Políticas e Procedimentos de Prevenção ao Branqueamento de Capitais e Combate ao Financiamento do Terrorismo e Proliferação de Armas de Destruição em Massa

Banco BIR, S.A

Detalhes do documento

Título:	Políticas e Procedimentos de Prevenção ao Branqueamento de Capitais e Combate ao Financiamento do Terrorismo e Proliferação de Armas de Destruição em Massa
Ficheiro:	DCOMP_Políticas e Procedimentos de Prevenção ao Branqueamento de Capitais e Combate ao Financiamento do Terrorismo e Proliferação de Armas de Destruição em Massa

Revisão do documento

Data:	Versão	Responsável	Motivo de intervenção
05-2025	V.5	DCOMP	Actualização
05-2025	V.5	DOQ	Formatação
05-2025	V.5	CI	Validação

Aprovado por:

Data:	Versão	Nome
02-06-2023	V.5	Conselho de Administração

Actualizações ao documento:

Versão	Data de entrada em vigor	Alterações
V.1	01-12-2015	Criação (CA.OS.MP.006.2015)
V.2	09-09-2019	Actualização (CA.OS.MP.006.2015)
V.3	08-12-2020	Actualização (CA.OS.007.2019)
V.4	15-05-2023	Actualização (CA.OS.007.2020)
V.5	02-06-2025	Actualização (CA.OS.005.2023)

Legislação/Regulação de suporte ao documento:

Diploma	Data de entrada em vigor	Assunto
Aviso n.º 02/2024	22 de Março	Regras e Procedimentos para a Implementação Efectiva das Condições de Exercício, Instrumentos, Mecanismos, Formalidades e Prestação de Informação, inerentes à Prevenção e Combate ao Branqueamento de Capitais e Financiamento do Terrorismo e da Proliferação de Armas de Destruição em Massa.
Regulamento n.º 5/2021	8 de Novembro	Prevenção e Combate ao Branqueamento de Capitais, Financiamento do Terrorismo.
Lei n.º 1/2012	12 de Janeiro	Designação e Execução de Actos Jurídicos Internacionais.
Decreto Presidencial n.º 2/18, de 11 de Janeiro	11 de Janeiro	Estabelece a organização e funcionamento da Unidade de Informação Financeira (UIF), prevendo a obrigação de comunicação pelas instituições financeiras de operações de determinado tipo de operações.
Decreto Presidencial n.º 214/13	13 de Dezembro	Regulamento da Lei da Designação e Execução de Actos Jurídicos Internacionais.
Lei n.º 5/20, de 27 de Janeiro	27 de Janeiro	Lei de Prevenção e Combate ao Branqueamento de Capitais do Financiamento do Terrorismo e da Proliferação de Armas de Destruição em Massa, que estabelece medidas de natureza preventiva e repressiva a prevenção do BC/FT, estabelecendo o regime sancionatório aplicável em caso de incumprimento.
Lei n.º 38/20	11 de Novembro	Lei que aprova o Código Penal Angolano
Lei n.º 19/17	25 de Agosto	Lei sobre a Prevenção e o Combate ao Terrorismo, estabelece medidas de naturezas preventivas, repressivas, investigativas e processuais especiais, de apoio e protecção às vítimas do terrorismo, da ocorrência do fenómeno do terrorismo, a factos praticados em território angolano por cidadãos

		nacionais ou estrangeiros, bem como a factos praticados no estrangeiro.
Instrução n.º 09/CMC/12-21	20 de Dezembro	Formulário de Declaração de Identificação de Pessoas Designadas.
Instrução n.º 10/CMC/12-21,	20 de Dezembro	Formulário de Declaração de Operação Suspeita.
Instrução n.º 13/CMC/12-21,	20 de Dezembro	Congelamento de Fundos e Recursos Económicos.
Recomendações do GAFI – Grupo de Acção Financeira	2022	Versão 2022
Instrutivo n.º 20/2020	09 de Dezembro	Define o modelo de Relatório de Prevenção do Branqueamento de Capitais e do Financiamento ao Terrorismo bem como a implementação da validação de Risco.
Instrutivo n.º 13/2018	19 de Setembro	Define os critérios de Prevenção do Branqueamento de Capitais e do Financiamento ao Terrorismo nas Operações de Comércio Internacional.
Lei n.º 12/24	04 de Julho	Lei que Altera a Lei n.º 38/20, de 11 de Novembro, Lei que Aprova o Código Penal Angolano.
Lei n.º 09/24	03 de Julho	Lei que Altera a Lei n.º 19/17, de 25 de Agosto, Lei sobre a Prevenção e o Combate ao Terrorismo.
Lei n.º 11/24	04 de Julho	Lei que Altera a Lei n.º 5/20 de 27 de Janeiro, Lei de Prevenção e Combate ao Branqueamento de Capitais, Financiamento do Terrorismo e Proliferação de Armas de Destruição em Massa.
Guia sobre Identificação e Comunicação de Pessoas, Grupos e Entidades Designadas – Congelamento de Fundos e Recursos Económicos	30 de Maio de 2024	Guia sobre Identificação e Comunicação de Pessoas, Grupos e Entidades Designadas – Congelamento de Fundos e Recursos Económicos.

Abreviaturas:

- ONU – Organização das Nações Unidas
- OFAC – Agência de Controlo de Activos Estrangeiros dos EUA
- EU – União Europeia
- BIR – Banco de Investimento Rural
- UIF – Unidade de Informação Financeira

ÍNDICE

CAPÍTULO I – ÂMBITO DE APLICAÇÃO E OBJECTIVOS

1.1. Âmbito

O Manual de Políticas e Procedimentos de Prevenção e Combate ao Branqueamento de Capitais e Financiamento do Terrorismo e Proliferação de Armas de Destruição em Massa (adiante "Manual") aplica-se, transversalmente, a todas as unidades de negócio do Banco de Investimento Rural, S.A. (adiante "BIR" ou "Banco BIR").

As normas constantes do presente Manual e adoptadas pelo Banco BIR, correspondem à aplicação dos princípios e orientações internacionais em matéria de Prevenção do Branqueamento de Capitais e Combate ao Financiamento do Terrorismo e Proliferação de Armas de Destruição em Massa (BC/FT-P), assim como dos imperativos legais em vigor, das exigências regulamentares estabelecidas pelo Banco Nacional de Angola (adiante "BNA") e das orientações da Unidade de Informação Financeira de Angola (adiante "UIF").

1.2. Objectivos

No presente Manual são definidas as Políticas e Procedimentos internos do BIR em matéria de Prevenção e Combate do BC/FT-P, tendo como principais objectivos:

- Garantir a implementação de um sistema eficiente de prevenção e combate do crime de branqueamento de capitais e do financiamento do terrorismo, e Proliferação de Armas de Destruição em Massa, sendo adoptada uma abordagem baseada no risco;
- Garantir o conhecimento pelo Banco BIR dos seus clientes ("*Know Your Costumer*"- "conheça o seu cliente"), da sua actividade e respectivas transacções ("*Know Your Transactions*"- "Conheça as suas Transacções/Pagamentos");
- Estabelecer o cumprimento das obrigações legais e regulamentares às quais o Banco se encontra sujeito;

- Sensibilizar os colaboradores do Banco pelo cumprimento das regras de prevenção e combate do branqueamento de capitais e do financiamento do terrorismo e responsabilizá-los em caso de incumprimento de tais regras;
- Assegurar que operações e transacções relacionadas ao comércio internacional observem procedimentos de diligência reforçada, por representarem um risco elevado de branqueamento de capitais, financiamento do terrorismo e infracções subjacentes;
- Estabelecer controlos apropriados para mitigação dos riscos identificados;
- Estabelecer mecanismos que garantam uma detecção eficaz de operações suspeitas e respectiva comunicação às Autoridades competentes, designadamente à Unidade de Informação Financeira.

O responsável pelo presente Manual é a Direcção de *Compliance* (DCOMP), sendo este sujeito à aprovação formal do Conselho de Administração (CA) do BIR.

As alterações/actualizações a este Manual devem ser aprovadas pelo Conselho de Administração, por proposta da Direcção de *Compliance* (DCOMP) e com conhecimento da Direcção de Auditoria Interna (DAI) e Direcção de Organização e Qualidade (DOQ).

CAPÍTULO II – ENQUADRAMENTO

2.1. Definições

«Cliente» Pessoa singular ou colectiva, nacional ou estrangeira, pública ou privada, coligada ou não, que celebra um contrato de abertura de conta com o Banco, a quem esta coloca à disposição produtos e serviços financeiros;

«*Know Your Customer*» Significa conhecer o seu cliente. A verificação KYC ou KYC é o processo obrigatório de identificação e verificação da identidade do cliente ao abrir uma conta e, periodicamente, ao longo do tempo da relação.

«Pessoas Politicamente Expostas (PPEs)» Indivíduos nacionais ou estrangeiros que desempenham ou desempenharam funções públicas proeminentes em Angola, ou em qualquer organização internacional; Para efeitos da presente Lei, consideram-se altos cargos de natureza política ou pública, de entre
outros, os seguintes:

1. Presidente da República ou Chefe de Estado;
2. Vice-Presidente da República;
3. Primeiro Ministro ou Chefe de Governo;
4. Órgãos Auxiliares do Presidente da República, ou membros do Governo, designadamente Ministros de Estado, Ministros, Secretários de Estado e Vice-Ministros e outros cargos ou funções equiparadas;
5. Deputados, Membros de Câmaras Parlamentares e equiparados;
6. Magistrados Judiciais dos Tribunais Superiores e da Relação, cujas decisões não possam ser objecto de recurso, salvo em circunstâncias excepcionais;
7. Magistrados do Ministério Público de escalão equiparado aos Magistrados Judiciais referidos no número anterior;
8. Provedor de Justiça e Provedor de Justiça-Adjunto;
9. Membros do Conselho da República, do Conselho de Segurança Nacional e demais Conselheiros de Estado;

10. Membros da Comissão Nacional Eleitoral;
11. Membros dos Conselhos Superiores da Magistratura Judicial e do Ministério Público;
12. Membros de órgãos de Administração e Fiscalização dos Bancos Centrais e outras autoridades de regulação e supervisão do Sector Financeiro;
13. Chefes de missões diplomáticas e de postos consulares;
14. Oficiais Generais das Forças Armadas e Oficiais Comissários das Forças de Segurança e Ordem Interna;
15. Membros de órgãos de administração e de fiscalização de empresas públicas e de sociedades de capitais exclusiva ou maioritariamente públicos, institutos públicos, associações e fundações públicas, estabelecimentos públicos, qualquer que seja o modo da sua designação, incluindo os órgãos de gestão das empresas integrantes dos sectores empresariais locais;
16. Membros do Conselho de Administração, Directores, Directores-Adjuntos e ou pessoas que exercem funções equivalentes numa organização internacional;
17. Membros dos órgãos executivos de direcção de Partidos Políticos;
18. Membros das administrações locais e do poder autárquico;
19. Líderes de confissões religiosas.

b) No âmbito da presente Lei, são também tratadas como pessoas politicamente expostas os membros da família e as pessoas muito próximas dos indivíduos acima mencionados, nomeadamente:

1. O cônjuge ou companheiro de união de facto;
2. Os parentes, até ao 3.º grau da linha colateral, os afins até ao mesmo grau, os respectivos cônjuges ou companheiros de união de facto;
3. Pessoas com reconhecidas e estreitas relações de natureza pessoal;
4. Pessoas com reconhecidas e estreitas relações de natureza societária ou comercial
5. nomeadamente:

(i) Qualquer pessoa singular, que seja notoriamente conhecida como proprietária conjunta de uma pessoa colectiva com o titular do alto cargo

de natureza política ou pública ou que com ele tenha relações comerciais próximas;

(ii) Qualquer pessoa singular que seja proprietária do capital social ou dos direitos de voto de uma pessoa colectiva ou do património de um centro de interesses colectivos sem personalidade jurídica, que seja notoriamente conhecido, tendo como único beneficiário efectivo o titular do alto cargo de natureza política ou pública.

