# Política de Prevenção e Gestão de Risco de Branqueamento de Capitais e Financiamento ao Terrorismo e Proliferação de Armas de Destruição em Massa

**Outubro 2024**

**V.5**

# Histórico do Documento

## Versões

| Versão | Data de Revisão | Sumário de Mudanças | Direcção |
|---|---|---|---|
| V.1 | 09.05.2014 | Versão inicial | DCOMPL |
| V.2 | 15.12.2016 | Adequação às melhores Práticas | DCOMPL |
| V.3 | 26.11.2020 | Alteração Regulamentar e Adequação às melhores práticas da *Corporate Governance* | DCOMPL |
| V.4 | 10.05.2022 | Alteração Regulamentar e Adequação às melhores práticas da *Corporate Governance* | DCOMPL |
| V.5 | 09.10.2024 | - Alteração da nomenclatura da Direcção.<br>- Ajuste da Política ao *template* actual;<br>- Revisão textual da Política e formatação;<br>- Alteração Regulamentar, devido a publicação de novas normas. | DCP |

## Validação – Grupo de Trabalho de Validação de Políticas

| Versão | Data de Validação |
|---|---|
| 5.0 | 09-10-2024 |

## Aprovação – Comissão Executiva

| Versão | Data de Aprovação |
|---|---|
| 5.0 | *Indicar "N/A" se aplicável* |

## Aprovação – Conselho de Administração

| Versão | Data de Aprovação |
|---|---|
| 5.0 | XX-YY-2024 |

## Distribuição

| Área |
|---|
| Conselho de Administração |
| Comissão Executiva |
| Assessoria à Comissão Executiva |
| Todas as Direcções do Banco Económico |

## Compromisso do Banco Económico

O Conselho de Administração do Banco Económico, ciente das suas responsabilidades perante os seus clientes, accionistas, parceiros e colaboradores, aprova e compromete-se a executar a presente Política.

| | |
|---|---|
| **Pedro Filipe Pedrosa Pombo Cruchinho**<br>Presidente do Conselho de Administração | |
| **Jorge Manuel Torres Pereira Ramos**<br>Presidente da Comissão Executiva | |
| **Katila Perera Santos Rigal**<br>Administradora Executiva | |
| **Elisa de Jesus Francês Baptista**<br>Administradora Executiva | |
| **Victor Hariany Neves Faria**<br>Administrador Executivo | |
| **Emanuel Maria Maravilhoso Buchartts**<br>Administrador Não Executivo Independente | |

# Índice

## 1. Enquadramento

O Banco Económico, S.A ("Banco ou designado por BE") assume como princípio fundamental do exercício da sua actividade a prevenção activa do branqueamento de capitais, combate ao financiamento do terrorismo e da proliferação de armas de destruição em massa ("PBC/CFT/PADM"), adoptando nesse domínio as práticas implementadas no mercado angolano, de acordo com a legislação e respectiva regulamentação em vigor em Angola, bem como as práticas internacionalmente reconhecidas.

O Banco adopta uma política de colaboração com as autoridades com competência nos domínios do combate ao Branqueamento de Capitais, Financiamento do Terrorismo e de Proliferação de Armas de Destruição em Massa, doravante abreviado por "BC/FT/PADM".

De forma a cumprir as normas legais e regulamentares a que se encontra sujeito, o Banco adopta normas e procedimentos internos que lhe permitam conhecer os seus Clientes e as actividades que desenvolvem, bem como as que possibilitem o exercício da actividade bancária e financeira de acordo com rigorosas regras deontológicas.

## 2. Âmbito

Esta política aplica-se a todas os Colaboradores do Banco Económico, S.A e poderá estender-se a todas as entidades do Grupo BE que se encontram dentro do perímetro de consolidação do Banco Económico, S.A., na medida da sua aprovação pelos respectivos Órgãos e, quando necessário, de adaptação à legislação e regulamento específico daquela entidade.

As regras e procedimentos contidos nesta Política têm natureza obrigatória e devem a todo o tempo ser integralmente observados pelos colaboradores do Banco e, bem assim, pelos seus colaboradores externos, entidades do Grupo, assessores e terceiros que actuem em nome do Banco.

## 3. Enquadramento Regulamentar

Esta Política foi elaborada para promover a observância das disposições legais e regulamentares vigentes bem como as regras internas adicionalmente estabelecidas pelo Banco no domínio da prevenção e combate ao branqueamento de capitais e do combate ao financiamento ao terrorismo e da Proliferação de Armas de Destruição em Massa ("PCBC/CFT/PADM"), não estando nenhum destinatário deste documento dispensado de consultar as normas jurídicas ou orientações em vigor a que o mesmo se reporta.

**No domínio internacional:**

- 40 recomendações do *GAFI/FATF*, revistas em 2017 (onde estão integradas as 9 recomendações relativas ao combate ao financiamento ao terrorismo).

**No domínio nacional:**

- Aviso n.º 01/22, de 28 de Janeiro sobre o Código do Governo Societário das Instituições Financeiras;
- Lei n.º 38/20 de 11 de Novembro, que Aprova o Código Penal;
- Lei n.º 14/21 de 19 de Maio – Do Regime Geral das Instituições Financeiras;
- Lei n.º 05/2020 de 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;
- Lei n.º 11/24 de 4 de Julho, altera 18 artigos da Lei n.º 05/20 - visa assegurar a conformidade e efetividade do ordenamento jurídico nacional perante riscos e impactos da criminalidade de referência.
- Lei n.º 1/12, de 12 de Janeiro – Lei sobre a Designação e Execução de Actos Jurídicos Internacionais;
- Lei n.º 22/15 de 31 de Agosto – Lei que aprova o Código de Valores Mobiliários;
- Lei n.º 09/20 de 16 de Abril de 2020, que altera o n. º1 do artigo 415º do Código de Valores Mobiliários aprovado pela Lei n.º 22/15 de 31 de Agosto;
- Lei n.º 19/17 de 25 de Agosto - Lei de Prevenção e Combate ao Terrorismo;
- Lei nº 09/24 de 3 de Julho, altera 4 artigos e adita o artigo n.º 50A da Lei nº 19/17 de 25 de Agosto, sobre a Prevenção e Combate ao Terrorismo;

- Aviso n.º 02/24 – Estabelece as regras e os procedimentos para a implementação efectiva das condições de exercício, instrumentos, mecanismos, formalidades e prestação de informação, inerentes à PCBC/FT/PADM;
- Instrutivo n.º 20/20 de 9 de Dezembro, sobre o Relatório de Prevenção ao Branqueamento de Capitais, Financiamento do Terrorismo e da Proliferação - Avaliação do Risco e Ferramentas e Aplicativos Informáticos.
- Directiva n.º 01/DSI/2012, de 10 de Maio, sobre a Comunicação de Operações Suspeitas de Branqueamento de Capitais;
- Directiva n.º 03/DSI/2012 de 24 de Julho, sobre a Identificação e Comunicação de Pessoas, grupos e Entidades Designados;
- Directiva n.º 04/DSI/2012 de 24 de Julho, sobre o Congelamento administrativo de fundos e recursos económicos.
- Carta Circular n.º 2/23 de 01 de Março Sobre a Divulgação de Medidas do Grupo de Acção Financeira (GAFI);
- Carta Circular n.º 2/24 de 20 de Março Sobre a Divulgação de Medidas do Grupo de Acção Financeira (GAFI);
- Outra legislação ou regulamentação em vigor que seja aplicável à actividade do Banco não elencada.

## 4. Objectivo

Esta política visa:

- Proteger o Banco para que não seja usado em actividades de branqueamento de capitais, do financiamento de actividades de terrorismo e de proliferação de armas de destruição em massa;
- Estabelecer o quadro no contexto do qual a conformidade com a legislação relativa ao Branqueamento de Capitais, Financiamento do Terrorismo e da proliferação será administrada;
- Assegurar o estabelecimento de regras procedimentos internos para a sensibilização, detecção, prevenção e comunicação das actividades de Branqueamento de Capitais, de Financiamento do Terrorismo e da Proliferação de Armas de Destruição em Massa.

## 5. Definições

Para efeitos da presente Política, entende-se por:

### Branqueamento de Capitais

O crime de **Branqueamento de Capitais** corresponde ao processo de ocultação da existência, origem ilegal ou a utilização de bens provenientes de actividades criminosas, de modo a fazer com que estes bens pareçam legítimos. Nos termos do artigo 82º da Lei n.º 05/2020, são considerados crimes de branqueamento de capitais, toda a actividade destinada a converter, transferir, auxiliar ou facilitar alguma operação de conversão ou transferência de vantagens, obtidas por si ou por terceiro, directa ou indirectamente, com o fim de dissimular a sua origem ilícita, ou de evitar que o autor ou participante dessas infrações seja criminalmente perseguido ou submetido a uma acção criminal.

### Terrorismo

Entende-se por **Terrorismo**, toda a actuação concertada e que visa prejudicar a integridade e a independência nacional e internacional, impedir, alterar ou subverter o funcionamento das instituições públicas e privadas, forçando-as a praticar actos ou a tolerar que se pratique, ou ainda intimidar certas pessoas, grupos de pessoas ou a população em geral, mediante:

- Crime contra a vida, a integridade física ou a liberdade das pessoas;
- Crime contra a segurança dos transportes e das comunicações, incluindo as informáticas, telegráficas, telefónicas, de rádio ou de televisão;
- Crime de produção dolosa de perigo comum, através de incêndio, explosão, libertação de substâncias radioativas ou de gases tóxicos ou asfixiantes, de inundação ou avalanche, desmoronamento de construção, contaminação de alimentos e águas destinadas a consumo humano ou difusão de doença, praga, planta ou animal nocivo;
- Actos que destruam ou que impossibilitem o funcionamento ou desviem dos seus fins normais, definitiva ou temporariamente, total ou parcialmente, meios ou vias de comunicação, instalações de serviços públicos ou destinadas ao abastecimento e satisfação de necessidades vitais da população;
- Investigação e desenvolvimento de armas biológicas ou químicas;
- Crimes que impliquem o emprego de energia nuclear, armas de fogo, biológicas ou químicas, substâncias ou engenhos explosivos, meios incendiários de qualquer

natureza, encomendas ou cartas armadilhadas, sempre que, pela sua natureza ou pelo contexto em que são cometidos, estes crimes sejam susceptíveis de afectar gravemente o Estado ou a população que se visa intimidar.

### Financiamento ao Terrorismo

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

### Proliferação de Armas de Destruição em Massa

Nos termos do artigo 83º da Lei n.º 05/2020, entende-se por "**Proliferação de Armas de Destruição em Massa**", aquele que por quaisquer meios, directa ou indirectamente, fornecer ou reunir fundos com a intenção de serem utilizados ou tiver conhecimento que podem ser utilizados total ou parcialmente no financiamento da proliferação de armas de destruição em massa.

### Beneficiário Efectivo

No contexto internacional, as recomendações do **GAFI** definem **Beneficiário Efectivo**", como sendo uma ou mais pessoas singulares que, em última instância detém ou controlam o cliente e/ou a pessoa singular em nome do qual a transação está a ser realizada. Em outro sentido, são as pessoas singulares que, efetivamente detém e usufruem do capital ou dos activos, direitos especiais, cargos ou funções relevantes, na pessoa colectiva.

### Beneficiário Efectivo de Fundos Fiduciários (*Trusts*) e outras pessoas coletivas de natureza não societária

Quando o Cliente for um *trust* ou uma outra pessoa colectiva de natureza não societária, consideram-se Beneficiários Efectivos:

a. O fundador (no caso dos *trusts*);
b. O administrador ou administradores fiduciários (*trustees*) de fundos fiduciários, ou os respetivos administradores no caso de outras pessoas colectivas de natureza não societária;
c. O curador, se aplicável;
d. Os beneficiários ou, se os mesmos não tiverem ainda sido determinados, a categoria de pessoas em cujo interesse principal o fundo fiduciário (*trust*), ou a

pessoa coletiva de natureza não societária, foi constituída ou exerce a sua actividade;

e. Qualquer outra pessoa singular que detenha o controlo final do fundo fiduciário (*trust*), ou da pessoa coletiva de natureza não societária, através de participação directa ou indirecta ou através de outros meios.

