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/03/2021

Publicado em:

14-10-2021

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

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.

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.

1.1.2. Revogação de Normativos

A presente Norma de Aplicação Permanente vem regulamentar pela primeira vez, a Política de Prevenção e Combate ao Branqueamento de Capitais, do Financiamento do Terrorismo e da Proliferação de Armas de Destruição em Massa, não revogando, por conseguinte, qualquer Normativo interno em vigor.

1.2. Enquadramento Legal e Normativos Internos

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

Internos:

- **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 n.º 1/2012, de 12 de Janeiro -** Lei da designação e aplicação de actos internacionais;
- **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;
- **Aviso n.º 14/2020 de 29 de Maio -** Regras de Prevenção e Combate ao Branqueamento e Capitais e Financiamento do Terrorismos financeiras bancárias sob a supervisão do Banco Nacional de Angola;
- **Aviso n.º 01/13 de 22 de Março -** Regulamenta as políticas e os processos que as Instituições Financeiras devem instituir no âmbito da Governação Corporativa;
- **Aviso n.º 02/13 de 19 de Abril -** Regulamenta as funções de Compliance dentro do sistema de controlo interno;
- **Aviso nº 06/2013 de 22 de Abril –** Serviço de Remessas de Valores;
- **Directiva n.º04/DSI/2012 de 24 de Julho -** Congelamento de Fundos e Recursos Económicos;
- **Directiva n.º03/DSI/2012 de 24 de Julho -** Identificação e Comunicação de Pessoas grupos e Entidades Designadas;
- **Directiva n.º 01/2012 de 10 de Abril -** Comunicação de Operações Suspeitas de Branqueamento de Capitais e Financiamento do Terrorismo.

Externos:

- 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).
- Compliance Officer – Responsável pela Coordenação e monitorização da implementação do Sistema de Branqueamento de Capitais;
- 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.

1.5. Órgãos de Estrutura Responsáveis

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

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;
- Obrigações;
- Regime Transgressional;
- Procedimentos Internos.

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 Prevenção de Branqueamento de Capitais (RPB);
- 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.

Com a mesma periodicidade, será efectuada uma revisão a esta Política e Procedimento de prevenção do branqueamento de capitais, do financiamento do terrorismo e da proliferação de armas de destruição em massa globalmente considerado.

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. Obrigações

2.3.1. 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 numero 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 adequadas as medidas de mitigação a serem aplicadas;
- Actualização continua das avaliações dos riscos da instituição sobre a analise;
- Utilização de mecanismos técnicos e tecnológicos apropriados para fornecer informações sobre as avaliações de risco as autoridades competentes;
- Demostração 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 e implementação dos referidos procedimentos, controlos e politicas, 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.

2.3.2. 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 relativa á cliente 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 pessoas colectiva ser não residente em território nacional, a identificação é feita mediante documento equivalente;
  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 colectiva 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 transação 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.

2.3.3. Obrigação de Recusa

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

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

Sempre que ocorra qualquer das situações previstas no número anterior, as entidades sujeitas devem 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, devem efectuar as comunicações previstas na lei e quando aplicável, ponderar pôr termo á relação de negócio.

2.3.4. 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 fectuadas 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.

2.3.5. Obrigação de Comunicação

O Banco por sua própria iniciativa, informa de imediato, a Unidade de Informação Financeira, sempre que saiba ou tenha razões suficientes para suspeitar que teve lugar, está em curso ou foi tentada uma operação susceptivel 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 numero 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 anexo na Lei.

2.3.6. Obrigação de Abstenção

O Banco sempre que constatar que uma determinada operação evidencia fundada suspeita e seja susceptivel de estar relacionada a prática de um crime, as entidades sujeitas, para além do cumprimento das obrigações decorrentes dos artigos 11º a 14º da lei nº 05/2020, devem abster-se de executar quaisquer operações relacionadas com o cliente.

Observado o previsto no ponto anterior, as entidades sujeitas devem imediatamente, comunicar por escrito, ou por qualquer outro meio, a Unidade de Informação Financeira, o fundamento das suas suspeições e solicitar confirmação da suspensão da operação.

A Unidade de Informação Financeira deve pronunciar-se sobre a confirmação da suspensão da operação prazo máximo de 3 (três) dias úteis, contados desde a data da recepção da comunicação, findo o qual, na falta de confirmação, a operação pode ser executada.

