 2 do artigo 14.º da Lei n.º 05/20, de 27 de Janeiro, deve adaptar-se ao risco associado à relação de negócio ou à transacção ocasional.

Conforme mencionado na alínea c) do n.º 1 do artigo 12 do Aviso em vigor, adicionalmente à informação relativa à origem dos fundos, deve ser solicitada informação relativa à origem dos rendimentos. As instituições financeiras devem demonstrar que têm conhecimento do modo como o cliente obtém os seus rendimentos, por exemplo, através de:

- Accionista/sócio de empresa;
- Emprego (salário e bónus);
- Heranças;
- Doações ou legados;
- Investimentos efectuados;
- Fundos de reforma.

As instituições financeiras devem tomar medidas adicionais de diligência para verificarem a proveniência dos fundos e rendimentos através da solicitação desta informação ao cliente e corroborando-a com documentação fidedigna e independente, por exemplo:

- Contratos;
- Testamentos;
- Activos e declarações de rendimentos.

Se for caso disso, as instituições financeiras devem tomar medidas adicionais que comprovem a origem dos fundos e/ou origem dos rendimentos das relações de negócio e das transacções ocasionais de risco elevado.

Aquando da obtenção de informações relativas à origem dos fundos e origem dos rendimentos, as instituições financeiras devem ter em conta os seguintes elementos

- São os fundos possivelmente provenientes de alguma actividade ilícita?
- São os fundos provenientes de um sector susceptível a actividades relacionadas com o branqueamento de capitais ou financiamento de terrorismo?
- A origem dos fundos e dos rendimentos corresponde com a informação de outro cliente?
- A natureza de movimento de fundos sugere alguma associação a actividades bancárias ou a serviços de remessas de valores paralelos?

A informação relativa à origem dos fundos não deve apenas ser utilizada no início da relação de negócio, mas sim durante toda a relação comercial com a instituição financeira. As instituições financeiras devem verificar se a origem dos fundos está em consonância com o conhecimento que têm do cliente, por exemplo, não faz sentido que uma empresa que apenas realize negócios locais receba fundos da Europa.

As operações fora da actividade "normal" do cliente não evidenciam, necessariamente, branqueamento de capitais ou envolvimento no financiamento de terrorismo, contudo, devem ser sustentadas por uma explicação aceitável.

4.3.2 Finalidade e natureza da relação de negócio ou da transacção ocasional

Nos termos da Lei n.º 05/20, de 27 de Janeiro, as instituições financeiras devem obter informações relativas à finalidade e natureza da relação de negócio ou da transacção ocasional. Note-se que o pedido de determinado produto ou serviço deve corresponder ao conhecimento que a instituição financeira tem do cliente, caso contrário, deve ser apresentado pelo cliente r uma explicação lógica relativamente à solicitação específica daquele produto ou serviço.

As informações relativas à finalidade e natureza da relação de negócio não são importantes apenas quando se inicia a relação de negócio, mas também, através da monitorização contínua, para determinar se o produto ou serviço é utilizado para a finalidade que foi inicialmente referida.

4.3.3 Actualização da informação do cliente

Após o início da relação de negócio, as instituições financeiras devem tomar medidas de forma a garantir que a documentação e informação disponível relativa ao cliente se mantêm actualizadas, e manter um acompanhamento contínuo da relação de negócio

4.4 Monitorização contínua

A monitorização contínua permite que as instituições financeiras tenham conhecimento da actividade normal do cliente e, por conseguinte, verificar comportamentos suspeitos susceptíveis de estarem relacionados com actividades criminosas.

O nível de monitorização contínua deve ser definido mediante o risco, ou seja, quando o risco do cliente for mais elevado, a natureza e extensão dos procedimentos de monitorização contínua devem ser adaptados em conformidade. Cada instituição financeira deve possuir um conjunto de indicadores-chave para tais clientes, tendo em consideração os seus antecedentes, tais como o país de origem e a fonte de rendimentos e o tipo de transacções envolvidas, entre outros.

Os componentes essenciais a qualquer sistema de monitorização são:

- Alertar para transacções ou actividades suspeitas para posterior análise;
- Assegurar que estes alertas são examinados por pessoa competente;
- Assegurar que existe o acompanhamento apropriado após o exame *supr*a mencionado.

A monitorização contínua pode ser dividida entre monitorização do cliente e monitorização da transacção. Estes dois tipos de monitorização serão abordados separadamente nos parágrafos seguintes.

4.4.1 Monitorização de clientes

A informação e documentação relativa ao cliente podem ser actualizadas de duas formas:

- Base regular; e/ou
- Desencadeada por um acontecimento particular.

A revisão da informação / documentação, numa base regular, irá depender do risco associado à relação de negócio (por exemplo, uma instituição financeira pode monitorizar um cliente de risco elevado mais frequentemente do que um cliente de baixo risco).

Um exemplo de uma monitorização com origem num acontecimento particular pode ser, para um cliente já existente, a caducidade ou proximidade da data de validade dos documentos de identificação.

Quando uma instituição financeira não tem informação suficiente sobre a relação de negócio, ou caso seja necessária informação adicional, deve pedir essa informação ao cliente. Com base nesta informação ou, se aplicável, através de uma explicação fornecida pelo cliente, a instituição financeira poderá reavaliar o risco associado ao cliente.

Se não houver nenhuma explicação considerada como justificativa, e a instituição financeira acredita ou tem motivos para suspeitar que a actividade poderá estar associada ao branqueamento de capitais ou ao financiamento de terrorismo, devem ser tomadas as medidas apropriadas, incluindo a comunicação de declaração de operação suspeita (DOS) à UIF.

4.4.2 Monitorização de transacções

A monitorização contínua inclui a verificação das transacções a serem levadas a cabo ou já efectuadas. Esta actividade é muitas vezes referida como 'monitorização da transacção'.

A instituição financeira determina através da monitorização das transacções, que a actividade do cliente está em conformidade com o esperado, tendo em conta a informação obtida, enquanto parte integrante do processo de diligência.

Caso se verifique a ocorrência de transacções que não estão de acordo com o conhecimento que a instituição financeira tem do cliente, a transacção deve ser investigada e deve-se procurar uma explicação para a diferença entre a transacção e a informação existente relativa ao cliente. Se não houver nenhuma explicação lógica, a transacção deve ser considerada suspeita e comunicada à UIF.

Os exemplos seguintes demonstram como o comportamento do cliente, manifestado através das transacções efectuadas, pode ser detectado pela monitorização da transacção:

- Número elevado de transacções, quando comparado com o histórico das transacções do cliente, ou com um grupo de clientes com um perfil semelhante;
- Conjunto de transacções, por exemplo, múltiplos depósitos bancários em dinheiro cujo montante agregado seja ligeiramente inferior ao limite definido por Lei para comunicar à UIF;
- Transacções para determinadas jurisdições.

A forma como a monitorização da transacção pode ser realizada depende da dimensão, da frequência da actividade do cliente e da sua natureza.

4.4.3 Natureza da monitorização

A monitorização poderá ser efectuada manualmente, por colaboradores da instituição, ou automaticamente, pelos sistemas de suporte ao negócio.

A escolha ou combinação de cada um destes métodos depende da dimensão, da estrutura, dos produtos e dos serviços da instituição, por exemplo alguns produtos e serviços implicam um número elevado de transacções, enquanto outros produtos e serviços implicam uma transacção ocasional ou um número limitado de transacções.

Por outro lado, a existência de clientes cujo perfil de risco seja mais elevado significa que a monitorização poderá ser mais frequente ou intensiva.

Quanto maior for o volume de transacções, mais difícil será a monitorização sem um sistema automático.

