BANCO SOL
O banco de todos nós

NORMA DE APLICAÇÃO PERMANENTE

POLÍTICA DE PREVENÇÃO E COMBATE AO BRANQUEAMENTO DE CAPITAIS E DO FINANCIAMENTO AO TERRORISMO E DA PROLIFERAÇÃO DE ARMAS DE DESTRUIÇÃO EM MASSA

NAP – DCP/03/2025

Publicado em:

08-07-2025

INDICE

1. DISPOSIÇÕES GERAIS

No presente capítulo apresentam-se disposições gerais referentes à Norma de Aplicação Permanente da Política de Prevenção e Combate ao Branqueamento de Capitais, do Financiamento do Terrorismo e da Proliferação de Armas de Destruição em Massa:

- Histórico de actualizações e revogação de Normativos internos;
- Enquadramento legal e Normativos internos associados;
- Objectivo e âmbito;
- Conceitos, abreviaturas e nomenclaturas;
- Órgãos de estrutura responsáveis;
- Conteúdos regulamentados.

BANCO SOL
O banco de todos nós

1.1. Histórico de Actualizações e Revogação de Normativos

1.1.1. Histórico de Actualizações

VERSÃO	DATA DE PUBLICAÇÃO	AUTOR	PRINCIPAIS ALTERAÇÕES
1	28/08/2019	Direcção de Organização e Qualidade	Primeira publicação da Política de Prevenção e Combate ao Branqueamento de Capitais, do Financiamento do Terrorismo
2	27/11/2020	Direcção de Organização e Qualidade	Foi inserido na designação da Politica a frase "e da Proliferação de Armas de Destruição em Massa" Foram feitas actualizações nos seguintes pontos da referida Politica: 2.3.1; 2.3.2; 2.5.6 e 2.5.13.
3	14/10/2021	Direcção de Organização e Qualidade	Foram feitas actualizações no número 2 e 3, do ponto 2.5.6.
4	24/11/2022	Direcção de Organização e Qualidade	Revisão periódica da Política no intuito de garantir a reengenharia: Actualização á nível do Enquadramento Legal e a linha e) do ponto 2.5.8
5	04/08/2023	Direcção de Organização e Qualidade	Actualização dos procedimentos
6	08/07/2025	Direcção de Organização e Qualidade	Revisão periódica da Política no intuito de garantir a reengenharia: Actualização á nível do Enquadramento Legal e procedimentos

1.1.2. Revogação de Normativos

A presente Norma de Aplicaão Permanente vem regulamentar, a Política de Prevenção e Combate ao Branqueamento de Capitais, do Financiamento do Terrorismo e da Proliferação de Armas de Destruição em Massa, revogando, por conseguinte, a versão anterior de 04/08/2023.

1.2. Enquadramento Legal e Normativos Internos

Consideram-se relevantes para a presente Norma de Aplicação Permanente os seguintes diplomas internos e externos:

- **Lei n.º 05/2020 de 27 de Janeiro** – Lei de Prevenção e Combate ao Branqueamento de Capitais e do Financiamento ao Terrorismo e da Proliferação de Armas de Destruição em Massa;
- **Lei nº 3/2014, de 10 de Fevereiro** – Lei sobre a Criminalização das Infracções Subjacentes ao B.C Decreto Presidencial n.º 212/13, de 13 de Dezembro, que estabelece a Organização e o Funcionamento da Unidade de Informação Financeira;
- **Lei n.º 1/2012, de 12 de Janeiro** - Lei da Designação e Aplicação de Actos Internacionais;
- **Aviso n.º 02/2024 de 11 de Março** - Regras de Prevenção e Combate ao Branqueamento e Capitais e Financiamento do Terrorismos financeiras bancárias sob a supervisão do Banco Nacional de Angola;

- **Aviso nº 06/2013 de 22 de Abril** – Serviço de Remessas de Valores;
- **Directiva n.º 04/DSI/2012 de 24 de Julho** - Congelamento de Fundos e Recursos Económicos;
- **Directiva n.º 01/2012 de 10 de Abril** - Comunicação de Operações Suspeitas de Branqueamento de Capitais e Financiamento do Terrorismo;
- 40 Recomendações do FATF/GAFI (Financial Action Task Force on Money Laundering / Grupo de Acção Financeira Internacional) publicadas em 1990 e revistas em 1996 e 2003 (incluindo as alterações de 22 de Outubro de 2004 à versão de 2003), sobre a prevenção da utilização do sistema internacional como meio de branquear capitais provenientes de actividades ilícitas;
- 9 Recomendações do FATF/GAFI, publicadas em 2001 e revistas em 2004, relativas ao combate ao financiamento ao terrorismo;
- Convenção de Viena: Convenção das Nações Unidas contra o Tráfico Ilícito de Estupefacientes e de Substâncias Psicotrópicas (1988);
- Convenção de Palermo: Convenção das Nações Unidas contra a Criminalidade Organizada Transnacional (2000);
- Convenção das Nações Unidas para a Supressão do Financiamento do Terrorismo (1999);
- Resolução do Conselho de Segurança da ONU n.º 1373 (2001) e Resolução do Conselho de Segurança da ONU n.º 1267 (1999) e resoluções sucessoras, relativas à prevenção e supressão do financiamento de actos terroristas.

1.3. Objectivo e Âmbito

A presente Norma de Aplicação Permanente visa definir a Política de Prevenção e Combate ao Branqueamento de Capitais, do Financiamento do Terrorismo e da Proliferação de Armas de Destruição em Massa no Banco, procedendo à explicitação dos conceitos de actividades de branqueamento de capitais, de actos ilícitos e financiamento ao terrorismo e estabelecimento de deveres da prevenção desses actos.

Tendo em conta as graves consequências do Branqueamento de Capitais, Financiamento do terrorismo e a Proliferação de Armas de Destruição em Massa no Sistema Financeiro, o Banco Sol considera ser um dever de todos os seus colaboradores, na sua actividade diária e no âmbito das suas funções, ter em conta e agir em conformidade com a legislação nacional e internacional, assim como com as orientações descritas nas politicas internas nesta matéria, no sentido de prevenirem a utilização dos produtos e serviços disponibilizados pela Instituição para efeitos dessas praticas.