«Pessoas de Perfil de Risco Elevado (PPRE)» - são aquelas que apresentam maior probabilidade de estar envolvidas em actividades ilegais que podem conduzir ao branqueamento de capitais ou ao financiamento do terrorismo. Essas pessoas, devido as suas características ou circunstâncias, representam um risco maior para o Banco.

«Beneficiário Efectivo» - a pessoa ou pessoas singulares que:

i) detêm, em última instância, uma participação no capital de uma pessoa colectiva ou a controlam e/ou a pessoa singular em cujo nome a operação está sendo realizada;

ii) exercem, em última instância, um controlo efectivo sobre uma pessoa colectiva ou entidade sem personalidade jurídica, naquelas situações onde as participações no capital/controlo são exercidas por meio de uma cadeia de participação no capital ou através de um controlo não directo;

iii) detêm, em última instância, a propriedade ou o controlo directo ou indirecto do capital da sociedade ou dos direitos de voto da pessoa colectiva, que não seja uma sociedade cotada num mercado regulamentado, sujeita a requisitos de informação consentâneos com as normas internacionais;

iv) têm o direito de exercer ou que exerçam influência significativa ou que controlam a sociedade independentemente do nível de participação.

b) No caso de entidades jurídicas que administrem ou distribuam fundos, a pessoa ou pessoas singulares que:

i) beneficiem do seu património quando os futuros beneficiários já tiverem sido determinados;

ii) sejam tidas como a categoria de pessoas em cujo interesse principal a pessoa colectiva foi constituída ou exerce a sua actividade, quando os futuros beneficiários não tiverem sido ainda determinados; e

iii) exerçam controlo do património da pessoa colectiva.

«Banco de Fachada (*Shell Bank*)» Banco constituído e autorizado a operar numa jurisdição, mas que não tem presença física nessa jurisdição e que não está filiada a um grupo financeiro regulamentado e sujeito a uma supervisão efectiva;

«Falso Positivo» Ocorre quando não há correspondência de nome durante o processo de triagem da entidade/cliente;

«Hit Positivo» Ocorre quando há correspondência de nome durante o processo de triagem da entidade/cliente;

«Hit» É a possível correspondência de nome durante o processo de triagem contra as listas de sanções que indica uma pessoa(s) sancionada(s).

«Diligência Reforçada» Conjunto de diligências acrescidas realizadas sempre que no âmbito do cálculo do score de risco dos clientes seja identificado um risco acrescido de BC/FT/P.

«**Financiamento do Terrorismo**» consiste no fornecimento, no depósito, na distribuição ou na recolha de fundos, por qualquer meio, de forma directa ou indirecta, com a intenção de os utilizar ou com o conhecimento de que serão utilizados, integralmente ou em parte, no planeamento ou para a execução de qualquer delito terrorista.

«Proliferação de Armas de Destruição em Massa» Processo pelo qual o agente fornece, recolhe ou detém fundos ou bens de qualquer tipo ou natureza, de origem lícita ou ilícita, bem como produtos ou direitos susceptíveis de serem transformados em fundos destinados à proliferação de armas com capacidade de causar um elevado número de mortos numa única utilização, quer sejam de armas nucleares, químicas ou biológicas, e de materiais relacionados.

«**Branqueamento de Capitais**» entende-se a participação em qualquer actividade que tenha como finalidade adquirir, deter, utilizar, converter, transferir, ocultar ou disfarçar

a natureza, a origem, a localização, a disposição, o movimento ou a propriedade efectiva de bens ou direitos sobre bens, sabendo que os ditos bens procedem de uma actividade ilícita ou da participação numa actividade ilícita.

O processo de branqueamento de capitais, apresenta-se em 3 (três) fases:

1. **Colocação –** pressupõe introduzir o numerário proveniente de actividades ilícitas em instituições financeiras ou não financeiras.
2. **Diversificação/Circulação –** indica a desvinculação dos rendimentos procedentes de uma actividade ilícita, através da utilização de diversas operações financeiras ou não financeiras complexas. Estas transacções têm como finalidade dificultar o seu controlo, ocultar a origem dos fundos e facilitar o anonimato.
3. **Integração –** indica o retorno dos rendimentos branqueados no sector da economia de onde procediam ou outro sector diferente, com uma aparência de legitimidade.

As Instituições Financeiras podem ser utilizadas em qualquer uma das fases do processo de Branqueamento de Capitais ou do processo de Financiamento do Terrorismo.

CAPÍTULO III – PROGRAMA DE PREVENÇÃO DO RISCO DE BC/FT-P

3.1. Sistema de Gestão do Risco de BC/FT-P

O Sistema de Gestão do Risco de BC/FT/P consiste na adequada identificação, avaliação e mitigação dos riscos de branqueamento de capitais e financiamento do terrorismo aos quais o BIR, no decorrer da sua actividade, se encontra exposto, possibilitando, desta forma, uma monitorização eficiente dos seus clientes e transacções e uma efectiva prevenção e detecção de operações potencialmente suspeitas.

O Sistema de Gestão do Risco de BC/FT/P do BIR contempla as seguintes vertentes:

- Modelo de Avaliação de Risco (*Scoring* – KYC);
- Sistemas de Filtragem de Clientes e Transacções;

- Políticas internas de Gestão do Risco de BC/FT/P;
- Modelo de *Governance*;
- Processos e Procedimentos Internos;
- Controlos instituídos de Mitigação dos Riscos;
- Informação de Gestão;
- Plano de Sensibilização e Formação.

O BIR nomeia, formalmente, um Responsável pela função de *Compliance*, encarregue de garantir o cumprimento das obrigações respeitantes à prevenção do branqueamento de capitais e financiamento do terrorismo e da proliferação de armas de destruição em massa. Este responsável é, oficialmente, denominado por "*Compliance Officer*".

As responsabilidades do *Compliance Officer* são, entre outras, as seguintes:

- Coordenar e monitorar a aplicação efectiva das políticas e dos procedimentos e controlos adequados à gestão eficaz dos riscos de branqueamento de capitais, financiamento do terrorismo e da proliferação de armas de destruição em massa a que a entidade financeira esteja ou venha a estar exposta;
- Participar na definição e emitir parecer prévio sobre as políticas e os procedimentos e controlos destinados a prevenir o branqueamento de capitais, financiamento do terrorismo e da proliferação de armas de destruição em massa;
- Acompanhar em permanência a adequação, a suficiência e a actualidade das políticas e dos procedimentos e controlos em matéria de prevenção do branqueamento de capitais, financiamento do terrorismo e da proliferação de armas de destruição em massa, propondo as necessárias actualizações, junto do Conselho de Administração e da Comissão de Auditoria e Controlo Interno;
- Participar na definição, acompanhamento e avaliação da política de formação interna da instituição financeira;
- Assegurar a centralização de toda a informação relevante que provenha das diversas áreas de negócio da Instituição Financeira;
- Comunicar, sem interferências internas ou externas, as operações mencionadas no artigo 17.º da Lei n.º 05/20, de 27 de Janeiro, à Unidade de Informação Financeira;

- Desempenhar o papel de interlocutor das autoridades de aplicação da lei e de supervisão e fiscalização, designadamente dando cumprimento à obrigação de comunicação prevista no artigo 17.º da Lei n.º 05/20, de 27 de Janeiro, assegurando o exercício das demais obrigações de comunicação e de colaboração;
- Apoiar a preparação e execução das avaliações de risco de Branqueamento de Capitais do Financiamento do Terrorismo e da Proliferação de Armas de Destruição em Massa, a que o Banco está exposto a nível de clientes individuais e de transacções, tendo em conta os principais factores de avaliação de risco consubstanciados nas boas práticas regulamentares e legais nacionais e internacionais;
- Coordenar a elaboração dos reportes, relatórios e demais informações a enviar ao Banco Nacional de Angola em matéria de prevenção ao Branqueamento de Capitais, Financiamento do Terrorismo e da Proliferação de Armas de Destruição em Massa;
- Assegurar que todos os colaboradores do Banco, independentemente da natureza do respectivo vínculo, têm conhecimento: i) Da identidade e dos contactos do *Compliance Officer;* ii) Dos procedimentos de comunicação àquela pessoa, das condutas e das actividades ou operações suspeitas que os mesmos detectem.

Para tal, o Banco assegura que a selecção do quadro de colaboradores afectos à área ou função *Compliance* é feita com base em elevados padrões éticos e exigentes requisitos técnicos e que informa o Banco Nacional de Angola a identidade e demais elementos necessários do *Compliance Officer*, bem como quaisquer alterações a esses elementos, logo que as mesmas se verifiquem.

O Sistema de Gestão do Risco de BC/FT/P assenta numa abordagem baseada no risco, permitindo ao Banco identificar os clientes que comportam maior risco e adequar as medidas de diligência e grau de monitorização de acordo com o nível de risco obtido.
Para tal, foram desenvolvidos mecanismos que permitem uma adequada avaliação de risco face às características intrínsecas dos seus clientes e da sua actividade, assim como, uma monitorização eficaz das relações de negócio estabelecidas, permitindo a efectiva mitigação do risco, prevenção e detecção da prática de crimes de BC/FT/P.

A caracterização da carteira de clientes do Banco em termos de risco de BC/FT/P determina a aplicação de medidas e controlos ajustados ao risco, permitindo um maior conhecimento e monitorização dos comportamentos e actividade transaccional dos clientes que comportam maior risco, face às suas características específicas, segmentos de negócio e produtos subscritos.

A classificação do risco dos clientes do Banco determina ainda o nível de diligência a aplicar, a frequência dos processos de actualização da informação e de reavaliação do risco, assim como a necessidade de aplicação de medidas adicionais de monitorização da actividade transaccional.

CAPÍTULO IV - POLÍTICAS GERAIS DE PREVENÇÃO DO BC/FT-P

4.1. Política de Gestão do Risco de BC/FT-P

A Política de Gestão de Risco de BC/FT do BIR, visa identificar os princípios gerais que suportam o sistema de gestão de risco do Banco, identificar os factores mitigadores de risco implementados, bem como, reflectir o apetite do BIR tendo por base os riscos identificados.

4.2. Política de Aceitação de Clientes

No âmbito do estabelecimento de relações de negócio, deve ser recolhida toda a informação e documentação suficiente que permita, razoavelmente, excluir o enquadramento de clientes em algumas situações de proibição. A política de aceitação de clientes é de carácter obrigatório, sem excepção, e aplicável a todos os segmentos de clientes, tendo de ser cumprida por todas as unidades de estrutura do Banco.