Independentemente da forma como a monitorização é conduzida é muito importante a formação dos colaboradores com o fim de desenvolverem competências para reconhecer e lidar com transacções que saibam, suspeitem ou tenham razões suficientes para suspeitar que estejam relacionadas com actividades criminosas.

4.5 Conservação de documentação

- Nos termos do disposto no artigo 16 da Lei n.º 05/20, de 27 de Janeiro e do inciso iv. da alínea d) do artigo 20.º do Aviso n.º 14/2020, de 22 de Junho adicionalmente quando se trate de clientes de risco elevado durante a relação de negócio (e.g., cópias ou registos de documentos oficiais de identificação como passaportes, bilhetes de identidade, carta de condução ou documentos similares);

Registo de transacções nacionais e internacionais (inclusive os montantes, e caso aplicável tipos de moeda envolvidos na transacção) que sejam suficientes para permitir a reconstituição de cada operação, de modo a fornecer se necessário, prova no âmbito de um processo criminal, nomeadamente transacções, as instituições financeiras devem conservar, no mínimo, por um período até 10 (dez) anos[4] os seguintes documentos:

- Cópias dos documentos ou outros suportes tecnológicos comprovativos do cumprimento da obrigação de identificação e de diligência, incluindo informação e documentação solicitada
- crédito/débito, cheques, etc.;
- Cópia de toda a correspondência comercial trocada com o cliente;
- Cópia das comunicações efectuadas pelas entidades sujeitas à Unidade de Informação Financeira e a outras autoridades competentes (e.g., cópias das Declarações de Operações Suspeitas);
- Registos dos resultados de investigações internas, assim como registo da fundamentação da decisão de não comunicação à Unidade de Informação Financeira e outras autoridades competentes pelo *Compliance Officer* (e.g, registo de investigações realizadas para determinar o motivo de transacções de montante elevado, complexos ou fora do padrão das transacções habitualmente realizadas pelo cliente), e;
- Cópia dos documentos ou registos relativos à formação prestada aos seus empregados e dirigentes.

Adicionalmente, e no caso de instituições financeiras bancárias, deve ser conservada toda a documentação relacionada com transacções realizadas com bancos correspondentes, nos termos do disposto no artigo 20.º do Aviso n.º 14/2020, 22 de Junho, pelo período acima referido.

De realçar que relativamente aos documentos objecto de conservação, estes devem ser conservados como documentos originais, na forma de documentos físicos ou através de qualquer outro processo tecnológico (e.g., formato electrónico ou digital) desde que se garanta às autoridades competentes a veracidade e a autenticidade dos mesmos, bem como a sua disponibilidade atempada, para que a autoridade competente os possa consultar, caso o solicite.

Note-se que o n.º 2 do artigo 9.º da Lei n.º 05/20, de 27 de Janeiro, estabelece especificamente para as instituições financeiras a obrigatoriedade de possuírem sistemas e instrumentos que lhes permitam responder, de forma pronta

[4] Excepto os documentos ou registos relativos a formações que devem ser conservados, no mínimo, por um período até 5 (cinco) anos, contados a partir do momento em que for efectuada a transacção ocasional ou após o fim da relação de negócio.

e completa, aos pedidos de informação apresentados pela Unidade de Informação Financeira e pelas demais entidades com competência nesta matéria, destinados a determinar se mantêm ou mantiveram, nos últimos 5 (cinco) anos, relações de negócio com uma determinada pessoa singular ou pessoa colectiva e qual a natureza dessas relações.

Dependendo da dimensão, natureza e complexidade do negócio, especialmente no caso de grupos financeiros, as instituições financeiras podem considerar a implementação de um sistema de gestão documental. Este sistema pode auxiliar na disponibilização e controlo dos documentos existentes num espaço comum a todos os utilizadores, independentemente da localização da filial, sucursal, agência, ou qualquer outra forma de representação.

O recurso a um sistema de gestão documental pode ser especialmente útil se o cliente terminar a relação de negócio que mantém com uma instituição do grupo, mas este continue a ser cliente de outra filial ou de outra instituição do grupo financeiro.

Não obstante a legislação e regulamentação em vigor não exigirem que os registos sejam mantidos em território nacional, recomendamos a manutenção dos mesmos em Angola, por forma a garantir a facilidade de acesso à documentação ou aos dados extraídos dos documentos, imediatamente, e sempre que solicitado internamente pelos responsáveis pela função de *compliance* ou de auditoria e pelos auditores externos, bem como pela Unidade de Informação Financeira e outras autoridades competentes.

Terminado o prazo de conservação de documentos estabelecido no Aviso n.º 14/2020, de 22 de Junho, excepto quando existam investigações em curso que impliquem a possível solicitação de informação ou documentação sobre o cliente ou transacção objecto de investigação, os registos podem ser destruídos de acordo com a política e procedimentos aprovados pela instituição.

4.6 Medidas de diligência simplificada

As instituições financeiras estão autorizadas a exercer procedimentos de diligência simplificada apenas nos casos de baixo risco que se encontram definidos legalmente, não podendo estes procedimentos ser aplicáveis pelo simples facto da instituição financeira definir um cliente como sendo de baixo risco.

De acordo com o artigo 13.º da Lei n.º 05/20, de 27 de Janeiro, são procedimentos de diligência simplificada, a dispensa do cumprimento das seguintes obrigações:

- Identificação e verificação da identidade dos seus clientes, e se aplicável, dos seus representantes, e do beneficiário efectivo,
- Obtenção de informação sobre a finalidade e a natureza pretendida da relação de negócio;
- Obtenção de informação relativa a clientes que sejam pessoas colectivas ou entidades sem personalidade jurídica, que permita compreender a estrutura de propriedade e de controlo do cliente; e,
- Obtenção de informação, quando o perfil de risco do cliente ou as características da operação o justifiquem, sobre a origem e o destino dos fundos movimentados no âmbito de uma relação de negócio ou na realização de uma transacção ocasional.

Conforme referido as instituições apenas estão dispensadas das obrigações referidas *supra* nas seguintes situações (que se encontram tipificadas na Lei n.º 05/20, de 27 de Janeiro):

- Quando o cliente seja o Estado ou uma pessoa colectiva de direito público, de qualquer natureza, integrada na administração central, provincial ou local; ou
- Quando o cliente seja uma autoridade ou organismo público, sujeito a práticas contabilísticas transparentes e a fiscalização, e;

► Não existam suspeitas de branqueamento de capitais ou de financiamento do terrorismo.

Contudo, realce-se que as instituições financeiras antes de aplicarem procedimentos de diligência simplificada devem, no mínimo, recolher informações suficientes (i.e., denominação social e morada) para determinar se o cliente se enquadra numa das situaçõesreferidas, recorrendo por exemplo à consulta de informação pública fiável.

Note-se que a simplificação dos procedimentos de diligência nos casos acima indicados, não dispensa a instituição de realizar a monitorização da relação de negócio de forma a identificar transacções suspeitas de branqueamento de capitais e de financiamento do terrorismo, nem de manter actualizados os elementos de informação obtidos no decurso da relação de negócio.[5]

De facto, e caso existam indicadores de que um cliente preenche uma das situações passíveis de serem objecto de procedimentos de diligência simplificados, mas que, no entanto, se verifique que este representa um risco elevado para a instituição financeira, esta deve realizar procedimentos de identificação e diligência adicional ou reforçada.

4.7 Medidas de diligência reforçada

Quando o risco de branqueamento de capitais ou de financiamento de terrorismo é elevado, a instituição deve realizar medidas adicionais ou reforçadas para mitigar esse risco, incluindo a recolha de informação suplementar mencionada no ponto 4.3.