Caso a entidade sujeita considere que a abstenção referida no primeiro ponto não é possível ou que, após consulta á Unidade de Informação Financeira, possa ser susceptivel de prejudicar a prevenção ou a futura investigação do Branqueamento de Capitais e do Financiamento ao Terrorismo ou da proliferação de Armas de Destruição em Massa, a retirada de operação pode ser realizada, devendo a entidade sujeita fornecer de imediato á Unidade de Informação Financeira, as Informações respeitantes á operação.

Quando confirme a suspeita, a Unidade de Informação Financeira deve requerer á Procuradoria Geral da República a homologação da decisão de suspensão da operação no prazo máximo de 7 (sete) dias úteis a contar da data da decisão estabelecida no ponto nº 3.

A procuradoria Geral da República deve pronunciar-se no prazo de 10 (dez) dias úteis a contar da data da solicitação da Unidade de Informação Financeira.

Caso a procuradoria Geral da República se pronuncie no sentido de não homologação da suspensão, a Unidade de Informação Financeira comunica imediatamente o facto á entidade sujeita para que está prossiga com a operação.

Caso a Procuradoria Geral da República não se pronuncie no prazo previsto no 6º ponto a Unidade de Informação Financeira comunica imediatamente á entidade sujeita que pode executar as operações relativamente ás quais tenha exercido o dever de abstenção.

2.3.7. Obrigação de Cooperação e Prestação de Informação

O Banco deve prontamente cooperar e prestar informação á Unidade de Informação Financeira, ás autoridades de supervisão e de fiscalização e quando por estas solicitadas, fornecer as informações sobre operações realizadas pelos clientes, apresentando ainda os documentos relacionados com as referidas operações;

O Banco deve possuir 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;

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

2.3.8. 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.

2.3.9. Obrigação de Controlo

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.

Os grupos financeiros e os grupos afins de instituições não financeira devem ser obrigados a desenvolver programas de combate ao Branqueamento de Capitais e do Financiamento ao Terrorismo e da Proliferação De Armas de Destruição em Massa a nível do grupo, os quais devem ser aplicados e adaptados a todas as sucursais e filiais maioritárias;

Os programas referidos no número anterior devem incluir as medidas bem como:

- Politicas e procedimentos de partilha de informação exigidos para o cumprimento do dever de identificação e diligência relativo aos clientes e para gestão do risco de branqueamento de capitais e do financiamento ao terrorismo e da proliferação de armas de destruição em massa;
- Prestação de informação a nível do grupo, relativa ás funções de controlo de conformidade, auditoria e/ou de Combate ao Branqueamento de Capitais e de luta contra o Financiamento do Terrorismo e da Proliferação de Armas de Destruição em Massa;
- Prestação quando necessário, de informação sobre clientes, contas e operações das sucursais e filiais, para efeitos de Combate ao Branqueamento de Capitais e de Luta Contra o Financiamento do Terrorismo e da Proliferação de Armas de Destruição em Massa;
- Garantia da confidencialidade e da boa utilização da informação partilhada.

O Banco deve assegurar a aplicação das medidas de Prevenção e Combate ao Branqueamento de Capitais e do Financiamento ao Terrorismo e da Proliferação de Armas de Destruição em Massa, em conformidade com as obrigações da Lei nº 05/2020, pelas suas sucursais, filiais e participadas em que detêm maioria ou controle, situadas no estrangeiros, onde as exigências mínimas do país de acolhimento são fracas e na medida em que a suas Leis e regulamentos o permitam;

No caso de o país de acolhimento não permitir a aplicação do disposto no número anterior, as entidades sujeitas são obrigadas a aplicar medidas adicionais adequadas, para gerir os riscos de Branqueamento de Capitais, de Financiamento ao Terrorismo e de Proliferação de Armas de Destruição em Massa e informar as autoridades de supervisão e fiscalização.

2.3.10. Obrigação de Formação

O Banco deve garantir a formação periódica e adequada aos seus colaboradores e membros dos órgãos de gestão, 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.

O Banco deve conservar, durante um período de 5 (cinco) anos, copia dos documentos ou registos relativos á formação prestada aos seus empregados e dirigentes.