4.2.1. Clientes Proibidos

Com base na classificação do risco de BC/FT/P, a instituição não pode aceitar estabelecer relações de negócio com as seguintes categorias de clientes:

- Pessoas incluídas em alguma das Listas oficiais de sanções;
- Pessoas sobre as quais se disponha de alguma informação de que se deduza poderem estar relacionadas com actividades ilícitas;
- Pessoas que tenham negócios cuja natureza seja impossível de verificar a legitimidade das actividades ou a procedência dos fundos;
- Envolvam contas cujos titulares ou representantes sejam clientes anónimos ou com nomes manifestamente fictícios;
- Pessoas que recusem dar informação ou a documentação requerida;
- Pessoas colectivas cuja estrutura accionista ou de controlo não se possa determinar;
- Casinos ou entidades de apostas não autorizadas oficialmente;
- Entidades financeiras residentes em países ou territórios em que não tenham presença física (designados por "bancos de fachada" ou "*shell banks*") e que não pertençam a um grupo financeiro regulado.
- Registados com um nome que não corresponde com o perfil e objecto social da empresa.
- Registados com uma denominação social diferente indicada da actividade ou serviço que presta.

4.3. Aceitação de Clientes dependente de Autorização Prévia

De acordo com o modelo de Gestão de Risco de BC/FT/P definido pelo Banco BIR (Política de Gestão de Risco de BC/FT (Capítulo V), os seguintes tipos de clientes, só serão admitidos mediante autorização do Órgão de Gestão:

- Clientes classificados com **Risco Alto**

- Clientes classificados como **PPE/Pessoa Politicamente Exposta**
- **Organizações sem fins lucrativos**
- **Casinos e/ou Casas de Jogo**

4.4. Modelo de *Governance*

O Modelo de *Governance* compreende as seguintes vertentes:

- Estrutura de *Governance*, incluindo a atribuição de responsabilidades e competências e a definição de linhas de reporte, assegurando o princípio da segregação de funções;
- Adequação de recursos técnicos e humanos e suporte tecnológico; e
- Informação de gestão, de forma a assegurar a monitorização e controlo do Sistema de Gestão do Risco de BC/FT.

No âmbito do sistema de Gestão do Risco de BC/FT, são envolvidas as seguintes unidades de estrutura do BIR:

Unidade de Estrutura	Principais áreas de intervenção
Conselho de Administração (CA) /Comissão Executiva (CE)	• Definição da estratégia de Gestão do Risco de BC/FT; • Aprovação das políticas, processos e procedimentos internos; • Aprovação do nível de exposição em termos de risco de BC/FT, em função dos resultados obtidos por aplicação do *Scoring* KYC à carteira de clientes do Banco BIR; • Aprovação de Entidades classificadas como Risco Alto e PPE's, de acordo com a hierarquia de aprovação definida; • Decisão de reporte de operações suspeitas, após comunicação apresentada pela DCOMP; • Análise dos resultados obtidos na sequência das avaliações efectuadas no âmbito do modelo de Gestão do Risco de BC/FT; • Garantir a efectiva implementação das medidas correctivas identificadas; • Assegurar o cumprimento por parte do Banco BIR das exigências regulamentares estabelecidas em matéria de prevenção dos crimes de BC/FT;

Unidade de Estrutura	Principais áreas de intervenção
	• Garantir que a DCOMP disponha de meios (humanos e técnicos) necessários ao desempenho eficaz das suas funções.
Direcção de *Compliance* (DCOMP)	• Identificação e avaliação dos riscos de BC/FT existentes; • Monitorização contínua, de forma a identificar a necessidade de eventuais ajustes ao programa de prevenção de BC/FT; • Revisão do Modelo de Avaliação de Risco de BC/FT; • Actualização dos processos, procedimentos e controlos de mitigação dos riscos identificados; • Aplicação dos processos e procedimentos internos definidos; • Emissão de parecer quanto às Entidades classificadas como Risco Alto e PPEs; • Análise dos resultados da filtragem de Entidades e Transacções; • Análise/Investigação de operações potencialmente suspeitas; • Monitorização contínua de clientes e transacções em função do grau de risco identificado e dos alertas definidos; • Reporte de operações suspeitas junto da Unidade de Informação Financeira; • Elaboração dos relatórios de gestão relativos ao modelo de Gestão de Risco de BC/FT e submissão à Comissão Executiva / Conselho de Administração; • Participação na definição, acompanhamento e avaliação da política de formação interna do Banco sobre a prevenção do BC/FT; • No âmbito do sistema de controlo interno, assegurar o cumprimento pelas unidades de negócio políticas, meios e procedimentos definidos em matéria de Prevenção do BC/FT;
Direcção de Auditoria Interna (DAI)	• Avaliação da adequação e eficácia do modelo e das políticas, processos, procedimentos e controlos instituídos; • Identificação de deficiências e proposta de medidas correctivas a serem implementadas.
Direcção de Sistemas de Informação (DSI)	• Implementação de equipamento tecnológico; • Disponibilização de ferramentas à Rede de Balcões e às áreas de controlo; • Extracção de informação necessária dos sistemas do Banco para a produção de relatórios da DCOMP; • Monitorização contínua dos sistemas informáticos;

Unidade de Estrutura	Principais áreas de intervenção
	• Implementação das alterações necessárias aos sistemas de informação, de forma a cumprir os requisitos funcionais, de negócio e de reporte definidos no âmbito do sistema de gestão de Risco de BC/FT. • Garantir o funcionamento e manutenção das ferramentas de *Scoring* KYC, desenvolvidas no âmbito do *Onboarding* de clientes; • Garantir o normal funcionamento da ferramenta de filtragem contra as Listas de Sanções, Listas de Países, Listas de Pessoas Politicamente Expostas (PEPs), entre outras Listas externas e internas que sejam adoptadas pelo Banco BIR;
Rede Comercial: Balcões, *Private,* Empresa	• Aplicação dos processos e procedimentos de identificação e diligência; • Recolha de informação e documentação necessárias, de acordo com os normativos internos e com as exigências legais e regulamentares existentes; • Conhecimento e acompanhamento dos clientes; • Realização da avaliação inicial de risco de BC/FT com recurso ao *Onboarding* de clientes; • Adequação no preenchimento do formulário *"Know Your Customer"- "* Conheça o seu Cliente"; • Exercício do dever de recusa e dever de abstenção; • Reporte à DCOMP de operações potencialmente suspeitas; • Colaborar com a DCOMP sempre que seja necessária informação adicional relativa aos clientes e transacções; • Participar, proactivamente, em acções de formação e sempre que forem convocados para esse fim.

4.5. Informação de Gestão

A Direcção de *Compliance* deve produzir relatórios de gestão, com o objectivo de reportar informação estatística relativa ao acompanhamento do Sistema de Gestão de Risco de BC & FT, assim como referente às análises realizadas em cumprimento dos deveres de exame, de diligência e de comunicação.

Os relatórios produzidos no âmbito do acompanhamento do Sistema de Gestão de Risco de BC & FT, devem ser, formalmente, submetidos à apreciação e aprovação do Administrador do Pelouro de *Compliance* (relatórios trimestrais), da Comissão Executiva

(relatórios mensais e/ou trimestrais) e do Conselho de Administração (CA) (relatórios anuais).

Encontram-se detalhados no Procedimento de Reporte de Informação de Gestão a estrutura, periodicidade e conteúdos dos relatórios de informação de gestão. São igualmente identificados no referido documento os intervenientes, e os sistemas de Tecnologias de Informação afectados.

CAPÍTULO V – PRINCÍPIOS E PROCEDIMENTOS DE PREVENÇÃO DO BC/FT-P

5.1. Obrigação de Identificação [1]

O BIR encontra-se sujeito ao dever de identificação, devendo exigir a identificação dos seus clientes, representantes e beneficiários efectivos sempre que:

- Estabeleçam relações de negócio;
- Efectuem transacções ocasionais de montante igual ou superior, em moeda nacional, ao equivalente a USD 15.000,00 (Quinze mil dólares dos Estados Unidos da América), independentemente da transacção ser realizada através de uma única operação ou de várias operações que aparentem estar relacionadas entre si;
- Surjam suspeitas de que as operações, independentemente do seu valor, estejam relacionadas com o crime de branqueamento de capitais ou de financiamento do terrorismo, tendo em conta a natureza da operação, a sua complexidade, carácter atípico face ao perfil ou actividade do Cliente;
- Existam dúvidas quanto à autenticidade ou à conformidade dos dados de identificação dos clientes.

[1] **Protecção de dados de carácter pessoal: o** tratamento de dados de carácter pessoal, assim como os ficheiros, automatizados ou não, criados para o cumprimento das disposições da vigente regulação em matéria de branqueamento de capitais e de financiamento do terrorismo, submetem-se ao disposto na Lei referente a protecção de dados de pessoais.

No exercício do dever de identificação importa que sejam cumpridos todos os requisitos conforme o Aviso do Banco Nacional de Angola n.º 2/2024, de 22 de Março e o previsto na checklist de abertura de conta em vigor.

A verificação de quaisquer elementos exigíveis para a abertura de conta apenas pode ser efectuada, mediante documentos originais ou cópia certificada dos mesmos.
É expressamente proibida a abertura de contas anónimas ou com nomes fictícios.

Neste sentido, todas as unidades de negócio do BIR, com maior responsabilidade para a Direcção Comercial, devem garantir um eficaz e completo conhecimento dos seus clientes, representantes e beneficiários efectivos, assim como da (s) respectiva (s) actividade (s), devendo:

- Confirmar e documentar a verdadeira identidade dos clientes com os quais se mantém qualquer tipo de relação comercial, dos seus representantes e beneficiários efectivos;
- Confirmar e documentar quaisquer informações adicionais recolhidas sobre o cliente, representantes e beneficiários efectivos, de acordo com o modelo de avaliação dos riscos de branqueamento de capitais e de financiamento do terrorismo;
- Garantir que as unidades de negócio do Banco BIR não realizam operações com indivíduos ou entidades cujas identidades não se podem confirmar, que não apresentem a informação necessária ou tenham fornecido informação falsa ou com incoerências significativas que não se possam esclarecer;
- Exigir os documentos de suporte dos poderes das pessoas autorizadas a realizar transacções financeiras em nome do cliente, devendo obter a identificação das pessoas e determinar a sua relação com o cliente;
- Determinar a verdadeira identidade da pessoa com a qual se estabeleça uma relação, se abra uma conta ou se execute uma operação importante (quer

dizer, os titulares beneficiários), quando o cliente actue por conta de terceiros ou nos casos em que existem dúvidas se o cliente age em seu próprio nome.

- Nas situações em que o cliente for uma pessoa colectiva ou um centro de interesses colectivos sem personalidade jurídica ou, em qualquer caso, sempre que haja conhecimento ou fundada suspeita de que um cliente não actua por conta própria, devem as entidades sujeitas obter do cliente informação que permita conhecer a identidade do beneficiário efectivo[2], devendo ser tomadas as adequadas medidas de verificação da mesma, em função do risco de branqueamento de capitais ou de financiamento do terrorismo.

5.2. Obrigação de Diligência

No âmbito do dever de diligência, e sem prejuízo do cumprimento do dever de identificação, deve o Banco aplicar medidas acrescidas de diligência tais como a solicitação de declarações de origem e destino de fundos, informação actualizada sobre o KYC em relação aos clientes e às operações que, pela sua natureza ou características, possam revelar um maior risco de branqueamento de capitais ou de financiamento do terrorismo.