A presente Política, assim como os procedimentos seguintes, aplicam-se a todos os colaboradores do Banco Sol.

1.4. Conceitos, Abreviaturas e Nomenclaturas

Apresenta-se de seguida a lista de siglas e conceitos utilizados ao longo da presente Norma de Aplicação Permanente:

- **DCP** – Direcção de *Compliance*;
- **DOQ** – Direcção de Organização e Qualidade;
- **BC** – Branqueamento de Capitais;
- **FT** – Financiamento ao Terrorismo;
- **PADM** – Proliferação de Armas de Destruição em Massa;
- RPB – Departamento de Prevenção ao Branqueamento de Capitais;
- **KYC** – *Know Your Customer* – Conheça o seu Cliente;

- **FATF /GAFI** – Grupo de Acção Financeira Internacional;
- **BEFs** – Beneficiários Efetivos;
- **ONU** – Organização das Nações Unidas;
- **OFAC** – Agencia de Controlo de Activos Estrangeiros dos EUA;
- **HMT** – *Her Majesty's Treasury* - (Departamento do Governo do Reino Unido responsável pelo desenvolvimento das finanças públicas e da política econômica do país);
- **CFSP** – Política Externa e de Segurança Comum da União Europeia;
- **PPE´s** – Pessoas Politicamente Expostas;
- ***Corporate*** - Grupo de pessoas ou uma empresa autorizada pelo Estado a agir como uma única entidade (uma entidade legal; uma pessoa legal no contexto legal) e reconhecida como tal na lei para determinados fins).
- ***Bankers Almanac*** – Instituição gestora de informações detalhadas sobre instituições financeiras em todo o mundo. Permite que os bancos gerenciem com segurança as decisões de risco da contraparte;
- ***Offshore*** – Paraíso Fiscal;
- **Financiamento do Terrorismo (FT):** Recolha de fundo destinados ao terrorismo, independentemente da licitude dos referidos fundos, conforme previsto no regime aplicável em matéria de Prevenção e Combate ao Terrorismo;
- **Financiamento da Proliferação de Armas de Destruição em Massa FP):** Práctica que visa financiar a proliferação de armas de destruição em massa, ou seja, transferir e exportar armas nucleares, químicas ou biológicas, ou materiais relacionadas, ta como estabelecido nas resoluções de Conselho de Segurança das Nações Unidas;
- **Branqueamento de Capitais:** Qualquer evento destinado a disseminar a natureza e a origem de fundo provenientes de actividades ilícitas previstas na Lei, de modo a fazer com que estes fundos pareçam legítimos. Regra geral este processo comporta 3 fases, nomeadamente colocação, ocultação e integração.
- **Inflacções Subjacentes ao Crime de PBCFT/P:** Factos ilícitos tipificados na Lei como crime e que constituem elementos essencial do crime de PBCFT/P;
- **Medidas Restritivas:** Medidas de natureza financeira, comerciais, diplomáticas ou outras que visam a modificação das actividades aplicáveis a jurisdições, identificação e comunicação de pessoas, grupos e entidades designadas com o propósito de combater o terrorismo e manter ou restaurar a paz e a segurança internacional, assim como a segurança nacional;
- **Compliance Office:** Responsável por coordenar e monitorizar da implementação do sistema de prevenção de branqueamento de capitais, financiamento do terrorismo e da proliferação de armas de destruição em massa, incluindo a supervisão dos procedimentos de controlo interno, a centralização da informação e comunicação de operações susceptíveis à Unidade de Informação Financeira e outras autoridades competentes.

1.5. Órgãos de Estrutura Responsáveis

A Direcção de *Compliance* é responsável pela permanente actualização da presente Norma de Aplicação Permanente.

É da responsabilidade dos Líderes, assegurar que o conteúdo da presente Política seja levado ao conhecimento dos seus Liderados.

1.6. Conteúdos Regulamentados

Na presente Norma de Aplicação Permanente encontram-se estabelecidas as regras e princípios orientadores, no que se refere a:

CAPÍTULO	NOME DO CAPÍTULO
2	Política de Prevenção e Combate ao Branqueamento de Capitais, do Financiamento do Terrorismo e da Proliferação de Armas de Destruição em Massa
3	Outorgamento

2. POLÍTICA DE PREVENÇÃO E COMBATE AO BRANQUEAMENTO DE CAPITAIS, DO FINANCIAMENTO DO TERRORISMO E DA PROLIFERAÇÃO DE ARMAS DE DESTRUIÇÃO EM MASSA

No presente capítulo apresentam-se regulamentados os seguintes temas:

- Introdução;
- Conceitos;
- Responsabilidades;
- Obrigações;
- Regime Transgressional;
- Procedimentos Internos;
- Aprovação e Alteração.

2.1. Introdução

O Banco compromete-se com os mais elevados padrões de BC/FT/PADM e *Compliance*, proporcionando aos seus colaboradores instruções e ferramentas de auxílio à prevenção da utilização do Banco como veículo de branqueamento de capitais, do financiamento do terrorismo e de Proliferação de armas de destruição em massa.

Os padrões estabelecidos nesta Política criam um quadro de prevenção e combate de branqueamento de capitais, do financiamento do terrorismo e de proliferação de armas de destruição em massa, estando alinhados com a estrutura interna e com as exigências legais e regulamentares. Estes padrões são aplicáveis à actividade do Banco em todos os territórios nos quais esteja habilitado a exercê-la.