2.4. Regime Transgressional

2.4.1. Multas

As transgressões no artigo anterior são puníveis nos seguintes termos:

a) Quando a infracção for praticada no âmbito da actividade de uma instituição financeira:
b) Com multa no valor de Kz: 45.645.800,00 (quarenta e cinco milhões, seiscentos e quarenta e cinco mil e oitocentos Kwanzas) a Kz: 4.564.580.000,00 (quatro mil milhões, quinhentos e sessenta e quatro milhões e quinhentos e oitenta mil kwanzas), se o agente for uma pessoa colectiva; e;
c) Com multa no valor de Kz: 5.705.725,00 (cinco milhões, setecentos e cinco mil, setecentos e vinte e cinco kwanzas) a Kz: 1.141.145.000,00 (mil milhões, cento e quarenta e um milhões e cento e quarenta e cinco mil kwanzas), se o agente for uma pessoa singular;
d) Quando a infracção for praticada no âmbito da actividade de uma instituição não financeira;
e) Com multa no valor de Kz: 2.282.290,00 (dois milhões, duzentos e oitenta e dois mil e duzentos e noventa kwanzas) a Kz: 1.141.145.000,00 (mil milhões, cento e quarenta e um milhões e cento e quarenta e cinco mil kwanzas), a 456.458.000,00 (quatrocentos e cinquenta e oito mil kwanzas) se o agente for uma pessoa singular.

2.4.2. Sanções Acessórias

Conjuntamente com as multas, podem ser aplicadas ao responsável por quaisquer das transgressões previstas no artigo 72º da lei nº 05/20 as seguintes sanções acessórias em função da gravidade da infracção e da culpa do agente:

a) Advertência, aplicável por apenas uma vez;
b) Interdição, por um período de até 3 (três) anos do exercício da profissão ou da actividade a que a transgressão respeita;
c) Inibição, por um período de 3 (três) meses a 3 (três) anos do exercício de cargos sociais e de funções de administração, de direcção, de chefia e de fiscalização em pessoas colecctivas abrangida pela presente lei, quando infractor seja membro dos órgãos sociais e exerça cargos de direcção, de chefia ou de gestão ou actue em representação legal ou voluntária da pessoa colectiva;
d) Interdição definitiva do exercício da profissão ou da actividade a qua as transgressões respeitem ou dos cargos sociais e de funções de fiscalização em pessoas colectivas a que se refere o ponto anterior;
e) Publicação da punição definitiva a expensas do infractor num jornal diário de difusão nacional.

2.5. Procedimentos Internos

2.5.1. Identificação e Verificação de Clientes

Considerando que o conhecimento do Cliente é um instrumento fundamental na luta contra a utilização do sistema financeiro para o branqueamento de capitais, financiamento do terrorismo e proliferação de armas de destruição em massa, o Banco compromete-se a só iniciar uma relação de negócio com Clientes que facultarem a informação exigida por lei e após análise dessa informação.

Para tal o Banco detém um manual de políticas de identificação de clientes e desenvolveu o processo de abertura de conta de modo a permitir que no momento em que sejam estabelecidas relações comerciais com o Cliente seja recolhida e registada informação sobre identidade, representação, domicílio, capacidade legal, ocupação ou objecto social dos Clientes, assim como outros dados de identificação, os quais devem sempre ser verificados através de documentos originais comprovativos ou cópias certificadas, dos quais o Banco deve manter cópias.

Banco aplica procedimentos de diligência, não apenas aos novos Clientes, mas também aos existentes, de um modo regular e em função do nível de risco existente.

Os dados mínimos que devem ser requeridos para identificação dos clientes são os seguintes:

2.5.2. Clientes Singulares

- Apelido e nome (s) próprio(s);
- Data e local de nascimento;
- Estado civil;
- Morada completa da residência ou, caso não seja possível, quaisquer outros contactos considerados válidos;
- Número do documento de identificação utilizado e respectiva data de validade e entidade emissora;
- Situação profissional e identificação da entidade empregadora (quando aplicável); e
- Origem e natureza dos fundos envolvidos na relação de negócio ou na transacção.