De acordo com o disposto em legislação e em regulação em vigor, os procedimentos de diligência reforçada devem ser aplicados em situações de risco elevado.

As instituições financeiras são obrigadas, por lei, a realizar procedimentos de diligência reforçada nas seguintes situações:

► Quando previsto legalmente (*vide* secções seguintes); e,

► Quando a avaliação de risco da instituição financeira indique que a relação de negócio ou transacção ocasional tem um risco elevado de BC e FT.

4.7.1 Pessoas Politicamente Expostas

As pessoas politicamente expostas (PEP's) representam um risco elevado devido à susceptibilidade de envolvimento em corrupção e, consequentemente, branqueamento de capitais e financiamento de terrorismo. Deste modo, será necessário aplicar procedimentos de diligência reforçada relativamente a relações de negócio e transacções ocasionais que ocorram com pessoas politicamente expostas estrangeiras.

As instituições financeiras devem estabelecer procedimentos adequados e baseados no risco para determinar se o cliente, o representante legal e/ou beneficiário efectivo podem ser considerados pessoa(s) politicamente exposta(s). Existem diversas abordagens possíveis para determinar se o cliente é um PEP, dependendo do modo de actuação específico de cada instituição financeira.

Para determinar se o cliente é um PEP, as instituições financeiras podem proceder, por exemplo, à consulta de registos públicos, ou através da sua sucursal que se encontra localizada no país onde reside o cliente, se aplicável. Por outro lado, instituições financeiras com elevado número de actividades internacionais podem optar por usar uma das listas relativas a PEP disponibilizadas por organizações internacionais.

[5] A instituição financeira bancária deve definir critérios para determinar se a informação recolhida é suficiente para verificar que o cliente se enquadra numa das categorias ou profissões acima referidas, nomeadamente, a existência de informação pública disponível que confirme a sua identidade.

Um PEP mantém o seu estatuto enquanto cumpre os requisitos constantes na definição de PEP referida na Lei n.º 05/2020, de 27 de Janeiro, e até um ano após abandonar o seu cargo. Contudo, as instituições financeiras devem continuar a efectuar procedimentos de diligência reforçada mesmo que o cliente tenha deixado de ser uma pessoa politicamente exposta, desde que continue a representar um risco acrescido de branqueamento de capitais ou de financiamento ao terrorismo, por motivos não relacionados com o seu estatuto de PEP.

As instituições financeiras devem verificar a identificação dos seus clientes PEP's no início e durante a relação de negócio. Se a instituição financeira verificar que o cliente adquiriu a condição de PEP durante a relação de negócio, esta deverá realizar procedimentos de diligência reforçada.

Considerando os riscos envolvidos, as instituições financeiras são obrigadas a obter a aprovação do Órgão de Gestão antes de estabelecerem relações comerciais com pessoas politicamente expostas.

As instituições financeiras podem também tomar as medidas necessárias para determinar a origem dos fundos e de riqueza dos PEP's, que serão utilizados durante a relação de negócio ou para a realização de transacções ocasionais. A razão de ser desta medida está relacionada com o facto dos recursos utilizados poderem estar ligados à corrupção ou outras actividades ilícitas.

A Lei n.º 05/20, de 27 de Janeiro, exige a monitorização contínua da relação de negócio. Neste sentido, deve-se prestar especial atenção aos possíveis riscos associados com um PEP. Estes riscos incluem:

- Recepção de fundos do Governo cuja explicação pode não ser clara;
- Pagamentos para realizarem actividades do Governo, para além do salário;
- Recepção de outros fundos de terceiros em que a relação subjacente não é clara;
- Informação pública sobre corrupção existente no país de origem do PEP.

4.7.2 Organizações sem fins lucrativos

As organizações sem fins lucrativos apresentam características que são susceptíveis de abusos em sede de branqueamento de capitais e de financiamento de terrorismo. Estas organizações são normalmente da confiança da sociedade, devido ao motivo que está por detrás da sua constituição, pelo que beneficiam de consideráveis recursos financeiros e recebem grandes montantes de dinheiro, dos quais, por vezes, não se consegue verificar de imediato a sua origem.

Para além disso, a maioria destas organizações sem fins lucrativos tem uma presença internacional, o que significa que podem realizar operações nacionais e internacionais, geralmente nas áreas, ou próximo das áreas, mais expostas à actividade terrorista.

Dependendo do enquadramento legal da organização ou do país, as organizações sem fins lucrativos muitas vezes são sujeitas a pouca ou nenhuma supervisão governamental, ou estão apenas sujeitas a algumas formalidades legais para o seu estabelecimento. As organizações terroristas podem tirar proveito destas características e fazer uso indevido das organizações sem fins lucrativos para encobrir ou suportar a sua actividade terrorista.

O facto das organizações sem fins lucrativos possuírem estas características, tornam-se mais vulneráveis para o branqueamento de capitais e financiamento de terrorismo. Note-se que isso não significa que estas organizações não sejam aceites como clientes pela instituição financeira.

Contudo, as instituições financeiras devem realizar procedimentos de diligência reforçada tal como estabelecido no artigo 16.º e 17.º dos Avisos em vigor de forma a mitigar os riscos associados a este tipo específico de organização.

As medidas de diligência, devem, no mínimo, assegurar a recolha da seguinte informação:

- Localização geográfica;
- Estrutura organizacional;

- Natureza das doações e voluntariado;
- Natureza e destino dos fundos, incluindo informação básica dos beneficiários.

A informação obtida deverá ser usada para se ter uma visão mais completa da sua estrutura, das operações, dos fundos e dos beneficiários. Esta informação permite à instituição financeira avaliar se a actividade da organização sem fins lucrativos no âmbito da relação de negócio ou transacção ocasional está de acordo com o objecto, estrutura e operações da mesma.

4.7.3 Estabelecimento de uma relação de negócio e realização de transacções sem a presença física do cliente

Em alguns casos, o início do processo de abertura de conta pode dar-se sem o cliente estar fisicamente presente. Existem vários exemplos desta situação, nomeadamente, quando um cliente deseja abrir uma conta através da *internet*, contratação de produtos telefonicamente, o cliente quer abrir uma conta e não se encontra presente na mesma jurisdição da instituição.

Se, por um lado, estes serviços proporcionam benefícios ao cliente, por outro lado, tornam difícil às instituições financeiras verificarem a identidade do cliente, por exemplo quando o cliente envia os referidos documentos electronicamente ou através de *fax.*

Como consequência, devem ser tomadas medidas adicionais que complementem a documentação requerida no âmbito do estabelecimento de uma relação de negócio presencial.

A título de exemplo, as instituições financeiras podem aplicar como medidas adicionais de diligência:

- Exigência de certificação do documento de identificação do potencial cliente; ou,
- Solicitação de outros documentos adicionais que confirmem que os documentos são de facto do cliente em questão.

Após a apresentação de documentação certificada ou adicional, a relação de negócio ou transacção ocasional pode ser estabelecida. Note-se que as medidas de diligência dependem do risco que o potencial cliente representa, devendo ser analisado casuisticamente qual a melhor forma de mitigar o risco.

O facto da relação de negócio ou transacção ocasional ter sido iniciada sem que o cliente estivesse presente não tem influência na análise de risco do mesmo, desde que o processo de verificação seja realizado nos termos já referidos.

Por outro lado, durante a relação de negócio, existem transacções efectuadas sem a presença física do cliente, ou, caso aplicável, o seu representante, ou o seu beneficiário efectivo (como por exemplo a solicitação de uma ordem de transacção através de carta), a verificação da identidade pode ser complementada por documentos ou informações suplementares consideradas adequadas para verificar os dados fornecidos pelo cliente de acordo com o perfil e o conhecimento que detém do cliente.