**Pessoas Politicamente Expostas**

São qualificadas como Pessoas Politicamente Expostas (PPE´s) indivíduos nacionais ou estrangeiros que desempenham ou desempenharam funções públicas proeminentes em Angola, ou em qualquer outro País ou jurisdição ou em qualquer organização Internacional nomeadamente:

- Presidente da República ou Chefe de Estado;
- Vice-Presidente da República;
- Primeiro-ministro ou Chefe de Governo;
- Órgãos Auxiliares do Presidente da República, os membros do Governo, designadamente Ministros de Estado, Ministros, Secretários de Estado e Vice-Ministros e outros cargos ou funções equiparadas;
- Deputados, Membros de Câmara Parlamentares e equiparados;
- Magistrados Judiciais dos Tribunais Superiores e da Relação, cuja decisões não possam ser objecto de recurso, salvo em circunstâncias excepcionais;
- Magistrados do Ministério Público de escalão equiparados aos Magistrados Judiciais referidos no número anterior;
- Provedor de Justiça e Provedor de Justiça-Adjunto, Membros do Conselho da República, Membros do Conselho de Segurança Nacional e demais Conselheiros de Estado;
- Membros da Comissão Nacional Eleitoral;
- Membros do Conselho Superiores da Magistraturas Judicial e do Ministério Público;
- Membros de órgãos de Administração e Fiscalização dos Bancos Centrais e outras autoridades de regulação e supervisão do Sector Financeiro;
- Chefes de missões diplomáticas e de postos consulares;
- Oficiais Generais das Forças Armadas e Oficiais Comissários das Forças de Segurança e Ordem Interna;
- Membros de Órgãos de Administração e de Fiscalização de empresas públicas e de sociedade de capitais exclusiva ou maioritariamente públicos, institutos públicos, associações e fundações públicas, estabelecimentos públicos, qualquer que seja o

modo da sua designação, incluído os Órgãos de Gestão das empresas integrantes dos sectores empresariais locas;

- Membros do Conselho de Administração, Directores, Directores-Adjunto e ou pessoas que exercem funções equivalentes numa organização internacional;
- Membros dos Órgãos Executivos de direção de partidos políticos;
- Membros das administrações locais e do poder autárquico;
- Líderes das confissões religiosas.

São também consideradas pessoas politicamente expostas, os membros da família e as pessoas muito próximas dos indivíduos acima mencionados, nomeadamente:

- O cônjuge ou companheiro de união de facto;
- 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;
- Pessoas com reconhecidas e estreitas relações de natureza pessoal;
- Pessoas com reconhecidas e estreitas relações de natureza societária ou comercial.

### Transacção Ocasional

Qualquer transacção efectuada pelas entidades obrigadas fora do âmbito de uma relação de negócio já estabelecida, caracterizando-se, designadamente, pelo seu caráter pontual.

### Medidas Restritivas, também designadas por Sanções

Refere-se a uma ação legal que limita ou impõe condições em determinadas situações na matéria de BC/FT/PDAM, ou seja, trata-se de um instrumento com carácter não punitivo, que é utilizado por instituições internacionais com a finalidade de exercer influência nas matérias de prevenção e repressão do terrorismo, promoção e defesa dos direitos humanos e da liberdade, dissuasão de eventuais conflitos armados ou a proibição do desenvolvimento de armas de destruição maciça.

### Congelamento

Inibição ou proibição temporária de transferências, conversão, disposição, alienação ou movimentação de quaisquer fundos ou activos detidos ou controlados por pessoas, grupos ou entidades designadas, ou a custódia ou controlo temporário de bens, produtos ou vantagens do crime. O congelamento de ativos não prejudica os direitos adquiridos por terceiros de boa-fé. O congelamento diz-se **imediato** quando se verifica prontamente a decisão da designação, comunicação ou tomada de conhecimento quer interna ou internacional ou da actualização da lista de designações ou de sanções respectivas,

incluída a lista do Comité de Sanções das Nações Unidas, conforme as resoluções aplicáveis do Conselho de Segurança das Nações Unidas, não podendo, no entanto, exceder o período de 24 horas.

**Abordagem Baseada em Risco "ABR"**

Refere-se à análise individual que deve ser feita à cada transação tendo como base os riscos que podem estar envolvidos.

## 6. Princípios Gerais

**Princípio da Universalidade**: todo e qualquer colaborador do Banco deve estar familiarizado com o Código de Conduta do Grupo, assim como das políticas internas que se aplicam à sua função e responsabilidades. O cumprimento deste princípio é transversal a todas as actividades exercidas no Banco, não obstante a sua antiguidade ou função, tem de promover uma cultura de compliance e agir com diligência e espírito de compromisso.

Para cumprimento deste princípio, o *Compliance Officer* do BE e de cada entidade do Grupo (EG) devem assegurar um adequado conhecimento dos regulamentos do Banco e políticas internas em todas as áreas do Grupo.

**Princípio de liderança:** O sentido de cumprimento das regras começa no topo, com poderes claros dado ao *Compliance Officer* pelos órgãos de gestão e uma estratégia de negócio e comunicação alinhadas com os princípios nucleares e valores-base de *compliance*.

O Grupo e todas as EG devem adoptar práticas e incentivos que reforcem e valorizem uma cultura de *compliance* forte em todas as atividades do Grupo.

**Princípio de legalidade, probidade e integridade:** De acordo com o Código de Conduta do Banco, a legalidade, probidade e integridade representam as fundações de uma forte cultura de *compliance*. Por essa razão, o Banco adoptou uma política de tolerância zero no tocante a quaisquer desvios a estes princípios. Os regulamentos existentes e as políticas internas (aplicáveis a cada empresa do Grupo) devem ser estritamente observados e cumpridos.

**Princípio de cooperação:** A cooperação e boa-fé são valores cruciais a serem promovidos por todas as Entidades e colaboradores do Grupo BE, em colaboração com o

*Compliance Officer* de cada empresa do Grupo na prossecução da sua função e responsabilidades. Isto implica o fornecimento de informação atempada, precisa e detalhada a pedidos efectuados seja pelos *Compliance Officer* da empresa do Grupo, ou pelo *Compliance Officer* do BE. Um compromisso pró-activo e a colaboração de todos os colaboradores com as equipas de *compliance* deve ser encorajada em cada empresa do Grupo.

Todas as empresas do Grupo, através dos seus *Compliance Officers*, terão de cooperar, no cumprimento de todas as disposições legais e regulatórias, com o *Compliance Officer* do BE, fornecendo informação sempre que solicitada, contribuindo para a obtenção de uma visão atempada e detalhada dos eventos do Grupo BE, riscos e medidas de mitigação e eficiência do sistema de controlo interno.

Este princípio, estende-se às demais instituições financeiras para efeito de BC/FT, quando a informação respeitante ao cliente ou a uma operação, seja comum entre elas e esteja sujeita a obrigações equivalentes, no que refere ao segredo profissional e a proteção de dados ou quando a troca de informação tem a finalidade de opor-se à concretização ou conclusão de uma fraude contra o sistema financeiro.

**Princípio da segregação de funções:** A estrutura organizacional e os processos criados para suportar o controlo e a gestão de riscos do *Compliance,* devem numa base permanente, assegurar a completa segregação de deveres entre a origem, a gestão e o controle dos riscos de *compliance*.

**Princípio das três linhas de defesa:** O Grupo BE adopta o princípio das três linhas de defesa como um elemento-chave da gestão do risco, para assegurar uma clara responsabilização pela tomada de risco no âmbito do negócio, uma vigilância e reporte eficiente do risco e uma garantia independente dada à Comissão Executiva bem como ao Conselho de Administração, respeitante aos níveis de risco intrínsecos, o respectivo enquadramento no apetite ao risco e estatuto do Sistema de Controlo Interno.

# 7. Avaliação do Risco de BC/FT/PADM

## 7.1. Políticas e Procedimentos

### 7.1.1 Obrigações Gerais

#### Obrigação de Identificação e Diligência

É dever do Banco, identificar os seus clientes, representantes e beneficiários efectivos, tratando-se de pessoas singulares ou colectivas, quer sejam titulares ou representantes,

antes do início da relação de negócio bem como aos clientes já existentes, sendo que esta verificação deve ser efectuada, através de documentos comprovativos originais de acordo com a legislação em vigor.

Sempre que esta identificação tenha lugar em momento posterior ao do início da relação de negócio, deve ser realizada dentro do prazo de 15 dias definidos na lei, a contar do início da relação de negócio. No caso dos clientes já existentes, esta obrigação ocorrerá conforme a relevância da operação e do risco de BC/FT.

É igualmente dever do Banco, proceder à identificação das partes aquando da realização de uma ou várias transações ocasionais, cujo montante seja superior em moeda nacional ou outra, ao equivalente a USD 15.000,00, conforme definido na legislação em vigor.

### Obrigação de Recusa

No início ou no decorrer da relação de negócio, o Banco deve recusar realizar transações ocasionais ou outras operações quando:

- Não obtenha os elementos identificados e os respectivos meios comprovativos relativos ao Cliente, seu representante e/ou Beneficiário Efectivo;
- Não obtenha a informação necessária para a aferição da qualidade de Beneficiário Efetivo e da estrutura de propriedade e de controlo do cliente;
- Não obtenha informação sobre a natureza, o objecto e a finalidade da relação de negócio;
- Não consiga verificar o cumprimento dos procedimentos necessários ao dever de atualização dos dados.

O Banco deve fazer constar de documento ou de registo escrito as possíveis razões para a impossibilidade do cumprimento dos procedimentos devidos, assim como a fundamentação do termo da relação de negócio já estabelecida.

Na eventualidade do cliente entregar os elementos em falta que estiveram na base da decisão do termo da relação de negócio, não sendo observada qualquer suspeita aos mesmos, poderá ser restabelecida a relação, sendo acompanhada de todos os procedimentos de identificação e diligência legalmente devidos.

### Obrigação de Conservação de Documentos

Os documentos comprovativos de identificação, bem como quaisquer outros documentos de registo das operações que permitam a sua reconstituição, devem ser conservados, nos

termos da Lei n.º 05/2020, por um período de 10 anos a contar da sua execução, ainda que a relação de negócio já tenha terminado.,

O Banco deverá manter cópias de todas as comunicações efetuadas ao abrigo do dever de comunicação e conservação de documentos.

Sem prejuízo do disposto nos números anteriores, o Banco deverá, em todo o caso, adoptar todas as medidas necessárias com vista a responder, de forma completa, aos pedidos de informação das autoridades destinados a determinar se mantêm, ou mantiveram, nos últimos 10 anos, relações de negócio com uma dada pessoa singular, colectiva ou análoga, e qual a natureza dessas relações.

### Obrigação de Comunicação

O Banco deverá informar de imediato a Direcção Nacional de Investigação e Acção Penal ("DNIAP") da Procuradoria-Geral da República ("PGR") e a Unidade de Informação Financeira ("UIF") sempre que saiba, suspeite ou tenha razões suficientes para suspeitar que certos fundos ou outros bens, independentemente do montante envolvido, provêm de actividades criminosas ou estão relacionados com o financiamento do terrorismo.

O Banco deverá comunicar ainda, numa base sistemática, a DNIAP da PGR e à UIF, ou quaisquer tipologias de operações que venham a ser definidas por regulamentação especifica.

A forma, o prazo, o conteúdo e os demais termos das comunicações sistemáticas efectuadas pelo Banco deverão obedecer aos moldes previstos na legislação em vigor.

As decisões de não exercer o dever de comunicação, serão revistas de forma crítica e mensalmente pelo administrador do pelouro, devendo ser apresentado ao Conselho de Administração os resultados dessa revisão.

### Obrigação de Abstenção

O Banco deve abster-se de executar operações que saiba ou suspeite estarem relacionadas com a prática de crime de branqueamento de capitais ou de financiamento ao terrorismo.

O Banco procede de imediato à execução do seu dever de comunicação (efetuados nos termos referidos supra) quando se abstiver de executar qualquer operação, informando as autoridades do fundamento por detrás dessa mesma abstenção.

O Banco apenas poderá executar as operações relativamente às quais tenha exercido o direito de abstenção quando:

- Não seja notificado, no prazo de 3 (três) dias úteis a contar da comunicação acima referida, da decisão da UIF de suspensão temporária da operação;
- Não seja notificado, dentro do prazo referido no ponto anterior, da decisão do DNIAP de não determinar a suspensão temporária da operação, nos termos da lei, podendo as mesmas serem executadas de imediato.

No caso de o Banco considerar que a abstenção da execução da operação não é possível, ou caso, após consulta à PGR e à UIF, se julgue que pode dificultar a investigação e persecução dos beneficiários da operação, esta pode ser realizada e o banco deverá fornecer, de imediato, à PGR e à UIF, informações a respeito da mesma, devendo tal documentação ser conservada por um período mínimo de 10 anos e colocados, em permanência, à disposição das autoridades setoriais.

Se notificado da decisão do DNIAP de suspensão temporária da operação, deverá o Banco suspender aquela mesma operação até que sujeita a apreciação judicial, que pronunciar-se-á sobre a manutenção, ou não, da suspensão temporária da operação.

### Obrigação de Cooperação e Prestação de Informação

O Banco presta toda a assistência requerida pela DNIAP, pela PGR e pela UIF, e pelas demais autoridades judiciárias e policiais competentes ou pelas autoridades competentes para a supervisão e fiscalização do cumprimento dos deveres legalmente estabelecidos.

### Obrigação de Sigilo

O Banco, os membros dos respetivos órgãos sociais, as pessoas que exerçam funções de direcção, de gerência ou chefia, bem como os seus colaboradores, mandatários e outras pessoas que lhes prestem serviço não podem revelar ao Cliente ou a terceiros que se encontra em curso uma investigação criminal ou que foram transmitidas informações legalmente devidas sobre uma operação.