2.5.3. Clientes Pessoas Colectivas

- Denominação social;
- Objecto social;

- Morada da sede;
- Detalhes da sua constituição;
- Número de identificação fiscal;
- Número de registo comercial;
- Finalidade e objecto da sua actividade;
- Detalhes relativos à sua estrutura legal e proprietária; e
- Origem e natureza dos fundos envolvidos na relação de negócio ou na transacção.

A Norma de Processo - Abertura de Conta, bem como as respectivas checklists de abertura de conta detalham as normas internas referentes a este tema.

Quando existirem indícios ou certeza de que um Cliente não actua por conta própria deve ser obtida informação suficiente para verificar e registar tanto a identidade dos representantes, procuradores ou mandatários, como das pessoas por conta das quais este actua.

O Compliance Officer pode determinar a recolha de informação adicional quando o Cliente exerça uma actividade considerada de risco potencial, tendo em consideração a informação de KYC.

2.5.4. Beneficiários Efectivos (BEFs)

Sempre que existam razões para crer que um Cliente não actua por conta própria, deve ser obtida informação sobre e verificada a identidade do beneficiário real e efectivo da transacção ou do património.

O Banco procede à identificação não só dos seus clientes, mas também dos seus representantes e, quando for o caso, dos beneficiários efectivos, exigindo os mesmos elementos e documentos comprovativos da identificação que exigiria ao cliente.

O beneficiário efectivo é a pessoa singular, que em última instância detêm, controla o cliente, ou em nome de quem é realizada uma determinada transacção.

A pessoa ou pessoas singulares que:

a) Detêm, em última instância, uma participação no capital de uma pessoa colectiva ou a controlam e/ou a pessoa singular em cujo nome a operação está sendo realizada;
b) Exercem, em última instância, um controlo efectivo sobre uma pessoa colectiva ou entidade sem personalidade jurídica, naquelas situações onde as participações no capital/controlo são exercidas por meio de uma cadeia de participação no capital ou através de um controlo não directo;
c) Detêm, em última instância, a propriedade ou o controlo directo ou indirecto do capital da sociedade ou dos direitos de voto da pessoa colectiva, que não seja uma sociedade cotada num mercado regulamentado, sujeita a requisitos de informação consentâneos com as normas internacionais;
d) Têm o direito de exercer ou que exerçam influência significativa ou que controlam a sociedade independentemente do nível de participação;
e) No caso de entidades jurídicas que administrem ou distribuam fundos, a pessoa ou pessoas singulares que:
f) Beneficiem do seu património quando os futuros beneficiários já tiverem sido determinados;
g) Sejam tidos como a categoria de pessoas em cujo interesse principal a pessoa colectiva foi constituída ou exerce a sua actividade, quando os futuros beneficiários não tiverem sido ainda determinados;
h) Exerçam controlo do património da pessoa colectiva.

2.5.5. Países de Risco

Alguns países podem ser qualificados como "Países de Risco", devido a perturbações políticas, conflitos armados, alto índice de crime organizado, reconhecido envolvimento na produção ou tráfico de estupefacientes, etc.

Manter relações comerciais com cidadãos de um País de Risco, com pessoas que estejam domiciliadas nesse País de Risco ou que mantenham regularmente uma actividade comercial com este tipo de países, pode expor o Banco a um maior risco. Deste modo, o Banco procede à filtragem de informação relativa a Clientes e operações contra listas de sanções (incluindo ONU, OFAC, HMT e CFSP)*, PPE's e informação adversa.

2.5.6. Pessoas Politicamente Expostas (PPE´s)

Nos termos da Lei n.º 05/2020, as pessoas enquadradas nesta categoria comportam um risco acrescido no que respeita ao branqueamento de capitais, financiamento do terrorismo e proliferação de arma de destruição em massa, que justifica a implementação de procedimentos reforçados de análise e conhecimento do Cliente – dever de diligência reforçado.

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.