Neste caso, a instituição deve identificar e avaliar o risco de BC/FT associado à transacção, e em função da avaliação do risco, tomar medidas de diligência reforçada para mitigar este risco.

4.7.4 Instituições correspondentes

De acordo com as práticas internacionais em vigor a relação de correspondência bancária caracteriza-se pela prestação de serviços financeiros por uma instituição financeira bancária ("Instituição financeira bancária") que age como agente ou canal de outra instituição financeira bancária ("Instituição correspondente") executando e/ ou processando pagamentos ou outras operações para clientes da instituição correspondente.

Esta situação representa um risco elevado para a instituição financeira bancária, que deve ser evitado através da execução de medidas de diligência que visem a sua atenuação.

Assim sendo, e dada a pressão internacional relativamente ao estabelecimento de um sistema bancário internacional íntegro e robusto, o risco reside na instituição financeira bancária (agente) porque é esta que realiza a prestação de serviços financeiros com os clientes da instituição correspondente, com os quais não possui uma relação directa, pelo que deverá ser esta instituição a definir medidas de mitigação do risco, como a identificação do país de origem e a verificação das políticas internas da instituição correspondente, bem como a verificação de que a instituição correspondente não permite que sejam mantidas contas anónimas nem contas sob nomes fictícios, etc.

4.7.5 Outras situações de alto risco

Existem situações de alto risco que se encontram fora do âmbito das disposições legais e regulamentares aplicáveis, nomeadamente, quando a avaliação do risco da própria instituição que determina que a relação de negócio ou transacção ocasional é de risco elevado pela combinação de diferentes factores.

Por exemplo, um cliente realiza negócios num sector ou está estabelecido num país conhecido por ser vulnerável ao branqueamento de capitais e ao financiamento do terrorismo, pelo que, nestas condições específicas, a instituição financeira pode considerar a relação de negócio como sendo de alto risco.

Nestes casos, a instituição financeira deve realizar procedimentos de diligência reforçada e deve, no mínimo, incluir informação relativa:

- Origem dos fundos;
- Origem dos rendimentos, e;
- Destino dos fundos.

As instituições financeiras devem reduzir a escrito o resultado destas medidas, assim como obter aprovação do Órgão de Gestão quando entendam como necessário.

4.8 Medidas de diligência relativas a transferências electrónicas

As instituições financeiras devem implementar políticas e procedimentos, baseados no risco, que garantam a monitorização das transferências electrónicas tanto na qualidade de instituição financeira do ordenante, do beneficiário da transacção ou como intermediária na cadeia de pagamentos. Esta monitorização visa garantir que pessoas singulares ou pessoas colectivas não tenham acesso a fundos provenientes de actividades criminosas realizadas por si ou por terceiros, bem como assegurar que a informação básica sobre o ordenante e o beneficiário da transacção está imediatamente disponível às autoridades competentes, incluindo a Unidade de Informação Financeira, sempre que solicitado.

Nos termos do disposto no n.º 41 artigo 3.º e do artigo 30.º da Lei n.º 05/20, de 27 de Janeiro, as instituições financeiras cuja actividade abranja transferências electrónicas devem incluir na mensagem ou no formulário de pagamento que acompanha a transferência, independentemente do seu montante, da natureza nacional ou internacional, a seguinte informação relativa ao ordenante da transferência[6], devidamente verificada:

- Nome completo;
- Número de conta (na ausência do número de conta, a transferência deve ser acompanhada por um número único de referência[7] que permita o rastreio da operação até ao seu ordenante);
- Endereço (a informação relativa ao endereço pode ser substituída pela data e local de nascimento do ordenante, pelo seu número de bilhete de identidade, ou pelo número de identificação de cliente), e;

[6] O n.º 8 do artigo 24.º da Lei n.º 34/11, de 12 de Dezembro determina que não são aplicáveis os procedimentos referidos às transferências resultantes de uma operação efectuada através da utilização de um cartão de débito ou de crédito, sempre que o número dos mesmos acompanhe a transferência, nem se aplicam às transferências de uma entidade financeira para outra, quando o ordenante e o beneficiário são entidades financeiras que actuam em nome próprio. Contudo quando o cartão de crédito ou débito é utilizado como um sistema de pagamento relativo a uma transferência electrónica entre duas pessoas os referidos procedimentos já serão aplicáveis.

[7] Definição encontra-se estabelecida na alínea j) do artigo 3.º da Lei n.º 05/20, de 27 de Janeiro.

► Quando for necessário, o nome da entidade financeira do ordenante.

Adicionalmente, a instituição poderá entender ser relevante incluir o nome do beneficiário e o seu número de conta quando tal conta seja utilizada para processar a transacção.

Quando as instituições financeiras do ordenante e do beneficiário estão localizadas em Angola, as transferências electrónicas não necessitam de incluir a informação mencionada acima, podendo apenas ser acompanhadas pelo número de conta ou um número único de referência que permita rastrear a operação até o seu ordenante. No entanto as instituições apenas devem aplicar o procedimento simplificado acima referido quando a instituição financeira do ordenante possa disponibilizar a informação solicitada, num prazo de 3 (três) dias úteis, contados a partir da recepção de um pedido da instituição financeira do beneficiário ou outras autoridades competentes.

A instituição financeira do ordenante apenas deve executar as transferências electrónicas acompanhadas da informação acima mencionada e conservar os registos das transferências, no mínimo, por período até 10 (dez) anos.

Adicionalmente, as instituições financeiras do ordenante e do beneficiário devem garantir a transmissão da informação acima mencionada, quando actuam como intermediários, na cadeia de pagamentos, devendo tomar medidas para identificar as transferências cuja informação sobre o ordenante ou beneficiário se encontre incompleta.

Note-se que, nos termos do disposto na Lei n.º 05/20, de 27 de Janeiro, sempre que por limitações técnicas não seja possível a transmissão das informações completas do ordenante, a instituição financeira intermediária deve conservar por um período até 10 (dez) anos toda a informação recebida pela instituição intermediária.

Na recepção de transferências electrónicas, as instituições financeiras beneficiárias devem tomar medidas baseadas na avaliação do risco, para identificar que a informação relativa ao ordenante da transferência está completa.

Caso a instituição financeira beneficiária identifique a existência de informação incompleta do ordenante, esta deve rejeitar a transferência ou solicitar à instituição financeira do ordenante informação completa sobre este, sem prejuízo das suas obrigações de identificação, verificação e diligência enunciadas na Lei n.º 05/20, de 27 de Janeiro.

Se a instituição financeira do ordenante não fornecer a informação mencionada, a instituição financeira do beneficiário deve tomar as medidas adequadas que, inicialmente, podem incluir a emissão de notificações como a fixação de prazos, antes de rejeitar qualquer transferência futura, restringir ou terminar a relação de negócio. Por fim, e adicionalmente às medidas mencionadas, caso a informação incompleta do ordenante seja considerada como um factor na avaliação de operações de transferência de natureza suspeita, as instituições financeiras devem informar a Unidade de Informação Financeira nos termos do disposto na **Secção 6** do presente documento.

A comunicação à Unidade de Informação Financeira pode também ocorrer quando existam motivos para suspeitar que a transferência está relacionada com pessoas, entidades ou grupos designados de acordo com as Resoluções do Conselho de Segurança das Nações Unidas (e.g., CSNU).

Neste caso, além de proceder à comunicação à Unidade de Informação Financeira, a instituição financeira deve recusar-se a realizar a transferência, e caso seja aplicável congelar os fundos de forma a cumprir com o disposto nos artigos 17.º e 18.º na Lei n.º 1/12, de 12 de Janeiro - Lei sobre a Designação e Execução de Actos Jurídicos Internacionais.

