POLÍTICA DE

PREVENÇÃO E COMBATE AO BRANQUEAMENTO DE CAPITAIS, DO FINANCIAMENTO DO TERRORISMO E DA PROLIFERAÇÃO DE ARMAS DE DESTRUIÇÃO EM MASSA (PC-BC/FTP)

BancoBNI

Banco de Negócios Internacional

ÍNDICE

1. Objectivo e Âmbito

A presente política estabelece os princípios e directrizes, o modelo de governo e as medidas adoptadas para Prevenção e Combate ao Branqueamento de Capitais, do Financiamento do Terrorismo e da Proliferação de Armas de Destruição em Massa (PC-BC/FTP), a fim de assegurar o cumprimento dos normativos legais e regulamentares, bem como das recomendações das entidades internacionais relevantes neste domínio.

Esta política aplica-se ao Banco, aos membros dos órgãos sociais e aos colaboradores.

2. Modelo de Gestão do Risco de BC/FTP

2.1.Modelo Organizacional

A prevenção, detecção e combate ao BC/FTP requerem a definição de um modelo de governo que permita identificar, avaliar, monitorizar, mitigar, controlar e reportar os riscos de BC/FTP, garantindo a segregação funcional dos órgãos envolvidos. O BNI operacionaliza o referido modelo através da implementação das três (3) linhas de defesa, assegurando através desta política a definição das suas respectivas competências e responsabilidades.

2.2.Principais Competências e Responsabilidades

Sem prejuízo do previsto nos regulamentos ou manuais de estrutura orgânica, no âmbito das obrigações a que o Banco está adstrito, relativamente à PC-BC/FTP, compete:

a) Ao Conselho de Administração (CA):

i) Aprovar as políticas, os procedimentos e os controlos internos proporcionais ao risco de BC/FTP identificado;

ii) Ter conhecimento adequado dos riscos de BC/FTP a que o Banco está exposto, bem como dos processos utilizados para identificar, avaliar, acompanhar e controlar esses riscos;

iii) Assegurar que a estrutura organizacional do Banco permita, a todo o tempo, a adequada execução das políticas, procedimentos e controlos internos, prevenindo conflitos de interesses e, sempre que necessário, promovendo a segregação de funções;

iv) Promover uma cultura institucional, referente à PC-BC/FTP, que abranja todos os colaboradores e membros dos órgãos sociais, sustentada por padrões elevados de ética e de integridade;

v) Proceder à nomeação do *Compliance Officer*, devendo garantir que este:

- Desempenhe as suas funções de modo independente, permanente, efectivo e com autonomia necessária para o exercício da função;
- Seja uma pessoa idónea, com qualificação profissional e disponibilidade adequadas à função;
- Disponha de meios e recursos técnicos, materiais e humanos necessários para o bom desempenho da função;
- Tenha acesso irrestrito e atempado à toda informação interna relevante para o exercício da função, em particular a informação referente à execução do dever de identificação e diligência e aos registos das operações efectuadas; e,
- Não esteja sujeito a potenciais conflitos funcionais.

vi) Acompanhar a actividade dos demais membros do órgão de gestão que tutelam áreas de negócio que estejam ou possam vir a estar expostas a riscos de BC/FTP;

vii) Acompanhar e avaliar periodicamente a eficácia das políticas, procedimentos e controlos internos em matéria de PC-BC/FTP, assegurando a execução das medidas adequadas à correcção das deficiências detectadas;

viii) Assegurar que não existam interferências no exercício da obrigação de comunicação, prevista no art. 17.º da Lei n.º 05/20, de 27 de Janeiro.

b) Ao Conselho Fiscal (CF):

i) Avaliar a suficiência das políticas e processos em vigor;

ii) Apreciar e emitir parecer quanto à veracidade e adequação do Relatório de PBC/FTP.

c) À Comissão de Auditoria e Controlo Interno (CACI):

i) Supervisionar a actuação da Função de *Compliance*;

ii) Analisar os relatórios emitidos pela Função de *Compliance* e avaliar a eficácia da gestão de risco de *compliance* e, em particular, de BC/FTP.

