

BANCO INTERNACIONAL DE MOÇAMBIQUE

Ordem de Serviço: OS0202 - Versão nº 11 - Em vigor desde 18-11-2025

Título: Políticas de Combate ao Branqueamento de Capitais e Financiamento ao Terrorismo

Aplicável a: BIM - Banco Internacional de Moçambique, S.A.

Atribuído a: COFF- Compliance Office

Sumário

A presente Política define os procedimentos atinentes aos deveres de prevenção e combate ao Branqueamento de Capitais, Financiamento ao Terrorismo e Financiamento da Proliferação de Armas de Destruição em Massa (BC/FT/FP).

Alterações à versão anterior

As alterações em relação à versão anterior visam alinhar os procedimentos à legislação vigente, tendo consistido nas seguintes actualizações:

- I. Actualização do sumário do normativo.
- II. Actualização da legislação aplicável ao longo do normativo, incluindo leis, avisos e decretos:
 - Substituição da Lei nº 11/2022, de 7 de Julho, pela Lei nº 14/2023, de 28 de Agosto, com as respectivas alterações introduzidas pela Lei nº 3/2024, de 22 de Março, pelo Decreto nº 53/2023, de 31 de Agosto;
 - Substituição do Aviso nº 4/GBM/2015, de 17 de Junho, pelo Aviso nº 10/GBM/2024, de 30 de Agosto;
 - Alteração do artigo 15 do Decreto nº 66/2014, de 29 de Outubro, pelo artigo 8 do Decreto nº 53/2023, de 31 de Agosto.
- III. **Na página 7, acréscimo de um novo capítulo 3 - Deveres de Avaliação do Risco**, o qual estabelece as medidas adoptadas pelo Banco para identificar, avaliar, compreender e mitigar os riscos de Branqueamento de Capitais (BC), Financiamento ao Terrorismo (FT) e Financiamento da Proliferação (FP), a que está exposto no exercício das suas actividades.
- IV. **Na página 7**, procedeu-se à reformulação, renumeração e actualização do anterior Capítulo 3 - Dever de Identificar, que passa a constituir o **Capítulo 4 - Deveres de Identificação, Verificação e Diligência**.

No âmbito desta alteração, foi removido o subponto 3.1 - *Customer Due Diligence / Know Your Customer (KYC)*, sendo o conteúdo reorganizado da seguinte forma:

“4. Deveres de Identificação, Verificação e Diligência

O Millennium Bim adopta todos os procedimentos necessários de identificação, verificação e diligência previstos na legislação e regulamentação em vigor e tem em consideração igualmente, as boas práticas internacionais nesta matéria.

A OS0203 - Política de Identificação, Aceitação e Diligência de Clientes, define as políticas para o cumprimento destes deveres, incluindo entre outros tópicos, as medidas de diligência simplificada e reforçada adoptadas pelo Banco.

- V. Na página 9, no **Capítulo 5. Dever de Vigilância Contínua**, foi efectuada a actualização dos dados que o Banco solicita aos clientes no âmbito da mitigação dos riscos BC/FT/FP.

As actualizações incidem sobre os elementos de informação requeridos para assegurar uma monitorização eficaz e contínua da relação de negócio, incluindo:

- a) Natureza e detalhes do negócio, da ocupação ou do emprego;
- b) Actualização permanente do domicílio, em função do risco do cliente;
- c) Documentação actualizada, no âmbito dos pontos 3.3.2 (Elementos a obter) e 3.3.3. (Qualidade dos Documentos Exigíveis) da OS0203-Política de Identificação, Aceitação e Diligência de Clientes;
- d) Origem dos fundos a serem usados na relação de negócio;
- e) Proveniência dos rendimentos iniciais e contínuos;
- f) Relações existentes entre os signatários e os respectivos beneficiários efectivos.