[2] Nos termos da Lei n.º 5/20, de 27 de Janeiro, entende-se por «Beneficiário efectivo», a pessoa ou pessoas singulares que:

1) Detêm, em última instância, uma participação no capital de uma pessoa colectiva ou a controlam e/ou a pessoa em cujo nome a operação está sendo realizada;
2) Exercem, em última instância, um controlo efectivo sobre uma pessoa colectiva ou entidade sem personalidade jurídica, naquelas situações onde as participações no capital/controlo são exercidas por meio de uma cadeia de participação no capital ou através de um controlo não directo;
3) Detêm, em última instância, a propriedade ou o controlo directo ou indirecto do capital da sociedade ou dos direitos de voto da pessoa colectiva, que não seja uma sociedade cotada num mercado regulamentado, sujeito a requisitos de informação consentâneos com as normas internacionais;
4) Têm o direito de exercer ou que exerçam influência significativa ou que controlam a sociedade independentemente do nível de participação.

ii. No caso de entidades jurídicas que administrem ou distribuam fundos, a pessoa ou pessoas singulares que:

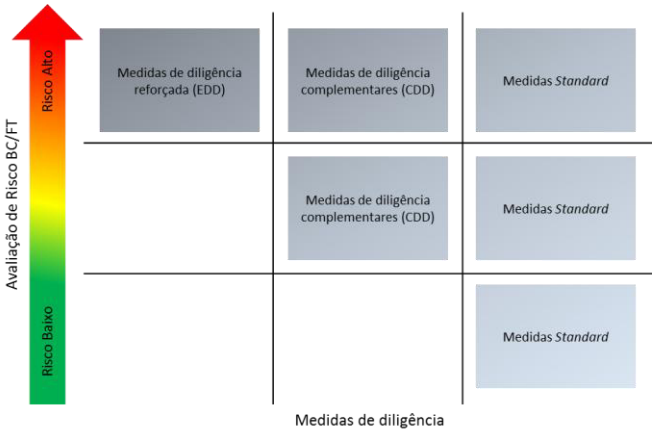
1) Beneficiam do seu património quando os futuros beneficiários já tiveram sido determinados;
2) Sejam tidos como a categoria de pessoas em cujo interesse principal a pessoa colectiva foi constituída ou exerce a sua actividade quando os futuros beneficiários não tiverem sido ainda determinados;
3) Exerçam controlo do património da pessoa colectiva;

5.3. Adequação ao grau de risco

Tendo em conta que cada cliente comporta um nível diferente de risco, a natureza e extensão da medida de diligência a ser aplicada depende da avaliação do risco associado a cada cliente, às características da relação de negócio, ao tipo de produto ou serviços subscritos, assim como às transacções e origem e destino dos fundos (artigo 9.º da Lei n.º 5/20, de 27 de Janeiro e o artigo 5.º do Aviso n.º 2/2024, de 22 de Março).

Assim, em função do resultado da avaliação do risco (*Scoring* - KYC), obtido no âmbito da abertura de conta, ou ao longo da relação de negócio decorrente da reavaliação de risco, deve ser obtida informação adicional sobre o cliente, representantes ou beneficiários efectivos e realizadas medidas de diligência complementar / reforçada (vide figura 1 *infra*):

Figura 1 – Medidas de diligência a aplicar consoante o grau de risco



5.4. Diligência Reforçada

Os procedimentos internos de diligência complementar e de diligência reforçada encontram-se definidos no documento "**Procedimentos de Diligência a Entidades e Clientes**".

Para além das medidas de diligência *standard*, devem ser aplicadas medidas acrescidas de diligência às operações realizadas à distância e, especialmente, às que possam

favorecer o anonimato, às Pessoas Politicamente Expostas (PPEs) que residam fora do território nacional, às operações de correspondência bancária com instituições de crédito estabelecidas em países terceiros ou a quaisquer outras que sejam designadas pelo BNA. Os procedimentos de diligência específicos respeitantes às relações de correspondência bancária encontram-se detalhados no normativo interno "**Procedimentos de correspondência bancária com base no risco de BC/FT**" e o procedimento de gestão de PPEs, encontra-se na "**Política de Clientes de Alto Risco**".

5.5. Dever de Monitorização Contínua

Para fins de monitorização contínua da relação de negócio, e dependendo da avaliação de risco de branqueamento de capitais e de financiamento do terrorismo, deve ser solicitada a seguinte informação:

- Natureza e detalhes do negócio, da ocupação ou do emprego;
- Registo de mudanças de domicílio;
- Origem dos fundos a serem usados na relação de negócio;
- Origem dos rendimentos iniciais e contínuos;
- As várias relações entre signatários e os respectivos beneficiários efectivos.

A informação *supra* é recolhida através do Formulário de Abertura de Cliente.
Relativamente às Entidades classificadas com Risco Médio e Risco Alto, é recolhida informação adicional, a qual é registada no Formulário de *Know Your Customer* ("**Formulário KYC**").

As áreas comerciais e a DCOMP, assim como as demais unidades de negócio do Banco, devem manter um acompanhamento contínuo das relações de negócio e examinar as operações realizadas, verificando a sua conformidade com a informação previamente obtida e o perfil de risco das Entidades.

No modelo de avaliação de risco definido, são estabelecidos os procedimentos de verificação periódica da actualidade e exactidão das informações referentes às Entidades

com base em critérios de materialidade e risco. As especificações referentes à monitorização contínua dos clientes encontram-se detalhados no normativo interno "**Monitorização Continua de Clientes**".

5.6. Obrigação de Recusa

Os colaboradores do BIR devem recusar a realização de operações sempre que o cliente não forneça a respectiva identificação, do representante ou do beneficiário efectivo, assim como nas circunstâncias em que não seja fornecida informação sobre a estrutura de controlo do cliente, a natureza e a finalidade da relação de negócio e a origem e o destino dos fundos.

Nestas situações em que, por causa imputável ao cliente, não seja possível realizar com o procedimento de identificação, verificação da identidade, diligência simplificada e ou reforçada, o Banco actua ao abrigo do disposto no artigo 15.º da Lei n.º 05/20, de 27 de Janeiro, e decide pôr termo à relação de negócio do seguinte modo:

a) Inibe qualquer movimentação de fundos ou outros bens associados à relação de negócio, incluindo através de quaisquer meios de comunicação à distância;
b) Entra em contacto com o cliente, no prazo máximo de 30 (trinta) dias, para que este indique a conta para a qual devem ser restituídos os fundos ou compareça pessoalmente perante o Banco, para a efectivação da restituição definidas pela Instituição Financeira; e
c) Conservam os fundos ou outros bens, mantendo os mesmos indisponíveis até que a sua restituição seja possível.

Caso o cliente, no contacto com o Banco, entregue os elementos cuja falta determinou a decisão de pôr termo à relação de negócio, e não se verificando qualquer suspeita, é feita uma reavaliação do pedido, efectuando todos os procedimentos de identificação e diligência legalmente devidos.

5.7. Obrigação de Abstenção

O dever de abstenção consiste na proibição de executar qualquer operação relacionada com determinado cliente, quando se constate que uma determinada operação evidencia fundada suspeita de estar relacionada com a prática de crimes de BC/FT-P.

Caso os colaboradores do Banco BIR suspeitem que determinada operação possa estar relacionada com a prática dos crimes de BC/FT-P, devem abster-se de executar a operação e informar de imediato a Direcção de *Compliance*. A Direcção de *Compliance* deve proceder à análise da operação, de acordo com os "**Procedimentos de Análise de Operações com Risco de BC/FT**", estabelecidos no **Capítulo VI** da presente Política e caso existam fundamentos que justifiquem a suspeição, deve proceder-se à respectiva comunicação à Unidade de Informação Financeira.

A operação deve manter-se suspensa até à recepção da decisão da UIF, decisão esta comunicada por escrito, ou por qualquer outro meio, podendo esta autoridade determinar a suspensão da respectiva execução.

A operação pode, todavia, ser realizada se a ordem de suspensão não for confirmada pela UIF, no prazo de 3 (três) dias a contar da comunicação realizada pelo Banco.

Caso a abstenção não seja possível ou, após consulta à Unidade de Informação Financeira, concluir-se ser susceptível de prejudicar a futura investigação no âmbito da prevenção do branqueamento ou do financiamento do terrorismo, a operação pode ser realizada, devendo a entidade sujeita fornecer, de imediato, à Unidade de informação Financeira, as informações respeitantes à operação.

5.8. Obrigação de Exame

O dever de exame consiste na obrigação de analisar, com especial atenção, qualquer conduta, actividade ou operação, cujos elementos caracterizadores a tornem particularmente susceptível de estar associada à prática dos crimes de BC/FT-P ou qualquer outro crime, nomeadamente:

- A natureza, a finalidade, a frequência, a complexidade, a invulgaridade e a atipicidade da conduta, actividade ou operação;
- A aparente inexistência de um objectivo económico ou de um fim lícito associado à conduta, actividade ou operação;
- O montante, a origem e o destino dos fundos movimentados;
- Os meios de pagamento utilizados;
- O sector de actividade e padrão/perfil comportamental dos intervenientes;
- O tipo de transacção ou produto que possa favorecer especialmente o anonimato.

A aferição do grau de suspeição evidenciado por uma actividade, comportamento ou operação não pressupõe a existência de qualquer tipo de documentação confirmativa da suspeita, antes decorrendo da apreciação das circunstâncias concretas, à luz de diligências exigíveis aos colaboradores do Banco.
Os procedimentos de análise das operações encontram-se detalhados no **Capítulo VI** da presente política.

5.9. Obrigação de Comunicação de Operações às Autoridades Competentes

O BIR encontra-se obrigado à comunicação de operações, nas seguintes circunstâncias:

- Sempre que saiba, suspeite, ou tenha razões suficientes para suspeitar que teve lugar, está em curso ou foi tentada uma operação susceptível de configurar a prática do crime de branqueamento de capitais ou de financiamento do terrorismo;

- Transacções em numerário de montante igual ou superior em moeda nacional ou equivalente em 15.000, 00 USD (Quinze Mil Dólares dos Estados Unidos da América); e
- Sempre que, 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 corresponda à identidade de uma pessoa, grupo ou entidade designada numa Lista de Sanções [3].

Aplica-se, igualmente, o dever específico de comunicação no caso de as operações revelarem especial risco de BC/FT-P, nomeadamente, quando se relacionam com um determinado país ou jurisdição sujeito a contra medidas adicionais decididas pelo Governo angolano.

As autoridades de supervisão do respectivo sector podem determinar o dever de comunicação imediata dessas operações à UIF, quando o seu montante for igual ou superior ao equivalente em moeda nacional a 15.000 (Quinze Mil Dólares Norte Americanos).

Quando as unidades de negócio ou colaboradores do Banco efectuem comunicações sobre operações ou actividades suspeitas à Direcção de *Compliance*, fica esta totalmente proibida de fornecer qualquer informação tanto interna como externamente sobre os Clientes ou operações a que se refere a informação sem cumprir com o dever de sigilo.

[3] **«Pessoas, grupos ou entidades designadas»,** pessoas, grupos ou entidades designadas (Directiva 03/DSI/2012 – BNA):

i. 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;

ii. 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;

iii. 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

iii. 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.

5.10. Procedimento interno para a comunicação de operações suspeitas

A unidade de negócio que detecte ou realize a operação suspeita deve comunicar de imediato por escrito, via *e-mail*, a Direcção de *Compliance* para análise e decisão.
Caso seja confirmada a suspeita, e após submissão do" Relatório de Incidência ao conhecimento da Administração, a comunicação à UIF deverá ser realizada em conformidade com a decisão da Direcção de Compliance.

A comunicação das operações à UIF deve ser realizada através de submissão electrónica dos formulários oficiais, através do *website* (*GoAml*) da UIF, ou quando não existam condições técnicas por parte da entidade para reportar, deve ser enviada por *e-mail* ou por correio.