d) À Comissão Executiva (CE):

i) Implementar uma cultura de *compliance* e, em particular, de PC-BC/FTP transversal ao Banco;

ii) Garantir que tem conhecimento adequado dos riscos de BC/FTP a que o Banco está exposto, bem como dos processos utilizados para identificar, avaliar, acompanhar e controlar esses riscos, devendo reportar ao Conselho de Administração sobre a eficácia e eficiência do modelo de gestão de risco de BC/FTP implementado e as deficiências detectadas que possam gerar riscos legais, sanções regulamentares, impacto reputacional ou financeiro;

iii) Garantir a definição, aprovação, implementação e divulgação de normas, processos, procedimentos e outros instrumentos internos de gestão de risco BC/FTP;

iv) Assegurar a existência de estruturas e meios adequados para a identificação, avaliação, monitorização, controlo e reporte do risco de BC/FTP;

v) Abster-se de qualquer interferência no exercício das obrigações previstas na Lei n.º 05/2020, de 27 de Janeiro, em especial no exercício do dever de comunicação e do dever de abstenção, sempre que, no cumprimento do dever de exame que o antecede, se conclua pela existência de potenciais suspeitas.

e) Ao *Compliance Officer*:

i) Coordenar e monitorar a implementação efectiva das políticas, procedimentos e controlos adequados à gestão eficaz dos riscos de BC/FTP a que o Banco está ou possa estar exposto;

ii) Participar na definição e emissão de pareceres sobre as políticas, procedimentos e controlos destinados à prevenção do BC/FTP;

iii) Acompanhar permanentemente a adequação, suficiência e a actualidade das políticas, dos procedimentos e controlos em matéria de PC-BC/FTP, propondo as necessárias actualizações;

iv) Participar na definição, acompanhamento e avaliação da política de formação interna do Banco;

v) Assegurar a centralização de toda a informação relevante proveniente das diversas áreas de negócio do Banco;

vi) Desempenhar o papel de interlocutor das autoridades de aplicação da lei e de supervisão e fiscalização, cumprindo com a obrigação de comunicação, prevista na legislação e regulamentação em vigor, assegurando o exercício das demais obrigações neste domínio, em particular a obrigação de cooperação e prestação de informação;

vii) Apoiar na preparação e execução das avaliações de risco previstas na legislação e regulamentação vigente; e,

viii) Coordenar a elaboração dos reportes, relatórios e demais informações para as autoridades competentes em matéria de PC-BC/FTP.

f) À terceira linha de defesa:

Direcção de Auditoria Interna (DAI): monitorizar, através de avaliações periódicas e independentes, a qualidade, adequação e eficácia das políticas, procedimentos e controlos em matéria de PC-BC/FTP, devendo assegurar o acompanhamento contínuo das deficiências identificadas, articulando, com os respectivos *owners* e restantes intervenientes no processo, os necessários esclarecimentos para a boa implementação das recomendações apresentadas.

g) À segunda linha de defesa:

Direcção de *Compliance* (DCP):

i) Assegurar a definição e implementação efectiva das políticas, procedimentos e controlos adequados à gestão eficaz dos riscos BC/FTP a que o Banco está exposto, garantindo que estes são adaptados e desenvolvidos tendo em conta a regulamentação em vigor e as melhores práticas internacionais;

ii) Acompanhar e avaliar os processos e procedimentos de controlo interno em matéria de prevenção e detecção de actividades criminosas, incluindo a PC-BC/FTP, assim como assegurar a centralização da informação e as comunicações legalmente devidas, neste âmbito, às autoridades competentes, designadamente a Unidade de Informação Financeira (UIF);

iii) Estabelecer procedimentos para identificação e avaliação do risco de BC/FTP, monitorização do Sistema de Controlo Interno de PC-BC/FTP, avaliação da eficácia e adequação dos recursos materiais e humanos à sua disposição e desenvolver os planos de formação anuais para os colaboradores que desempenham funções relevantes neste domínio.

h) À primeira linha de defesa:

Unidades de Negócio e de Suporte:

i) Garantir o cumprimento das normas legais e regulamentares associadas às suas áreas de actuação e demonstrar conhecimento e controlo efectivo na adesão e adequação das mesmas;

ii) Disponibilizar informação relevante para identificação e gestão do risco de BC/FTP, de forma total, livre e incondicional;

iii) Desenvolver acções de controlo, no âmbito da sua esfera de actuação para assegurar que os colaboradores desempenham adequadamente as suas funções, analisando eventuais desvios face aos objectivos estabelecidos, mantendo canais de comunicação apropriados e suficientes e garantindo que os riscos de BC/FTP estão devidamente identificados;

iv) Assegurar a manutenção da base de dados de clientes, promovendo a actualização dos elementos de informação obtidos no decurso da relação de negócio;

v) Detectar e comunicar operações suspeitas pelos canais habilitados para este efeito;

vi) Colaborar com a 2.ª linha de defesa na implementação e melhoria do sistema de controlo interno no âmbito da PC-BC/FTP.

3. Abordagem ao Programa de PC-BC/FTP

O Banco implementou um programa de PC-BC/FTP para identificar, monitorizar e impedir as actividades de natureza criminosa, nos termos do disposto na Lei de Prevenção e Combate ao Branqueamento de Capitais, do Financiamento do Terrorismo e da Proliferação de Armas de Destruição em Massa, em vigor.

Este programa assenta numa Abordagem Baseada no Risco (ABR), ou seja, o Banco deve identificar e avaliar as áreas potencialmente vulneráveis ao BC/FTP, bem como definir os controlos para os diferentes riscos identificados, destacando-se quatro (4) componentes inerentes ao programa de PC-BC/FTP:

a) Modelo orgânico e funcional;

b) Políticas;

c) Processos;

d) Programa de formação e sensibilização.

4. Obrigações em Sede de PC-BC/FTP

4.1. Obrigação de Avaliação de Risco

O Banco implementa medidas adequadas para identificar, avaliar, compreender e mitigar os riscos de BC/FTP a que está ou venha a estar exposto ao nível do cliente individual, da transacção e do próprio Banco, tendo em consideração os seguintes factores:

a) Natureza, dimensão e complexidade da actividade desenvolvida pelo Banco;

b) Países ou territórios em que o Banco opera directamente ou através de terceiros pertencentes ou não ao mesmo grupo;

c) Áreas de negócio, bem como produtos e serviços;

d) Natureza do cliente;

e) Histórico do cliente;

f) Natureza, dimensão e complexidade da actividade desenvolvida pelo cliente;

g) Países ou territórios de origem do cliente, ou em que estes tenham domicílio, ou de algum modo, desenvolvam a sua actividade;

h) Forma de estabelecimento da relação de negócio;

i) Canais de distribuição dos produtos e serviços disponibilizados, bem como meios de comunicação utilizados; e,

j) Riscos identificados e comunicados pelas autoridades competentes.

O Banco deve realizar anualmente o processo de avaliação de risco institucional, tendo como referência o período compreendido entre Janeiro e Dezembro do ano transacto, devendo as avaliações serem submetidas ao Banco Nacional de Angola (BNA).

O processo supramencionado deve, para além dos factores enunciados, considerar o perfil dos accionistas, a adequação das ferramentas e aplicativos informáticos, o nível de conhecimento e de integridade dos membros do CA e dos colaboradores sobre as matérias relacionadas com o BC/FTP, atribuindo a cada factor um ponderador de risco.

As avaliações de risco devem ser adequadas às características, dimensão e complexidade do Banco e devidamente documentadas, de modo a detalhar a forma como este os identificou e avaliou, bem como aferir a qualidade dos meios e procedimentos de controlo destinados à sua mitigação.

4.1.1. Modelo de Avaliação do Risco de BC/FTP

A metodologia desenvolvida para a avaliação do risco de BC/FTP engloba quatro (4) componentes:

a) Identificação e avaliação detalhada dos riscos inerentes de BC/FTP aplicáveis ao Banco;

b) Avaliação da eficácia e eficiência do SCI do Banco em matéria de PC-BC/FTP;

c) Mapeamento dos riscos e controlos, com a determinação do risco residual e avaliação do mesmo face ao nível de tolerância definido pelo CA;

d) Definição de medidas correctivas e respectivo plano de implementação para mitigar riscos que estejam acima do nível de tolerância definido.