Para tal, o Banco desenvolveu um programa de prevenção e repressão de branqueamento de capitais, do financiamento do terrorismo e de proliferação de armas de destruição em massa, visando garantir que:

- Todos os clientes e contrapartes do Banco sejam devidamente identificados, bem como sejam cumpridas as diligências de Conhecimento do Cliente *(KYC – Know Your Customer),* e ainda, sejam mantidos registos dos procedimentos realizados;
- O Banco esteja em estrito acordo com a regulamentação aplicável, aderindo às boas práticas bancárias não só na identificação dos clientes e contrapartes, mas também das operações financeiras por estes realizadas, para fins de prevenção de branqueamento de capitais, do financiamento do terrorismo e de proliferação de armas de destruição em massa;
- São envolvidas todas as áreas directas ou indirectamente relacionadas com a actividade;
- Exista uma clara definição de procedimentos e responsabilidades;
- Seja dada formação aos colaboradores do Banco, com vista a permitir um completo e adequado cumprimento do programa de prevenção estabelecido;
- Eventuais indícios de branqueamento de capitais, do financiamento do terrorismo e de proliferação de armas de destruição em massa sejam comunicados, às autoridades competentes, de acordo com a regulamentação aplicável;
- De uma forma genérica, diminua o risco de utilização do Banco para a prática dessas actividades criminosas, contribuindo não só para a prevenção de tais actividades e suas consequências sociais, mas também para a protecção da solidez, integridade, estabilidade, reputação e imagem do Banco;
- Compete ao Conselho de Administração proceder à definição e implementação do presente programa e à sua avaliação. Para tal, definiu o Conselho de Administração, como unidade de estrutura responsável por acompanhar em primeira linha a implementação operacional do programa e garantir o seu cumprimento, a Direcção de *Compliance* (DCP), em particular o Departamento de AML e Avaliação de Risco de Entidades e Clientes (RAA);
- É da responsabilidade de todos os colaboradores o cumprimento integral do programa que, em cada momento, se encontre em vigor.

O Banco garantirá que o programa seja do conhecimento geral dos colaboradores e que estes podem obter esclarecimentos sobre o mesmo, sempre que tal se mostre necessário.

Anualmente ou sempre que tal se mostre necessário, face às alterações do ambiente normativo, será realizada uma auditoria interna à implementação do programa.

2.2. Conceitos

De acordo com os padrões internacionais, nomeadamente os que resultam das 40+9 recomendações do FATF\GAFI, e com a legislação nacional, o branqueamento tem na sua base um outro crime. Trata-se do processo pelo qual os produtos de uma actividade criminosa são dissimulados para ocultar a sua origem ilícita.

Assim, o branqueamento de capitais pode ser definido como:

- A conversão ou a transferência de bens, quando o autor tem o conhecimento de que esses bens são provenientes de qualquer infracção ou infracções ou da participação nessa ou nessas infracções, com o objectivo de ocultar ou dissimular a origem ilícita desses bens ou de ajudar qualquer pessoa envolvida na prática dessa ou dessas infracções a furtar-se às consequências jurídicas dos seus actos;
- A ocultação ou a dissimulação da verdadeira natureza, origem, localização, disposição, movimentação, propriedade de bens ou direitos a eles relativos, com o conhecimento de que provêm de uma infracção/ou infracções ou da participação nessa ou nessas infracções; e
- A aquisição, a detenção ou a utilização de bens, com o conhecimento, no momento da sua recepção, de que provêm de qualquer infracção ou infracções ou da participação nessa ou nessas infracções.

Por sua vez, o financiamento do terrorismo pode definir-se como o fornecimento ou recolha de fundos, por qualquer meio, directa ou indirectamente, com a intenção de os utilizar ou quando exista conhecimento de que possam ser utilizados, total ou parcialmente, no planeamento, preparação ou prática de um crime de terrorismo, por exemplo, a tomada de reféns, a falsificação de documentos administrativos ou a direcção de um grupo terrorista, independentemente de esses fundos terem origem em actividades lícitas.

Atendendo a que os principais métodos utilizados pelas organizações terroristas com vista à transferência de fundos entre diversas localizações são, em larga medida, análogos aos utilizados na prática do crime de branqueamento de capitais, é corrente, sobretudo após o 11 de Setembro de 2001, considerar-se de forma agregada o Combate ao Branqueamento de Capitais e ao Financiamento do Terrorismo. Tal é o entendimento subjacente a esta Política.

Quer o branqueamento de capitais, quer o financiamento do terrorismo compreendem três fases: (i) colocação, (ii) circulação e (iii) integração, embora com significados e abrangência diferentes.

No branqueamento de capitais, no início da cadeia, estão sempre actividades ilícitas, cujos fundos gerados são colocados em algum ponto do circuito financeiro e económico legal (Colocação). Posteriormente, são executadas operações de transformação e/ou transferência dos valores introduzidos, de modo a tornar difícil a detecção da origem e do rasto (Circulação). Por fim, os fundos são canalizados para actividades lícitas, nomeadamente para a aquisição de bens de luxo, de valores mobiliários ou imobiliários e para a realização de investimentos em actividades económicas (Integração).

2.3. Responsabilidades

No âmbito das suas atribuições cabe:

1. Conselho de Administração:
   I. Promover a aplicação das políticas e dos procedimentos e controlos em matéria de prevenção do branqueamento de capitais, financiamento do terrorismo e da proliferação de armas de destruição em massa;
   II. Promover uma cultura institucional em sede de prevenção BCFT/P, baseada num sistema de controlo interno adequado e eficaz considerando, para o efeito, os riscos de BCFT/P a que o Banco se encontra potencialmente exposto;
   III. Promover avaliações periódicas da eficácia do sistema de controlo interno;
   IV. Diligenciar, em última instância pela verificação da conformidade da presente Política com a legislação em vigor.;
   V. Promover uma cultura exigente de contratação de colaboradores que garante o seu compromisso com o combate ao BCFT/P e diligenciar para que previamente à contratação de colaboradores para o desempenho de funções de maior sensibilidade nesta área seja concretizada, de modo fundamentado, uma avaliação da sua confiabilidade e credibilidade;

VI. Nomear o responsável da função de Compliance para exercer as funções e com as condições de independência e disponibilidade de meios exigidos pelas normas aplicáveis;

VII. Receber directamente através do administrador do pelouro, os reportes dos responsáveis pela função de controlo interno com informações relativas aos sistemas de combate de BCFT/P e à identificação de situações susceptíveis de configurar riscos referentes a tais práticas ilícitas.