4.8.1 Deveres específicos dos prestadores de serviços de remessas

Os prestadores de serviços de remessas quando controlam a transferência electrónica, tanto na perspectiva do ordenante como do beneficiário, possuem deveres de monitorização reforçada devendo:

► Analisar todas as informações relativas ao ordenante e ao beneficiário para determinar se existe motivos para suspeitar que podem estar envolvidos em práticas criminosas, e;

- Submeter uma Declaração de Operação Suspeita (DOS) em qualquer dos países afectados pela transferência electrónica suspeita, e disponibilizar as informações relevantes da transacção à Unidade de Informação Financeira nos termos do disposto na **Secção 6** do presente documento.

5 Clientes inaceitáveis

Existem situações onde o risco relacionado com o cliente não pode ser mitigado através de procedimentos de identificação e diligência. Um caso ilustrativo destas situações encontra-se na Lei n.º 05/20, de 27 de Janeiro, que proíbe as instituições financeiras de estabelecerem relações de correspondência com bancos de fachada.

Adicionalmente, caso a instituição financeira determine como parte da sua avaliação de risco que o risco associado a um certo cliente é inaceitável, a relação de negócio não deve ser estabelecida ou a transacção não deve ser executada.

As seguintes relações são sempre inaceitáveis quando:

- O cliente é ou está associado a pessoas ou entidades sancionadas, designadas por organizações como as Nações Unidas e o Governo de Angola, entre outras;
- Existam relações de correspondência com um banco de fachada ou um banco que tenha relações de correspondência com um banco fachada;
- Envolvam contas cujos titulares ou representantes sejam clientes anónimos ou com nomes manifestamente fictícios;
- Os procedimentos de identificação e diligência não possam ser cumpridos, por exemplo:
  - A identidade do cliente não possa ser verificada;
  - O cliente dê informação fictícia;
  - O cliente esteja relutante em facultar informação relativa à origem dos fundos, a estrutura da sua empresa, a natureza e o propósito da relação de negócios ou transacção:
  - A estrutura de propriedade da empresa seja complexa e não transparente, sem uma explicação lógica.

Adicionalmente, as instituições financeiras devem proibir contas numeradas que possam ser usadas como contas anónimas. As contas numeradas[8] devem estar sujeitas exactamente aos mesmos procedimentos de identificação, verificação e diligência de todas as outras contas.

Estas contas oferecem a possibilidade de protecção adicional na identificação do cliente, contudo, essa identidade deve ser conhecida por um número suficiente de colaboradores da instituição para que se realizem procedimentos adequados e suficientes de diligência.

6 Comunicações à Unidade de Informação financeira

A Lei n.º 05/20, de 27 de Janeiro, e o Decreto Presidencial n.º 02/18, de 11 de Janeiro definem quais os indicadores de uma operação suspeita. Estes indicadores podem ser divididos em indicadores objectivos e subjectivos que serão abordados separadamente nos pontos abaixo.

8 A instituição bancária apenas disponibiliza um número de conta, não sendo revelado/divulgado o nome do cliente, por questões de sigilo bancário.

Note-se que existem características específicas às transacções que devem ser consideradas pelas instituições quando se determina a possibilidade da actividade estar relacionada com branqueamento de capitais ou financiamento do terrorismo.

Estas características incluem:

- Natureza;
- Complexidade;
- Comportamento habitual;
- Volume da transacção;
- Ausência de justificação económica;
- Probabilidade de estar relacionada com algum tipo de outro crime.

6.1 Indicadores subjectivos

Os indicadores subjectivos não descrevem situações específicas que as instituições financeiras precisam sempre de comunicar. No caso de indicadores subjectivos, as instituições financeiras devem comunicar quando tenham conhecimento, suspeita, ou motivos razoáveis para suspeitar que a actividade está associada ao branqueamento de capitais ou financiamento do terrorismo.

Esta declaração de operação suspeita implica que a instituição irá precisar de fazer a sua própria avaliação, com base na informação que lhe foi disponibilizada, sendo que esta avaliação pode ocorrer tendo em conta circunstâncias específicas da actividade.

Quando uma instituição financeira suspeita ou tem motivos razoáveis para acreditar que uma transacção poderá estar relacionada com branqueamento de capitais ou financiamento do terrorismo, esta deve rever a informação que dispõe relativamente ao cliente.

A existência de uma explicação que faça sentido, à luz da relação de negócio, pode ser motivo suficiente para que não se considere a operação como sendo suspeita. Caso não haja nenhuma explicação lógica para a actividade, e tendo por base a informação recolhida junto do cliente, a actividade deve ser reportada à Unidade de Informação Financeira.

6.1.1 Comunicação de operações suspeitas

O artigo 17.º da Lei n.º 05/20, de 27 de Janeiro e o artigo 18.º do Decreto Presidencial n.º 02/18, de 11 de Janeiro, determinam que as instituições financeiras devem comunicar de imediato à Unidade de Informação Financeira sempre que:

- Possuem conhecimento de que a actividade é, poderá estar ou estará relacionada com o branqueamento de capitais ou financiamento do terrorismo;
- Existe suspeita de que a actividade é, poderá estar ou estará relacionada com o branqueamento de capitais ou financiamento do terrorismo, ou;
- Existem motivos suficientes para que haja suspeita de que a actividade é, poderá estar ou estará relacionada com o branqueamento de capitais ou financiamento do terrorismo.

Existem três formas diferentes de determinar se uma actividade está relacionada com branqueamento de capitais ou financiamento do terrorismo: conhecimento, suspeita e motivos razoáveis para a suspeita.

O conhecimento significa que o indivíduo descobre ou sabe que uma transacção ou pessoa está associada a branqueamento de capitais ou financiamento do terrorismo.

A suspeita é um conceito mais subjectivo e não se baseia nas mesmas provas como quando existe conhecimento. A suspeita baseia-se geralmente, em certas circunstâncias, que indicam um possível envolvimento no branqueamento de capitais ou financiamento de terrorismo.

Existem características específicas às transacções que devem ser

Quanto ao motivo razoável refere-se a uma suspeita mais objectiva e que irá depender de um colaborador específico da organização envolvida. O nível de experiência e conhecimento irão influenciar se o colaborador em causa deve ter motivos suficientes para suspeitar.

Nem sempre uma actividade anormal pode ser considerada suspeita, pelo que qualquer actividade que não pareça comum deve ser analisada de forma a determinar se é necessário exercer a obrigação de comunicação.

Os indícios de que uma actividade pode estar relacionada com o branqueamento de capitais ou financiamento do terrorismo podem surgir não só quando são solicitadas transacções, mas também no âmbito de monitorização das actividades do cliente como parte do processo de revisão periódica das transacções do cliente.

Exemplos de transacções suspeitas podem ser encontrados no documento "Orientações relativas aos critérios de suspeição e tipologias criminais" publicado pela UIF.

6.1.2 Comunicação de pessoas, grupos ou entidades designadas

A Lei n.º 1/12, de 12 de Janeiro - Lei sobre a Designação e Execução de Actos Jurídicos Internacionais - estabelece a autoridade para a designação de Estados, pessoas, grupos e entidades, assim como o mecanismo para aplicação de medidas restritivas específicas aos mesmos, com o fim de combater o terrorismo, quando tal seja requerido por qualquer acto internacional relativo à manutenção e restauração da paz e segurança, tais como Resoluções do Conselho de Segurança das Nações Unidas, e quando seja necessário para proteger a segurança nacional. Prevê igualmente o regime penal pelo incumprimento de medidas restritivas impostas pela lei.