Com o objectivo da realização deste exercício, o Banco implementou dois modelos de suporte à avaliação do risco de BC/FTP, nomeadamente:

a) *Business Risk Assessment* (BRA): consiste na realização de uma avaliação global dos riscos de BC/FTP associados à actividade de negócio do Banco; e,

b) Matriz de Risco e Controlos (MRC) : engloba a avaliação da robustez do SCI em matérias de PC-BC/FTP face aos riscos de BC/FTP inerentes às actividades do Banco (i.e. avaliação da capacidade de mitigação efectiva desses riscos).

4.2. Obrigação de Identificação e Diligência

4.2.1. Identificação

O procedimento de identificação de clientes deve ser entendido como a verificação do conjunto de elementos necessários para o estabelecimento ou manutenção de uma relação de negócio, de acordo com as normas legais e regulamentares.

Deste modo, o Banco adopta medidas específicas para determinar a verdadeira identidade dos seus clientes e se aplicável, dos seus representantes legais e do Beneficiário Efectivo (BEF), sempre que:

a) Seja estabelecida qualquer relação de negócio ou existam suspeitas de crimes de BC-FTP;

b) Existam dúvidas quanto à autenticidade ou à conformidade dos dados de identificação dos clientes previamente adquiridos.

Adicionalmente, o Banco pode adaptar a natureza e a extensão dos procedimentos de verificação da identidade, em função dos riscos associados à relação de negócio ou à transacção ocasional;

Os elementos de identificação e os comprovativos que devem ser recolhidos previamente ao estabelecimento de uma relação de negócio ou a realização de transacções ocasionais, independentemente do risco de BC/FTP concretamente identificado, estão definidos nas *Checklists* de Abertura de Contas em vigor.

4.2.2. Diligência

O Banco implementa medidas de diligência que se traduzem num conjunto de processos que permitem obter conhecimento razoável sobre a identidade de um cliente, assim como

conservar a informação necessária para compreender a natureza do seu negócio, a sua actividade e o seu perfil de risco.

O Banco procede à adopção de medidas de diligência em função da classificação de risco de BC/FTP dos seus clientes, sendo que estas medidas correspondem aos padrões mínimos e necessários para o estabelecimento de relações de negócio com os mesmos, de acordo com o previsto no normativo legal.

As medidas de diligência devem considerar, em particular, os seguintes aspectos:

a) O período de diligência (programada ou não programada);

b) A extensão da diligência, nomeadamente:

   i) Normal — *Customer Due Diligence* (CDD);

   ii) Reforçada ou alargada — *Enhanced Due Diligence* (EDD); e

   iii) Simplificada;

c) A especificidade da diligência.

4.2.3. Classificação de Clientes

O Banco desenvolveu um Modelo de Classificação de Risco de BC/FTP aplicável a todos os clientes, aos seus representantes legais e/ou BEF, o qual, actuando em tempo real para efeitos de atribuição de nível de risco, se baseia na ponderação das características do cliente individual, conhecidas no âmbito do cumprimento da obrigação de identificação e diligência. Este modelo permite, através de um *scoring*, atribuir a cada cliente um nível de risco ajustado e diferenciado.

4.3.Obrigação de Recusa

O Banco deve recusar a abertura de conta, o início da relação de negócio ou a realização de qualquer transacção quando não obtiver:

a) Os elementos identificativos e os respectivos meios comprovativos previstos para identificação e verificação da identidade do cliente, do seu representante legal e/ou do BEF;

b) Informação sobre a estrutura de propriedade e controlo do cliente, a natureza, a finalidade da relação de negócio, a origem e destino dos fundos;

No âmbito da obrigação de recusa, o Banco deve analisar as possíveis razões para a não obtenção dos elementos, dos meios ou da informação acima referida e sempre que suspeite que a não prestação da informação está relacionada com a prática de um crime de BC/FTP deve:

a) Comunicar imediatamente à Unidade de Informação Financeira (UIF);

b) Quando aplicável, ponderar pôr termo à relação de negócio, ou em alternativa, proceder o bloqueio de qualquer movimentação enquanto a informação em falta não for disponibilizada.

4.4. Obrigação de Conservação

O Banco deve conservar, em suporte electrónico ou noutros meios que permitam a sua fácil localização e o acesso imediato, por um período de 10 (dez) anos, a contar do momento em que for efectuada a transacção ou após o fim da relação de negócio, toda a documentação produzida no ambito da relação de negócio estabelecida.