2. À Comissão de Controlo Interno e Auditoria (CACI):

I. Supervisionar a actuação da função de *Compliance*.

3. À Comissão Executiva (C.E.)

I. Aprovar os procedimentos, normativos e outros instrumentos internos necessários à aplicação da Política.

II. Assegurar a implementação efectiva da presente Política, garantindo que os princípios e procedimentos definidos pelo Conselho de Administração sejam operacionalizados com os meios, estruturas e controlos adequados.

2.4. Obrigações

2.4.1. Obrigação de Avaliação de Risco

O Banco deve adoptar medidas para identificar, avaliar, compreender e mitigar os Riscos á nível dos clientes individuais da transação e da Instituição, tendo em conta os seguintes factores:

- Natureza, dimensão e complexidade da actividade desenvolvida pela entidade sujeita;
- Países ou áreas geográficas em que a entidade sujeita exerça actividade, directamente ou através de terceiros, pertencentes ou não ao mesmo grupo;
- Áreas de negócio desenvolvidas pela entidade sujeita, bem como produtos, serviços e operações disponibilizadas;
- Natureza do cliente;
- Histórico do cliente;
- Natureza, dimensão e complexidade da actividade desenvolvida pelo cliente;
- Países ou áreas geográficas em que o cliente exerça actividade directamente ou através de terceiros, pertencentes ou não ao mesmo grupo;
- Forma de estabelecimento da relação de negócio;
- Localização geográfica do cliente da entidade obrigada ou que se tenha domiciliado ou de algum modo desenvolva a sua actividade;
- Transacções efectuadas pelo cliente;
- Canais de distribuição dos produtos e serviços disponibilizados, bem como dos meios de comunicação utilizados no contacto com os clientes.

Para efeitos do disposto do número anterior, o Banco deve desenvolver e implementar ferramentas e/ou sistemas de informação para gestão eficaz do risco de branqueamento de capitais, de financiamento ao terrorismo e da proliferação de armas de destruição em massa.

A natureza e dimensão das avaliações de risco devem estar adequadas as características, dimensão e complexidade da nossa Instituição.

As medidas apropriadas referidas no nº 1 do presente artigo, devem incluir:

- Documentação sobre os riscos inerentes à realidade operativa especifica da entidade sujeita e a forma como esta os identificou e avaliou, bem como sobre a adequação dos meios e procedimentos de controlo destinados a mitigação dos riscos identificados e avaliados sobre o modo como as entidades sujeitas monitorizam a adequação e eficácia destes meios;
- Consideração de todos os factores de risco relevantes antes de determinar a nível de risco global e o tipo e dimensão adequada as medidas de mitigação a serem aplicadas;
- Actualização continua das avaliações dos riscos da Instituição sobre a análise;
- Utilização de mecanismos técnicos e tecnológicos apropriados para fornecer informações sobre as avaliações de risco as autoridades competentes;
- Demonstração da adequação dos procedimentos adoptados, sempre que tal lhes seja solicitado pela competente autoridade de supervisão ou de fiscalização.

O Banco deve ainda:

- Desenvolver e implementar as políticas internas, procedimentos e controlos aprovados pelo respectivo órgão de gestão, de modo a permitir gerir e mitigar os riscos por elas identificados ou que lhes tenham sido comunicados pelas autoridades competentes;
- Monitorar a implementação dos referidos procedimentos, controlos e políticas, e aperfeiçoá-los, quando necessário;
- Executar medidas reforçadas de gestão e mitigação eficaz de riscos altos, quando sejam identificados e medidas simplificadas nos casos de risco diminuto;
- Garantir que a realização das medidas simplificadas ou reforçadas referidas na alínea anterior aborde a avaliação de riscos e as orientações das autoridades de supervisão e fiscalização.

2.4.2. Obrigação de identificação e Diligência

O Banco deve efectuar a devida Identificação e Diligência do cliente e se aplicável, dos seus representantes legais e do beneficiário efectivo, sempre que:

- Estabeleçam relações de negócio;
- Efectuem transacções ocasionais:
    1. Com um valor igual ou superior a USD 15.000 ao equivalente, em moeda nacional ou noutra moeda, independentemente de se tratar ou não de uma única operação ou de parte integrante de várias operações aparentemente vinculadas;
    2. De qualquer transferência electrónica de valor igual ou superior ao equivalente, em moeda nacional ou noutra moeda estrangeira.
- Existam suspeitas de crime de Branqueamento de Capitais ou de Financiamento do Terrorismo e de Proliferação de Armas de Destruição em Massa; e,
- Existam dúvidas quanto à autenticidade ou à conformidade dos dados de identificação dos clientes previamente adquiridos.

As medidas de diligência relativas aos clientes a serem tomadas são as seguintes:

- Identificar e verificar a identidade dos clientes e das pessoas que os representam:

1. No caso de pessoas singulares, a verificação da identidade deve ser efectuada mediante a apresentação de documento comprovativo válido em que exiba uma fotografia do qual conste o nome completo, assinatura, morada, a data de nascimento e a nacionalidade;
2. No caso de clientes que sejam pessoas colectivas a identificação faz-se mediante a apresentação de documento original ou fotocópia da certidão de escritura pública de constituição ou documento equivalente, certidão do registo comercial, publicação em Diário da República, alvarás, licença válida emitida pela entidade competente e o número de identificação fiscal;
3. No caso de pessoa colectiva ser não residente em território nacional, a identificação é feita mediante documentos equivalentes;
4. A identificação de centros de interesses colectivos sem personalidade jurídica constituídos de acordo com o direito estrangeiro ou instrumentos legais semelhantes deve incluir a obtenção e verificação do nome dos administradores (trustes), instituidores (settlor) e beneficiários.