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. Nestes casos, são adoptados os seguintes procedimentos:

1. Banco solicitará informação adicional, nomeadamente, sobre a origem do património e dos fundos envolvidos nas relações de negócio ou outra informação que considere relevante.
2. A abertura de qualquer conta por um PPE tem de ser aprovada pela Comissão Executiva. Para o efeito, o Compliance Officer é responsável por elaborar um relatório que será entregue a Comissão Executiva, a quem caberá a autorização de abertura da respectiva conta.
3. A Comissão Executiva deve tomar uma decisão sobre a abertura da conta no prazo máximo de 48h, a contar da apresentação do relatório do Compliance a mesma.
4. 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, o Gestor do Cliente, ao tomar conhecimento desse facto, deve actualizar imediatamente o KYC respeitante ao Cliente.
5. As relações que o Banco estabeleça com Clientes PPE serão revistas trimestralmente pelo Gestor do Cliente com a supervisão do respectivo Director. Caso o quadro político, a posição do Cliente ou a natureza da relação concreta com o Cliente se altere consideravelmente, o Compliance Officer deve ser imediatamente informado e proceder-se-á à reapreciação completa e global do processo desse Cliente.

A Direcção de Compliance é responsável pela monitorização contínua das operações associadas às contas tituladas por PPE. Para o efeito, receberá um relatório com as operações ou transacções que se destinem ou tenham sido requeridas por contas tituladas por PPE.

O Compliance Officer é responsável por elaborar mensalmente um relatório sobre a actividade das contas tituladas por PPE.

2.5.7. Entidades Sem Fins Lucrativos

Devido ao risco de branqueamento de capitais e de financiamento do terrorismo que estas entidades incorporam pela natureza das suas actividades, o Banco considera que as mesmas deverão ser alvo de diligência reforçada.

Assim, cabe à Direcção de Compliance recolher informação adicional nomeadamente, identificação das localizações de actuação, estrutura organizacional, natureza das doações e do voluntariado, bem como da natureza e beneficiários dos fundos.

A Direcção de Compliance é igualmente responsável por elaborar um parecer sobre a abertura de conta para clientes classificados como entidades sem fins lucrativos.

2.5.8. Relações de Correspondência Bancária

As relações de correspondência bancária comportam um risco elevado para o Banco que deve ser acautelado através da execução de medidas de diligência reforçada que visem a sua mitigação, nomeadamente através da:

a) Obtenção de informação sobre a natureza da actividade do banco correspondente, respectivos processos de controlo interno em matéria de branqueamento de capitais e o financiamento do terrorismo, assegurando a sua adequação e eficácia;
b) Apreciação, com base em informação publicamente conhecida, da reputação do banco correspondente e as características da respectiva supervisão incluindo, por exemplo, a plataforma Bankers Almanac enquanto fonte de referência;
c) Prévia autorização por parte da Comissão Executiva e Conselho de Administração do Banco da relação de correspondência bancária;
d) Formalização por escrito das respectivas responsabilidades sempre que o Banco estabeleça relações de correspondência envolvendo instituições estabelecidas em países terceiros.

Foram implementados procedimentos para a monitorização das actividades de correspondência bancária:

a) Solicitação da identificação do País de origem do Banco correspondente em questão e verificação do risco acrescido ao mesmo;
b) Solicitação das políticas e procedimentos internos do Banco correspondente em sede de combate ao branqueamento de capitais e do financiamento ao terrorismo;
c) Solicitação das políticas de identificação e aceitação de clientes do Banco correspondente, no intuito de se verificar os procedimentos quanto a permissão de abertura de contas anónimas e/ou com nomes fictícios;
d) Verificar e analisar a informação divulgada pelos meios de comunicação existentes, no propósito de se averiguar o nível reputacional do Banco correspondente em questão;
e) Anualmente e sempre que seja necessário, a Direcção de Compliance em consonância com a Direcção de Banca de Investimentos, solicitam ao Banco correspondente a actualização da informação descrita nos procedimentos acima relatados.

2.5.9. Identificação e Verificação de Contrapartes Associadas a Transacções Ocasionais

Está legalmente previsto que o Banco tem de identificar e verificar a identidade dos ordenantes, sempre que estes efectuem transacções ocasionais iguais ou superiores a USD 15.000.

Uma transacção é considerada ocasional quando ocorre fora do âmbito de uma relação de negócio já estabelecida.

De modo a cumprir com o estabelecido na legislação Angolana, o Banco determinou que todos os depositantes, sejam clientes ou não do Banco, que efectuem depósitos em numerário igual ou superior a USD 15.000 ou equivalente em Kwanzas, sejam identificados através da apresentação de documento identificativo no acto do depósito. Esta informação deverá ficar registada na Declaração Justificativa de Origem e Destino de Fundos, que deverá ser preenchida no momento da ocorrência da transacção e assinada pelo depositante.