### Obrigação de Controlo

O Banco deve adoptar políticas e procedimentos de controlo interno, avaliação e gestão de risco, auditoria interna e de comunicação que possibilitem o cumprimento dos deveres legais a que está sujeito e sejam aptos a prevenir a realização de operações relacionadas com o BC/FT/PADM.

### Obrigação de Formação

O Banco deve implementar mecanismos de formação para que todos os seus dirigentes e colaboradores conheçam as obrigações a que estão sujeitos no domínio da prevenção do BC/FT/PADM, e estejam habilitados no conhecimento da mesma com a finalidade de garantir o domínio permanente e atualizado sobre as operações que possam estar relacionadas com este tipo de ilícitos.

O Banco assegura que são ministradas às pessoas referidas no parágrafo anterior, acções específicas e regulares de formação adequada a cada sector de actividade, que as habilitem a reconhecer operações que possam estar relacionadas com o BC/FT/PADM.

No caso de colaboradores recém-admitidos cujas funções relevem directamente no âmbito de prevenção do branqueamento de capitais e do financiamento do terrorismo, deverá proporcionar-lhes formação adequada sobre as políticas, procedimentos e controlos internamente definidos para o efeito.

As acções de formação são asseguradas por pessoas ou entidades com reconhecida competência e experiência no domínio da prevenção e combate ao branqueamento de capitais e ao financiamento do terrorismo e deverão ser precedidas de parecer favorável da Direcção de *Compliance*.

O Banco manterá um registo actualizado e completo das acções de formação realizadas, conservando o registo das mesmas pelo prazo de 10 anos a contar da sua realização e colocando-o, em permanência, à disposição das autoridades.

### Obrigações no Domínio da Proteção e Tratamento de Dados

O Banco fica autorizado a realizar os tratamentos de dados pessoais necessários ao cumprimento dos deveres legalmente previstos.

O tratamento de dados pessoais pelo Banco tem como finalidade exclusiva a prevenção do branqueamento de capitais e do financiamento do terrorismo, não podendo os mesmos ser tratados para quaisquer outros fins, incluindo fins comerciais, sem prejuízo do que resultar das demais leis aplicáveis ao tratamento de dados pessoais.

O Banco assegura a eliminação de dados pessoais assim que se mostrem decorridos os prazos de conservação associados ao dever de conservação.

### Obrigações Específicas

Enquanto entidade financeira, o Banco está especialmente obrigado a cumprir com o seguinte:

- Não é permitida a abertura, a manutenção ou e a existência de contas anónimas, assim como a utilização de denominações ou nomes fictícios;
- Devem ser aplicadas medidas de diligência reforçada às relações transfronteiriças de correspondência bancária com instituições estabelecidas em países terceiros, obtendo informação sobre a natureza da sua actividade, processos de controlo interno em matéria de branqueamento de capitais e do financiamento do terrorismo e características da respetiva supervisão;
- Sempre que estabeleça relações de correspondência envolvendo instituições estabelecidas em países terceiros, o Banco deve reduzir a escrito as responsabilidades respetivas de cada instituição.

É vedado o estabelecimento de relações de correspondência com bancos de fachada. Não é permitida a movimentação de contas de pessoas falecidas pelos herdeiros, sem a apresentação de documentos legalmente comprovados.

### 7.1.2 Processo de Aceitação de Clientes

O estabelecimento de qualquer relação de negócio é enquadrado no respeito dos requisitos legais e regulamentares em vigor e, neste contexto, deve ser objeto de não aceitação quando se trate:

- De contrapartes com reputação, associada a actividades criminosas, ou de difícil comprovação o conhecimento da origem do património insuficientemente justificado;
- De contrapartes que no processo de abertura de conta, recusem a entrega de informação ou documentação necessária para o cumprimento das obrigações legais e regulamentares a que o banco se encontra sujeito;
- De bancos de fachada, entidades que exerçam actividade própria ou equivalente à de uma entidade financeira, que sejam constituídas em país ou jurisdição em que não disponham de presença física que envolva uma efetiva direção e gestão, não configurando presença física a mera existência de um agente local ou funcionários subalternos, que não se integrem num grupo financeiro regulado;
- Contas correspondentes de transferência (*payable through accounts)* - Contas disponibilizadas pelos correspondentes que, diretamente ou através de uma subconta, permitem a execução de operações, por conta própria, por parte dos clientes do banco respondente ou outros terceiros;

- Contas Anónimas – o Banco não procede à abertura e manutenção de contas de entidades anónimas ou controladas por indivíduos anónimos ou sob nomes manifestamente fictícios;
- De entidades sancionadas, nomeadamente integrando listagens internacionais de referência obrigatória no circuito bancário;
- De entidades com perfil de risco específico, por via de indicadores considerados relevantes no contexto da prevenção do BC/FT/PADM relativamente a determinados segmentos de negócio (p.ex: gestão ou comercialização de moeda digital; jogo online e em casinos / *gambling*) ou determinadas jurisdições de risco (p.ex. Centros *off-shore* e não cooperantes).

**Clientes Inaceitáveis**

O Banco não aceita a abertura de conta de Clientes não identificados ou de contas numeradas. São considerados Clientes de risco de BC/FT/PADM inaceitável os seguintes casos:

- Clientes relacionados com países, entidades ou indivíduos sancionados pela ONU, União Europeia, bancos de fachada, entidades anónimas ou controladas por indivíduos anónimos e;
- Ausência de informação sobre a natureza, propósito do negócio, origem e destino dos fundos do cliente.

Decorrente da análise dos riscos de BC/FT/PADM que motivem a adopção de medidas reforçadas, para as situações legalmente indicadas como de risco potencialmente mais elevado, as relações de negócio novas ou existentes que se integrem nestas situações ou noutras definidas internamente em função do seu grau de risco, serão alvo de aceitação condicionada (sujeita a escrutínio da Direcção de *Compliance*).

### 7.1.3 Processo de Identificação e Conhecimento dos Clientes

Considerando que o conhecimento do Cliente é um instrumento fundamental na luta contra a utilização do sistema financeiro para o BC/FT/PADM, o Banco compromete-se a iniciar uma relação de negócio apenas com os Clientes que apresentarem a informação exigida por lei, em conformidade. Este processo foi desenvolvido para permitir que no momento anterior ao início das relações de negócio com o Cliente seja recolhida e registada toda a informação sobre o Cliente, assim como dos seus Beneficiários Efectivos (se aplicável).

Todos os dados de identificação relevantes deverão ser verificados através de documentos originais comprovativos ou cópias certificadas, dos quais o Banco deve manter cópias.

A Direcção de *Compliance* pode determinar a recolha de informação adicional quando o Cliente exerça uma actividade considerada de risco potencial, tendo em consideração a informação de *Know Your Customer*.

Os procedimentos de identificação e diligência previstos no presente capítulo, concernentes aos Clientes e respetivos representantes, assim como aos seus Beneficiários Efectivos, deverão ser observados sempre que o Banco:

a. Estabeleça relações de negócio (relação de natureza comercial ou profissional que se prevê venha a ser ou seja duradoura);
b. Efetue transações ocasionais cujo montante seja superior em moeda nacional ou outra, ao equivalente a **USD 15.000,00** quer seja através de uma única operação, quer através de várias operações que aparentem estar relacionadas entre si;
c. Suspeite que as operações, independentemente do seu valor e de qualquer excepção ou similar, possam estar relacionadas com o BC/FT/PADM;
d. Tenha dúvidas sobre a veracidade ou a adequação dos dados de identificação dos clientes previamente obtidos.

## Elementos identificativos

### Pessoas Singulares

Na identificação de pessoas singulares, serão recolhidos os seguintes elementos:

a. Fotografia;
b. Nome completo;
c. Assinatura;
d. Data de nascimento;
e. Nacionalidade constante do documento de identificação;
f. Tipo, número, data de validade e entidade emitente do documento de identificação;
g. Número de identificação fiscal ou equivalente emitido por autoridade estrangeira competente;
h. Profissão e entidade patronal, quando existam;
i. Natureza e montante do rendimento;

j. Endereço completo da residência permanente e, quando diverso, do domicílio fiscal;
k. Naturalidade;
l. Outras nacionalidades não constantes do documento de identificação. No caso dos representantes dos clientes, o Banco verifica igualmente o documento que habilita tais pessoas a agir em representação dos mesmos.

A verificação da informação deve ser comprovada mediante a apresentação dos seguintes documentos válidos, dos quais constem os elementos identificativos previstos no ponto anterior:

- Documento de identificação original, válido, emitido por entidade pública competente, com fotografia, do qual conste o nome completo, a assinatura, a data de nascimento e a nacionalidade;
- Declaração de serviço, recibo de salário, contrato de trabalho ou documento equivalente idóneo, desde que evidencie a natureza e o montante do rendimento;
- Comprovativo de morada.

### Pessoas Colectivas ou Entidades sem Personalidade Jurídica

Na identificação de pessoas coletivas ou de entidades sem personalidade jurídica, são recolhidos os seguintes elementos:

a. Denominação social completa da pessoa colectiva ou entidade sem personalidade jurídica;
b. Objecto social e natureza do negócio;
c. Endereço da sede, local em que os órgãos de gestão exerçam a sua actividade, escritório de representação ou estabelecimento estável;
d. Número de Identificação Fiscal (NIF);
e. Número de Matrícula do Registo Comercial;
f. Identidade dos titulares de participações no capital da estrutura societária da pessoa colectiva; e,
g. Identidade dos titulares do órgão de administração ou órgão equivalente, bem como de outros quadros superiores relevantes com poderes de gestão;
h. Identidade dos procuradores da pessoa colectiva e respectivos mandato.

A verificação da informação deve ser comprovada mediante a apresentação dos seguintes documentos válidos, dos quais constem os elementos identificativos previstos acima:

- Certidão do Registo Comercial ou outro documento público comprovativo, nomeadamente o exemplar do Diário da República contendo a publicação do Estatuto ou certidão notarial de escritura de constituição;
- Acta da Assembleia Geral Constituinte assim como a acta de alteração à estrutura accionista de sócios;
- Procuração ou outro documento legalmente admissível para conferir mandato, no caso de procuradores.

### Momento de Verificação da Identidade

A verificação da identidade pode ser completada dentro do prazo legalmente determinado, quando se verificar cumulativamente os seguintes pressupostos:

a. Se tal for necessário para não interromper o desenrolar normal do negócio;
b. O contrário não resulte de norma legal ou regulamentar aplicável à actividade do Banco;
c. A situação em causa apresente um risco reduzido de BC/FT/PADM, expressamente identificado enquanto tal pelo Banco;
d. O Banco dê execução às medidas adequadas a gerir o risco associado àquela situação, nomeadamente através da limitação do número, do tipo ou do montante das operações que podem ser efetuados.

### Procedimentos de Diligência Complementares à Identificação

O Banco deverá ainda, de modo regular e em função do grau de risco de cada Cliente:

a. Tomar medidas adequadas para compreender a estrutura de propriedade e de controlo do Cliente, com vista à aferição da qualidade de Beneficiário Efectivo (quando aplicável);
b. Obter informação sobre a finalidade e a natureza da relação de negócio;
c. Obter informação sobre a origem e o destino dos fundos movimentados no âmbito de uma relação de negócio ou na realização de uma transacção ocasional, quando o perfil de risco do Cliente ou as características da operação o justifiquem;
d. Manter um acompanhamento contínuo da relação de negócio, a fim de assegurar que tais transacções se adequam ao conhecimento que a entidade tem das atividades e do perfil de risco do Cliente;
e. Manter actualizados os elementos de informação obtidos no decurso da relação de negócio, devendo os mesmos ser actualizados pelo menos a cada cinco anos, nos

casos de **risco baixo**, a cada 3 anos no caso de **risco médio** e anualmente nos casos de **risco alto**.

### Obrigações Relativas aos Beneficiários Efectivos

Antes de se estabelecer uma relação de negócio ou realizar qualquer transacção ocasional o Banco afere a qualidade do beneficiário efectivo e recolhe os respetivos elementos identificativos, sempre que:

a. O cliente, os seus beneficiários efetivos, a relação de negócio ou operação representem um risco acrescido de BC/FT/PADM;
b. A qualidade de beneficiário ou beneficiários efetivos seja(m) a pessoa ou pessoas singulares que detêm a direção de topo do Cliente;
c. Quando actuem como administradores fiduciários (*trustees*) ou exerçam função similar em fundos fiduciários explícitos (*express trusts*) ou em centros de interesses colectivos sem personalidade jurídica com estrutura ou funções análogas; ou que seja determinado por regulamentação específica ou por decisão das autoridades sectoriais competentes.