A referida lei estabelece ainda o mecanismo de congelamento administrativo de fundos e recursos económicos pertencentes, possuídos ou detidos, directa ou indirectamente, individualmente ou em conjunto, por pessoas, grupos ou entidades designadas pelo Comité de Sanções das Nações Unidas, conforme a Resolução do Conselho de Segurança das Nações Unidas n.º 1267, e pela autoridade competente a nível nacional.

Havendo necessidade de se estabelecerem medidas de diligência e monitorização em função do risco de financiamento do terrorismo, as instituições financeiras devem confrontar, no início e durante a relação de negócio ou antes da realização de uma transacção, a identidade de um cliente, efectivo ou potencial, ou de qualquer outra pessoa, grupo ou entidade envolvida numa relação de negócio ou transacção, com os dados das pessoas, grupos ou entidades designadas pelo Comité de Sanções da Nações Unidas ou pelo Governo de Angola, de modo a determinar se a sua identidade corresponde a uma pessoa, grupo ou entidade designada.

Quando a instituição financeira sabe, suspeita ou tem motivos suficientes para suspeitar, que a identidade do cliente, efectivo ou potencial, ou qualquer outra pessoa, grupo ou entidade envolvida numa relação de negócio ou transacção corresponde a uma pessoa, grupo ou entidade designada, deve comunicar imediatamente este facto à UIF de acordo com o previsto no artigo 17.º da Lei n.º 05/20, de 27 de Janeiro.

Note-se que as instituições financeiras se encontram obrigadas, à luz do disposto no artigo 17.º da Lei n.º 1/12, de 12 de Janeiro, a congelar de forma imediata e sem qualquer aviso prévio, todos os fundos ou recursos económicos pertencentes, possuídos ou detidos, directa ou indirectamente, individualmente ou em conjunto, por:

- Pessoas, grupos e entidades designadas pelo Comité de Sanções das Nações Unidas conforme a Resolução do Conselho de Segurança das Nações Unidas n.º 1267, mediante a Lista actualizada pelo referido Comité de Sanções, bem como por pessoas, grupos ou entidades agindo em seu nome; e;

- Por pessoas, grupos e entidades designadas pela autoridade nacional competente pela designação e aplicação de medidas restritivas nos termos da Lei n.º 1/12, de 12 de Janeiro às quais tenham sido aplicadas medidas restritivas de natureza financeira.

Adicionalmente, nos termos da Lei n.º 1/12, de 12 de Janeiro, podem ainda ser aplicadas outras medidas restritivas específicas (embargos comerciais, restrições de entrada, permanência ou trânsito de pessoas e entidades em território nacional, entre outras) a pessoas, grupos ou entidades designadas pela autoridade nacional competente pela designação e aplicação de medidas restritivas.

6.2 Indicadores objectivos

Os indicadores objectivos implicam que exista sempre a comunicação à Unidade de Informação Financeira desde que estejam cumpridos os requisitos legais.

O artigo 17.º da Lei n.º 05/20, de 27 de Janeiro, conjugado com as alíneas b) e c) artigo 19.º, do Decreto Presidencial n.º 35/11, de 15 de Fevereiro, obriga as instituições financeiras a informar sobre:

- Transacções em numerário que ultrapassem o limite de USD 15.000,00 (quinze mil Dólares dos Estados Unidos da América) ou equivalente em moeda nacional, e
- Quando tal obrigação for emitida por uma autoridade de supervisão competente, as transacções acima de USD 5.000,00 (cinco mil Dólares dos Estados Unidos da América) ou equivalente em moeda nacional para países ou jurisdições, que estejam sujeitos a medidas adicionais.

A instituição financeira que informa não necessita de ter a suspeita do envolvimento em branqueamento de capitais e financiamento do terrorismo, basta que a actividade preencha as condições descritas no artigo 17.º da Lei n.º 05/20, de 27 de Janeiro, e do artigo 19.º do Decreto Presidencial n.º 02/18, de 11 de Janeiro, para ser objecto de comunicação à Unidade de Informação Financeira .

6.3 Prazo de comunicação de operações suspeitas

No âmbito do artigo 17.º, da Lei n.º 05/20, de 27 de Janeiro, as instituições financeiras estão obrigadas a comunicar imediatamente.

O termo "*imediatamente*" deve ser interpretado como "*logo que seja razoavelmente possível*" a instituição se ter familiarizado com a actividade suspeita, havendo a possibilidade de detectar actividades suspeitas numa fase posterior à execução.

Neste sentido, veja-se o seguinte exemplo: a primeira transacção de um cliente não levanta suspeita, contudo, após ser efectuada a terceira transacção, há motivos razoáveis para suspeitar que aquelas transacções estão ou poderão estar relacionadas com o branqueamento de capitais ou o financiamento de terrorismo.

A primeira transacção deve ser reportada juntamente com as transacções posteriores.

Note-se que, no caso de uma transacção, que atinge os critérios de reporte legalmente definidos (por exemplo, quando um cliente realiza uma transacção em dinheiro superior a USD 15.000,00 (quinze mil Dólares dos Estados Unidos da América) ou equivalente em moeda nacional, tal transacção deve ser reportada de imediato.

6.4 Formas de comunicação de operações suspeitas

Ao reportar uma actividade suspeita à Unidade de Informação Financeira a instituição deve preencher o formulário relativo à Declaração de Operação Suspeita (DOS). Este documento assegura que toda a informação necessária à sua análise está incluída no mesmo.

O formulário relativo à DOS (bem como o respectivo guia de preenchimento) pode ser encontrado no site do Banco Nacional de Angola na seguinte hiperligação:

http://www.bna.ao/Conteudos/All/lista.aspx?idc=881&idl=1

Quando a instituição financeira sabe, ou tem motivos suficientes para suspeitar, que a identidade do cliente, efectivo ou potencial, ou qualquer outra pessoa, grupo ou entidade envolvida numa relação de negócio ou transacção

corresponde a uma pessoa, grupo ou entidade designada, deve comunicar imediatamente este facto à Unidade de Informação Financeira, através do Formulário relativo à Declaração de Identificação de Pessoas Designadas (DIPD).

O formulário relativo à DIDP (bem como o respectivo guia de preenchimento) pode ser encontrado no *site* do BNA na seguinte hiperligação:

http://www.bna.ao/Conteudos/All/lista.aspx?idc=881&idl=1

O artigo 17.º da Lei n.º 05/20, de 27 de Janeiro, obriga as entidades a facultar informação relativa aos seus clientes ou transacções suspeitas, sempre que for solicitada pelas autoridades competentes. Este artigo prevê a possibilidade da UIF solicitar informação adicional sobre a pessoa, grupo ou entidade reportada.

6.5 Procedimentos de consentimento prévio

Nos termos do disposto no artigo 7.º do Decreto Presidencial n.º 02/18, de 11 de Janeiro, a Unidade de Informação Financeira deve tomar uma decisão relativamente à comunicação de uma DOS num espaço de 3 (três) dias úteis, contados a partir da recepção da mesma.

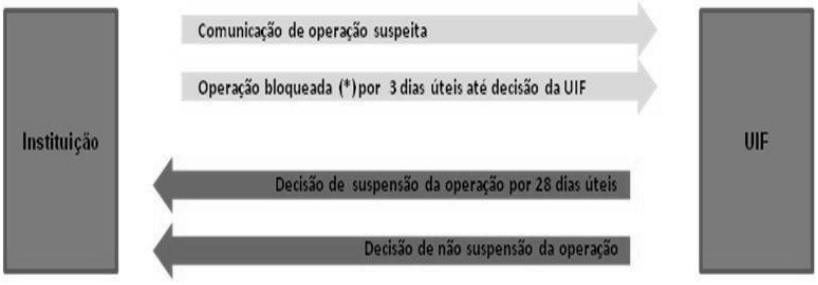
Com efeito, a instituição financeira deve abster-se de executar a operação reportada até receber autorização para prosseguir com a transacção, o que significa que a instituição financeira é obrigada a estabelecer controlos que previnam que a transacção ocorra enquanto aguarda pela decisão da Unidade de Informação Financeira , nos 3 (três) dias úteis definidos por Lei.