- Identificar e verificar os beneficiários efectivos, utilizando informações de fontes credíveis, devendo exigir no mínimo, a seguinte informação:
  1. Documento autenticado que confirme a identidade do beneficiário efectivo;
  2. Cópia do acordo fiduciário, dos estatutos da sociedade ou outro documento equivalente;
  3. Acta da Assembleia Geral constituinte, assim como a acta de alteração da estrutura accionista ou de sócios;
  4. Outra informação fidedigna, que esteja publicamente disponível e a Instituição financeira bancária considere relevante.
- Obter informação sobre a finalidade e a natureza pretendida da relação de negócio;
  1. Obter informação relativa a clientes que sejam pessoas colectivas ou entidade sem personalidade jurídica, que permita compreender a natureza dos negócios do cliente, a participação de controlo no capital social, os nomes dos membros dos órgãos de gestão;
  2. Obter informação, quando o perfil de risco do cliente ou as características da operação o justifiquem, sobre a origem e o destino dos fundos movimentos no âmbito de uma relação de negócio ou na realização de uma transacção ocasional e solicitar documentação de suporte;
  3. Manter um acompanhamento continuo da relação de negócio, a fim de assegurar que tais operações são consistentes com o conhecimento que a entidade sujeita possui do cliente, dos seus negócios e do seu perfil de risco;
  4. Manter actualizados os elementos de informação obtidos no decurso da relação de negócio.
- Sempre que a entidade sujeita tenha conhecimento ou fundada suspeita de que o cliente não actua por conta própria, deve tomar medidas adequadas que lhe permitam conhecer a identidade da pessoa ou entidade por conta de quem o cliente está actuar, nomeadamente dos beneficiários efectivos;
- As entidades sujeitas devem também verificar se os representantes dos clientes se encontram legalmente habilitados a actuar em seu nome ou representação;
- A obrigação de identificação prevista no nº 2 do presente artigo, deve aplicar-se aos clientes já existentes e a verificação da identidade desses clientes será objecto de regulamentação emitida pelas autoridades de supervisão e fiscalização.

O Banco não estabelece relação de negócio ou realiza qualquer transacção ocasional, sem ter sido cumprido o dever de identificação, excepto se tal se mostrar indispensável para a execução da operação, situação em que os procedimentos de identificação serão cumpridos no mais curto prazo possível.

Não é permitido pelo Banco qualquer movimento a débito ou a crédito na conta, após o depósito inicial, nem a disponibilização de quaisquer instrumentos de pagamento sobre a conta ou a alteração da sua titularidade, sem

que se tenha procedido à cabal verificação da identidade do cliente, no estrito cumprimento das disposições legais ou regulamentares aplicáveis.

O Banco aplica procedimentos de diligência, não só em relação a novos clientes, mas também aos existentes, de um modo regular e em função do nível de risco existente.

O Banco procede ao registo e armazenamento no sistema de suporte à actividade de todas as informações consideradas relevantes relativas ao cliente. Efectua-se ainda registo de eventuais riscos acrescidos pela utilização do Banco para operações de branqueamento de capitais e de financiamento de terrorismo.

Entre outras diligências, que considere necessária, o Banco recorrerá à averiguação da presença do nome do cliente em listas de restrições, bem como obterá informações sobre a reputação do mesmo, origem dos fundos e objectivo da operação.

O Banco não dará início à relação de negócio, caso não consiga obter todas as informações que considere necessárias ou aquelas de que disponha indiquem que deverá abster-se de o fazer.

O Banco obriga-se, no entanto, a demonstrar que os procedimentos adoptados são adequados.

Nos termos da lei e das boas práticas, o Banco poderá simplificar ou reforçar o seu dever de diligência.

Nestes termos, o Banco deve cumprir com os seguintes tipos de diligência:

DILIGÊNCIA ORDINÁRIA	DILIGÊNCIA SIMPLIFICADA	DILIGÊNCIA REFORÇADA	DILIGÊNCIA CONTÍNUA
Efectuada de forma padronizada a todos os Clientes.	Efectuada a entidades com risco comprovadamente reduzido de BC/FT & PADM	Efectuada a entidades com risco alto, PPE's e risco médio (quando aplicável)	Assenta no processo contínuo de avaliação de risco na perspectiva de perfil de Cliente, como no perfil transaccional.

As diligências a realizar sobre os Clientes estão dependentes dos riscos identificados e reconhecidos no processo de abertura de conta, que impactam no respectivo cálculo do risco. Consequentemente, e em função dos riscos identificados, será determinada a necessidade de realização de diligências simplificadas, ordinárias ou reforçadas.

- **Medida de Diligência Ordinária**

No contexto das diligências ordinárias, os Clientes são alvo dos procedimentos de identificação ordinários que se encontram dispostos na legislação e na regulamentação interna em vigor, sendo que, face à realidade operativa específica do Banco, a **diligência ordinária** é aplicável à generalidade da carteira de Clientes do Banco e consubstancia-se essencialmente na recolha dos elementos de identificação tipificados na Lei e regulamentação interna necessários para qualquer relação de negócio.

De sublinhar que, antes de se proceder ao estabelecimento ou manutenção de qualquer relação de negócio ou da realização de operações, o Banco deve garantir que adoptou as medidas de diligência adequadas à recolha dos elementos identificativos e respectivos comprovativos, dos Clientes.

- **Medida de Diligência Simplificada**

No âmbito dos procedimentos de identificação e comprovativos dos Clientes, nos termos da Lei e regulamentação em vigor, o Banco pode proceder à aplicação de medidas de diligência simplificada. A aplicação deste tipo de diligência encontra-se limitado às situações em que se identifique um risco comprovadamente reduzido de BC/FT & PADM quer nas relações de negócio, quer nas transacções ocasionais, quer ainda nas restantes operações que sejam realizadas. A avaliação do risco deverá ser realizada pelo Banco ou pelas autoridades de supervisão e fiscalização. Para efeitos da consideração de risco comprovadamente reduzido são considerados alguns factores, nomeadamente:

a) O motivo da relação de negócio;
b) Nacionalidade;
c) Segmentação do cliente pelo sector de actividade;

d) Os rendimentos/ patrimónios;
e) Estimativa do volume semanal, mensal e anual das operações;
f) País de destino das Operações Internacionais;
g) Identificação dos Beneficiários Efectivos (caso existam).