Em acréscimo, o Banco deve:

a. Exigir documento autenticado que confirme a identidade do beneficiário efectivo;
b. Solicitar uma cópia do acordo fiduciário ou acordo de parceria, ou outro documento equivalente;
c. Exigir um acta da assembleia-geral constituinte assim como a acta de alteração à estrutura accionista ou de sócios; e
d. O estabelecimento ou o prosseguimento da relação de negócio ou transacção ocasional na verificação do cumprimento das obrigações de registo, determinadas na lei.

### Obrigação de Identificação nas Transações Ocasionais

O Banco, antes de efectuar uma transacção ocasional cujo montante seja superior em moeda nacional ou outra, ao equivalente a USD 15.000,00, independentemente da transacção ser realizada mediante uma única operação ou através de várias operações que aparentem estar relacionadas, deve recolher e registar toda a informação sobre o Cliente e dos seus Beneficiários Efectivos (se aplicável).

O Banco deverá verificar a actualidade dos elementos de identificação apresentados, independentemente de estes já terem sido recolhidos aquando da realização de uma transacção ocasional anterior.

### Medidas Simplificadas de Identificação e Diligência

O Banco pode adoptar procedimentos de diligencia simplificada, quando dispõe de informação suficientemente credível na identificação de um risco reduzido de BC/FT/PADM nas relações de negócios, nas transações ocasionais ou nas operações que executa, desde que estejam devidamente enquadradas nas seguintes categorias;

a. Estado ou uma pessoa colectiva de direito público, de qualquer natureza, integrada na administração central ou local;
b. Autoridade ou organismo público sujeito a práticas contabilísticas transparentes e objecto de fiscalização; e,
c. Pessoas singulares titulares de conta bancária simplificada.

A verificação desta categoria de clientes por meio de critérios definidos pelo banco, vão determinar a recolha suficiente da informação que deve ser reportada ao Banco Nacional de Angola, sempre que for possível.

O Banco deve definir critérios que vão determinar se a informação pública recolhida é suficiente para aferir e confirmar que os clientes acima se enquadram numa das categorias acima referida.

A adopção de medidas simplificadas de diligência só é admissível na sequência de uma avaliação dos riscos pelo próprio Banco ou pelo Banco Nacional de Angola.

São indicativos de risco mais reduzido:

a. Risco diminuído inerente ao cliente:
   - Sociedades com acções admitidas à negociação em mercado regulamentado, sujeitas ao dever de informação que garante transparência adequada dos respetivos beneficiários efetivos;
   - Administrações ou empresas públicas;
   - Clientes que residam em zonas geográficas de risco mais baixo, apuradas de acordo com a Lei n.º 5/20.

b. Risco diminuído inerente aos produtos e serviços, operação ou canal de distribuição:
   - Produtos ou serviços financeiros limitados e claramente definidos, que tenham em vista aumentar o nível de inclusão financeira de determinados tipos de clientes;
   - Produtos em que os riscos de BC/FT/PADM são controlados por fatores, de imposição de limites de carregamento ou a transparência da respetiva titularidade, incluindo certos tipos de moeda electrónica.

São exemplos de medidas simplificadas:

a. A redução da frequência dos elementos identificativos recolhidos;
b. A redução da intensidade do acompanhamento contínuo e da profundidade da análise das operações, quando os montantes envolvidos são de valor baixo face ao perfil do cliente;
c. A ausência de recolha de informações especificas e a não execução de medidas específicas que permitam compreender o objeto e a natureza da relação negocial, quando seja razoável inferir o respetivo objecto e a natureza da relação através das próprias características da operação efectuada.

### Medidas Reforçadas de Identificação e Diligência

O Banco reforçará as medidas adoptadas no âmbito do dever de identificação e diligência quando for identificado pelo Banco ou pelo Banco Nacional de Angola, um risco acrescido de BC/FT/PADM nas relações de negócio, nas transações ocasionais ou nas operações que se efectuem.

O Banco aplicará medidas reforçadas de identificação e diligência sempre que:

a. se realizem transacções ocasionais, efectuem operações ou de algum outro modo se relacionem com pessoas singulares e coletivas ou análogas, estabelecidas em países terceiros de risco elevado;
b. o estabelecimento da relação de negócio ou a realização da transacção ocasional tenha lugar sem que o cliente ou o seu representante estejam fisicamente presentes;
c. os Clientes, seus representantes ou Beneficiários Efetivos sejam Pessoas Politicamente Expostas;

d. O Banco actue enquanto correspondente no quadro de relações de correspondência com respondentes de países terceiros.

No âmbito das medidas reforçadas de identificação e diligência e, em particular, no que diz respeito às Pessoas Politicamente Expostas, o Banco deve:

a. Adoptar procedimentos adequados para determinar se o Cliente pode ser considerado uma Pessoa Politicamente Exposta, e a sua efectiva situação de residência, no país ou fora do território nacional.
b. Adoptar procedimentos para que os colaboradores obtenham autorização da Direcção de *Compliance* antes de estabelecer relações de negócio com tais Clientes;
c. Tomar as medidas necessárias para determinar a origem do património e dos fundos envolvidos nas relações de negócio ou nas transacções ocasionais;
d. Efectuar um acompanhamento contínuo e diligência reforçada na relação de negócio com estas entidades.

São exemplos de medidas reforçadas:

a. A obtenção de informação adicional sobre os Clientes, os seus representantes ou Beneficiários Efetcivos, bem como sobre as operações planeadas ou realizadas;
b. A realização de diligências adicionais para comprovação da informação obtida;
c. A intervenção de níveis hierárquicos mais elevados, dentro do Banco, com vista a autorizar o estabelecimento de relações de negócio e/ou a execução de operações;
d. A intensificação da profundidade ou da frequência dos procedimentos de monitorização da relação de negócio;
e. A redução dos intervalos temporais para actualização da informação e demais elementos colhidos no exercício do dever de identificação e diligência;
f. A monitorização do acompanhamento da relação de negócio pelo *Compliance Officer*.
g. A exigibilidade da realização do primeiro pagamento relativo a uma dada operação através de meio rastreável com origem em conta de pagamento aberta pelo cliente junto de entidade que, não se situando em país terceiro de risco elevado, comprovadamente aplique medidas de identificação e diligência equivalentes as do Banco.

Ainda neste âmbito, o Banco deve obter informação adicional sobre os seus **Clientes, Representantes** e **Beneficiários Efectivos**, solicitando o seguinte:

a. A origem e legitimidade do património;
b. A legitimidade dos fundos envolvidos na relação de negócio ou na transacção ocasional;
c. A reputação dos clientes, dos seus representantes ou dos beneficiários efectivos;
d. Membros próximos da família e pessoas reconhecidas como estreitamente associadas;
e. As actividades anteriormente desenvolvidas; e,
f. O número, a dimensão e a frequência das transações que se estimam realizar no âmbito da relação de negócio.

### Private Banking

Para este segmento de clientes, o banco deve adotar as seguintes medidas reforçadas proporcionais aos riscos existentes:

a. A intervenção da Comissão Executiva para a:
    - Autorização do estabelecimento da relação de negócio;
    - Aprovação da avaliação de risco associada à relação de negócio e posteriores revisões.
b. A monitorização da relação de negócio pelo *Compliance Officer* ou por outro colaborador da área de *Compliance* que não esteja directamente envolvido no relacionamento comercial com o cliente;
c. Reanálise do risco e demais elementos associados às relações de negócio a que seja atribuído um grau de risco alto, numa base anual.

### 7.1.4 Pessoas Politicamente Expostas

Nos termos da Lei n.º 5/2020, as pessoas enquadradas nesta categoria comportam um risco acrescido de BC/FT/PADM, que justifica a implementação de procedimentos de diligência reforçada para o conhecimento do Cliente.

O conceito de **Pessoas Politicamente Expostas** (PPE) será interpretado pela Direcção de *Compliance* de acordo com as leis em vigor em Angola e as melhores práticas e entendimentos internacionais. Nos relatórios bimestrais de actividade da Direcção de

*Compliance* é indicado o número de contas de clientes PPE que foram abertas durante o período em análise.

O Banco qualifica como sendo PPE as contas em que qualquer dos seus intervenientes identificados nos documentos de abertura de conta seja enquadrado nessa categoria.

Se no decurso do seu relacionamento comercial com o Banco, um titular de uma conta num determinado momento passar a estar enquadrado na categoria de PPE, a Direcção de *Compliance* ao tomar conhecimento desse facto, no âmbito das rotinas diárias de filtragem de clientes deve atualizar imediatamente o KYC respeitante ao Cliente.

Em relação aos Clientes PPE, o Banco mantém o registo dos interesses e actividades de cada um ao longo do tempo, o que contribui para a compreensão e identificação do risco relativo ao BC/FT/PADM.

As relações que o Banco estabeleça com Clientes PPE devem ser revistas anualmente, pela área de negócio e enviado o devido enquadramento à Direcção de *Compliance*. Caso o quadro político, a posição do Cliente ou a natureza da relação concreta com o Cliente se altere consideravelmente, deve proceder-se à reapreciação completa e global do processo desse Cliente.

Nas medidas de diligencia reforçadas realizadas às Pessoas Politicamente Expostas, o banco deve garantir que:

a. A informação relativa aos processos de identificação e mitigação relacionados com PPE's seja comunicada aos seus colaboradores, para os quais a mesma seja relevante;

b. Os processos referidos na alínea anterior, façam parte do seu programa de

c. formação sobre prevenção de branqueamento de capitais, financiamento do terrorismo e da proliferação de armas de destruição em massa; e,

d. Os procedimentos utilizados tenham em conta uma avaliação com base no risco dos serviços ou produtos adquiridos, circunstâncias individuais, origem e montante dos fundos do cliente.

### 7.1.5 Bancos Correspondentes

Um Banco Correspondente é uma Instituição Financeira com a qual o Banco estabelece um acordo de parceria, para esta o representar ou ser representado.

Compete a Direcção de *Compliance* coordenar todas as acções e comunicações associadas à PCBC/FT/PADM, realizadas no âmbito das relações de correspondência.

As relações de correspondência bancária comportam um risco alto de BC/FT/PADM para o Banco e, como tal, deverão ser realizados procedimentos e controlos adicionais que visam a sua mitigação, nomeadamente:

a. Aplicação dos procedimentos de diligência reforçada que, entre outros, deverão incluir a obtenção de informação sobre a natureza da actividade do banco correspondente, os respetivos acionistas e *Compliance* regulamentar, bem como sobre a adequabilidade e efetividade do seu sistema de controlo interno para a PCBC/FT/PADM e Sanções;
b. Aprovação da relação de correspondência bancária por parte da Comissão Executiva, após parecer da Direcção de *Compliance*;
c. Apreciação, com base em informação publicamente conhecida, da reputação do banco correspondente e das características da respetiva supervisão; e,
d. Aplicação de medidas de monitorização reforçadas sobre as transacções.

Adicionalmente, todas as relações de correspondência bancária estão sujeitas a contratos específicos detalhados e reduzidos a escrito.

O Banco toma as medidas necessárias de acordo com as normas e as boas práticas existentes, relativamente ao estabelecimento ou manutenção de relações com Bancos Correspondentes.

### 7.1.6 Jurisdições de Alto Risco

As jurisdições de alto risco são consideradas pelo Grupo de Acção Financeira (GAFI) como jurisdições que possuem deficiências estratégicas significativas em seus regimes de combate ao branqueamento de capitais, ao financiamento do terrorismo e da proliferação de armas de destruição em massa, e que ainda não efectuaram progressos suficientes para suprir as referidas deficiências e/ou não acordaram com o GAFI um plano de acção

para esse efeito. Neste contexto, as jurisdições offshore também são consideradas localizações geográficas de alto risco.

No âmbito da identificação de relações de negócios, transacções ocasionais e operações que envolvam as jurisdições citadas no ponto anterior e para proteger o sistema financeiro internacional dos riscos de BC/FT/PADM, o Banco deve adoptar as medidas de diligência reforçada e contramedidas, divulgadas na Lei nº 05/2020 de 27 Janeiro e na Carta Circular nº 02/2023 e Carta Circular nº 02/2024.

É procedimento do Banco, efectuar a actualização da lista de países terceiros e jurisdições de risco considerando os relatórios de organizações governamentais ou internacionais neste domínio. Os índices listados abaixo servem igualmente para a consulta de informação complementar:

- Corruption Perceptions Index 2023;
- GAFI / FATF – Grupo de Acção Financeira Internacional;
- AML Basel Index.

## 7.2. Análise e Monitorização

### 7.2.1 Clientes de Risco Elevado

A abordagem baseada no risco é um mecanismo utilizado para identificar, gerir e mitigar o risco de BC/FT/PADM e deve incluir sistemas de controlo adequados com a finalidade de contribuir para a redução do risco de fraude e potenciais perdas financeiras.