- **Formulário Oficial da UIF:**

  As operações suspeitas devem ser comunicadas através da submissão de Declaração de Operação Suspeita (DOS), as quais devem ser preenchidas de acordo com o respectivo "Guia de preenchimento da (DOS)", disponíveis nos *websites* da UIF e do BNA[4].

5.11. Comunicação de Pessoas e Entidades Designadas

Sempre que o BIR tiver conhecimento, suspeitar ou tiver 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 que uma transacção corresponde a uma pessoa, grupo ou entidade designada, deve comunicar este facto à UIF.
As pessoas e entidades designadas são detectadas através do processo de filtragem realizado no âmbito da abertura de conta e ao longo da relação de negócio.

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

- **Formulário Oficial da UIF:**

As pessoas e entidades designadas devem ser comunicadas através da submissão de Declaração de Identificação de Pessoas e Entidades Designadas (DIPD), as quais devem ser preenchidas de acordo com o respectivo "Guia de preenchimento da (DIPD)", disponíveis nos *websites* da UIF e do BNA[5].

5.12. Comunicação de Transacções em Numerário

As transacções em numerário de montante igual ou superior em moeda nacional ou equivalente a 15.000,00 USD (Quinze Mil Dólares dos Estados Unidos da América), são submetidas todos os dias e directamente à Unidade de Informação Financeira, via *web (GoAml)*, pela Direcção de *Compliance* (DCOMP), no formato xml.

A comunicação de operações em numerário não está dependente de um juízo de suspeição, sendo objecto de comunicação obrigatória. O reporte das operações deve ser efectuado independentemente das transacções serem realizadas mediante uma única operação ou através de várias operações que aparentem estar relacionadas.

O fraccionamento ou estruturação das transacções pode ser utilizado para evitar algum dos registos ou comunicações sistemáticas em virtude da legislação aplicável contra o branqueamento de capitais e o financiamento do terrorismo.

5.13. Obrigação de Conservação de Documentos

O Banco BIR deve conservar, por um período mínimo de 10 (dez) anos, todos os registos, que devem incluir:

- Cópia dos documentos ou outros suportes tecnológicos comprovativos do cumprimento da obrigação de identificação e de diligência;

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

- Registo de transacções nacionais e internacionais que sejam suficientes para permitir a reconstituição de cada operação, de modo a fornecer, se necessário, provas no âmbito de um processo criminal;
- Toda a documentação relacionada com transacções realizadas com Bancos correspondentes;
- Registo dos resultados de investigações internas, assim como registo da cópia das comunicações efectuadas pela instituição financeira bancária à Unidade de Informação Financeira e outras autoridades competentes;
- Fundamentação da decisão de não comunicação à Unidade de Informação Financeira e outras autoridades competentes pelo *Compliance Officer*;
- Cópia de toda a correspondência comercial trocada com o cliente;
- Recomendações em matéria de prevenção de BC/FT efectuadas pela Direcção de Auditoria Interna (DAI).

Adicionalmente, o BIR deve conservar, durante um período de 5 (cinco) anos, cópia dos documentos ou registos relativos a formação prestada aos seus colaboradores, incluindo os Órgãos de Gestão e Administração.

A referida documentação será conservada adequadamente para que seja localizada facilmente e se garanta a sua confidencialidade.

O sistema de arquivo deve assegurar a adequada gestão e disponibilidade da documentação, tanto para efeito de controlo interno, como para efeito de resposta atempada e sempre que solicitada pelo BNA, pela UIF e demais Autoridades competentes.

5.14. Obrigação de Cooperação

O Banco, através da Direcção de *Compliance*, deve prestar, prontamente, cooperação ao Banco Nacional de Angola e à Unidade de Informação Financeira, quando por estas solicitadas, fornecendo-lhes as informações sobre certas operações realizadas pelos clientes e apresentar os documentos relacionados com determinadas operações.

Deverá igualmente cooperar com as autoridades judiciárias e policiais competentes, após o início de processos de investigação formal.

Os pedidos de informação, ofícios e/ou notificações relativamente aos crimes de BC/FT-P dirigidos ao Banco emitidos por Tribunais ou qualquer outra Autoridade, deverão ser enviados a Secretaria da Administração, devendo esta dar conhecimento à Comissão Executiva e à Direcção de Compliance.

Todos estes pedidos de informação, ofícios e/ou notificações recebidos pelas Autoridades Competentes, relativamente aos crimes de BC/FT-P, devem ser registados com a data de recepção numa base de dados mantida pela Direcção de *Compliance* para o efeito. Igualmente, as respostas oficiais emitidas pelo Banco, devem ser registadas no mesmo suporte. Deverá ser registada a seguinte informação, quando aplicável:

- N.º do Ofício/Notificação;
- Designação da Autoridade competente;
- Nome/Designação e N.º da Entidade (Cliente do Banco BIR) e conta (s) associada (s);
- Data de recepção / data da resposta;
- Outra informação relevante.

Para além do respectivo arquivo físico dos documentos recebidos e emitidos, devem ser digitalizados e arquivados em suporte digital pela DCOMP. Todos os ofícios enviados pelo BIR às Autoridades Competentes, referentes aos crimes de BC/FT-P, devem ser assinados por, pelo menos, 2 (dois) Administradores Executivos. O envio da resposta à entidade solicitante deve obedecer os seguintes princípios e formatos de comunicação:

- Meio de submissão *e-mail:* deve-se incluir aviso de recepção;
- Entrega presencial: deve-se garantir a assinatura comprovativa da recepção da segunda via pelo destinatário.

5.15. Obrigação de Sigilo

As comunicações sobre esta matéria têm um carácter estritamente confidencial.

O Banco, os membros dos respectivos órgãos sociais ou que nelas exerçam funções de direcção, de gestão ou chefia, os seus empregados, os mandatários e outras pessoas que lhes prestem serviço a título permanente, temporário ou ocasional, não podem revelar ao cliente ou a terceiros, que transmitiram as comunicações legalmente devidas ou que se encontra em curso uma investigação criminal.

O incumprimento desta norma é considerado como infracção muito grave para os responsáveis da infracção.

5.16. Obrigação de Controlo

O BIR deve aplicar as políticas e os procedimentos internos que se mostrem adequados ao cumprimento dos deveres legalmente estabelecidos, designadamente em matéria de controlo interno, avaliação e gestão do risco e de auditoria interna, a fim de eficazmente prevenir e detectar a prática do crime de BC/FT-P.

5.17. Obrigação de Formação

O Banco deve garantir a formação permanente em matéria de prevenção e detecção do branqueamento de capitais e do financiamento do terrorismo aos seus colaboradores, conforme as suas diferentes necessidades, em particular, aos recém-admitidos, colaboradores de *front - office*, de supervisão ou com funções de *Compliance*, Auditoria, Gestão do Risco e Gestão Comercial.

A Direcção de *Compliance* desenvolverá as acções de formação, em consonância com o DCH, e será realizado um registo de todas as acções de formação efectuadas, deixando evidência da data, lugar, duração de cada curso e nome dos participantes.

O BIR estabelece como objectivo prioritário a adopção das medidas necessárias para que todos os colaboradores recebam a referida formação.

As medidas devem incluir acções de formação específicas e regulares, adequadas ao sector de actividade bancário, que habilitem os colaboradores do Banco a reconhecer operações que possam estar relacionadas com a prática dos crimes de BC/FT-P e actuar de acordo com a legislação em vigor.

Neste sentido, são incluídos no "Programa de Formação Anual" acções de formação específicas, dirigidas aos colaboradores do Banco, incluindo os Órgãos de Gestão e Administração, as quais terão em conta as normas internacionais, a legislação e regulamentação em vigor em Angola nesta matéria, assim como as "Orientações" emitidas pela Unidade de Informação Financeira (UIF).

As acções formativas devem incluir, no mínimo, conteúdos sobre as seguintes matérias:

- Políticas e normativos internos do Banco;
- Processos e procedimentos internos de identificação, diligência, comunicação de operações, abstenção e recusa;
- Sistema de controlo interno e de avaliação de risco no âmbito da prevenção de BC/FT/P;
- *Templates* e formulários internos;
- Modelo de gestão de risco de BC/FT/P;
- Tendências de actividades/práticas associadas ao BC/FT/P;
- Tipologias de operações suspeitas.

Independentemente dos planos gerais de formação, a Direcção de *Compliance* deve manter, permanentemente, informados todos os colaboradores de todas as modificações normativas nesta matéria, assim como de todas as novas modalidades, técnicas ou procedimentos que se detectem como susceptíveis de serem utilizados para a prática dos crimes de BC/FT-P.

CAPÍTULO VI – IDENTIFICAÇÃO / DETECÇÃO DE OPERAÇÕES E MONITORIZAÇÃO

O processo de identificação/detecção de operações e de monitorização visa o acompanhamento da actividade transaccional dos clientes (durante e após a execução das transacções), com vista à identificação de comportamentos e operações suspeitas de BC/FT/P.

A monitorização realizada deve incidir sobre transacções individuais e sobre fluxos de transacções que compõem padrões comportamentais/perfis transaccionais dos Clientes, englobando a análise histórica das transacções efectuadas, assim como a análise de tipologias de operações com maior risco/mais vulneráveis à prática de BC/FT-P.

6.1. Identificação e Detecção de Operações Suspeitas e Monitorização

A Direcção de *Compliance*, assim como as áreas comerciais e demais unidades de negócio, devem colocar em prática os procedimentos adequados para o controlo e análise das operações suspeitas de estarem relacionadas com os crimes de BC/FT-P, com a finalidade de identificar e reportar essas operações às Autoridades Competentes.
A identificação das operações suspeitas pode ocorrer através das seguintes categorias de detecção:

i. Detecção de *outliers* face ao padrão comportamental/perfil transaccional da Entidade:

Para este efeito, devem ser tidos em conta as características específicas das operações e dos respectivos intervenientes, tais como:

- Tipo / Natureza e complexidade das operações;

- Atipicidade no quadro da actividade normal do cliente: deve verificar-se se a operação (operações) é disruptiva face ao padrão comportamental típico do Cliente atendendo os seguintes factores:
  - Valores envolvidos;
  - Meios de pagamento utilizados;
  - Frequência / Velocidade;
  - Países e jurisdições envolvidos na transacção: deve-se verificar se a operação (operações) envolvem Países, territórios ou regiões diferentes daqueles declarados pela Entidade no âmbito da abertura de conta);
- Situação financeira/patrimonial dos intervenientes: deve-se verificar se o tipo de actividade e/ou montante das operações da Entidade é adequado à actividade expectável declarada pela Entidade no âmbito da abertura de conta;
- Sector de Actividade do cliente: deve-se verificar se alguma (s) operação (operações) cujo âmbito e a natureza não seja compatível (ou é pouco usual) com o tipo de cliente (ex: considerando o objectivo da relação de negócio, o propósito da conta, o sector de actividade);
- Origem e destino dos fundos: deve ser analisada a justificação da origem e destino dos fundos, verificando se os depósitos em numerários efectuados apresentam algum tipo de suspeição/ irregularidade (incluindo depósito inicial);
- Justificação económica das operações: deve verificar-se se alguma (s) operação (operações) apresenta uma finalidade e características distintas do padrão normal associado à respectiva tipologia dessas operações.

ii. Enquadramento das operações numa tipologia de operações suspeitas

- Na identificação e detecção de operações suspeitas devem ser tidas em conta as tipologias de operações suspeitas divulgadas pelas Organizações Internacionais, Supervisores e outros Organismos (**Anexo II A.** a presente política).

iii. Relacionamento e agregação de transacções

- Consiste na detecção de operações suspeitas através da agregação ou associação de transacções realizadas pelos Clientes e partes relacionadas.

iv. Filtragem contra Listas de Sanções/ Listas de Suspeitos

- Identificação de operações suspeitas através da filtragem dos intervenientes (ordenantes / beneficiários), assim como dos países, jurisdições ou territórios de origem e destino das operações.