A Diligência Simplificada não dispensa o Banco de realizar a monitorização da relação de negócio de forma a identificar operações fora dos padrões e efectuar a alteração da classificação de risco do Cliente, agravando ou não o risco no decurso da relação de negócio.

- **Medida de Diligência Reforçada**

Sempre que o Banco ou respectivas autoridades sectoriais identifiquem um risco acrescido de BC/FT & PADM, independentemente da sua origem e/ou natureza, o Banco garante o reforço das medidas adoptadas no âmbito da obrigação de identificação e diligência.

As medidas de diligência reforçada deverão ser aplicadas nos seguintes momentos:

- Antes ou no momento da manutenção da Relação de Negócio, bem como na adesão produtos e serviços;
- Na realização de transacções ocasionais;
- Durante a relação de negócio com base a monitorização da entidade/ movimentos;
- Antes da realização de transacções de Clientes que apresentem um risco elevado de BC/FT & PADM.

Momentos de Diligência Reforçada

O modo a verificarmos a autenticidade dos elementos de identificação ou para atestar a legitimidade de determinadas operações, é solicitado aos clientes informações suplementares, como: Preenchimento do Modelo 530A (Modelo de Justificação de origem/ destino dos fundos);

a) Apresentação de documentos de suporte a justificação prestada, (documentos jurídicos legais);
b) Efectivação de visita ao estabelecimento dos Clientes (com a apresentação do modelo de visitas preenchido e com fotografias do local); (quando necessário);
c) A realização de pesquisas em canais de informação público/ privados idóneos, bem como pesquisas nas ferramentas de screening´s do Banco;
d) A análise detalhada das informações contidas na documentação facultada pelos Clientes;
e) A consulta dos registos de créditos dos Clientes no sistema CIRC, bem como o questionamento do motivo dos créditos existentes, e a consulta referente a liquidação ou não destes;
f) Quando clientes PPE´s, requereremos a intervenção ao nível hierárquico superior (Comissão Executiva), para a decisão de aceitação ou não do estabelecimento da relação de negócio;
g) Outras medidas que venham a ser identificadas pela Direcção de *Compliance* no contexto de PBC/PFT/PPADM.

Todas as diligências realizadas no âmbito dos procedimentos de identificação e diligência dos Clientes são alvo de registo centralizado e da respectiva conservação em sistemas, de modo que seja possível a todo o tempo consultar a informação referente aos Clientes, bem como disponibilizar esta informação às autoridades afins, de acordo ao plasmado na Lei n.º 05/2020.

- **Medida de Diligência Continua**

O Banco efectua de forma regular à monitorização dos clientes com o objectivo de assegurar a actualização periódica e extraordinária de informação, identificação de rupturas de perfil e da realização, tentativa de operações suspeitas de Branqueamento de Capitais e Financiamento ao Terrorismo e da Proliferação de Armas de Destruição em Massa bem como, avaliação do perfil de risco face às medidas restritivas/entidades designadas.

A monitorização dos Clientes deverá ser capaz de identificar, de forma tempestiva, alterações relevantes ao padrão comportamental (operativo ou funcional), dos Clientes, bem como a presença de entidades de risco alto, nomeadamente no que concerne:

a) À origem e destino dos fundos;

b) Ao propósito das operações;
c) A alterações em termos de valores e volumes de operações;
d) À intervenção de entidades terceiras;
e) À intervenção de PPE's, membros da família e pessoas muito próximas;
f) À intervenção de entidades designadas;
g) Entre outros, que possam vir a ser determinados pelo Banco.

A ferramenta de AML PBC/PFT/PPADM (EAGLE), assegura os procedimentos adequados na gestão eficaz dos riscos de BC/FT & PADM nomeadamente no que concerne quer na actualização dos elementos identificativos dos Clientes, quer na monitorização comportamental dos mesmos.

2.4.3. Obrigação de Recusa

Sem prejuízo do dever de comunicação e caso os requisitos previstos nos artigos 11º a 14º, da Lei 05/2020, não possam ser cumpridos, o Banco deve:

- Recusar a abertura de conta;
- Recusar o início da Relação de negócio;
- Recusar a realização da transacção;
- Extinguir a relação de negócio.

Sempre que ocorra qualquer das situações previstas no número anterior, o Banco deve analisar as circunstâncias que a determinaram e, se suspeitarem que a situação pode estar relacionada com a prática de um Crime de Branqueamento de Capitais e de Financiamento ao Terrorismo ou de Proliferação de Armas de Destruição em Massa, deve efectuar as comunicações previstas na lei e quando aplicável, ponderar pôr termo á relação de negócio.

2.4.4. Obrigação de Conservação

O Banco conserva por um período de 10 (dez) anos, contados a partir do momento em que for efectuada a transacção ou após o fim da relação de negócio, no mínimo, os seguintes documentos:

- Cópias dos documentos ou outros suportes tecnológicos comprovativos do cumprimento da obrigação de identificação e de diligência incluindo a conservação de registos sobre a classificação dos clientes;
- Registo de transacções, incluindo toda informação original e do beneficiário da transacção, para permitir a reconstituição de cada operação, de modo a fornecer se necessário, prova no âmbito de um processo criminal;
- Cópia de toda a correspondência comercial trocada com o cliente;
- Cópia das comunicações efectuadas pelas entidades sujeitas á Unidade de Informação Financeira e outras autoridades competentes;
- Registos dos resultados das analises internas, assim como o registo da fundamentação da decisão das entidades sujeitas no sentido de não comunicarem estes resultados a Unidade de Informação Financeira ou a outras autoridades competentes;
- A informação referida no número anterior deve ser colocada a disposição da Unidade de Informação Financeira e das demais autoridades competentes.
- O Banco deve conservar, durante um período de 5 (cinco) anos, cópia dos documentos ou registos relativos à formação prestada aos seus colaboradores e dirigentes.