Caso a instituição não cumpra o acima mencionado, está a cometer uma transgressão nos termos do artigo 72.º da Lei n.º 05/20, de 27 de Janeiro.

A UIF deverá decidir se a transacção apresenta uma suspeita fundada e em função da sua decisão dará, ou não, autorização para que se prossiga com a operação. Caso a UIF não dê resposta, no prazo de 3 (três) dias úteis, a entidade que reporta poderá dar continuidade à transacção.

De acordo com disposto no artigo 7.º do Decreto Presidencial, de 11 de Janeiro, a UIF poderá suspender qualquer operação em curso, suspeita de branqueamento de capitais ou financiamento de terrorismo, por um período de 28 (vinte e oito) dias, ou mais, desde que acompanhado pela ordem do tribunal.

Neste sentido, veja-se o seguinte esquema:



(*) Não existirá bloqueio da operação caso esta tenha ocorrido

Se a UIF se decidir pela suspensão da execução da decisão, esta deve requerer à Procuradoria-Geral da República a confirmação da decisão de execução da suspensão, no prazo de dez dias úteis a contar da decisão referida.

6.6 Papel do *Compliance Officer*

Primeiramente, as instituições financeiras devem implementar procedimentos de forma a garantir que o processo interno de comunicação de operação suspeita ao *Compliance Officer* é especialmente rápido, não devendo

ultrapassar, regra geral as 24 (vinte e quatro) horas, de modo a assegurar o cumprimento das normas legais que determinam uma imediata comunicação da operação suspeita à Unidade de Informação Financeira.

Seguidamente, o *Compliance Officer* deve determinar para cada comunicação interna de actividade suspeita, se há uma justificação aceitável para a suspeita.

Caso este decida que a actividade se enquadra no âmbito da obrigação de comunicação, então deve submeter à UIF uma Declaração de Operação Suspeita (DOS). Até o *Compliance Officer* decidir se a actividade se insere, ou não, no âmbito da obrigação de comunicação, qualquer actividade respeitante àquele cliente, incluindo transferências electrónicas em que o cliente esteja envolvido, deve ser reportada ao *Compliance Officer*.

Todos os relatórios internos de actividades suspeitas devem ser documentados, bem como todos os motivos que levaram o *Compliance Officer* a definir se a actividade era suspeita ou não. Caso uma DOS /DIPD seja submetida à UIF, uma cópia desta comunicação bem como o respectivo relatórios internos devem ser conservados.

6.7 Relação da instituição financeira com o cliente

O artigo 20.º da Lei n.º 05/20, de 27 de Janeiro, determina que as instituições financeiras e os seus empregados não podem revelar qualquer DOS que tenha sido submetida à UIF e sobre a qual está a decorrer uma investigação. A instituição financeira não deve apenas manter esta obrigação de sigilo com o cliente, mas também com terceiros. A revelação da identidade de quem comunicou informações ao abrigo do dever de comunicação de operações suspeitas previstas no n.º 2 do artigo 21.º da Lei n.º 05/20, de 27 de Janeiro, é crime.

A proibição de revelar informação relativa às denúncias feitas à UIF não se limita apenas à comunicação de DOS, mas também às comunicações internas relacionadas actividades suspeitas submetidas à consideração do *Compliance Officer*.

Se surgirem suspeitas quanto à verdadeira identidade do titular da conta no estabelecimento ou no decurso da relação de negócio com o cliente ou durante a realização de uma transacção ocasional, a instituição financeira deve verificar (no início ou durante a relação de negócio) a identidade do titular da conta e/ou do beneficiário efectivo, e caso aplicável realizar uma declaração de operação suspeita à Unidade de Informação Financeira, nos termos do disposto no **Secção 6** do presente documento.

No entanto, as instituições devem ter em consideração que durante a identificação e verificação de identidade, os clientes não devem ser alertados para o facto que está a decorrer uma comunicação interna ou que foi comunicada uma declaração de operação suspeita, porque pode comprometer esforços futuros por parte das autoridades competentes.

Assim, se a instituição financeira tem motivos para acreditar que a realização das medidas de diligência acima indicadas comprometer esforços futuros por parte das autoridades competentes, a instituição financeira pode não realizar estas medidas e submeter imediatamente uma Declaração de Operação Suspeita.

Os colaboradores devem receber formação sobre estes temas quando estão a conduzir procedimentos de diligência, nomeadamente os cuidados a tomar quando solicitam informações adicionais aos clientes relativamente a transacções ou actividades que não estejam em consonância com o perfil do cliente.

Anexo I: Lista sobre o conjunto de categorias de crimes subjacentes ao crime de branqueamento de capitais (elencados no glossário das 40 Recomendações do GAFI/FATF)

- Participação num grupo criminoso organizado e em acções ilegítimas para obtenção de fundos, nomeadamente através de chantagem, intimidação ou outros meios;
- Terrorismo, incluindo o financiamento do terrorismo;
- Tráfico de seres humanos, incluindo tráfico de órgãos ou tecidos humanos e tráfico ilícito de migrantes;
- Exploração sexual, incluindo a exploração sexual de crianças;
- Tráfico de estupefacientes e de substâncias psicotrópicas;
- Tráfico de bens roubados e de outros bens;
- Corrupção;
- Suborno;
- Fraude;
- Contrafacção de moeda;
- Contrafacção;
- Pirataria de produtos;
- Crimes contra o ambiente, incluindo tráfico de espécies protegidas;
- Homicídio;
- Ofensas corporais graves;
- Rapto;
- Sequestro;
- Tomada de reféns;
- Roubo ou furto;
- Contrabando;
- Extorsão;
- Falsificação;
- Pirataria;
- Utilização abusiva de informação privilegiada e manipulação do mercado;
- Crimes fiscais

Anexo II: Exemplo de uma matriz de risco

A matriz de risco *infra* é um exemplo de como as instituições financeiras podem combinar diferentes factores de risco.

Neste exemplo, o factor de risco do produto está combinado com o factor de risco do cliente de forma a simplificar a matriz. A matriz em apreço está baseada no princípio onde a maior categorização do risco prevalece.

Produto / Cliente	Baixo	Normal	Alto
Baixo	**Baixo**	**Normal**	**Alto**
Normal	**Normal**	**Normal**	**Alto**
Alto	**Alto**	**Alto**	**Alto**
Inaceitável	**Inaceitável**	**Inaceitável**	**Inaceitável**

[1]O factor de risco do produto não demonstra a categoria "inaceitável", dado que as instituições financeiras, por princípio, não oferecem produtos que podem ser classificados como inaceitáveis.