Na Norma de Processo - Depósito de Numerário encontram-se detalhados os procedimentos referentes aos depósitos em numerário.

2.5.10. Controlo e Conservação da Documentação

O gestor de Cliente é responsável pela obtenção de toda a documentação necessária para a abertura de conta, incluindo os formulários preenchidos e assinados. Em todos os casos cabe ao Departamento de Manutenção de Contas verificar o cumprimento dos requisitos para a abertura de conta.

Nos casos em que no processo falte algum documento, o Compliance Officer poderá, excepcionalmente, autorizar a abertura da conta. Caso o Compliance Officer autorize a abertura de conta com requisitos incompletos, apresentará sempre fundamentação sumária.

No âmbito da função de controlo, em relação à abertura de novas contas, o Compliance Officer acompanhará todas as situações de documentação em falta, bem como a actualização dos dados sobre os Clientes. Para tal, o Departamento de Manutenção de Contas enviará à Direcção de Compliance um relatório mensal sobre o estado de documentação referente à abertura de novas contas. Após análise da informação, o Compliance Officer poderá determinar o encerramento de uma conta por falta de requisitos.

O Banco manterá em arquivo toda a documentação recolhida para a abertura de conta e para a realização de operações.

Conservar-se-ão em arquivo por um período de 10 anos, a partir do momento em que for efectuada a transacção ou após o fim da relação de negócio, no mínimo os seguintes documentos:

a) Cópias dos documentos ou outros suportes tecnológicos comprovativos do cumprimento da obrigação de identificação e de diligência;
b) Registo de transacções que sejam suficientes para permitir a reconstituição de cada operação, de modo a fornecer se necessário prova no âmbito de um processo criminal;
c) Cópia de toda a correspondência comercial trocada com o cliente;
d) Cópia das comunicações efectuadas pelas entidades sujeitas à Unidade de Informação Financeira e outras autoridades competentes.

2.5.11. Monitorização de Transacções

Deve ser examinada com especial atenção qualquer operação, independentemente do seu montante, que gere suspeitas de estar relacionada com branqueamento de capitais, financiamento do terrorismo e proliferação de armas de destruição em massa. Para este efeito, no normativo MNA.OBS.220 - Operações Potencialmente Suspeitas ao Branqueamento de Capitais são elencados os exemplos mais comuns de operações suspeitas de branqueamento de capitais.

Se da análise efectuada se concluir pela existência de indícios razoáveis ou certezas de relação da operação com práticas de branqueamento de capitais, financiamento ao terrorismo e proliferação de armas de destruição em massa, a operação em questão deve ser objecto de comunicação imediata às autoridades competentes.

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 respectiva execução; (iii) controlo a posterior realizado pela Direcção de Compliance após a execução da operação.

O Banco, através da análise diária e automática de dados do sistema informático, efectua o controlo de operações que impliquem alterações de titularidade de valores, nomeadamente:

a) Operações em numerário, iguais ou superiores a USD 15.000 ou equivalente em Kwanzas;
b) Transferências de e para países sobre contra-medida ou sancionado;
c) Transferências iguais ou superiores a USD 15.000 ou equivalente em Kwanzas, com destino a um país Offshore;

d) Transacções iguais ou superiores a USD 15.000 ou equivalente em Kwanzas, com destino a um país de risco;
e) Créditos realizados num período de 1 dia consecutivo, com montante acumulado superior a USD 15.000 ou equivalente em Kwanzas;
f) Créditos realizados num período de 3 dias consecutivos, com montante acumulado superior a USD 15.000 ou equivalente em Kwanzas;
g) Créditos realizados num período de 10 dias consecutivos, com montante acumulado superior a USD 30.000 ou equivalente em Kwanzas;
h) Débitos realizados num período de 1 dia consecutivo, com montante acumulado superior a USD 15.000 ou equivalente em Kwanzas;
i) Débitos realizados num período de 3 dias consecutivos, com montante acumulado superior a USD 15.000 ou equivalente em Kwanzas;
j) Débitos realizados num período de 10 dias consecutivos, com montante acumulado superior a USD 30.000 ou equivalente em Kwanzas;
k) Clientes que efectuem mais de 10 transacções a crédito em 6 dias consecutivos, com montante máximo acumulado de USD 3.000 ou equivalente em Kwanzas;
l) Clientes que efectuem mais de 15 transacções a crédito em 12 dias consecutivos, com montante máximo acumulado de USD 5.000 ou equivalente em Kwanzas;
m) Clientes que efectuem mais de 10 transacções a débito em 6 dias consecutivos, com montante máximo acumulado de USD 3.000 ou equivalente em Kwanzas;
n) Clientes que efectuem mais de 15 transacções a débito em 12 dias consecutivos, com montante máximo acumulado de USD 5.000 ou equivalente em Kwanzas.