- VI. Ainda na página 9, foi inserido o **Capítulo 6 - Dever de Actualização de Dados**, o qual estabelece que o Banco deve realizar diligências e procedimentos periódicos com o objectivo de assegurar a actualidade, exactidão e completude das informações que detenha ou deva deter relativamente a:

- **Elementos identificativos de clientes, representantes e beneficiários efectivos**, bem como todos os documentos, dados e informações obtidos no exercício dos deveres de identificação e diligência;
- **Outros elementos de informação exigidos pela legislação em vigor**, aplicáveis ao contexto da prevenção e combate ao Branqueamento de Capitais, Financiamento ao Terrorismo e Financiamento da Proliferação.

- VII. Na página 10, actualização do capítulo 7. **Dever de Exame**, tendo sido efectuada o acréscimo do ponto 4 e a actualização dos pontos 6 e 7, associados à alínea g), passando a constar com a seguinte redacção:

- 4. O local de origem e de destino das operações;
- 5. Meios de pagamento utilizados;
- 6. Natureza, actividade, padrão operativo, a situação económico-financeira e perfil dos intervenientes;
- 7. Tipo de transacção, produto, estrutura societária ou centro de interesses colectivos sem personalidade jurídica que possa favorecer especialmente o anonimato.

- VIII. Na página 13, no **Capítulo 8 - Dever de Abstenção**, foi actualizada a redacção do primeiro parágrafo e inserido um terceiro parágrafo, passando a constar da seguinte forma:

“No âmbito de dever de abstenção, sempre que se constate que uma determinada operação evidencia fundada suspeita de constituir crime, nos termos do disposto na Lei nº 14/2023, de 28 de Agosto, o Banco, deve abster-se de executar quaisquer operações relacionadas com o pedido do cliente. O Banco, deve informar de imediato ao Ministério Público (PGR - Procuradoria-Geral da República) e ao GIFiM (Gabinete de Informação Financeira de Moçambique) de que se absteve de executar a operação, podendo o Ministério Público determinar a suspensão da execução da operação suspeita, notificando, para o efeito, o Banco.”

Nos casos do cumprimento do dever de abstenção, não poderá, em caso algum, ser revelada ao cliente a comunicação de operação suspeita à PGR e ao GIFiM.

IX. **Nas páginas 13 a 14**, foram inseridos dois novos capítulos 10 e 11:

➤ **Capítulo 10. Política de Não-Aceitação**

Este capítulo estabelece que o Banco deve rejeitar a abertura ou manutenção de relações comerciais que apresentem riscos elevados ou incompatíveis com os deveres de prevenção consagrados na legislação em vigor, sem prejuízo da articulação com os demais deveres legais aplicáveis.

➤ **Capítulo 11 - Dever de Cumprimento de Medidas Restritivas**

O Banco deve dispor de mecanismos permanentes, rápidos e seguros que assegurem a execução imediata, plena e eficaz das medidas restritivas, incluindo o bloqueio ou suspensão de operações nos casos de cumprimento das obrigações de congelamento decorrentes de sanções financeiras impostas por autoridades nacionais ou internacionais.

X. **Na página 18**, no Capítulo 17. Bancos Correspondentes, acréscimo do último parágrafo com o seguinte texto:

“Os princípios orientadores da aprovação, monitoria e controlo aplicáveis ao estabelecimento ou manutenção de relações de banca de correspondência encontra-se devidamente descrita na OS0234 - Política de Selecção e Relacionamento com Bancos Correspondentes.”

XI. **Na página 19**, no Capítulo 18. Auditoria Interna, actualização da sublínea (vii) passando para o seguinte:

“(vii) Rever, em especial, os processos de *due diligence* e de KYC realizados para clientes, produtos, serviços ou canais de distribuição identificados como de alto risco; Verificar o tratamento diligente dos alertas de BC/FT/FP, e se os alertas gerados são prontamente encerrados com uma avaliação de risco adequada.