Assim, relativamente às contas e aos Clientes a quem são aplicáveis factores susceptíveis de agravar o grau de risco específico, o Banco:

a) No processo de Aceitação, define as categorias de Clientes em que a abertura de conta ou sua manutenção deva ser recusada ou condicionada a processo especial de autorização, estando nesta última incluídas as PPE. Estas entidades, em observância ao expresso na lei, e desde que averiguado o seu estatuto, deverão ser submetidas a um processo de *KYC* com informação detalhada, estando previsto ao nível dos normativos internos, a obrigatoriedade de requerer autorização do *Compliance Officer* e da Comissão Executiva, e o registo em sistema da classificação do Cliente como PPE, o que determina a classificação automática de risco alto;
b) Desenvolve uma operativa de pré-validação de entidades e contas, que consiste na prévia confirmação por parte da Direcção de *Compliance,* da conformidade

documental do processo de abertura de conta e *Know Your Customers*, relativamente a entidades cujo Risco de *AML (Money Laundering)* seja considerado alto ou cujos critérios de elegibilidade assim o determinem;

c) Dispõe de um processo de classificação de risco de Clientes em tempo real, mediante *scoring*. A sua articulação com o aplicativo de filtragem de entidades, com os critérios implementados para pré-validação obrigatória de entidades e contas e, ainda, com processos de monitorização prioritária dos alertas emitidos, faz parte da estratégia de monitorização que o Banco tem implementado, para tratamento e acompanhamento das situações consideradas de risco alto. O Banco define ainda, com base em critérios de graduação e diferenciação de risco, áreas de negócio que são merecedoras de acompanhamento com controlo acrescido, de que é exemplo a Rede de *Private Banking*;

d) Tem disponível um sistema de *Workflow*, que possibilita a qualquer Colaborador comunicar à Direcção de *Compliance*, situações ou operações com elevado índice de suspeição, designadamente nos casos de entidades classificadas manualmente de risco alto, merecedoras, por natureza de acompanhamento diferenciado.

e) A definição da natureza e extensão destes procedimentos deve ser efectuada no quadro e em conformidade com o modelo global dos riscos de BC/FT/PADM, internamente definido pelo Banco em função do seu perfil específico.

### 7.2.2 Organização e Gestão de Risco

Os responsáveis pelas áreas de negócio e de suporte do Banco, são também responsáveis por:

- Implementar, controlar e verificar o grau de cumprimento dos procedimentos de prevenção e controlo na sua unidade orgânica, mantendo informado a Direcção de *Compliance*.
- Conhecer e acompanhar as ocorrências ligadas ao BC/FT/PADM verificadas na sua unidade orgânica, mantendo informado a Direcção de *Compliance*.
- Sugerir e implementar, em colaboração com a Direcção de *Compliance*, os procedimentos de controlo adicionais e as medidas cautelares que considerar necessárias, com base nas especificidades da sua unidade orgânica, com o objectivo de detectar e impedir a realização de operações suspeitas.

O **Conselho de Administração do Banco** é responsável pela implementação e aplicação das políticas e dos procedimentos e controlos em matéria de prevenção do BC/FT/PADM, incumbindo-lhe em especial:

- Aprovar as políticas e os procedimentos e controlos internos adequados à actividade do Banco e, bem assim, proceder à respetiva actualização, sendo responsável, em particular pela revisão e actualização da presente Política, com periodicidade anual;
- Ter conhecimento adequado dos riscos de BC/FT/PADM a que o Banco se encontra exposto, bem como dos processos utilizados para identificar, avaliar, acompanhar e controlar esses riscos;
- Assegurar que a estrutura organizacional do Banco permite, a todo o tempo, a adequada execução das políticas e dos procedimentos e controlos adequados, prevenindo conflitos de interesses e, sempre que necessário, promovendo a separação de funções no seio da organização;
- Promover uma cultura de prevenção do BC/FT/PADM que abranja todos os colaboradores do Banco cujas funções sejam relevantes para efeitos da prevenção do BC/FT/PADM, sustentada em elevados padrões de ética e de integridade e, sempre que necessário, na definição e aprovação de códigos de conduta apropriados;
- Designar *Compliance Officer* para o Cumprimento do Normativo;
- Acompanhar a actividade dos demais membros da Direcção de topo, na medida em que estes tutelem áreas de negócio que estejam ou possam vir a estar expostas a riscos de BC/FT/PADM;
- Acompanhar e avaliar periodicamente a eficácia das políticas e dos procedimentos e controlos aprovados e implementados, assegurando a execução das medidas adequadas à correção das deficiências detetadas nos mesmos.

**Incumbirá ao *Compliance Officer*:**

- Participar na definição e emitir parecer prévio sobre as políticas e os procedimentos e controlos destinados a prevenir o branqueamento de capitais e o financiamento do terrorismo;
- Acompanhar, em permanência, a adequação, a suficiência e a actualidade das políticas e dos procedimentos e controlos em matéria de prevenção do BC/FT/PADM, propondo as necessárias atualizações;

- Participar na definição, acompanhamento e avaliação da política de formação interna do Banco;
- Assegurar a centralização de toda a informação relevante que provenha das diversas áreas de negócio do Banco;
- Desempenhar o papel de interlocutor das autoridades judiciárias, policiais e de supervisão e fiscalização, designadamente dando cumprimento ao dever de comunicação do Banco e assegurando o exercício das demais obrigações de comunicação e de colaboração as e com as autoridades relevantes.

**O *Compliance Officer* deverá:**

- Exercer as suas funções de modo independente, permanente, efectivo e com autonomia decisória necessária a tal exercício, qualquer que seja a natureza do seu vínculo com o Banco;
- Dispor de idoneidade, de qualificação profissional e de disponibilidade adequadas ao exercício da função;
- Dispor de meios e recursos técnicos, materiais e humanos adequados, incluindo os colaboradores suficientes ao bom desempenho da função;
- Tem acesso irrestrito e atempado a toda a informação interna relevante para o exercício da função, em particular a informação referente à execução do dever de identificação e diligência e aos registos das operações efetuadas;
- Não se encontra sujeito a potenciais conflitos funcionais, em especial quando não se verifique a segregação das suas funções.

A **Direcção de Auditoria Interna** é responsável por monitorizar e testar regularmente o desenho, a eficácia e efectividade desta política, facultando também assim uma garantia adicional ao Conselho de Administração nestas matérias.

Compete ao Responsável pela Direcção de Auditoria Interna, monitorizar a actuação das áreas funcionais e da Direcção de *Compliance* e realizar testes de desenho e de efectividade aos controlos no âmbito de PCBC/FT/PADM. Para tal o Banco deverá:

- Avaliar continuamente a aplicabilidade dos procedimentos em vigor;
- Definir e monitorizar os principais riscos e respectivos indicadores associados ao BC/FT/PADM;
- Garantir uma estratégia de formação eficaz; e,

- Efetuar periodicamente testes de eficácia sobre os procedimentos e sistemas adotados.

Adicionalmente, e com o objectivo de obter uma visão mais profunda e independente sobre a efectividade e eficiência da Política, o Banco deve também promover regularmente auditorias externas especializadas sobre estas matérias.

A **Direcção de *Compliance*** efectua, de forma periódica (pelo menos anualmente) e independente, o controlo prévio e/ou a monitorização a posteriori da qualidade, adequação e eficácia das políticas, procedimentos e sistemas de controlo adoptados em matéria de prevenção do BC/FT/PADM. Este controlo é realizado em paralelo com os trabalhos realizados pela função de auditoria interna e pelos auditores externos.

O **Conselho de Administração do Banco**, conjuntamente com a Direcção de *Compliance*, identificam os riscos concretos de BC/FT/PADM existentes no contexto da realidade operativa específica do Banco, incluindo os riscos associados:

- À natureza, dimensão e complexidade da actividade prosseguida pelo Banco;
- Aos respectivos Clientes;
- As áreas de negócio desenvolvidas, bem como aos produtos, serviços e operações disponibilizados pelo Banco, com particular atenção aos riscos que possam derivar da oferta de produtos ou operações susceptíveis de favorecer o anonimato;
- Novas práticas comerciais, mecanismos de distribuição ou métodos de pagamento, bem como da utilização de novas tecnologias em produtos novos ou pré-existentes;
- Aos canais de distribuição dos produtos e serviços disponibilizados, bem como aos meios de comunicação utilizados no contacto com os clientes;
- Aos países ou territórios de origem dos clientes da entidade obrigada, ou em que estes tenham domicílio ou, de algum modo, desenvolvam a sua actividade;
- Aos países ou territórios em que a entidade obrigada opere, directamente ou através de terceiros, pertencentes ou não ao mesmo grupo.

O Banco terá em conta, o grau de probabilidade e de impacto de cada um dos riscos concretamente identificados, e o risco global do Banco e das respectivas áreas de negócio.

Para efeitos do cumprimento do parágrafo anterior, o **Conselho de Administração do Banco** reunirá com a **Direcção de Compliance** com vista a avaliar a adequação contínua dos procedimentos de mitigação dos concretos riscos de BC/FT/PADM a que o Banco, se

encontra sujeito e, sempre que aplicável, propõe e aprova as alterações aos normativos internos relativos a matérias de BC/FT/PADM.

O Responsável pela Direcção de *Compliance* disponibiliza bimestralmente para a Comissão Executiva do Banco um relatório relativo à sua actividade onde inclui os trabalhos e controlos realizados, durante o período de referência, relativamente aos riscos de BC/FT/PADM identificados, à eficácia dos procedimentos implementados e, sempre que aplicável, sugere mecanismos adicionais adequados à mitigação de novos riscos que sejam identificados.

O Conselho de Administração do Banco, dotará a Direcção de *Compliance* de meios materiais e humanos adequados para que o mesmo esteja adequadamente capacitado para cumprir as suas funções de forma célere, informada e independente.

Os Colaboradores do Banco assumem um papel relevante no que diz respeito à PCBC/FT/PADM. Como tal, todos os Colaboradores do Banco são responsáveis por garantir que cumprem com as disposições desta Política.

Na realização das suas funções diárias, os Colaboradores devem:

- Permanecer vigilantes à possibilidade de ocorrência de situações de BC/FT/PADM;
- Reportar imediatamente a Direcção de Compliance todas as suspeitas de BC/FT/PADM;
- Cumprir com todos os procedimentos relativos à identificação dos Clientes, abertura e manutenção de contas, monitorização de contas, manutenção e registo da documentação, e colaboração na prestação de informação a Direcção de *Compliance*; e,
- Assegurar que os Clientes não sejam alertados sobre quaisquer reportes às autoridades sobre as respetivas transacções.

Os Colaboradores são também responsáveis por completar todas as formações de PCBC/FT/PADM que lhes forem atribuídas, e subsequentemente aplicar diligentemente os conhecimentos adquiridos nessas formações, de acordo com as respetivas funções/responsabilidades.

### 7.2.3 Formação de Pessoal

Serão ministrados a todos os colaboradores do Banco, que nas suas funções, directa ou indirectamente estejam participem em temas relacionados com a prevenção do BC/FT/PADM, cursos de formação específica sobre a matéria em causa, os quais serão

supervisionados pela Direcção de *Compliance*. As sessões de formação realizam-se com a periodicidade máxima de 1 (um) ano e sempre que exista nova regulamentação que o justifique.

No caso de colaboradores recém-admitidos cujas funções relevem directamente no âmbito da prevenção do branqueamento de capitais e do financiamento do terrorismo, o Banco, imediatamente após a respectiva admissão e até um máximo de 6 meses, proporciona-lhes formação adequada sobre as políticas, procedimentos e controlos internamente definidos em matéria de prevenção do BC/FT/PADM.

Na medida do necessário, a Direcção de *Compliance* e a Direcção Jurídica podem desenvolver ferramentas de formação e esclarecimento de dúvidas sobre o tema da prevenção do BC/FT/PADM e as medidas adoptadas pelo Banco, sendo os colaboradores do Banco notificados por e-mail de qualquer alteração à presente Política ou de qualquer outro documento relevante que a ela se reporte.

Os formandos, no final de cada formação ministrada terão obrigatoriamente de ser avaliados de modo a ser possível verificar os conhecimentos adquiridos.

### 7.2.4 Processos e Controlos Mitigadores dos Factores de Risco de BC/FT/PADM

O Banco é responsável pela adopção de mecanismos e procedimentos de controlo interno, avaliação e gestão de risco, auditoria interna e de comunicação que possibilitem o cumprimento dos deveres legais a que está sujeito, e que sejam capazes de prevenir a ocorrência de operações relacionadas com o BC/FT/PADM.

#### Avaliação dos riscos de BC/FT/PADM

O desenho dos processos contempla as actividades primárias destinadas a executar as operações, identificar e aceitar os seus intervenientes, bem como, as actividades de controlo, realizadas pelas áreas de execução, pela Direcção de *Compliance* e pela Direcção de Auditoria Interna.

Para o efeito, o Banco define os seus controlos com base numa avaliação anual da respetiva exposição aos riscos de BC/FT/PADM. A metodologia de avaliação de risco tem por base os seguintes factores de risco identificados pelo Banco:

- Características da base de Clientes;
- Canais de distribuição dos produtos e serviços;
- País de residência e de nacionalidade dos Clientes;
- Sectores de atividade dos Clientes; e,

- Segmentos de negócio.