4.5.Obrigação de Comunicação

O Banco deve, por iniciativa própria, informar imediatamente a UIF sempre que saiba ou tenha razões suficientes para suspeitar que teve lugar, está em curso ou foi tentada uma operação susceptível de estar associada à prática do crime de BC/FTP ou de qualquer outro crime. Esta operação pode envolver uma única transacção ou ser parte integrante de várias transacções aparentemente vinculadas.

A informação referente às operações suspeitas, às pessoas designadas ou politicamente expostas, apenas pode ser usada em sede de um processo penal, não podendo ser revelada, em caso algum, a identidade de quem as forneceu.

4.6. Obrigação de Abstenção

Sempre que se constate que uma determinada operação evidencia fundada suspeita e seja susceptível de constituir crime, o Banco, para além do cumprimento da obrigação de identificação e diligência, medidas de diligência reforçada, deve abster-se de executar quaisquer operações relacionadas com o cliente.

Sempre que observado o cumprimento da obrigação de abstenção, o Banco deve imediatamente comunicar por escrito, ou por qualquer outro meio, à UIF, o fundamento das suas suspeições e solicitar suspensão da operação.

A UIF deve, por sua vez, pronunciar-se sobre a confirmação da suspensão da operação no 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.

Se o Banco considerar que a abstenção da execução da operação não é possível ou que, após consulta à UIF, possa ser susceptível de prejudicar a prevenção ou a futura investigação do BC/FTP, a referida operação pode ser realizada, devendo o Banco fornecer, de imediato, à UIF as informações respeitantes à operação.

4.7.Obrigação de Cooperação e Prestação de Informação

O Banco deve prontamente cooperar e prestar informação à UIF, às autoridades de supervisão e de fiscalização e, quando por estas solicitadas, fornecer as informações sobre operações realizadas pelos clientes e apresentar os documentos relacionados.

O Banco implementa soluções informáticas e instrumentos para que, prontamente e integralmente, possa responder aos pedidos de informação apresentados pela UIF e pelas demais entidades competentes, destinados a determinar se mantêm ou mantiveram, nos últimos 10 (dez) anos, relações de negócio com uma determinada pessoa singular ou colectiva e qual a natureza dessas relações.

Sempre que tiver início um processo de investigação formal, o Banco deve cooperar e fornecer todos os dados solicitados pelas autoridades judiciárias e policiais competentes.

4.8.Obrigação de Sigilo

O Banco, os membros dos órgãos sociais, as pessoas que exercem funções de gestão, colaboradores, mandatários e outras pessoas que lhe prestam serviço a título permanente, temporário ou ocasional, não podem revelar ao cliente ou a terceiros, que transmitiram as comunicações legalmente devidas ou que está em curso uma investigação sobre uma determinada operação ou actividade.

4.8.1. Protecção na Prestação de Informação

As informações prestadas, no cumprimento das obrigações previstas nesta política, pelo Banco ou colaboradores às autoridades competentes não constituem violação de qualquer

obrigação de segredo imposta por via legislativa, regulamentar ou contratual, nem implicam, para quem as preste, responsabilidade disciplinar, civil ou criminal.

O Banco abstém-se de quaisquer ameaças ou actos hostis e, em particular, de quaisquer práticas laborais desfavoráveis ou discriminatórias contra quem preste informações, documentos ou quaisquer outros elementos, não podendo tal prestação de informação, por si só, servir de fundamento para promoção, pelo Banco, de qualquer procedimento disciplinar, civil ou criminal relativamente ao autor da comunicação, excepto se as mesmas forem deliberadas e manifestamente infundadas.

4.9.Obrigação de Controlo

O Banco adopta um conjunto de políticas, procedimentos e controlo internos adequados à gestão dos riscos de BC/FTP e ao cumprimento das normas legais e regulamentares nesta matéria. Estas políticas, procedimentos e controlos devem compreender:

a) A definição de um modelo de gestão de risco eficaz, com práticas adequadas à identificação, avaliação e mitigação dos riscos de BC/FTP;

b) A definição de critérios exigentes na contratação de colaboradores, bem como a definição de programas de formação contínua adequados;

c) A existência de uma estrutura de controlo interno independente para testar o sistema de PC-BC/FTP;

d) A implementação de um sistema de controlo de conformidade com a designação de um responsável pelo seu cumprimento ao nível da direcção.