XII. **Na página 20**, actualização do Anexo I - Modelos de Atribuição do Risco AML.

XIII. **Nas páginas 22 a 24**, actualização do Anexo II - GLOSSÁRIO.

Índice

1.ENQUADRAMENTO	5
2. OBJECTIVO, ÂMBITO E PROCESSO DE REVISÃO.....	5
3. DEVERES DE AVALIAÇÃO DO RISCO	6
4. DEVERES DE IDENTIFICAÇÃO, VERIFICAÇÃO E DILIGÊNCIA	7
4.1. Abordagem Baseada no Risco (<i>Risk Based Approach</i>)	7
5. DEVER DE VIGILÂNCIA CONTÍNUA	8
6. DEVER DE ACTUALIZAÇÃO DE DADOS	8
7. DEVER DE EXAME	9
8. DEVER DE ABSTENÇÃO.....	12
9. DEVER DE RECUSA.....	12
10.POLÍTICA DE NÃO-ACEITAÇÃO	13
11.DEVER DE CUMPRIMENTO DE MEDIDAS RESTRITIVAS.....	13
12.DEVER DE COMUNICAR OPERAÇÕES SUSPEITAS.....	14
13.DEVER DE SIGILO PROFISSIONAL	15
14.DEVER DE CONSERVAÇÃO	16
15.DEVER DE COLABORAÇÃO	16
16.DEVER DE FORMAÇÃO.....	16
17.BANCOS CORRESPONDENTES	17
18.AUDITORIA INTERNA	17
19.DISPOSIÇÕES FINAIS.....	18
ANEXO I - MODELOS DE ATRIBUIÇÃO DO RISCO AML.....	20
ANEXO II - GLOSSÁRIO	22

1. ENQUADRAMENTO

A presente Ordem de Serviço tem por objectivo transmitir as principais linhas de orientação e directrizes de política geral aplicada pelo Millennium Bim.

A globalização da actividade financeira e o rápido desenvolvimento das tecnologias de informação são factores que proporcionam novas oportunidades de crescimento económico, mas que simultaneamente, aumentam o risco associado ao branqueamento de capitais (BC).

O reinvestimento dos proveitos do crime em actividades legais e a existência de operadores e organizações em conluio com estas práticas, perturbam fortemente o mercado e a sua eficiência, enfraquecendo a economia.

Por estas razões e para além das medidas usuais aplicadas contra o crime organizado, outro tipo de acções preventivas no combate ao BC foram adoptadas no sector financeiro e, recentemente, alargadas à luta contra o financiamento ao terrorismo e financiamento da proliferação de armas de destruição em massa (FT/FP) nas interligações que estes crimes tem com o sistema financeiro.

O Millennium Bim aceita de forma séria e responsável o desafio do combate ao BC/FT/FP, dedicando esforços em acções e instrumentos de combate a este crime, na convicção de que este tipo de atitude estará sempre associado aquilo que se considera ser a defesa da integridade do Banco e da sua reputação, bem como a manutenção de elevados padrões de ética profissional. O Millennium Bim dá prioridade máxima às políticas direccionadas para a prevenção do seu envolvimento ou utilização em possíveis acções de BC/FT/FP, que possam prejudicar a sua reputação e estabilidade.

Assim, o Banco adopta medidas internas, procedimentos, programas de formação e mecanismos de controlo, com vista a garantir a conformidade de todos os seus colaboradores com o enquadramento legal e regulamentar vigente nesta matéria.

2. OBJECTIVO, ÂMBITO E PROCESSO DE REVISÃO

- a) Prevenir o uso dos serviços e produtos fornecidos pelo Banco para efeitos do BC/FT/FP é um dos meios mais eficazes de oposição ao crime organizado e uma ferramenta importante na identificação e combate à actividade criminal;
- b) Tendo em conta as graves consequências do BC/FT/FP na comunidade e no sistema financeiro, o Millennium Bim 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 sobre BC/FT/FP assim como com as orientações e políticas internas do Millennium Bim nesta matéria, no sentido de prevenirem a utilização dos produtos e serviços disponibilizados pelo Grupo para efeitos de prevenção de BC/FT/FP.

↳ A presente política e os procedimentos seguintes aplicam-se a todas unidades orgânicas, em particular aos balcões do Millennium Bim. Esta política tem por objectivo descrever os deveres assumidos pelo Millennium Bim no combate e prevenção ao BC/FT/FP.