O risco do Banco é mitigado pelo sistema de controlo interno de PCBC/FT/PADM, sendo a Direcção de *Compliance* responsável por efectuar a avaliação dos riscos. No caso de a avaliação identificar que determinados riscos não estão a ser devidamente mitigados, a Direcção de *Compliance* deverá propor um plano de acção para implementar novos controlos e/ou rever os existentes. O Banco deve garantir que possui toda a informação relevante acerca das pessoas e entidades com quem se relaciona. Desta forma, o Banco deverá garantir que adopta uma metodologia de *due diligence* baseada no risco. Com esta abordagem, as contrapartes que apresentem riscos altos de BC/FT/PADM devem ser consideradas como de risco alto, devendo ser realizadas diligências e monitorizações reforçadas. O Banco deverá actualizar de forma regular a informação de *due diligence* de contrapartes durante a relação de negócio, de forma a assegurar uma classificação do risco exacta. A *due diligence* deverá ser revista se algum acontecimento indicar que o risco associado ao cliente tenha alterado (e.g. transacções bloqueadas ou até mesmo rejeitadas ou informação negativa proveniente de fontes públicas de informação). No caso de clientes classificados como sendo de risco alto, as diligências reforçadas deverão ser revistas, pelo menos, anualmente.

### Sistema de Filtragem

A filtragem ("*screening*") assume um papel relevante na identificação dos riscos associados ao BC/FT/PADM. Como tal, o Banco deverá implementar controlos que permitam a filtragem de Clientes e respetivas partes relacionadas relevantes (e.g. BEFs, assinantes, procuradores, entre outros), Transacções, Fornecedores e Colaboradores, em linha com o disposto nesta Política.

Os sistemas de filtragem automática utilizados pelo Banco deverão cumprir os requisitos mínimos de *fuzzy matching* (correspondência aproximada). Este mecanismo permite a configuração de uma percentagem de correspondência, sendo que apenas serão alvo de investigação os alertas com um nível de semelhança superior ao valor definido, permitindo assim a atribuição de uma classificação probabilística, por cada caso resultante da filtragem. Os sistemas de filtragem deverão ser calibrados de acordo com a avaliação de risco do Banco.

Os sistemas de filtragem do Banco têm em consideração as listagens mais actuais referentes a PPE´s e Sanções, nomeadamente ONU, União Europeia, *OFAC* etc., bem como

a listagem de "*Bad Guys*" onde constam igualmente as entidades divulgadas pelo Banco Nacional de Angola.

A filtragem deverá ser efetuada a:

- Todos os novos Clientes e respetivas partes relacionadas relevantes, fornecedores e Colaboradores;
- Todos os Clientes existentes do Banco no mínimo mensalmente;
- Quando existem alterações na informação de contrapartes;
- Quando são realizadas novas adições às listas de Sanções e de PPE´s; e,
- Nas transferências e pagamentos emitidos/recebidos dos clientes que tenham destino/origem outros bancos.

Para efeitos da presente Política, salienta-se que, para além da possível auto declaração de um cliente enquanto PPE, é o sistema de filtragem que actua enquanto controlo de identificação dos PPE's para o posterior processo de diligência reforçada. No mesmo contexto, é este o sistema utilizado para identificar partes sancionadas, com as quais o Banco não pode estabelecer relações de negócio ou, sendo estas relações pré-existentes à Sanção, deverão ser alvo de congelamento e reporte às Autoridades.

### Classificação de Risco dos Clientes

Os processos de defesa reputacional do Banco e de PCBC/FT/PADM, enquadrados numa lógica de diferenciação e graduação do risco BC/FT/PADM, apenas se tornam verdadeiramente eficazes com a aplicação das políticas de classificação, análise e monitorização que permitam perceber, em permanência, o nível de risco da entidade. Nestas circunstâncias, todos os Clientes do Banco são classificados como sendo de:

- **Risco Alto:** Clientes classificados como PPE's, Clientes ou Beneficiários Efetivos referenciados em processos judiciais ou tributários devido a investigações em matéria de prevenção de BC/FT/PADM, Clientes residentes em jurisdições *offshore* ou residentes em países de risco elevado, Relações de Correspondência Bancária, Organizações não lucrativas, Clientes do segmento ***Private banking*** e Clientes a quem tenha sido atribuída esta classificação pela Direcção de *Compliance*. O período de actualização dos dados associados a este nível de risco do cliente é **anual** ou após prazo de validade expirado;

- **Risco Médio:** Clientes que possuem factores susceptíveis de conduzir ao agravamento de um risco não negligenciável para o Banco, tais como a profissão ou actividade do Cliente, o objecto do negócio da entidade e o perfil transaccional na utilização de produtos e serviços. A atribuição desta classificação de nível de risco poderá igualmente ser efectuada pela Direcção de Compliance. O período de actualização dos dados associados a este nível de risco do cliente é de 3 em 3 anos ou após prazo de validade expirado;

- **Risco Baixo:** Clientes (particular ou uma pessoa colectiva) cuja origem dos fundos seja facilmente identificável ou cujas operações, usualmente, apresentam-se adequadas e em conformidade com o seu perfil transaccional. Na sequência da análise do perfil do cliente, a atribuição deste nível de risco pode igualmente ser efectuada pela Direcção de *Compliance*. O período de actualização dos dados associados a este nível de risco do cliente é de 5 em 5 anos ou após prazo de validade expirados.

Durante a relação de negócio estabelecida com os clientes ou garantes, o Banco efectua diligências e procedimentos periódicos e não periódicos com o objectivo de assegurar a actualidade, exatidão e completude da informação que já dispõe.

As áreas de negócio são responsáveis pela obtenção de toda a documentação necessária para a abertura de conta, incluindo os formulários preenchidos e assinados. Em todos os casos, cabe a Direcção de Compliance verificar o cumprimento dos requisitos para a abertura de conta e apenas em casos excepcionais poderá autorizar a abertura de uma conta em cujo processo falte algum documento, assegurando o respetivo bloqueio da conta até resolução da situação. Caso o Direcção de *Compliance* recuse a abertura de conta por falta de requisitos, apresentará sempre fundamentação sumária.

No âmbito da função de controlo, em relação à abertura de novas contas, a Direcção de *Compliance* acompanhará todas as situações de documentação em falta, bem como a actualização dos dados sobre os Clientes.

O Banco manterá em arquivo toda a documentação por um período de 10 anos recolhida para a abertura de conta e para a realização de operações. Os documentos comprovativos das operações conservar-se-ão pelo mesmo período a contar do momento de execução das ordens. Será mantido um registo as pessoas e entidades clientes do Banco durante os últimos 10 anos.

### Encerramento de Contas a Pedido da Direcção de *Compliance*

Na execução das suas funções de controlo, acompanhamento e monitorização, e prevenção de riscos gerais de BC/FT/PADM, a Direcção de *Compliance*, mediante determinadas circunstâncias, pode pedir o encerramento de contas de clientes como medida última de mitigação de risco.

Existem 2 formas de encerramento de contas a pedido da Direcção de *Compliance*:

a) Resultante de um processo de abertura de conta em que se decide recusar o contrato;
b) Resultante de diligências efectuadas na área das transações.

Os pedidos de fecho por instrução do Banco e/ou por Decisão do *Compliance*, são executados e registados por via de ferramentas informáticas que garantem a necessária rastreabilidade, e exclusivamente efetuados por colaboradores com a responsabilidade definida para o efeito. O estado dos pedidos, é rigorosamente controlado e acompanhado, até que se garanta a efetivação do fecho da conta.

### Riscos Gerais Inerentes a Movimentações em Numerário

Esta matéria ganha especial relevância no que respeita aos circuitos de BC/FT/PADM, pelo que é pertinente uma abordagem reforçada de controlo, de identificação dos depositantes e intervenientes nas operações de movimentação de numerário em geral, em função das circunstâncias concretas da operação. Neste contexto inscreve-se a utilização do mecanismo de solicitação da Declaração de Proveniência e Destino de Fundos (DPDF) para determinadas tipologias de operações, para além dos correntes deveres de identificação dos depositantes. Para as operações ocasionais respeitam-se as mesmas regras.

## 7.2.5 Análise e Controlo de Operações

Deve ser examinada com especial atenção qualquer operação, independentemente do seu montante, que gere suspeitas de estar relacionada com BC/FT/PADM. Para este efeito, no Anexo 1 são elencados os exemplos mais comuns de operações suspeitas de branqueamento.

Se da análise efectuada se concluir pela existência de indícios razoáveis ou certezas de relação da operação com práticas de BC/FT/PADM, a operação em questão deve ser objecto de comunicação imediata às autoridades competentes.

**Operações de Clientes**

a. Genericamente, as operações estão sujeitas a: (i) controlo geral realizado por qualquer colaborador do Banco com contacto com a operação; (ii) controlo prévio realizado pela Direcção de *Compliance* antes da respetiva execução; (iii) controlo a posteriori realizado pelo Direcção de *Compliance* após a execução da operação.
b. O Banco faz uma análise diária a posteriori (dia +1) das operações realizadas pelos seus clientes em cada segmento, por via de dados extraídos do sistema do Banco, com base no nível de risco dos clientes. É efectuado o seguinte controlo:
    - ✓ O controlo diário de operações, por montante definido de acordo com o segmento e com o nível de risco do cliente.
    - ✓ O controlo diário de operações em moeda nacional igual ou superiores a USD 15.000,00.
    - ✓ O controlo sobre transações em dinheiro acumuladas durante um determinado período que superem na sua totalidade em moeda nacional ou superiores a USD 15.000,00.
    - ✓ O controlo de operações de Clientes cuja origem ou destino sejam países de risco elevado.

O Banco adoptará medidas que possibilitem determinar o perfil de cada Cliente na realização de operações de modo a identificar situações de desvio, que devam ser analisadas mais detalhadamente. A Direcção de *Compliance*, sempre que necessita, solicita às áreas de negócio informação adicional sobre a actividade de cada Cliente com o Banco.

Quando a natureza ou o volume das operações activas ou passivas de os Clientes não corresponder com a sua atividade ou antecedentes operacionais, o *Compliance* solicita à área de negócio informação adicional referente à origem e / ou destino dos fundos e motivos dos mesmos.

Quando a natureza ou volume da operação não corresponde à actividade do cliente e a informação de origem / destino de fundos acima referidos, não se considera completa e clara pela área de negócio, o mesmo deve assinalar a ocorrência e comunicar a operação do Cliente a Direcção de *Compliance*.

O Banco dará especial atenção a situações em que numa mesma conta, sem causa que o justifique, tenham vindo a ser creditadas verbas através de depósitos em numerário por um número elevado de pessoas.

No âmbito da obrigação de análise e controlo das operações realizadas constituí obrigatoriedade de as áreas de negócio solicitar aos clientes uma DODF, para as seguintes situações:

a. Operações em numerário em moeda nacional igual ou superiores a USD 15.000,00;
b. Operações em numerário quando o interveniente não é parte na conta para montantes em moeda nacional igual ou superiores USD 5.000,00;
c. Transferências em moeda nacional igual ou superiores a USD 15.000,00 de/para jurisdições *offshore*;
d. Sempre que o *Compliance* considerar adequado face ao nível de risco do cliente, à sua actividade e à operação em si.

A declaração de origem de fundos deverá, quando aplicável, ser acompanhada de documentação associada à operação.

Sempre que, em resultado do exercício da obrigação de observação, o Banco decida não proceder à comunicação da operação às autoridades competentes, faz constar de documento ou registo:

a. Os fundamentos da decisão de não comunicação, incluindo os motivos que sustentam a inexistência de factores concretos de suspeição;
b. A referência a quaisquer eventuais contactos informais que, no decurso daquela observação, tenham sido estabelecidos com a Unidade de Informação Financeira e com as autoridades judiciárias e policiais, com indicação das respetivas datas e dos meios de comunicação utilizados.

As conclusões da análise nos termos acima descritos quanto à decisão de não comunicação de uma operação devem ser conservadas pelo período mínimo de 10 anos, ficando permanentemente ao dispor dos auditores e entidades de supervisão e fiscalização.

### Operações com Bancos Correspondentes

As operações com bancos correspondentes pressupõem sempre o estabelecimento de uma relação prévia de negócio em que são considerados todas as Obrigações de Identificação e Diligência previstos na presente política.

Estas operações são controladas pelo Direcção de *Compliance*, a posteriori, numa base de filtragem, por via de informação extraída do sistema do Banco, com base em critérios dos

países de risco, identificação das partes intervenientes das operações, motivos e frequência das operações.

**Operações de *Trade Finance***

Nas operações de *Trade Finance*, nomeadamente no momento do pedido da abertura da carta de crédito, o Direcção de *Compliance* valida previamente a operação tendo em conta a identificação das partes intervenientes, a mercadoria em causa e países de origem e destino, bem como se a operação se enquadra na actividade das partes intervenientes.