Anexo III: Exemplo de uma matriz de diligência

Baixo	**Estado ou pessoa colectiva de direito público, parte da Administração central, provincial ou local**	**Diligência simplificada**	**• Aprovação da linha de negócio**	**• Revisão da documentação do cliente a cada 3 anos • Nivel suficiente de monitorização da transacção**
Normal	**Todos os clientes que não são classificados como de risco baixo, alto ou inaceitável**	**Diligência "normal"**	**• Aprovação da linha de negócio**	**• Revisão da documentação do cliente a cada 2 anos • Nivel suficiente de monitorização da transacção**
Alto	**• O cliente é uma pessoa politicamente exposta • Relações de correspondência bancária • Organizações não lucrativas • Clientes do segmento *"Private banking"* •Clientes que são de maior risco**	**Diligência reforçada**	**• Aprovação do Órgão de Gestão • Consulta do D. Compliance**	**• Revisão anual da documentação do cliente • A monitorização da transacção é mais abrangente e adequada aos riscos**
Inaceitável	**•O cliente é um banco fachada • O cliiente é conhecido por permitir a utilização das contas por um banco fachada • Contas anónimas ou com nomes manifestamente ficticios • Clientes que são considerados inaceitáveis**	**O nivel de diligência necessário para determinar a inaceitabilidade do cliente**	**• Não existe aprovação - o cliente não deve ser aceite • Consulta com Departamento de Compliance de acordo com o procedimento de encaminhamento da informação**	**• Inaplicável**

Anexo IV: Glossário de termos

Termo / Expressão	Significado
Beneficiário efectivo	Pessoa singular, que em última instância detêm, controla o cliente, ou em nome de quem é realizada uma determinada transacção.
Cliente	Pessoa singular, pessoa colectiva ou qualquer outra entidade jurídica com a qual a instituição financeira estabelece ou estabeleceu um relação de negócio ou efectue uma transacção ocasional
Compliance officer	Responsável pela implementação e monitorização do programa de prevenção de prevenção de BC e FT, sendo igualmente responsável pela centralização de informação e comunicação de operações susceptíveis de branqueamento de capitais e financiamento do terrorismo à Unidade de Informação Financeira e outras autoridades competentes
Diligência	Conjunto de actividades que permitem às instituições financeiras estarem, razoavelmente, satisfeitas quanto ao conhecimento que possuem sobre a identidade de um cliente, assim como obter e conservar a informação necessária para compreender a natureza do seu negócio, actividades e o seu perfil de risco,
Diligência reforçada	Conjunto de actividades de natureza adicional ou reforçada face às medidas de diligência devido ao risco do cliente assumido pela instituição financeira ser elevado
Fundos	Quaisquer, instrumentos, recursos ou disponibilidades financeiras, independentemente da sua natureza, da forma que revistam e da sua titulação, bem como quaisquer transacções sobre os mesmos realizadas, tais como: i. Activos financeiros de qualquer natureza, corpóreos ou incorpóreos, tangíveis ou intangíveis, móveis ou imóveis, adquiridos por qualquer meio, de origem legítima ou ilegítima, os documentos ou instrumentos jurídicos sob qualquer forma, incluindo a forma electrónica ou a digital que demonstrem o direito de propriedade ou um interesse sobre tais bens, designadamente, créditos bancários, cheques de viagem, cheques bancários, ordens de pagamento, acções, títulos de crédito, obrigações, saques bancários e letras de crédito; ii. Quaisquer juros, dividendos, proveitos ou valores que acresçam ou sejam gerados pelos fundos ou outros activos designados no ponto i) da alínea presente alínea.
"Know your customer"	Medidas de diligência realizadas pela instituição financeira para determinar a identidade de um cliente, assim como obter e conservar a informação necessária para compreender a natureza do seu negócio e actividades e o seu perfil de risco
Infracção subjacente ao branqueamento de capitais	Factos ilícitos puníveis com pena de prisão que tenha duração mínima superior a 6 (seis) meses
Mitigação do risco	Reduzir a vulnerabilidade e a extensão do risco de branqueamento de capitais e financiamento do terrorismo. Quanto mais elevado o risco, mais abrangentes devem ser as medidas de controlo a implementar. Por oposição, quanto mais baixo, menos medidas necessitam ser implementadas.

Monitorização de transacções	Escrutínio das transacções a serem levadas a cabo ou já efectuadas pelo cliente de forma a identificar transacções suspeitas de estarem relacionadas com actividades criminosas
Pessoas, grupos ou entidades designadas	Pessoas, grupos ou entidades designadas pelo Comité de Sanções das Nações Unidas contra a rede Al-Qaeda e os Talibã conforme a Resolução do Conselho de Segurança das Nações Unidas n.º 1267, mediante a Lista actualizada pelo referido Comité de Sanções, assim como pelo Governo de Angola, mediante outras Listas, relativas à aplicação de medidas restritivas.
Private Banking	Serviço especializado vocacionado para clientes com altos valores patrimoniais prestado pelas instituições financeiras bancárias
Programa de prevenção do BC e FT	Sistema de políticas e processos, assente numa estrutura organizacional, sob os quais a instituição financeira funciona assegurando o cumprimento dos requisitos legais e regulamentares em sede da prevenção de BC e do FT, assim como dos parâmetros de risco assumidos pela instituição financeira relativamente a BC e FT e medidas restritivas.
Risco	Possibilidade de ocorrer um acontecimento futuro com impacto negativo na situação líquida das instituições financeiras, considerando-se, designadamente, as seguintes categorias: risco de crédito: o proveniente do incumprimento dos compromissos financeiros contratualmente estabelecidos por parte de um mutuário ou de uma contraparte nas operações; risco de estratégia: o proveniente de alterações adversas no ambiente de negócios, da incapacidade de resposta a estas alterações e de decisões de gestão estratégica inadequadas; risco de liquidez: o proveniente da incapacidade da instituição financeira cumprir as suas responsabilidades quando estas se tornarem exigíveis; risco de mercado: o proveniente de movimentos adversos nos preços de obrigações, acções ou mercadorias (*commodities*); risco operacional: o proveniente da inadequação dos processos internos, pessoas ou sistemas, bem como dos eventos externos. Inclui o risco de sistemas de informação e de *compliance*: risco de *compliance*: o proveniente de violações ou incumprimento de leis, regras, regulações, contratos, práticas prescritas ou *standards* éticos; risco de sistemas de informação: o proveniente da inadequação das tecnologias de informação em termos de processamento, integridade, controlo e continuidade, proveniente de estratégias ou utilizações inadequadas; risco de reputação: o proveniente da percepção adversa da imagem das instituições financeiras por parte de clientes, contrapartes, accionistas, investidores, supervisores e opinião pública em geral; risco de taxa de câmbio: o proveniente de movimentos adversos nas taxas de câmbio resultando das posições cambiais originadas pela existência de instrumentos

	financeiros denominados em diferentes moedas; risco de taxa de juro: o proveniente de movimentos adversos nas taxas de juro resultando de desfasamentos no montante, nas maturidades ou nos prazos de prefixação das taxas de juro observados nos instrumentos financeiros com juros a receber e a pagar.
Relação de negócio	Relação de natureza comercial ou profissional entre as entidades sujeitas e os seus clientes que, no momento em que esta, efectivamente, se estabelece, se prevê que venha a ser, ou seja duradoura;
Sanções financeiras	Medidas restritivas implementadas por organizações internacionais ou por países (a título individual) aplicáveis a jurisdições, pessoas ou entidades com o propósito de combater o terrorismo e manter ou restaurar a paz e a segurança internacional. A nível internacional, as sanções financeiras são adoptadas por vários países ou jurisdições contra um país que viole disposições de direito internacional.
Sistema de controlo interno	Conjunto integrado de políticas e processos, com carácter permanente e transversal a toda instituição financeira, realizados pelo órgão de administração e demais colaboradores no sentido de se alcançarem os objectivos de eficiência na execução das operações, controlo dos riscos, fiabilidade da informação contabilística e de suporte à gestão, e cumprimento dos normativos legais e das directrizes internas.
Transacção ocasional	Qualquer transacção efectuada pelas entidades sujeitas fora do âmbito de uma relação de negócio.