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.

Quando a natureza ou o volume das operações activas ou passivas dos Clientes não corresponder com a sua actividade ou antecedentes operacionais, o gestor do Cliente deverá detectar a ocorrência e comunicar uma alteração significativa na operação do Cliente à Direcção de Compliance.

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

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.

Mensalmente, o Compliance Officer é responsável por apresentar ao administrador (a) do Pelouro um relatório com as principais actividades desenvolvidas no âmbito da prevenção do branqueamento de capitais, financiamento do terrorismo e proliferação de armas de destruição em massa e respectivas situações detectadas.

2.5.12. Comunicação de Operações Suspeitas

Qualquer operação que possa ser considerada suspeita por apresentar indícios de estar relacionada com a prática de branqueamento de capitais ou financiamento ao terrorismo, assim como qualquer circunstância posterior relacionada com essas operações, deve ser objecto de comunicação imediata ao Compliance Officer.

2.5.13. Procedimento de Comunicação

O colaborador do Banco que detecte uma operação suspeita de branqueamento de capitais, financiamento do terrorismo e proliferação de armas de destruição em massa deverá comunicá-lo em simultâneo ao responsável pela sua unidade orgânica e ao Compliance Officer que, após análise à operação, decidirá sobre a comunicação à Unidade de Informação Financeira.

2.5.14. Congelamento de Fundos

O Banco é obrigado à congelar, sem aviso prévio, todos os fundos/recursos económicos pertencentes ou detidos, directa/indirectamente, nos seguintes casos que venham a ser detectados:

- Clientes relacionados com países, entidades ou indivíduos sancionados, de acordo com descrito na legislação Angolana e Resoluções do Conselho de Segurança das Nações Unidas ou outro organismo internacionalmente aceite,
- Bancos de fachada; e
- Entidades anónimas, ou controlados por indivíduos anónimos.

2.5.15. Isenção de Responsabilidade

Nos termos da Lei n.º 05/2020, as comunicações de boa-fé realizadas não constituem violação do dever de segredo, nem implica a responsabilização de quem efectue a comunicação.

2.5.16. Dever de Confidencialidade

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

Não é permitido e constitui violação de dever legal dar conhecimento ao Cliente ou à terceiros, excepto às pessoas e órgãos especialmente designados internamente e às autoridades competentes, sobre o facto de estar em curso uma investigação a uma operação, pela sua possível ligação a branqueamento de capitais, financiamento do terrorismo e proliferação de armas de destruição em massa.

O incumprimento da obrigação de sigilo constitui contra-ordenação punível com coima de USD 25 000 a USD 2 500 000, se o agente for uma pessoa colectiva, ou coima de USD 12 500 a USD 1 250 000, se o agente for uma pessoa 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 até 3 anos ou pena de multa.

2.5.17. Formação e Sensibilização de Colaboradores

Serão ministrados a todo os colaboradores do Banco cursos de formação específica sobre a prevenção do branqueamento de capitais, financiamento do terrorismo e proliferação de armas de destruição em massa. As sessões de formação realizam-se com a periodicidade que o Compliance Officer entender adequada de forma presencial ou E-learning.

Envio de e-mails de sensibilização de como proceder sobre algumas matérias de branqueamento de capitais, financiamento do terrorismo e proliferação de armas de destruição em massa.

Na medida do necessário, o Compliance Officer e a Direcção de Organização e Qualidade (DOQ) podem desenvolver ferramentas de formação e esclarecimento de dúvidas sobre o tema da prevenção do branqueamento de capitais e do financiamento ao terrorismo 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