2.4.5. Obrigação de Comunicação

O Banco por sua própria iniciativa, informa de imediato, à Unidade de Informação Financeira, sempre que saiba ou tenha razões suficientes para suspeitar que teve lugar, está em curso ou foi tentada uma operação susceptível de estar associada á pratica do Crime de Branqueamento de Capitais ou de Financiamento ao Terrorismo e de Proliferação de Armas de Destruição em Massa ou de qualquer outro crime.

Para efeitos do disposto no número anterior a operação pode envolver uma única transacção ou ser parte integrante de várias transacções aparentemente vinculadas.

As entidades sujeitas devem ainda comunicar á Unidade de Informação Financeiras, todas as transacções em numerário igual ou superior em moeda nacional ou outra moeda equivalente, conforme descrição da tabela em anexa na Lei de BC/FT.

Neste sentido, o Compliance Officer assegura o cumprimento da **obrigação de comunicação** à Unidade de Informação Financeira (UIF), de quaisquer factos que indiciem a prática do crime de BC/FT & PADM, bem como os reportes diários sobre todas as transacções em numerário igual ou superior em moeda nacional ou outra moeda, equivalente a **USD 5 000,00,** conforme determinado no Ponto 3 do Artigo 17.º da Lei n.º 05/2020, sendo estes:

- Troca entre notas de denominação baixa por notas de denominação alta;
- Quando se realiza a troca em moedas diferentes;
- Quando um cliente compra e/ou líquida cheques, cheques de viagem ou métodos de pagamento semelhantes;
- Quando envolver valores mobiliários;
- Quando satisfaçam dois ou mais dos seguintes indicadores: Montantes não contados; em moeda estrangeira; Não depositados em conta própria; que sejam transferidos para uma conta no exterior.

Para o efeito, o Compliance Officer deve utilizar os seguintes modelos:

- Comunicação de Transacções em Numerários (DTN);
- Comunicação de Operação Suspeita (D.O.S);
- Comunicação de Entidades e Grupos de Pessoas Designadas (DIPD);
- Comunicação Espontânea.

A comunicação de operações consideradas suspeitas no âmbito de BC/FT & PADM é uma obrigação transversal a todos os Colaboradores do Banco, devendo os Colaboradores reportar à Direcção de Compliance (DCP), e consequentemente, é da responsabilidade desta (Direcção), a análise da referida suspeição e a decisão sobre a comunicação, ou não às autoridades competentes nesta matéria.

Complementarmente, o Banco deve assegurar que toda a informação e documentação, bem como as análises realizadas, é devidamente arquivada encontrando-se à disposição das autoridades competentes sempre que solicitada. Neste sentido, o Banco dispõe de um arquivo digital que conserva as informações por um período de 10 (dez) anos, contados a partir do momento em que for efectuada a transacção ou após o fim da relação de negócio.

A identidade do colaborador que comunica a operação suspeita não deve ser revelada.

2.4.6. Obrigação de Abstenção

Sempre que se constate que uma determinada operação evidencia fundada suspeita e seja susceptível de estar relacionada a prática de um crime, o Banco, para além do cumprimento das obrigações previstas dos artigos 11º a 14º da Lei nº 05/2020, deve abster-se de executar quaisquer operações relacionadas com o cliente..

2.4.7. Obrigação de Cooperação e Prestação de Informação

O Banco coopera e presta informação à Unidade de Informação Financeira, as autoridades de supervisão e de fiscalização e quando por estas solicitadas, fornece as informações sobre operações realizadas pelos clientes, apresentando ainda os documentos relacionados com as referidas operações;

O Banco possui sistemas e instrumentos que lhes permitam responder pronta e integralmente aos pedidos de informação apresentados pela Unidade de Informação Financeira e pelas demais entidades com competência nesta matéria, destinados a determinar se mantêm ou mantiveram, nos últimos dias 10 (dez) anos relações de negócio com uma determinada pessoa singular ou colectiva e qual natureza dessas relações, e mantem as informações a nível da formação prestada aos seus colaboradores e dirigentes por um período de 5 (cinco) anos.

O Banco deve ainda cooperar e fornecer todos os dados solicitados pelas autoridades judiciárias competentes.

2.4.8. Obrigação de Sigilo

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

2.4.9. Obrigação de Controlo

1. O Banco deve implementar programas de Prevenção de Branqueamento de Capitais e do Financiamento ao Terrorismo e da Proliferação de Armas de Destruição em Massa, adequados ao sector de actividade, ao risco respectivo a dimensão da actividade comercial em questão e que incluam as seguintes politicas, procedimentos e controlo internos:
    - Sistemas de controlo de conformidade, incluindo a nomeação de um responsável ao nível da direcção;
    - Uma estrutura de controlo interno independente para testar o sistema de Prevenção e do Combate ao Branqueamento de Capitais e do Financiamento ao Terrorismo e da Proliferação de Armas de Destruição em Massa;
    - A definição de um modelo eficaz de gestão de risco com prática adequadas á identificação, avaliação e mitigação dos riscos de Branqueamento de Capitais e do Financiamento ao Terrorismo e de Proliferação de Armas de Destruição em Massa a que entidade sujeita esteja ou venha a estar exposta.
2. O Banco monitoriza a implementação das medidas de prevenção e combate ao branqueamento de capitais, financiamento do terrorismo e proliferação de armas de destruição em massa (BCFT/P) nas suas filiais e participadas onde detém a maioria ou controlo.
3. Para garantir uma prevenção eficaz no âmbito do grupo económico, o Banco assegura, nos termos legais, a partilha segura de informações e a protecção da confidencialidade dos dados.

2.4.10. Obrigação de Formação

O Banco garante a formação periódica e adequada aos seus colaboradores e membros do Conselho de Administração, visando o cumprimento das obrigações impostas pela presente Lei e respectiva regulamentação em matéria de prevenção de Branqueamento de Capitais e do Financiamento ao Terrorismo e de Proliferação de Armas de Destruição em Massa e informar as autoridades de supervisão e fiscalização.