O Banco mantém uma cultura de responsabilidade e de *compliance*, pelo que dispõe de um canal específico, independente e confidencial, que assegura internamente, de forma adequada, a recepção, o tratamento e o arquivo das comunicações de irregularidades relacionadas com eventuais violações à Lei de Prevenção e Combate ao Branqueamento de Capitais, do Financiamento do Terrorismo e da Proliferação de Armas de Destruição em Massa e irregularidades relacionadas com a integridade do Banco, alegadamente cometidas por membros dos órgãos sociais, por colaboradores ou outras pessoas, no âmbito da prestação de serviços.

4.10. Obrigação de Formação

O Banco dispõe de um Plano de Formação adequado às funções concretamente exercidas pelos colaboradores e membros dos órgãos sociais. Este visa assegurar o cumprimento das obrigações a que o Banco está adstrito em matéria de *compliance* e, em particular, de PC-BC/FTP, pelo que permite um conhecimento pleno, permanente e actualizado sobre:

a) O enquadramento jurídico vigente e aplicável;

b) As políticas, procedimentos e os controlos definidos e implementados pelo BNI para gestão eficaz do risco de *compliance* e, em particular, de BC/FTP ;

c) As orientações, recomendações e informações emanadas pelas autoridades judiciárias, policiais, de supervisão ou pelas associações representativas do sector;

d) As tipologias, tendências e técnicas associadas ao BC/FTP;

e) As vulnerabilidades dos produtos e serviços disponibilizados pelo Banco e os riscos específicos emergentes;

f) Os riscos reputacionais e as consequências de natureza contra-ordenacionais decorrentes da inobservância dos deveres preventivos do BC/FTP;

g) As responsabilidades profissionais específicas em matéria de PC-BC/FTP e, em especial, os procedimentos associados ao cumprimento dos deveres preventivos e detectivos.

O Banco mantém um registo permanentemente actualizado das participações dos colaboradores e membros dos órgãos sociais nas acções de formação, bem como a conservação da cópia dos documentos ou registos relativos às sessões ministradas por um período de cinco (5) anos.

4.11. Obrigação Específica de Exame e Comunicação

O Banco presta especial atenção às relações de negócio e às transacções com clientes de ou para países que não aplicam ou aplicam de forma insuficiente os requisitos internacionais em matéria de PC-BC/FTP, reduzindo a escrito os resultados do exame efectuado a essas relações de negócio e transacções.

Sempre que as operações revelem especial risco de BC/FTP, nomeadamente quando se relacionem com um determinado país ou jurisdição sujeita à contramedidas adicionais decididas pelo Estado Angolano, por organizações internacionais competentes ou por autoridades de supervisão e fiscalização, o Banco deve imediatamente comunicá-las à UIF, quando o seu montante for superior, em moeda nacional ou outra moeda, ao equivalente a USD 5 000,00 (cinco mil dólares dos Estados Unidos).

Se, em resultado do exercício da obrigação de exame, o Banco decidir não proceder à comunicação às autoridades competentes de uma operação que tenha sido objecto de análise, deve fazer constar do documento ou registo:

a) Os fundamentos da decisão de não comunicação, com inclusão, pelo menos, da informação tão completa quanto possível, sobre as operações comunicadas e outras que com ela estejam ou possam estar relacionadas, bem como dos motivos que sustentam a inexistência de factores concretos de suspeição;

b) A referência a quaisquer eventuais contactos informais estabelecidos com aquelas autoridades, com indicação das respectivas datas e dos meios de comunicação utilizados.

5. Disposições Finais

5.1. Conflitos de Interesses

À prevenção e gestão de situações que configurem reais ou potenciais conflitos de interesses é aplicável a Política de Prevenção, Identificação e Gestão de Conflitos de Interesses em vigor no Banco.

5.2. Avaliação

Compete à Direcção de Auditoria Interna (DAI) avaliar o cumprimento das regras desta política e demais normativos internos complementares a esta em termos de matérias éticas, deontológicas e prudenciais.