2.1. Métodos e Procedimentos de Prevenção do Branqueamento de Capitais Financiamento do Terrorismo e Financiamento de Proliferação de Armas de Destruição em Massa

- a) O Millennium Bim incorpora as melhores práticas e princípios internacionais subjacentes ao enquadramento normativo em vigor sobre a prevenção da utilização do sistema financeiro para efeitos de prevenção e combate ao BC/FT/FP, em conformidade com legislação em vigor, a par, designadamente, com as definições e conceitos resultantes da **Lei 14/2023, de 28 de Agosto com as devidas alterações introduzidas pela Lei 3/2024, de 22 de Março, Decreto 53/2023, de 31 de Agosto, e Aviso 10/GBM/2024, de 30 de Agosto;**
- b) As medidas detalhadas de natureza preventiva estão reflectidas nos diversos documentos existentes de procedimentos internos. Todas as unidades e colaboradores deverão agir de acordo com estes documentos, bem como os princípios e procedimentos normalizados neles definidos.

O presente documento é revisto numa base anual, nos termos definidos na **OS0125** sendo que, por imperativo legal ínsito na secção I do Capítulo II do Aviso **10/GBM/2024, de 30 de Agosto**. O Conselho de Administração é o órgão competente para aprovação do presente normativo e subsequentes alterações/revisões.

3. DEVERES DE AVALIAÇÃO DO RISCO

O Millennium bim adopta medidas apropriadas para identificar, avaliar, compreender e mitigar os riscos de BC/FT/FP a que estão expostas, ao nível do cliente, da transacção e da instituição, tendo em conta os seguintes factores:

- a) A natureza, dimensão e complexidade da actividade desenvolvida;
- b) Os países ou áreas geográficas em que exerce actividade, directamente ou através de terceiros, pertencentes ou não ao mesmo grupo;
- c) As áreas de negócio desenvolvidas, bem como produtos, serviços e operações disponibilizados;
- d) A natureza e histórico do cliente, incluindo a actividade por ele desenvolvida;
- e) A localização geográfica do cliente da instituição financeira, ou onde este se encontre domiciliado ou exerça a sua actividade;
- f) Os canais de distribuição dos produtos e serviços disponibilizados, bem como dos meios de comunicação utilizados no contacto com os clientes.

A avaliação do risco deve ser redigida em documento, que deve ser mantido juntamente com todas as informações de suporte e disponibilizados às autoridades de supervisão competentes.

Deve ser feita, anualmente, uma avaliação do modelo de gestão do risco e, eventualmente, propor-se alterações e ou simplificações, melhor identificadas após o cumprimento de todos os procedimentos previstos no Decreto 53/2023 de 30 de Agosto.

4. DEVERES DE IDENTIFICAÇÃO, VERIFICAÇÃO E DILIGÊNCIA

O Millennium Bim adopta todos os procedimentos necessários de identificação, verificação e diligência previstos na legislação e regulamentação em vigor, tendo igualmente em consideração as boas práticas internacionais nesta matéria.

A OS0203 - Política de Identificação, Aceitação e Diligência de Clientes, define as políticas para o cumprimento destes deveres, incluindo entre outros tópicos, as medidas de diligência simplificada e reforçada adoptadas pelo Banco.