Todos os colaboradores recebem formação com vista a reconhecerem quando estamos diante a uma Pessoa Politicamente Exposta, bem como operações que possam estar relacionadas com a prática de crimes de Branqueamento de Capitais e de Financiamento ao Terrorismo.

As formações são ministradas tanto no formato *E-Learning*, como presencial.

O Banco deve conservar, durante um período de 5 (cinco) anos, copia dos documentos ou registos relativos a formação prestada aos seus colaboradores e membros do Conselho de Administração.

2.4.11. Obrigação de Selecção de Colaboradores *

O Banco garante a avaliação fundamentada da confiabilidade e credibilidade de colaboradores que pretenda indicar para funções de maior sensibilidade e risco na realização integral da sua actividade bem como da sua integridade.

O Banco deve igualmente avaliar a confiabilidade e credibilidade dos prestadores de serviços que contrata para realização de serviços sensíveis à sua integridade e actividade.

Relações de Correspondência Bancária

a) **Como banco correspondente**: O Banco não presta serviços de correspondência bancária.
b) **Como banco respondente**, no âmbito da execução de transferências de fundos, o Banco assegura:
   - Conhecer todo o percurso dos fundos confiados aos seus bancos correspondentes, desde a recepção pelos ordenantes até à sua disponibilização aos beneficiários finais no país ou jurisdição de destino;
   - Identificar todos os intervenientes nesse circuito, garantindo que apenas participam pessoas devidamente autorizadas para o processamento de transferências de fundos;
   - Adoptar medidas adequadas na recepção de transferências electrónicas, assegurando a integridade e exatidão das informações relativas ao ordenante e ao beneficiário, em conformidade com as boas práticas de processamento directo;
   - No estabelecimento de relações, aplicar procedimentos de diligência apropriados, com uma abordagem baseada no risco. A formalização da relação está sujeita à aprovação da Comissão Executiva e documentada em suporte próprio.
c) Relações com bancos de fachada: O Banco não estabelece qualquer relação de negócio com bancos de fachada.

Combate à Corrupção e ao Suborno

O Banco mantém um compromisso firme e intransigente contra todas as formas de corrupção, suborno e outras práticas ilícitas relacionadas ao BCFT/P. Nenhum colaborador ou membro dos órgãos sociais deve se envolver, directa ou indirectamente, em actividades que possam estar associadas a essas práticas. Esse compromisso está formalizado em uma política específica sobre o tema.

Medidas Restritivas

O Banco implementa mecanismos eficazes para identificar de imediato pessoas, grupos ou entidades designadas, garantindo o cumprimento das medidas restritivas impostas por organizações como a Organização das Nações Unidas (ONU), o Office of Foreign Assets Control (OFAC), a União Europeia (UE) e outras entidades competentes.

Essas medidas incluem:

- Congelamento de fundos exclusivamente para entidades designadas pela ONU;
- Proibição de transacções;
- Extinção de relações de negócio com indivíduos, grupos ou entidades sancionadas.

Os procedimentos correspondentes estão formalizados em documento próprio.

Comunicação de Irregularidades

1. Os colaboradores podem denunciar, de forma confidencial, eventuais irregularidades relacionadas ao BCFT/P ou à integridade da organização, através do canal de ética independente disponível no website do Banco. Esse canal garante a recepção, o tratamento e o registo seguro das comunicações.
2. O Banco compromete-se a não adoptar práticas laborais discriminatórias ou prejudiciais contra colaboradores que efectuem denúncias. Quando realizadas de boa-fé, as denúncias não poderão servir de fundamento para medidas disciplinares, civis ou criminais contra o denunciante.
3. Esse compromisso está formalizado em uma política específica sobre o tema.

2.4.12. Relatório

O Banco envia, anualmente, um relatório específico sobre o seu sistema de controlo interno e demais elementos informativos a definir por instrução, para a prevenção do branqueamento de capitais, financiamento do terrorismo e da proliferação de armas de destruição em massa.

O reporte é enviado ao Banco Nacional de Angola até dia 31 de Janeiro de cada ano, reportando-se ao período compreendido entre 1 de Janeiro e 31 de Dezembro do ano anterior, e deve seguir o modelo a definir por instrução, que concretizará igualmente os termos do envio do mesmo.

2.5. Incumprimento

As excepções à presente Política requerem a aprovação prévia do Conselho de Administração.

2.6. Dúvidas e Omissões

As dúvidas e as omissões, resultantes da interpretação e da aplicação da presente Política, são resolvidas pelo Conselho de Administração.

2.7. Aprovação, Alteração

A presente Política entrará em vigor na data da sua aprovação pelo Conselho de Administração, devendo ser revista anualmente ou, extraordinariamente quando justificável, mantendo o histórico das versões, de forma a possibilitar a consulta das alterações efectuadas.

A presente Política encontra-se disponível para consulta no sítio da e Intranet e Internet do Banco.

3. OUTORGAMENTO

O Conselho de Administração

António André Lopes
Presidente do Conselho de Administração

Osvaldo Salvador de Lemos Macaia
Presidente da Comissão Executiva

Ema Carla Lemos Coelho Gonçalves
Administradora Executiva

Paula Maria Tavares Monteiro
Administradora Executiva

Sandro Geovaldo Nogueira Fernandes da Silva
Administrador Executivo

Samahina de Sousa da Silva Saúde
Administrador Executivo

Vladimir Patrício Castelo Branco da Cunha
Administrador Executivo

Viriato Diaguenda Fernandes Capita
Administrador Executivo

Luís Reis Paulo Cuanga
Administrador Não-Executivo

Tatiana Olívia da Cunha dos Anjos
Administradora Não-Executiva

António Daniel Pereira dos Santos
Administrador Independente

Noé José Baltazar
Administrador Independente

Francisco Domingos Fortunato
Administrador Independente