5.3. Incumprimento

O incumprimento do estabelecido nesta política constitui violação grave dos deveres de conduta e, em consequência, é susceptível de aplicação de medidas disciplinares, sanções contratuais ou eventual responsabilidade criminal.

5.4. Revisão e Actualização

Esta política deve ser revista sempre que necessário ou sempre que se verifiquem alterações relevantes no mercado, na orientação estratégica do Banco e/ou na regulamentação emitida pelos órgãos de supervisão.

Compete à DCP elaborar e manter actualizada a presente política, sujeitando-a à apreciação da Comissão de Auditoria e Controlo Interno (CACI), ficando esta responsável pela submissão desta e das propostas de revisão à aprovação do CA.

5.5. Divulgação e Acesso

Esta política deve ser divulgada a todos os colaboradores através dos órgãos de comunicação interna definidos e está disponível para consulta no sítio de Internet do Banco.

Todos os exemplares impressos são considerados cópias não controladas.

A presente Política entra em vigor no dia seguinte ao da sua divulgação.

Conselho de Administração
BNI — Banco de Negócios Internacional

Anexo I — Conceitos e Definições

a) *Adverse Media* (ou notícia negativa): é definida como qualquer tipo de informação desfavorável em matéria de PC-BC/FTP, identificada em uma ampla variedade de notícias consideradas como de fontes de domínio público;

b) Beneficiário Efectivo (BEF):

i) A pessoa ou pessoas singulares que:

- 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;
- 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;
- Detêm em última instância, a propriedade ou o controlo directo ou indirecto de 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;
- Têm o direito de exercer ou que exerçam influência significativa ou que controlam a sociedade independentemente do nível de participação.

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

- Beneficiem do seu património quando os futuros beneficiários já tiverem sido determinados;
- 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;
- Exerçam controlo do património da pessoa colectiva.

c) Branqueamento de Capitais (BC): é o processo pelo qual os autores de actividades criminosas encobrem a origem dos bens e rendimentos (vantagens) obtidos ilicitamente, transformando a liquidez proveniente dessas actividades em capitais reutilizáveis legalmente, através da dissimulação da origem ou do verdadeiro proprietário dos fundos;

d) Cliente: pessoa singular ou colectiva, nacional ou estrangeira, pública ou privada, coligada ou não, que celebra contrato de abertura de conta com o BNI a quem este coloca à disposição, produtos e serviços financeiros;

e) Colaborador: qualquer pessoa singular que, em nome ou no interesse do Banco e sob a sua autoridade ou na sua dependência, participe na execução de quaisquer operações, actos ou procedimentos próprios da actividade prosseguida por aquele, independentemente de ter com o mesmo um vínculo de natureza laboral (colaborador interno) ou não (colaborador externo);

f) *Compliance Officer*: responsável pela coordenação e monitorização da implementação do sistema de prevenção de branqueamento de capitais, do financiamento do terrorismo e da proliferação de armas de destruição em massa, incluindo os respectivos procedimentos de controlo interno, bem como pela centralização da informação e comunicação de operações susceptíveis de branqueamento de capitais, do financiamento do terrorismo e da proliferação de armas de destruição em massa à Unidade de Informação Financeira (UIF) e outras autoridades competentes;

g) Conflito de Interesses: ocorre quando um colaborador, pelo exercício das suas funções, possa intervir ou influenciar uma decisão ou processo decisório, em que tenha directa ou indirectamente interesse pessoal, de que possa retirar potencial vantagem para si próprio, para familiares, amigos ou conhecidos;

h) *Customer Due Diligence* (CDD — diligência devida do cliente): é o procedimento padrão de diligência para entender e avaliar os riscos colocados por um cliente ou as suas transacções;

i) *Enhanced Due Diligence* (EDD — melhoria das diligências): é uma diligência profunda em relação a um Cliente (ou partes relacionadas), geralmente adoptada quando é identificado um factor de risco elevado;

j) Entidade: qualquer pessoa singular ou colectiva, bem como qualquer acordo sem personalidade jurídica, incluindo clientes e não clientes.