4.1. Abordagem Baseada no Risco (*Risk Based Approach*)

- a) O Millennium Bim desenvolve um sistema de classificação de risco de BC (risco AML, conforme Anexo I) aplicável a todos os clientes, o qual actuando em tempo real para efeitos de atribuição de nível de risco, se baseia na ponderação das características do cliente, conhecidas no decurso do procedimento KYC (actividade profissional, país de residência, perfil transaccional expectável, estatuto de Pessoa Politicamente Exposta, entre outros). Este sistema permite, através de um *scoring* automatizado, atribuir a cada cliente um nível de risco ajustado e diferenciado em «baixo, médio e alto»;
- b) Foi ainda claramente definida uma política de aceitação de clientes (OS0203), que estipula os princípios orientadores sobre o tipo de clientes com que o Banco está disposto a iniciar ou manter relações comerciais, designadamente para efeitos de risco de BC (AML);
- c) Embora as orientações relativas à matéria de combate ao BC/FT/FP sejam aplicadas a todos os novos clientes, devem as mesmas ser igualmente aplicadas aos clientes existentes com base em critérios ponderados de materialidade e risco. Sendo o processo de classificação de risco AML dos clientes dinâmico, os procedimentos adequados deverão ser aplicados a todos os clientes e contas existentes conforme o risco que lhes seja atribuído ou que vejam o seu risco agravado de acordo com os critérios decididos pelo Banco, em sintonia com a legislação e regulamentação em vigor, em cada momento, relativa a esta matéria. É necessário garantir que, todas as operações em contas activas já existentes sejam continuamente monitorizadas e qualquer padrão incomum ou não adequado no funcionamento das mesmas desencadeie um processo de reavaliação da classificação do cliente com base na actualização do respectivo *due diligence*;
- d) Em consonância com o exposto, é necessário assegurar que todas as contas de empresas, partidos políticos, organizações religiosas e de caridade, fundações, *trusts*, veículos *offshore* e, entre outros, dos clientes que recorrem exclusivamente a novas tecnologias com plataformas *On-Line (Internet e Mobile Banking)* ou que mantêm sobretudo relações não presenciais e à distância, estejam sujeitas a normas ajustadas de KYC que permitam assegurar a obtenção da identidade dos seus beneficiários últimos, bem como o perfil transaccional das referidas contas;
- e) Os processos de defesa reputacional do Banco e de combate ao BC/FT/FP, enquadrados numa lógica de diferenciação e graduação do risco AML, apenas se tornam verdadeiramente eficazes com a aplicação das políticas de classificação, análise e monitorização que permitam perceber,

em permanência, o nível de risco da entidade. Nestas circunstâncias, todos os clientes do Millennium Bim são classificados tendo em conta as pontuações que constam na tabela abaixo, que obedecem os procedimentos descritos na [NP0009-Medidas de Prevenção do Crime de Branqueamento de Capitais e Financiamento ao Terrorismo](#).

Cientes Particulares e Empresas:

Pontuação de Risco Particulares	Nível de Risco
Pontuação de Score <=30	Risco Baixo
Pontuação de Score 31-90	Risco Médio
Pontuação de Score > 90	Risco Alto

5. DEVER DE VIGILÂNCIA CONTÍNUA

Os princípios de *Due Diligence* são aplicam-se não apenas aos procedimentos de identificação de clientes aquando da abertura de conta ou início de uma relação de negócio, mas também à detecção, monitorização e acompanhamento regular da relação comercial e das transacções que não sejam conformes ao seu perfil.

Deste modo, atendendo aos níveis de risco de BC/FT/FP, e de crimes conexos, o Millennium bim solicita aos clientes a seguinte informação:

- a) Natureza e detalhes do negócio, da ocupação ou do emprego;
- b) Actualização permanente do domicílio, em função do risco do cliente;
- c) Documentação actualizada, conforme os pontos 3.3.2 (Elementos a obter) e 3.3.3. (Qualidade dos Documentos Exigíveis) da [OS0203 - Política de Identificação, Aceitação e Diligência de Clientes](#);
- d) Origem dos fundos a serem utilizados na relação de negócio;
- e) Proveniência dos rendimentos iniciais e contínuos;
- f) Relações existentes entre os signatários e os respectivos beneficiários efectivos.

6. DEVER DE ACTUALIZAÇÃO DE DADOS

O Millennium bim realiza diligências e procedimentos periódicos, com o objectivo de assegurar a actualidade, exactidão e a completa informação de que já dispõe, ou que deva dispor, relativamente a:

- a) Elementos identificativos de clientes, representantes e beneficiários efectivos, bem como todos os demais documentos, dados e informações obtidas no exercício dos deveres de identificação e diligência;
- b) Outros elementos informativos previstos na legislação em vigor.