Em qualquer caso, o Banco poderá pôr em funcionamento qualquer outro tipo de ferramenta ou controlo tendente à detecção de operações susceptíveis de serem consideradas como suspeitas.

A Direcção de *Compliance* valida igualmente, a priori, todas as operações de cartas de crédito transferíveis e de remessas documentárias.

### 7.2.6 Comunicação de Operações Suspeitas

Qualquer operação que possa ser considerada suspeita por apresentar indícios de estar relacionada com a prática de BC/FT/PADM, assim como qualquer circunstância posterior relacionada com essas operações, deve ser objecto de comunicação imediata à Direcção de *Compliance*, que agirá em conformidade, nomeadamente no que respeita ao cumprimento da Obrigação de Comunicação às autoridades competentes.

O Banco deverá comunicar ainda, numa base sistemática, ao DNIAP da PGR e à UIF, quaisquer tipologias de operações que estejam definidas na legislação em vigor.

A forma, o prazo, o conteúdo e os demais termos das comunicações sistemáticas efetuadas pelo Banco, deverão obedecer aos moldes previstos na legislação em vigor.

**Procedimento de comunicação**

O colaborador do Banco que detete uma operação suspeita de BC/FT/PADM deverá comunicá-la de imediato e em simultâneo ao responsável pela sua unidade orgânica e à Direcção de *Compliance* que, após análise à operação concluirá pela comunicação ou não da operação à UIF e ao DNIAP da PGR.

O procedimento interno de comunicação deve ser especialmente rápido, de modo a assegurar a observância das normas legais que exigem uma imediata comunicação da operação suspeita às autoridades competentes.

### Conteúdo das comunicações

A comunicação de operações suspeitas deve conter a seguinte informação:

a. Identificação das pessoas singulares ou coletivas que participem na operação suspeita e a relação entre as mesmas;
b. Relação das operações e datas a que se referem, com indicação da sua natureza, moeda em que se realizam, montante, lugar ou lugares de execução, finalidade e instrumentos de pagamento ou cobrança utilizados;
c. Invocação dos indícios que conduziram à suspeita de que a operação possa estar relacionada com BC/FT/PADM.

### Comunicação ao DNIAP da PGR e UIF

Sempre que lhe seja comunicada uma suspeita sobre uma operação a Direcção de *Compliance* deve dar prioridade à sua análise. O envio da participação às autoridades competentes de operações suspeitas de branqueamento de capitais ou financiamento ao terrorismo será efetuado pela Direcção de *Compliance*.

### Isenção de responsabilidade

Nos termos da Lei n.º 5/2020, as comunicações de boa-fé realizadas não constituem violação do dever de segredo, nem implicam a responsabilização de quem efectue a comunicação.

### Dever de confidencialidade

O teor das comunicações e a identidade do colaborador que primeiro tenha efectuado as comunicações terão caráter estritamente confidenciais.

Constitui violação de dever legal, dar conhecimento ao Cliente ou a terceiros, sobre o facto de estar em curso uma investigação a uma operação pela sua possível ligação a BC/FT/PADM, com excepeçãp das pessoas e órgãos especialmente designados internamente e às autoridades competentes.

O incumprimento da obrigação de sigilo constitui contraordenação punível com multa tanto para a pessoa coletiva ou particular.

A revelação ou o favorecimento da descoberta da identidade de quem forneceu informações que levaram à investigação de determinada operação é punido com pena de prisão ou multa, nos termos da lei.

## 7.3. Sanções e Aplicação de Contramedidas

### 7.3.1 Regime de Sanções e Medidas Restritivas

Conforme já referenciado nesta Política, clientes relacionados com países, entidades ou indivíduos sancionados não são aceitáveis para iniciar ou manter uma relação de negócio com o BE. O objectivo das medidas restritivas é o de evitar que certos indivíduos, entidades ou grupos usem de meios que possam violar a paz e a segurança internacional, apoiar o terrorismo ou financiar a proliferação de armas de destruição em massa. Para o efeito, procura garantir que nenhum fundo ou outros activos ou serviços de qualquer tipo sejam disponibilizados às pessoas designadas enquanto estas permanecerem sujeitas às medidas restritivas.

Por conseguinte, o BE encontra-se sujeito aos regimes de sanções nacionais e internacionais emitidas pelas seguintes autoridades competentes:

1. **União Europeia**, para garantir a sua interligação com o comércio internacional e a facilitar a utilização dos seus serviços de acordo com as necessidades de circulação europeia dos seus Clientes;
2. **Conselho de Segurança das Nações Unidas**, com o objectivo de garantir a integridade do sistema financeiro;
3. ***Office of Foreing Assets Control (OFAC)***, no que respeita às operações com os Estados Unidos de América (EUA) e/ou com US Person e/ou em USD.

O BE adopta mecanismos e procedimentos de controlo interno na avaliação e gestão do risco de *compliance* face a Sanções Internacionais, complementado com um sistema de filtragem contra listas de sanções, garantindo que estas são actualizadas com a regularidade adequada e que os Clientes são alvo de filtragem no âmbito de abertura, estabelecimento e manutenção da relação de negócio, e ainda, numa base regular, sempre que forem introduzidas alterações nas listas em apreço.

#### Medidas Restritivas

As medidas restritivas aplicáveis pelo Banco caso seja identificada uma correspondência com as Listas de sanções são as seguintes:

**a) Congelamento de todos fundos ou bens, sem demora:** congelar sem demora (imediatamente ou num período não superior a 24 horas) e sem aviso prévio à pessoa, entidade ou grupo designado, todos os fundos ou outros activos:

**i.** Detidos ou controlados, total ou conjuntamente, directa ou indirectamente, por uma pessoa, entidade ou grupo designado na Lista de designação nacional de Terroristas ou na Lista de sanções;

**ii.** Derivados ou gerados a partir de fundos ou outros activos referidos na alínea a); ou

**iii.** Qualquer indivíduo ou entidade que actue em nome ou sob a direcção de qualquer indivíduo, entidade ou grupo designado.

A obrigação de congelar imediatamente não impede que sejam creditados nas contas congeladas quaisquer juros ou outros ganhos em dívida sobre as contas congeladas e pagamentos em dívida nos termos de contratos, acordos ou obrigações estabelecidas anteriormente ao congelamento dos activos.

**b) Não disponibilização de fundos, activos ou serviços:** O Banco não deve disponibilizar fundos e outros activos ou prestar serviços relacionados, no todo ou em parte, directa ou indirectamente, ou para o benefício de qualquer pessoa ou entidade designada na lista de designação nacional ou na lista de sanções.

Para designações em listas de sanções internacionais como as listas da ***OFAC, UKHNTM EU***, ou quaisquer outras listas emitidas por organizações internacionais relevantes distintas das listas da ONU, **o Banco deve aplicar uma abordagem baseada no risco para a identificação, avaliação e mitigação dos riscos concretos de BC/FT/PADM relativamente às pessoas e entidades designadas nas referidas listas.** Assim, o Banco Economico, S.A, deve adoptar medidas proporcionais aos riscos de cada transação, prevenindo e mitigando os crimes de branqueamento de capitais e financiamento ao terrorismo.

## Comunicação

Sempre que o Banco tiver conhecimento de uma correspondência positiva ou parcialmente positiva de um cliente efectivo, potencial ou qualquer outra pessoa, grupo ou entidade envolvida numa relação de negócio ou transacção, deve comunicar imediatamente à UIF, de acordo com a obrigação prevista na Lei nº 05/2020, de 27 de Janeiro. Esta comunicação deve ser efectuada por via dos mecanismos e canais disponibilizadas pela própria UIF, nomeadamente, pelo preenchimento da Declaração de Identificação de Pessoas Designadas ("DIPD") na plataforma goAML, ou pelo preenchimento do formulário físico de Declaração de Identificação de Pessoas Designadas ("DIPD").

Sempre que aplicável, e, visando a melhor definição dos padrões de acção comercial são igualmente disseminadas tais recomendações pelas funções de primeira linha de defesa pelos meios de comunicação disponíveis para o efeito.

**Protocolo de Investigação**

Geralmente, as listas de Sanções contêm instruções claras referentes à imposição de restrições ou, possivelmente, à proibição total de transacções com determinados indivíduos e/ou entidades de um determinado país.

### 7.3.2 Responsabilidade Contraordenacional

Sem prejuízo da responsabilidade penal pelo crime de branqueamento a que podem estar sujeitas tanto as pessoas singulares como as pessoas coletivas ou de outras disposições sancionatórias conexas aplicáveis a cada caso concreto, estão tipificadas contraordenações pelo incumprimento dos deveres e obrigações impostas pela Lei n.º 05/2020 de 27 de Janeiro, pelas quais podem ser responsabilizadas: (i) As entidades financeiras; (ii) As entidades não financeiras; (iii) As pessoas singulares que sejam titulares de funções de administração, gerência, direção, chefia ou fiscalização, representantes, trabalhadores ou demais colaboradores, quer sejam permanentes ou ocasionais.

A responsabilidade da pessoa colectiva ou análoga apenas é excluída quando o agente actua contra ordens ou instruções expressas daquela.

O incumprimento dos deveres e obrigações impostos pela Lei n.º 05/2020 são punidos com contraordenação.

No âmbito da atividade do Banco, podem ser aplicadas, a título de sanção, as seguintes coimas:

- Kz 45 645 800,00 a Kz 4 564 580 000,00, se o agente for a pessoa coletiva;
- Kz 5 705 725,00 a Kz 1 141 145 000,00, se o agente for uma pessoa singular.

Fora do âmbito da actividade do Banco, mas ainda no âmbito da actividade de outra entidade financeira, podem ser aplicadas, a título de sanção, as seguintes coimas:

- Kz 2 282 290,00 a Kz 1 141 145 000,00, se o agente for a pessoa coletiva;
- Kz 1 141 145,00 a Kz 456 458 000,00, se o agente for uma pessoa singular.

Como sanções acessórias, podem ainda ser aplicadas as seguintes medidas:

- Advertência, aplicável por apenas uma vez;

- Interdição, por um período até 3 (três) anos, do exercício da profissão ou da actividade a que a transgressão respeita;
- Interdição, por um período até 3 (três) meses a 3 (três) anos do exercício de cargos sociais e de funções de administração, de direção, chefia e de fiscalização em pessoas colectivas sujeitas;
- Interdição definitiva do exercício da profissão ou da actividade a que as transgressões respeitem ou dos cargos sociais e de funções de fiscalização em pessoas colectivas a que se refere o ponto anterior;
- Publicação da punição definitiva a expensas do infractor num jornal diário de difusão nacional.

# 8. Estrutura Organizacional

## 8.1. Conselho de Administração

Órgão que em primeira instância é responsável por garantir o cumprimento das obrigações legais e regulamentares do Banco em matéria de PBC/FT/PADM, e que estabelece, implementa e aprova as políticas, sistemas e controlos que visam mitigar o risco de BC/FT/PADM.

Na sua actuação, cabe ao Conselho de Administração, enquanto órgão com competência para deliberar sobre qualquer assunto da administração da sociedade definir, formalizar, implementar, divulgar e periodicamente rever a Política de PBC/FT/PADM.

O Conselho de Administração deverá igualmente definir as medidas necessárias para assegurar que o *Compliance Officer* possua:

- Autoridade e independência necessárias para desenvolver as suas responsabilidades previstas na lei;
- Os recursos adequados ao exercício das suas funções em matéria de prevenção do BC/FT/PADM;
- O acesso a toda a informação relevante que esteja na posse do Banco por forma a poder exercer adequadamente as suas funções em matéria de prevenção BC/FT/PADM.

## 8.2. Comissão Executiva

A Comissão Executiva garante e define as políticas inerentes a gestão de risco e prevenção de BC/FT/PADM.

## 8.3. Direcção de *Compliance*

Em acordo com esta Política, a Função *Compliance* é responsável por:

- Estabelecer processos para detectar e avaliar o risco decorrente do incumprimento das obrigações legais e dos deveres da instituição, bem como para correcção das deficiências detectadas.
- Avaliar os processos de prevenção e detecção de actividades criminosas, incluindo a prevenção do BC/FT/PADM, assim como assegurar as comunicações legalmente devidas neste âmbito com as autoridades competentes, designadamente a Unidade de Informação Financeira;
- Estabelecer um programa de trabalho que delimite as actividades a efectuar e preconize diferentes tipos de abordagem de acordo com o risco envolvido;
- Informar o órgão de gestão sempre que haja circunstâncias que possam motivar alterações nas políticas e procedimentos instituídos;
- Examinar transacções que pelo seu montante ou características, possam estar relacionadas com o BC/FT/PADM.

## 8.4. Comissão de Controlo Interno e Auditoria

A Comissão de Controlo Interno garante a supervisão da Função *Compliance*, na gestão de risco e prevenção de BC/FT/PADM.