k) Financiamento do Terrorismo e da Proliferação de Armas de Destruição em Massa (FTP): recolha de fundos destinados ao terrorismo e/ou a proliferação de armas de destruição em massa, independentemente da licitude dos referidos fundos;

l) *Know Your Customer* (KYC — conhecer o seu cliente): é um repositório estruturado de informação sobre o cliente ou entidade;

m) Operações Suspeitas: todo e qualquer acto de um cliente que indicie ou configure a tentativa de ocultar ou dissimular a natureza, origem, localização ou propriedade de bens, direitos ou valores oriundos directa ou indirectamente da prática de um crime, com vista a dar-lhes uma aparência lícita;

n) Origem da Riqueza: significa a origem do património total do cliente (por exemplo, herança, poupanças);

o) Origem dos Fundos: significa a origem dos fundos envolvidos na relação comercial ou transacção ocasional, incluindo tanto a actividade que gerou os fundos (por exemplo, o salário) como os meios utilizados para os transferir;

p) Pessoas Politicamente Expostas (PPE): 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;

q) Transacção Ocasional: qualquer transacção pontual que seja realizada pelas instituições financeiras fora do âmbito de uma relação de negócio previamente estabelecida.

Anexo II — Enquadramento Legal e Regulamentar

Esta política está alinhada com as disposições legais e regulamentares aplicáveis em Angola, nomeadamente:

a) Lei n.º 12/24, de 4 de Julho — altera a Lei n.º 38/20, de 11 de Novembro (Lei que aprova o Código Penal Angolano);

b) Lei n.º 11/24, de 4 de Julho — altera a Lei n.º 5/20, de 27 de Janeiro (Lei de Prevenção e Combate ao Branqueamento de Capitais, do Financiamento do Terrorismo e da Proliferação de Armas de Destruição em Massa);

c) Lei n.º 10/24, de 3 de Julho — altera a Lei n.º 13/15, de 19 de Junho (Lei da Cooperação Judiciária Internacional em Matéria Penal);

d) Lei n.º 9/24, de 3 de Julho — altera a Lei n.º 19/17, De 25 De Agosto (Lei sobre a Prevenção e o Combate ao Terrorismo);

e) Lei n.º 14/21, de 19 de Maio — Lei do Regime Geral das Instituições Financeiras;

f) Lei n.º 38/20, de 11 de Novembro — Código Penal Angolano;

g) Lei n.º 05/20, de 27 de Janeiro — Lei de Prevenção e Combate ao Branqueamento de Capitais, do Financiamento ao Terrorismo, e da Proliferação de Armas de Destruição em Massa;

h) Lei n.º 19/17, de 25 de Agosto — Lei sobre a Prevenção e o Combate ao Terrorismo;

i) Lei n.º 13/15, de 19 Junho — Lei de Cooperação Judiciária Internacional em Matéria Penal;

j) Lei n.º 01/12 de 12 de Janeiro — Lei sobre a Designação e Execução de Actos Jurídicos Internacionais;

k) Lei n.º 22/11, de 17 de Junho — Lei da Protecção de Dados Pessoais;

l) Aviso n.º 02/2024 — Regras de Prevenção e Combate ao Branqueamento de Capitais e Financiamento ao Terrorismo e da Proliferação de Armas de Destruição em Massa;

m) Aviso n.º 01/2023, de 30 de Janeiro — Abertura, Movimentação e Encerramento de Contas Bancárias;

n) Aviso n.º 01/2022, de 28 de Janeiro — Código do Governo Societário das Instituições Financeiras;

o) Regulamento n.º 05/2021, de 8 de Novembro — Prevenção e Combate ao Branqueamento de Capitais, do Financiamento do Terrorismo e da Proliferação de Armas de Destruição em Massa, da Comissão do Mercado de Capitais (CMC).

6. Controlo do documento

PROPRIEDADES DO DOCUMENTO	
Nome	Política de Prevenção e Combate ao Branqueamento de Capitais, do Financiamento do Terrorismo e da Proliferação de Armas de Destruição em massa (Pc-Bc/Ftp)
Data de Aprovação	01/08/2025
Data de Entrada em Vigor	29/08/2025
Disponibilização	Este documento encontra-se disponível e actualizado através do site público do Banco BNI.