Como parte da monitorização e actualização contínuas do perfil de risco de AML dos seus clientes, o KYC é actualizado periodicamente, de acordo com o perfil de risco:

- (i) Anual para clientes com grau de risco AML Alto;
- (ii) Até 3 anos para clientes com graus de risco AML Médio e AML baixo,

Esta actualização é realizada em conformidade com o processo instituído na [NP0305 - Processo de Actualização Permanente \(on going\) de Dados de Clientes](#) e [OS0203 - Política de Identificação, Aceitação e Diligência de Clientes](#).

O Millennium Bim dispõe de várias fontes de informação sobre os seus clientes, tanto internas como externas, e actualiza regularmente esses dados, mantendo o registo de transacções recentes, contrapartes envolvidas e da sua relação com o cliente.

7. DEVER DE EXAME

Uma abordagem baseada no risco, como método utilizado pelo Millennium Bim com o intuito de identificar, gerir e mitigar o risco de BC/FT/FP, deve incluir métodos e sistemas de controlo adequados para avaliar e prevenir a concretização daquele risco.

No âmbito do dever de exame, devem, também, ser observados os procedimentos legalmente instituídos e de acordo com os procedimentos descritos na [NP0009 - Medidas de Prevenção do crime de Branqueamento de Capitais](#).

Para isso:

- a) Com base na legislação em vigor¹ e em factores que contribuem para a definição do nível de risco, o Banco Millennium Bim procede à classificação dos clientes através cálculo de grau de risco AML, considerando os diferentes factores e respectivos pesos na classificação, processo em permanente actualização e que permite a classificação de todas as entidades, numa actualização de base diária, factor preponderante e com impacto directo em todas as actividades de monitorização e controlo baseado no risco;
- b) Com base no perfil de risco AML, considerando o risco inerente de BC/FT/FP, bem como o perfil transaccional ou histórico de transacções, baseado no rendimento declarado e saldos médios verificados são gerados alertas sobre transacções diárias e sobre variações comportamentais consideradas num intervalo temporal, aquilatando da adequação das operações analisadas face ao perfil do cliente e obtendo a evidência da sua conformidade através de informações ou comprovativos documentais. Nos casos em que seja notória alguma suspeita de irregularidade ou ilícito potenciador de risco reputacional para o Banco, são emitidas recomendações e controlada a sua execução, podendo nos casos mais graves, ser decidido o encerramento da relação comercial;
- c) Com base na utilização do sistema de filtragem de entidades e transacções, em interacção directa com outros aplicativos do Banco, procede-se, em tempo real, à monitorização e análise de alertas de entidades incluídas ou constantes de listas internas e externas (listas mandatórias: e.g. Organização das Nações Unidas/União Europeia/**OFAC** - *Office of Foreign Assets Control*), com o objectivo de verificar a “coincidência” ou não, com as entidades constantes naquelas listas. No

¹ Dentre os quais se destacam a [Lei 14/2023, de 28 de Agosto com as devidas alterações introduzidas pela Lei 3/2024, de 22 de Março, Decreto 53/2023, de 31 de Agosto, e Aviso 10/GBM/2024, de 30 de Agosto](#).

- caso de se verificar a concordância exacta com alguma das entidades constantes nas listas internacionais e internas fica vedada ao Banco a execução da transacção; nos restantes casos, em que não se verifique concordância absoluta, procede-se a diligências reforçadas de controlo;
- d) O Millennium Bim mantém um investimento contínuo na formação de todos os seus colaboradores, incluindo acções presenciais, genéricas ou específicas, o fornecimento de informação regular, através da publicação de documentação relevante no *site* interno (o qual funciona como um verdadeiro repositório de legislação aplicável, normas internas e manuais de formação), programas de formação *on-job* e *e-learning* ou, ainda, através da divulgação da informação na rede interna;
 - e) O perfil de risco dos clientes é revisto sempre que se registem alterações das operações nos termos prescritos no artigo 8 do Decreto 53/2023, de 31 de Agosto. O Banco adoptou uma medida mais conservadora que prevê a revisão diária;
 - f) O objectivo do controlo implementado é proteger o Banco dos diversos riscos e monitorizar de forma permanente a execução das operações, assegurando a sua conformidade com o enquadramento legal, as políticas e procedimentos internos pré-definidos tendo em conta o perfil do cliente envolvido, permitindo a detecção de transacções com indícios ou suspeitas relevantes para efeitos de BC/FT/FP;
 - g) O Millennium Bim adoptou e implementou várias ferramentas informáticas que lhe permitem, de uma forma automática, o controle e monitorização de clientes e transacções e a identificação das transacções ou clientes que merecem uma examinação com especial cuidado e atenção, por terem determinados elementos que potencialmente se relacionem com a prática de crime de BC/FT/FP.