A análise e investigação das operações suspeitas pode ser despoletada através dos seguintes mecanismos:

- **Identificação e detecção de operações suspeitas pela Direcção de *Compliance*** – através das monitorizações contínuas das entidades e contas;
- **Identificação e detecção de operações suspeitas pela Rede Comercial** - no contacto directo com os clientes via *front-office* e outras unidades de negócio;
- **Monitorização reforçada de Entidades** – através do acompanhamento dos clientes de risco alto.

6.2. Identificação e Detecção de operações suspeitas pela Direcção de *Compliance*

Para efeitos de identificação e detecção de operações potencialmente suspeitas, o BIR definiu parâmetros e indicadores de risco, que são utilizados como critérios de selecção de transacções e são objecto de análise permanente por parte da Direcção de *Compliance.*

A Direcção de *Compliance* deve analisar as operações que geram "alertas", por se enquadrarem nos parâmetros de risco definidos, procurando identificar se existem

indícios de suspeição ou se as operações efectuadas se enquadram na actividade normal do cliente.

Na análise das transacções, a Direcção de *Compliance* deve ter em conta o perfil dos intervenientes e as características das operações, tal como descrito no ponto anterior.

Caso a movimentação se considere enquadrada com o padrão comportamental/perfil transaccional das Entidades, os alertas serão encerrados. A conclusão da análise das operações deve ser documentada por escrito, com a fundamentação do encerramento dos "alertas". Caso as operações apresentem sustentados motivos de suspeita, deve proceder-se à abertura de um "Caso" e realizadas diligências adicionais.

6.3. Identificação e Detecção de operações suspeitas pela Estrutura Comercial (*front-office*) e outras Unidades de Negócio

Todas as unidades de negócio devem aplicar medidas de monitorização da relação comercial com o cliente, incluindo o escrutínio das operações efectuadas por forma a garantir que estas são consistentes com o conhecimento do Banco sobre a Entidade e o respectivo perfil comercial e de risco, incluindo a origem e destino dos fundos movimentados.

Na identificação e detecção de operações suspeitas devem ser tidas em conta as tipologias de operações suspeitas elencadas no **Anexo II – A** da presente política.

As unidades de negócio devem seguir os procedimentos internos que estabelecem a forma de proceder quando existe a necessidade de comunicação de operações suspeitas.

A Direcção de *Compliance* para que esteja, em conformidade com a legislação aplicável, realiza a análise/investigação necessária e, caso existam fundamentos para a suspeita, realiza as comunicações devidas às Autoridades competentes (ponto 15 do Capítulo V).

6.4. Monitorização de Entidades (risco alto, PPEs, referenciadas por autoridades competentes)

Para efeitos de monitorização da actividade transaccional das Entidades do BIR, é adoptada uma abordagem baseada no risco. De acordo, com o "processo de Monitorização

de Entidades", a Direcção de *Compliance* deve efectuar uma análise da actividade transaccional das seguintes Entidades:

- **Entidades classificadas com Risco Alto**: devem ser alvo de uma monitorização, acompanhando o histórico mensal das operações realizadas (tipo, montantes, frequência, volume, complexidade, destino, etc.) durante um período de 6 (seis) meses após o início da relação de negócio;

- **Entidades classificadas com Risco Alto e sejam PPEs**: devem ser alvo de uma monitorização, acompanhando o histórico mensal do tipo, montantes e volume de transacções que efectuam, durante o período de 1 (um) ano;
- Clientes que tenham realizado operações com indícios de suspeição, mas que o processo de escrutínio tenha sido concluído com a aplicação da medida de monitorização, sem, no entanto, terem sido alvo de comunicação junto das Autoridades Competentes. Nestes casos, a Direcção de *Compliance* deverá monitorizar a actividade dos clientes mensalmente durante um período de 3 (três) meses;
- Pessoas singulares ou colectivas referenciadas por Autoridades Judiciais ou Judiciárias, pela Unidade de Informação Financeira ou pelo Banco Nacional de Angola (durante o período e com a frequência determinada pela Autoridade competente);
- Entidades referenciadas em situações de conhecimento público, sempre que se considere que as mesmas apresentam risco acrescido de BC/FT.

A desmarcação das Entidades para efeitos de monitorização reforçada, aplicando critérios de risco, pode ocorrer quando ocorram as seguintes circunstâncias:

- Após o período de monitorização, caso seja determinado o "**Encerramento da Monitorização**"; ou

- Caso o Cliente seja reclassificado como Risco Médio ou Baixo, no âmbito da reavaliação de risco, e já exista um conhecimento da operativa do cliente.

6.5. Investigação das Operações pela Direcção de *Compliance*

A Direcção de *Compliance* deve analisar as operações que geraram alerta e, caso existam motivos de suspeição, deverá abrir um "Caso" e realizar diligências adicionais de investigação.

A investigação deve considerar como elenco exemplificativo de operações potencialmente suspeitas (**Anexo II-A**), tendo em consideração as características específicas do cliente e da sua actividade transaccional, nomeadamente:

- Natureza da entidade (Particulares/ENIs; Empresas e Institucionais);
- Caracterização de risco dos intervenientes no contrato;
- Perfil transaccional da Entidade / padrão comportamental.

O processo de investigação compreende igualmente:

- Pesquisa em fontes públicas abertas e fechadas, permitindo avaliar a credibilidade e actualidade da informação existente, a idoneidade das entidades envolvidas, os dados financeiros e económicos da entidade ou do sector em que se insere, bem como identificar possíveis relações de grupo entre as contrapartes;

- Obtenção de documentação de suporte às transacções através das outras unidades de negócio, bem como, esclarecimentos adicionais que permitam sustentar as conclusões da investigação.

Caso o alerta incida sobre contratos alvo de anteriores alertas, com igual tipologia de risco, o processo de análise assenta nos moldes anteriormente referidos, devendo ser dada particular atenção aos seguintes pontos:

- Validação e eventual actualização da informação anteriormente recolhida, nomeadamente no que respeita aos dados pessoais, natureza do contrato e titularidade do mesmo;
- Eventuais alterações significativas ao perfil de movimentação, face à análise anterior.

Após a realização das diligências de investigação, a Direcção de *Compliance* emite um "Parecer/**Relatório de Incidência**" que é submetido à Comissão Executiva (após revisão pelo Responsável da Direcção de *Compliance*), nas seguintes situações:

i. Sempre que o resultado da investigação seja "**Caso encerrado com confirmação de suspeita** "e seja proposta uma das seguintes medidas:
   a. Reporte do cliente às Autoridades competentes; e/ou
   b. Encerramento da conta.
ii. Quando o caso envolva entidades de risco alto e/ou PPEs;
iii. Quando as operações que determinaram a investigação envolvam Entidades referenciadas pelas Autoridades competentes.

O "Parecer/**Relatório de Incidência**" deve conter, no mínimo, a seguinte informação:

- **Origem da análise/incidência**:
  - Identificação pela Direcção de *Compliance* – análise de alertas;
  - Identificação pelas Direcções Comerciais ou outras Unidades de Negócio;
  - Identificação pela Direcção de Operações;
  - Monitorização de Entidades (risco elevado /PPEs); ou
  - Monitorização de Entidades referenciadas pelas Autoridades competentes;
- **Nível de Risco da Entidade** (*Scoring* KYC);

- **Detalhe do comportamento/operação suspeita e motivos de suspeição** (identificação e justificação de factos relevantes associados à movimentação da conta e contrapartes identificadas);
- **Informação adicional recolhida e documentação de evidências** (informação sobre pesquisas efectuadas e esclarecimentos obtidos que permitam sustentar as conclusões da investigação);
- **Conclusão da análise/incidência**:
  - Caso encerrado sem suspeita;
  - Caso encerrado sem suspeita com monitorização; ou
  - Caso encerrado com confirmação de suspeita;
- **Se aplicável, proposta de medidas a aplicar**:
  - Reporte do cliente às Autoridades competentes;
  - Prolongamento do período de monitorização/sujeição a monitorização por período determinado; e/ou
  - Encerramento da conta.

CAPÍTULO VII – CONTROLO DE INTERVENIENTES SUJEITOS A CONTRAMEDIDAS FINANCEIRAS

7.1. Filtragem de Entidades e de Transacções

O BIR deve 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 em Listas de Sanções, de modo a determinar se a sua identidade corresponde a uma pessoa, grupo ou entidade designada.

7.2. Filtragem de Entidades

A filtragem de Entidades é realizada através da *Lexis Nexis Compliance Link/Eagle AML*. De acordo com estas soluções informáticas caso exista correspondência, ou semelhança entre a identidade da Entidade e uma pessoa ou entidade sancionada, a Direcção de *Compliance* deve realizar medidas de diligência adicionais, de forma a determinar se a correspondência se confirma ou se é um Falso Positivo.

7.3. Filtragem e Bloqueio de transacções

No processo de emissão e recebimento de operações SWIFT, assim como de operações transfronteiriças não processadas automaticamente através do sistema SWIFT (ex: remessas documentárias), deve ser realizada a filtragem das operações contra as Listas de Sanções (ONU, OFAC e EU), através da ferramenta de filtragem e antes da execução da operação.

Devem ser filtrados todos os dados das operações, nomeadamente:

(i) Dados de todos os intervenientes – ordenante (s) e beneficiário (s); e

(ii) Países, jurisdições, regiões ou territórios de origem ou de destino das transacções.

Caso seja detectado um *hit* entre a identificação dos intervenientes e a identidade de uma pessoa ou entidade designada a transacção deve ficar pendente até que se conclua a análise do *hit* (para confirmação da correspondência).

Filtragem	Análise	Intervenientes
Falso Positivo Directo: o *hit* decorre de informação que não está directamente relacionada com o teor da operação, nem com os seus intervenientes, tratando-se de uma ´falsa´ coincidência	• Não é necessário realizar diligências adicionais • A operação deverá ser assim justificada e devidamente autorizada na filtragem.	• Direcção de Compliance

Filtragem	Análise	Intervenientes
(ex. Angola -Portugal vs. Angola - Argélia)		
Falso Positivo Potencial: o *hit* é gerado pelo facto de algum elemento da operação coincidir efectivamente com um elemento constante nas Listas de Sanções, a operação deverá ser analisada em detalhe.	• É necessário realizar diligências adicionais ("**Procedimentos de análise do resultado da Filtragem "*matching*"**) • Necessidade de obter um conhecimento detalhado da operação, podendo ser necessário solicitar informação adicional à Rede Comercial, incluindo os documentos de suporte à transacção.	• Direcção de Compliance • Balcão • DOP

➢ Confirmação do "*hit*":

Confirmando-se a correspondência, ou seja, caso a Direcção de *Compliance* conclua que se trata de uma pessoa ou entidade designada numa Lista de Sanções, a transacção deve ser bloqueada. Seguidamente, a Direcção de *Compliance* deve proceder à respectiva comunicação à UIF através da submissão de uma "DIPD"- Declaração de Pessoas e Entidades Designadas.

Caso estejamos perante uma transacção de ou para um país, jurisdição, região ou território sujeito a contramedidas financeiras (sanções financeiras/embargos), de acordo com listagem oficial partilhada por entidade competente, a transacção deve igualmente ser bloqueada.