## 8.5. Áreas de Negócio, suporte e Controlo

Cada área do Banco é responsável por monitorizar o cumprimento dos controlos de PBC/FT/PADM, garantindo sempre a respectiva interligação com as demais unidades orgânicas, e os reportes à Direcção de *Compliance* de toda a informação necessária.

## 8.6. Direcção de Auditoria Interna

A Direcção de Auditoria Interna é responsável por monitorar, avaliar e testar, regularmente e anualmente a eficácia do programa de Prevenção de BC/FT/PADM.

## 9. Incumprimento

O incumprimento das regras descritas nesta Política pode ser considerado violação grave dos deveres de conduta e, em consequência, pode dar lugar à aplicação de medidas disciplinares, sanções contratuais ou a eventual responsabilidade criminal.

## 10. Interpretação

A presente Política deve ser interpretada em conformidade com as normas legais e estatutárias que sejam aplicáveis cabendo, ao Conselho de Administração resolver as dúvidas de interpretação que possam surgir.

## 11. Divulgação

A presente Política será objecto de divulgação, para consulta, no *site* de Intranet e Internet do Banco.

A Direcção de Capital Humano divulgará, igualmente, a presente Política através de acções de formação (*e-Learning*) para todos Colaboradores do Banco e Sociedades Participadas.

## 12. Alterações e Aprovação

A presente Política é revista com uma periodicidade mínima anual. A Direcção de *Compliance* pode, no entanto, propor ao Conselho de Administração a revisão da Política num prazo inferior, sempre que se considere oportuno.

A presente Política e o seu respectivo anexo foram aprovados pelo Conselho de Administração do Banco, podendo apenas ser alterada por deliberação deste órgão.

A mesma também poderá ocorrer sempre que se verifiquem alterações no contexto em que o Banco desenvolve as suas actividades, nomeadamente quando ocorrem alterações legais ou quaisquer outras consideradas relevantes.

## 13. Considerações Finais

A coordenação e execução da Política de Prevenção e Gestão de Risco de BC/FT/PADM é da Direcção de *Compliance*, onde deve ser dirigida quaisquer questões relacionadas a esta política.

## 14. Revogação

A presente Política revoga a versão anterior publicada em Maio de 2022.

## 15. Anexos

### 15.1. Anexo I. Exemplos de operações suspeitas

1. Branqueamento de capitais com recurso a operações em numerário
   - ✓ Branqueamento de capitais com recurso a operações em numerário - Movimentação de contas, com importâncias significativas (em numerário) e não usuais, tituladas por pessoas singulares ou colectivas, cujas actividades conhecidas apontariam para a utilização de outro tipo de instrumento (v.g. Cheques, transferências bancárias).
   - ✓ Número elevado de créditos em numerário de pequeno montante, mas cujo valor agregado é significativo.
   - ✓ Aumento substancial dos saldos sem causa aparente, em resultado de créditos em numerário, em particular se forem, num prazo curto, subsequentemente transferidos para uma conta e/ou localização geográfica não associada normalmente à movimentação do cliente.
   - ✓ Depósitos elevados em numerário, em particular por cidadãos não residentes, cuja origem não é cabalmente justificada, sendo, por exemplo, invocados motivos como a "fuga ao Fisco".
   - ✓ Clientes que ordenam grandes transferências de e/ou para o estrangeiro, com indicação de pagamento ou recebimento em numerário.
   - ✓ Operações frequentes de câmbio manual, ou com notas de denominação reduzida, ou com divisas de reduzida circulação internacional.
   - ✓ Operações de troca de notas de pequena denominação por notas de denominação elevada (na mesma ou em divisa diferente).
   - ✓ Operações de compra/venda de moeda estrangeira, de montante consideravelmente elevado, sem justificação face à actividade declarada do cliente.
   - ✓ Depósitos em numerário de valor significativo, efectuados através de caixas automáticas ou caixas para depósitos noturnos.
   - ✓ Depósitos que, com alguma regularidade, contenham notas falsas. - Liquidação em numerário de aplicações em instrumentos financeiros.

- ✓ Pagamentos ou depósitos frequentes em cheques de viagem e notas estrangeiras (sobretudo se muito manuseadas ou não contadas).

2. Operações de branqueamento com recurso a depósitos bancários
   - ✓ Clientes que apresentem documentos de difícil verificação por parte da Instituição Financeira.
   - ✓ Movimentação da conta caracterizada por um grande número de créditos de pequeno montante e um pequeno número de débitos de valor avultado.
   - ✓ Depósitos ou empréstimos *back-to-back* com filiais ou associadas não residentes, especialmente se estabelecidas em países conhecidos como produtores de drogas ou utilizados no tráfico internacional de estupefacientes.
   - ✓ Contas que apresentem saldos aparentemente não compatíveis com a facturação do negócio em causa, ou manutenção de um número de contas inconsistente com a actividade do cliente.
   - ✓ Contas, de pessoas singulares ou colectivas, cuja movimentação, envolvendo fundos avultados, não se relaciona com a actividade do titular.
   - ✓ Clientes (pessoas singulares ou colectivas) que apenas recorrem à instituição para movimentação da respectiva conta (sobretudo quando a mesma registe saldos médios elevados), não havendo, portanto, lugar à prestação de outros serviços financeiros.
   - ✓ Grandes débitos em contas até aí "inactivas" ou em conta que acabou de ser alimentada com uma transferência do estrangeiro.
   - ✓ Contas tituladas ou que podem ser movimentadas por um elevado número de entidades sem qualquer explicação aparente.
   - ✓ Contas que apenas são utilizadas para transferência de fundos, nomeadamente de e para o estrangeiro.
   - ✓ Clientes que não reclamam nem negoceiam remunerações vantajosas, relativamente a depósitos com saldos médios elevados.
   - ✓ Contas de correspondentes, cujo padrão de movimentação ou nível de saldos registe alterações relevantes, sem razão aparente.
3. Operações com recurso a crédito
   - ✓ Pedidos de empréstimos com base em garantias ou activos depositados na Instituição Financeira, próprios ou de terceiros, cuja origem é desconhecida e cujo valor não se coaduna com a situação financeira do cliente.

- ✓ Solicitação de créditos por parte de clientes pouco conhecidos que prestam como garantia activos financeiros ou avais bancários de Instituições Financeiras estrangeiras e cujo negócio não tem ligação aparente com o objectivo da operação.
- ✓ Reembolso inusitado de créditos malparados ou amortização antecipada de empréstimos, sem motivo lógico aparente.
- ✓ Empréstimos liquidados com fundos de origem incerta ou que não são consistentes com a actividade conhecida do cliente.
- ✓ Operações de crédito cujas amortizações ou liquidação sejam, em regra, liquidadas através de numerário em conta. Em particular, comerciantes que encaminhem numerosas operações de crédito ao consumo, sendo posteriormente grande percentagem das mesmas liquidadas antecipadamente através da entrega de numerário, em nome dos respectivos clientes (beneficiários).
- ✓ Uso de cartas de crédito ou de outros métodos de financiamento para movimentar fundos entre países quando a actividade comercial internacional declarada não se coaduna com o sector económico em questão, ou com os quais o cliente não mantenha relações de negócio.

4. Operações com recursos a transferências
   - ✓ Transferências electrónicas com entrada e saída imediata da conta, sem qualquer explicação lógica.
   - ✓ Transferências efectuadas de e/ou para jurisdições fiscalmente mais favoráveis, sem que existam motivos comerciais consistentes com a actividade conhecida do cliente.
   - ✓ Instruções para que a instituição transfira fundos para o exterior na expectativa da entrada de fundos, por vezes de montante similar, mas com outra origem.
5. Outras operações
   - ✓ Cliente representado por uma sucursal, filial ou banco estrangeiro de países normalmente associados com a produção e/ou tráfico de estupefacientes.
   - ✓ Abertura e movimentação de conta por parte de cliente cuja área de residência ou de trabalho se situa fora da área de influência do balcão.
   - ✓ Recusa do cliente em fornecer a informação necessária para formalizar um crédito ou qualquer serviço. - Representantes de empresas que evitam o contacto com a instituição financeira.

- ✓ Intervenção nas operações das designadas sociedades écran, geralmente de criação recente, e com objecto social muito difuso ou que não corresponde às actividades pretensamente geradoras dos fundos movimentados.
- ✓ Compra/venda de valores mobiliários, cujos montantes não se coadunam com a actividade usual do cliente, ou transferências de carteiras, com ou sem alteração dos respectivos titulares, sem qualquer justificação.
- ✓ Gestão de patrimónios em que a origem dos fundos não é clara.
- ✓ Utilização acrescida de cofres de aluguer, seja no número dos seus utentes, seja na frequência da sua utilização, particularmente no que se refere aos pertencentes a clientes recentes ou pouco conhecidos.
- ✓ Depósito de bens, não compatíveis com a actividade conhecida do cliente, acompanhados eventualmente de solicitação de emissão de declaração comprovativa pela instituição financeira.

A análise deverá ser feita caso a caso, com base em indícios de suspeição, a fim de ser tomada a decisão de informar as entidades competentes, independentemente da operação se encontrar ou não incluída na presente lista.

## 15.2. Anexo 2. Lista não exaustiva dos factores e tipos indicativos de risco potencialmente mais elevado

1. Factores de risco inerente ao cliente:
   - ✓ Relações de negócio que se desenrolem em circunstâncias invulgares;
   - ✓ Clientes residentes ou que desenvolvam atividade em zonas de risco geográfico mais elevado, apuradas de acordo com o n.º 3 do presente anexo;
   - ✓ Pessoas coletivas ou centros de interesses coletivos sem personalidade jurídica que sejam estruturas de detenção de ativos pessoais;
   - ✓ Sociedades com accionistas fiduciários (*nominee shareholders*) ou que tenham o seu capital representado por acções ao portador;
   - ✓ Clientes que prossigam atividades que envolvam operações em numerário de forma intensiva;
   - ✓ Estruturas de propriedade ou de controlo do cliente que pareçam invulgares ou excessivamente complexas, tendo em conta a natureza da atividade prosseguida pelo cliente.
2. Fatores de risco inerentes ao produto, serviço, operação ou canal de distribuição:

- ✓ *Private banking*;
- ✓ Produtos ou operações suscetíveis de favorecer o anonimato;
- ✓ Pagamentos recebidos de terceiros desconhecidos ou não associados com o cliente ou com a atividade por este prosseguida;
- ✓ Novos produtos e novas práticas comerciais, incluindo novos mecanismos de distribuição e métodos de pagamento, bem como a utilização de novas tecnologias ou tecnologias em desenvolvimento, tanto para produtos novos como para produtos já existentes.

3. Fatores de risco inerentes à localização geográfica:
   - ✓ Países identificados por fontes idóneas, tais como os relatórios de avaliação mútua, de avaliação pormenorizada ou de acompanhamento publicados, como não dispondo de sistemas eficazes em matéria de prevenção e combate ao BC/FT/PADM, sem prejuízo do disposto na presente lei relativamente a países terceiros de risco elevado;
   - ✓ Países ou jurisdições identificadas por fontes credíveis como tendo um nível significativo de corrupção ou de outras atividades criminosas;
   - ✓ Países ou jurisdições sujeitas a sanções, embargos, outras medidas restritivas ou contramedidas adicionais impostas, designadamente, pelas Nações Unidas e pela União Europeia;
   - ✓ Países ou jurisdições que proporcionem financiamento ou apoio a actividades ou actos terroristas, ou em cujo território operem organizações terroristas.

## 15.3. Anexo 3. Jurisdição de risco baixo ou com regulamentação equivalente à jurisdição angolana

- ✓ Países terceiros que dispõem de sistemas eficazes em matéria de prevenção e combate ao branqueamento de capitais e ao financiamento do terrorismo;
- ✓ Países ou jurisdições identificadas por fontes credíveis como tendo um nível reduzido de corrupção ou de outras actividades criminais.
- ✓ Países terceiros que estão sujeitos, com base em fontes idóneas, tais como os relatórios de avaliação mútua, de avaliação pormenorizada ou de acompanhamento publicados, a obrigações de prevenção e combate ao BC/FT/PADM coerentes com as recomendações revistas do GAFI e que implementam eficazmente essas obrigações.

## 15.4. Anexo 4. Actividades de Risco Elevado

- ✓ Comércio de diamantes (ou outras pedras preciosas, safiras, esmeraldas, rubis, etc);
- ✓ Negócios com o estado ou seus intermediários;
- ✓ Comércio de arte ou antiguidades;
- ✓ Cambistas;
- ✓ Comércio de armas;
- ✓ Comércio de materiais sensíveis (tecnologia de ponta, químicos, indústria aeroespacial);
- ✓ Negócio de jogo;
- ✓ Comércio de petróleo ou outras *commodities;*
- ✓ Obras públicas ou construção civil;
- ✓ Actividade desportiva profissional;
- ✓ Religião;
- ✓ Sindicatos ou associações de trabalhadores;
- ✓ Organizações não-governamentais