- **Falso Positivo:**

Caso a Direcção de *Compliance* conclua que se trata de um Falso Positivo, deve autorizar a execução da transacção por parte da Direcção de Operações (DOP).
A conclusão da análise deverá ser devidamente registada e fundamentada pela DCOMP, incluindo a justificação para a realização da operação ou o motivo da recusa (registo efectuado em base de dados mantida pela DCOMP e na ferramenta de filtragem).

7.4. Congelamento de Fundos e Recursos Económicos

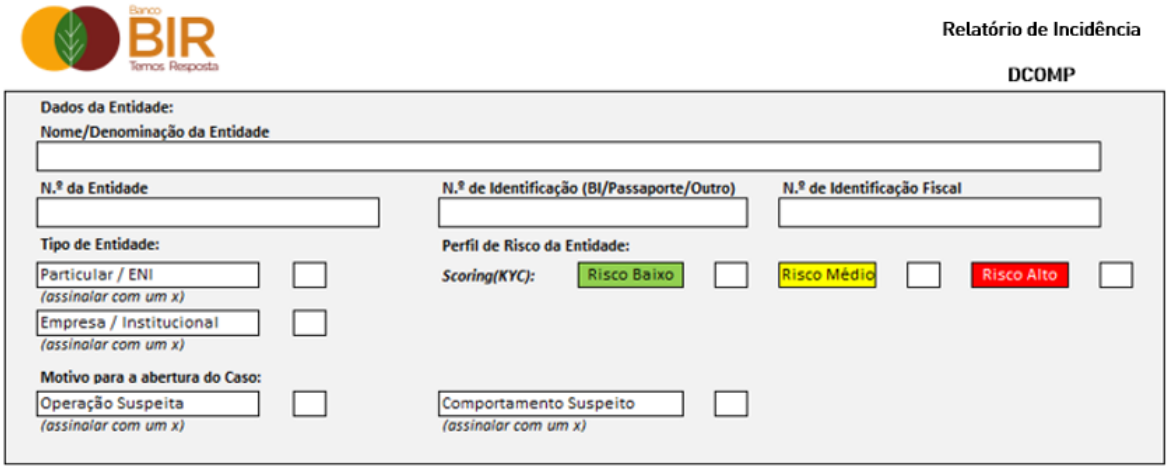
O BIR encontra-se proibido de colocar à disposição fundos ou recursos económicos ou outros serviços conexos, directa ou indirectamente, de pessoas, grupos e entidades designadas pelo Comité de Sanções das Nações Unidas, conforme a Resolução do Conselho de Segurança das Nações Unidas n.º 1267, e pela Autoridade competente a nível nacional. Encontra-se também obrigado a proceder ao congelamento, de forma imediata e sem qualquer aviso prévio, de todos os fundos ou recursos económicos pertencentes, possuídos ou detidos, directa ou indirectamente, individualmente ou em conjunto, por essas pessoas, grupos e entidades e comunicar a UIF e ao BNA.

Em conformidade com o previsto na lei, sempre que o BIR tenha conhecimento, suspeite ou tenha razões suficientes para suspeitar, que a identidade do ordenante, do beneficiário ou de qualquer outra pessoa/entidade envolvida numa transacção corresponde à identidade de uma pessoa, grupo ou entidade designada, deve abster-se de executar a operação. A Direcção de *Compliance* deve efectuar a comunicação à Unidade de Informação Financeira e aguardar a emissão da Instrução por esta Entidade, dos termos do congelamento.

Até à recepção da Instrução, os fundos ou recursos económicos congelados ficam detidos ou sob o controlo do Banco

CAPÍTULO VIII – ANEXOS

ANEXO I – *Template* de "Relatório de Incidência"



Relatório de Incidência

DCOMP

Dados da Entidade:

Nome/Denominação da Entidade

N.º da Entidade

N.º de Identificação (BI/Passaporte/Outro)

N.º de Identificação Fiscal

Tipo de Entidade:

Particular / ENI (assinalar com um x)

Empresa / Institucional (assinalar com um x)

Perfil de Risco da Entidade:

Scoring(KYC): Risco Baixo | Risco Médio | Risco Alto

Motivo para a abertura do Caso:

Operação Suspeita (assinalar com um x)

Comportamento Suspeito (assinalar com um x)

ANEXO II -Tipologia de Operações Suspeitas

A presente secção tem por objectivo orientar os colaboradores do BIR na identificação e detecção de operações com risco potencial de associação a actividades de branqueamento de capitais e financiamento do terrorismo.

Trata-se de uma lista que enumera possíveis casos de operações ligadas com o branqueamento de capitais.

A. Tipologia de operações ou actividades suspeitas identificadas pela Unidade de Informação Financeira para os Bancos e instituições financeiras não bancárias ligadas à moeda e crédito [6]

Neste sector, podemos encontrar alguns indicadores de operações susceptíveis de estarem relacionadas com o BC/FT/P:

- Um potencial cliente ter um montante elevado em numerário na sua posse e abre várias contas ou adquire vários produtos com variações nos nomes das contas;

[6] *Website* da Unidade de Informação Financeira de Angola – "Orientações Gerais da UIF"

- Um potencial cliente ter na sua posse várias moedas diferentes e desejar efectuar operações cambiais como parte da transacção;
- O cliente estruturar uma operação de forma a fraccionar o valor total em várias operações de montante mais reduzido, de modo a evitar que os limites estabelecidos sejam ultrapassados (*smurfing*);
- Um cliente estrangeiro utilizar serviços de remessas alternativos (ARS) para transferir montantes significativos de dinheiro, sob a falsa finalidade de transferir dinheiro para a família no país estrangeiro;
- O cliente adquirir vários produtos financeiros similares e movimentar fundos entre os mesmos, efectuando como suplemento pagamentos em numerário;
- O alto valor patrimonial de um cliente não ser compatível com as informações a seu respeito nem com o respectivo negócio;
- Um cliente utilizar repetidamente um endereço, mas alterar frequentemente os nomes envolvidos;
- O número de telefone profissional ou da residência do cliente ser desconectado ou ser detectado que os mesmos são inexistentes aquando da tentativa de efectuar o primeiro contacto num curto espaço de tempo após a abertura da conta;
- O cliente estar envolvido numa actividade pouco usual para o tipo de pessoa ou o tipo de negócio.

B. Catálogo exemplificativo de operações de risco para entidades de crédito

(i) Alterações não usuais e/ou frequentes no tipo ou natureza dos meios de pagamento, sem reflexo na conta do cliente:

- Troca de moeda estrangeira por notas de valor facial elevado realizado por uma mesma pessoa ou por várias de forma aparentemente concertada, de uma só vez ou de forma fraccionada em operações de baixo montante espaçadas no tempo;
- Aquisição de meios de pagamento ao portador (cheques bancários, dinheiro electrónico, *traveller* cheques) contra a entrega de numerário de forma sistemática ou por montante importante.

(ii) Operações atípicas em numerário

- Aumento significativo de depósitos em numerário, realizados por qualquer pessoa ou sociedade sem causa aparente, especialmente, se os depósitos forem mais tarde transferidos, dentro de um curto espaço de tempo, para um destino que não esteja normalmente relacionado com a actividade ou negócio do cliente;
- Clientes que transferem grandes quantidades de capitais para o estrangeiro, seguido de instruções para pagar em numerário;
- Depósitos de grandes quantidades de numerário, realizados em condições destinadas a evitar o contacto directo com o pessoal do Banco;
- Grande número de pessoas singulares que efectuam depósitos na mesma conta sem explicação adequada;
- Depósitos em numerário, como forma principal de alimentar a conta, que regista pagamentos de bens valiosos ou sumptuosos (imóveis, barcos de recreio, veículos de luxo, jóias);
- Depósitos em numerário em notas de valor facial elevado, sendo normal, no tipo de negócio de que se trata, utilizar notas de valor facial mais baixo;
- Depósitos de numerário, de montante relevante, efectuados directamente no cartão de crédito, sem passar pela conta de depósito à ordem e que gera um saldo positivo a favor do dito cartão.

(i) Actividade não habitual em contas bancárias:

- Qualquer pessoa ou sociedade cujas contas não mostrem actividades bancárias normais ou de negócios, mas que as utilizam para receber ou debitar somas importantes que não tenham uma finalidade ou relação clara com o titular da conta e/ou seu negócio (p. ex.: um aumento substancial no volume de movimentação numa conta);
- Clientes que têm contas em várias instituições financeiras, na mesma localização geográfica, e especialmente quando o Banco sabe que existe um processo de consolidação regular de tais contas previamente ao pedido de uma transferência dos fundos;
- Equilíbrio entre os pagamentos e os depósitos realizados no mesmo dia ou no dia anterior;

- Contas de sociedades que efectuam pagamentos através de transferências a um número limitado de supostos fornecedores, com fundos previamente recebidos em numerário ou através de transferências de supostos clientes que apresentam coincidência, ou quase, nos montantes dos movimentos com os supostos fornecedores;
- Levantamento de elevados montantes de uma conta previamente adormecida/inactiva ou de uma conta que acaba de receber do estrangeiro um elevado montante não esperado;
- Aumentos significativos de depósitos em numerário ou de depósitos em instrumentos negociáveis por um escritório de profissional liberal ou empresa, usando as contas abertas em nome de um terceiro, especialmente se os depósitos forem transferidos rapidamente entre outra empresa cliente e a conta fiduciária;
- Contas que registam repetidos créditos por pagamento de lotarias e prémios de jogos de azar;
- Créditos por devoluções de impostos e/ou subvenções que se produzem de forma repetitiva e em quantia significativa, associadas, em particular, com comércio em Angola, relativamente a clientes que não tenham uma actividade empresarial ou comercial real que as justifique;
- Emissão sistemática de cheques ao portador por quantidades iguais ou inferiores ao valor de AOA = 300.000 ou o equivalente em moeda estrangeira;
- Clientes, pessoas colectivas que efectuam mais operações utilizando numerário que através de outros meios de pagamento e de cobrança habituais para esse tipo de actividade comercial;
- Transferências de fundos entre as contas de diversas sociedades abertas, com pessoas singulares (administradores, autorizados, procuradores) coincidentes e/ou com domicílios comuns (sede ou morada de correspondência);
- Abertura de contas em nome de novas sociedades por parte das mesmas pessoas singulares (administradores, autorizados, procuradores) com direcções ou domicílios comuns a outras sociedades com contas na entidade que aparentemente terão cessado as suas actividades (sociedade efémeras);

- Recepção de transferências electrónicas procedentes do estrangeiro em que não figure a identidade do ordenante ou o número de conta origem da transferência;
- Realização na mesma data de múltiplas operações de depósito através de numerário ou outros instrumentos monetários e por quantidades que são por sistema ligeiramente inferiores ao limite que se exigiria a sua identificação ou justificação obrigatória, especialmente se a numeração dos ditos documentos é sequencial;
- Créditos de cheques por montantes elevados, a favor de terceiros e endossados ao nosso Cliente;
- Contas em nome de menores de idade ou incapazes, cujos representantes realizam grande número de operações ou movimentos nas ditas contas.

(ii) Utilização não habitual de estruturas societárias fictícias, de empresas já existentes ou de associações ou fundações com escassa actividade real:

- Operações através de contas de sociedades nacionais participadas por sociedades constituídas em paraísos fiscais ou países de risco e representadas por profissionais independentes ou outros intermediários, que recebem transferências procedentes do exterior por montantes elevados;
- Operações realizadas por sociedades nacionais com actividade económica real que em certo momento recebem transferências desde paraísos fiscais ou países de risco com a finalidade de aumentar o capital, efectuar suprimentos ou operações similares, sem que se verifiquem mudanças na administração da sociedade ou em seus representantes;
- Operações de sociedades de recente constituição e capital social reduzido que, desde a sua abertura, recebem ou emitem transferências para o exterior por montantes elevados, para pagamento ou recebimento de material informático, telemóveis, ou similares e recebem ou emitem transferências nacionais com origem ou destino num número diminuto de sociedades do mesmo sector, mantendo uma operativa importante durante um período curto de tempo,

cessando logo a mesma ou sendo substituídas por outras sociedades que ocupam a sua posição;

- Operações realizadas por sociedades dedicadas à importação de veículos cujos fundos procedem na sua maior parte de depósitos em numerário ou de transferências ordenadas desde um número de sociedades relacionadas;
- Contas abertas em Portugal que recebem pequenas transferências ordenadas por particulares, geralmente desde o estrangeiro, em pequenos montantes individuais, mas somando uma quantidade global importante, sem que se identifique na operativa da conta movimentos apropriados a uma actividade empresarial (custos com o pessoal, pagamento de matérias-primas, fornecimentos de terceiros, etc.). Geralmente, dos fundos recebidos efectuam- se levantamentos em numerário e/ou transferências para paraísos fiscais ou de países de risco. Esta operativa é especialmente relevante no sector de empresas de serviços de investimento, quando actuam sem a correspondente autorização e/ou não aparecem nas suas contas evidência da realização dos investimentos e em como se aplicaram os fundos recebidos;
- Depósitos em contas de associações ou fundações, a título de doação, peditório ou actividade similar em quantia relevante num dado momento, sem que se conheça a existência de catástrofe ou campanha publicitária que justifique as cobranças, remetendo posteriormente a maior parte dos fundos para países em que não exista conhecimento de que desenvolvem actividades de forma habitual;
- Movimentos em contas de pessoas colectivas (sociedades, fundações, associações, etc.) desde que se operem, em geral, os pagamentos e que carecem de encargos de segurança social, salários, impostos, água, fornecimento eléctrico, entre outros, apresentando, apesar de tudo, um volume de movimento de fundos relevante, sem que se identifique relação com o uso declarado da conta.

(iii) Movimentos de fundos internacionais atípicos, não usuais ou sem justificação económica, em quantias relevantes:

- Clientes que alimentam as suas contas através de depósitos de numerário e retiram os fundos através levantamentos no ATM, especialmente no estrangeiro, em países considerados exportadores de substâncias de substâncias estupefacientes. Podem coincidir no tempo os depósitos com os levantamentos. É frequente contratar diversos cartões associados à mesma conta. Os levantamentos atingem geralmente o limite diário permitido para este tipo de operações;
- Utilização de cartas de crédito e outros métodos de financiamento comercial, para movimentar capitais entre países nos quais o dito comércio não é lógico em relação ao negócio normal do cliente ou introduzindo mudanças no nome, direcção ou lugar de pagamento da carta de crédito, no momento imediatamente anterior ao pagamento da mesma;
- Utilização de facturas e justificativos de importações, seguros, ou justificativos de transporte de mercadorias evidentemente falsos, como suporte a transferências remetidas do exterior;
- Utilização sistemática de sobrefacturação ou subfacturação em operações de comércio internacional, reflectindo um preço muito superior ou inferior ao do mercado, habitualmente conhecidos, conforme a experiência da entidade em operações similares anteriores;
- Cliente que actua como cobrador de fundos de outras pessoas da mesma nacionalidade, em pequenas quantias, agrupando-as e enviando-as para o exterior, actuando como transmissor informal de fundos;
- Movimentos de fundos realizados por fundações ou associações constituídas em Angola e constituídas principalmente por cidadãos estrangeiros;
- Contas de particulares (geralmente estrangeiros) ou de sociedades (habitualmente sociedades de responsabilidade limitada de recente constituição e com capital social mínimo), que registam desde a sua abertura fortes depósitos em numerário e imediatas transferências para o exterior, mantendo saldos baixos

em relação com o volume de fundos que transitam pela conta, suportando as operações em actividades económicas de difícil comprovação;

- Contas sob a titularidade de pessoas singulares (habitualmente não residentes), que dizem ser comerciantes ou simples intermediários em operações de comércio exterior, nas quais se registam directamente depósitos em numerário elevados ou depósitos em numerário de montante mais pequeno mas desde diferentes pontos do país, ordenando imediatamente transferências para o exterior por montantes elevados, resultando ser os beneficiários empresas distribuidoras (normalmente de países asiáticos) de produtos muito variados e com actividade económica diversificada.

(iv) Empréstimos, linhas de crédito ou operações de cativo, com ou sem garantia:

- Clientes que cancelam inesperadamente empréstimos problemáticos ou que de uma forma reiterada amortizam antecipadamente empréstimos de quantia relevante, principalmente com entregas de numerário;
- Empréstimos garantidos por terceiras pessoas que não aparentam ter qualquer relação com o cliente e que resultam na sua não liquidação e, no final, um dos avalistas é quem paga;
- Pedido de empréstimo apoiado por activos depositados na entidade financeira ou com terceiros, cuja origem é desconhecida ou cujo valor não tem relação com a situação do cliente;
- Pedido de empréstimos garantidos por activos depositados em paraísos fiscais ou países de risco;
- Pedido de empréstimo, linha de crédito e operação de activo por parte de um cliente cuja capacidade de reembolso formalmente declarada (declarações de impostos) é ostensivamente inferior à sua capacidade de reembolso real e a diferença é quantitativamente relevante;
- Empresas ou particulares residentes que se financiam com empréstimos ou entradas de capital do exterior, sendo que quem empresta é uma pessoa singular ou entidade não financeira;

(v) Pessoas Politicamente Expostas de países, jurisdições, regiões ou territórios de Risco:

- Contas abertas em Angola por pessoas que ocupam cargos políticos proeminentes, altos cargos ou similares, (directores de empresas públicas, etc.) em países geralmente não democráticos, incluindo os familiares próximos e que recebem fundos do exterior que aplicam na compra de activos imobiliários ou financeiros de quantia relevante ou a constituição de depósitos elevados;
- Operações em numerário ou instrumentos monetários logo abaixo dos montantes sobre os quais existe a obrigação de informar as autoridades;
- Operações de elevados montantes, que não estão de acordo com o tipo de conta ou com os depósitos do titular e as fontes de riqueza;
- Operações efectuadas através de circuitos ilógicos, sem motivo aparente, excepto o de ocultar a identidade do proprietário dos fundos;
- Pedido de uma operação indicando que deve ser movimentada por terceiras pessoas;
- Operações canalizadas através de jurisdições com sigilo bancário ou através de entidades sedeadas em países com escassa regulamentação em matéria de identificação de Clientes;
- Operações que envolvem fundos que tem a sua origem em contas de um banco central ou banco propriedade de governo;
- Transferências efectuadas de ou para outras contas de pessoas públicas relevantes;
- Entrada de fundos por qualquer via que são imediatamente transferidos por montante similar para outra instituição num terceiro país;
- Recusa em dar informação sobre o motivo ou sentido económico das transferências emitidas ou recebidas;
- Perguntas sobre a forma de evitar as exigências de reporte de operações às autoridades ou do alcance das leis de sigilo bancário, ou outras normas sobre comunicação de operações suspeitas;
- Oferta de garantias outorgadas por instituições *offshore* ou sedeadas numa jurisdição com sigilo bancário impenetrável.

(vi) Falta de dados, falta de contacto deliberado com o BIR ou despreocupação pela rentabilidade ou vantagens dos produtos:

- Clientes que não agem em seu próprio nome e que não querem revelar a verdadeira identidade do beneficiário;
- Resistência em facultar a informação normal ao abrir uma conta, fornecendo informação mínima ou falsa ou presta informação que é difícil de verificar pelo BIR;
- Clientes que têm um grau aceitável de "cultura financeira", mas que declinam facilitar informação que em circunstâncias normais lhes permitiria aceder a um crédito ou a outros serviços bancários que seriam vantajosos;
- Representantes de empresas que evitam injustificadamente o contacto com o BIR;
- Utilização insuficiente das vantagens bancárias normais, como por exemplo, não aproveitar taxas de juro para saldos credores elevados;
- Dificuldades reiteradas para a entidade em contactar com o cliente no domicílio ou no telefone indicado pelo Cliente, produzindo-se devoluções de correio por desconhecimento do cliente nessa morada;
- Clientes apresentados à entidade por pessoas conhecidas e reputadas (escritórios de profissionais liberais, empresários, etc.), e que se verifica que esta apresentação pretende facilitar os deveres de conhecimento dos dados do Cliente;
- Clientes sobre os quais aparecem notícias em meios de comunicação que os relacionam com actividade delituosas susceptíveis de gerar benefícios económicos;
- Clientes com um interesse maior do que o normal em estabelecer relações directas e pessoais com o responsável do Balcão e com os seus empregados, com a finalidade de aliviar os deveres ou controlos da entidade;
- Clientes que mostrem curiosidade acerca dos sistemas, controlos e políticas internas da entidade em matéria de prevenção de branqueamento de capitais e financiamento do terrorismo.

(vii) Contas de correspondente com entidades estrangeiras insuficientemente conhecidas e/ou localizadas em paraísos fiscais:

- Pedido de subscrição de relações de correspondente com entidades financeiras estrangeiras constituídas em zonas de risco a respeito das quais não existe aplicação de políticas de prevenção de branqueamento de capitais;
- Contas abertas em Angola por uma entidade financeira, que figura como titular da conta, estruturada em várias subcontas para reflectir especificamente as operações realizadas por clientes da entidade financeira formalmente titular da conta;
- Contas abertas em Angola por entidades financeiras estrangeiras que mantenham abertas contas de correspondente com bancos de fachada;
- Atitudes não usuais de empregados e representantes das instituições financeiras;
- Mudanças nas características do colaborador, por exemplo, forma de vida sumptuosa sem ter relação com a sua situação expectável ou o nível de rendimentos;
- Mudança nos resultados do colaborador ou representante, por exemplo, o comercial que vende produtos contra numerário e que tem um aumento notável ou inesperado dos seus resultados;
- Qualquer contacto com um representante no qual a identidade do último beneficiário ou pessoa que corresponde permanece oculta, contrariamente ao procedimento normal para o tipo de negócio;
- Empregados cuja função implique a relação com clientes e que resistam a aceitar mudança de funções que levem não continuar a executar as mesmas actividades.

ANEXO III - Lista sobre o conjunto de categorias de crimes subjacentes ao crime de branqueamento de capitais (elencados no glossário das 40 Recomendações do GAFI complementada pela Lei n.º 38/20 de 11 de Novembro, Lei que aprova o Código Penal Angolano) e a Lei n.º 12/24, que Altera a Lei n.º 38/20, de 11 de Novembro, Lei que Aprova o Código Penal Angolano.

- Participação num grupo criminoso organizado e em acções ilegítimas para obtenção de fundos, nomeadamente através de chantagem, intimidação ou outros meios;
- Terrorismo, incluindo a proliferação de armas de destruição em massa;
- 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.

CAPÍTULO VIII PERIODICIDADE DE ACTUALIZAÇÃO

O referido manual deve ser actualizado, numa periodicidade mínima anual, todavia, poderá ser revisto, sempre que existir esta necessidade, desde que devidamente fundamenta e /ou evidenciada.