Todas as análises têm de ser reduzidas a escrito e relevam especialmente os seguintes elementos²:

1. Natureza, finalidade, frequência, complexidade, invulgaridade e a atipicidade da conduta, actividade ou operação;
2. Aparente inexistência de objectivo económico ou de fim lícito associado à conduta, actividade ou operação;
3. Montante, origem e destino dos fundos movimentados;
4. O local de origem e de destino das operações;
5. Meios de pagamento utilizados;
6. Natureza, actividade, padrão operativo, situação económico-financeira e perfil dos intervenientes;
7. Tipo de transacção, produto, estrutura societária ou centro de interesses colectivos sem personalidade jurídica que possa favorecer especialmente o anonimato.

As actividades de monitorização e controlo incluem, mas não estão a elas limitadas, as seguintes práticas:

1. Monitorização e controlo de clientes e transacções com nível de risco AML elevado;
2. Monitorização e controlo de transacções envolvendo países de risco AML elevado;

² Para mais detalhe sobre operações suspeitas e factores de risco consultar o manual operativo de prevenção do Branqueamento de capitais e Financiamento ao Terrorismo.

3. Monitorização e controlo de transacções complexas e/ou extraordinárias;
 4. Monitorização da consistência entre as transacções e a informação recolhida sobre a actividade do cliente, perfil de risco e património financeiro numa base permanente. Esta actividade envolve não só transacções pontuais (alertas diários) mas também a análise temporal do perfil transaccional do cliente em termos de montantes médios e quantidade de transacções executadas (alertas mensais);
 5. Controlo, por meios informáticos, de transacções que excedam um valor pré-determinado (por nível de risco do cliente) e se as mesmas são consistentes com o perfil do cliente;
 6. Monitorização e controlo de transacções pontuais relacionadas que, no seu todo, excedam o limite legal requerido;
 7. Monitorização de transacções ocasionais fraccionadas que no seu conjunto representam valores iguais ou superiores a 900.000,00 MT (novecentos mil Meticais);
 8. Monitorização de transacções ocasionais ou depósitos realizados por terceiros;
 9. Monitorização e controlo de transacções envolvendo entidades sujeitas a sanções e embargos diversos, constantes nas listas de entidades suspeitas emitidas pela Organização das Nações Unidas, União Europeia e *Office of Foreign Assets Control* (com o objectivo do controlo do cumprimento dessas restrições decretadas internacionalmente), assim como listas de jurisdições consideradas *offshore*, listas de jurisdições que integram o *Corruption perception index*, listas internas, impedindo/restringindo transacções ou obrigando a *Enhanced Due Diligence*. Neste âmbito, o Millennium Bim define prioridades de actuação em tempo real, de acordo com o motivo que determinou a “filtragem” da operação;
 10. Controlo da conclusão e actualização da informação e documentos do cliente que deverão ser mantidos em suporte de papel ou informático, assim como informação adicional que deverá ser incluída em transferências electrónicas de fundos;
 11. Controlo de transacções apresentadas por meios não fidedignos ou de forma não presencial.
- h) Independentemente dos critérios supramencionados e qualquer que seja o nível de risco *AML* do cliente, do país envolvido na transacção ou da complexidade e periculosidade da mesma, deve ser dada especial atenção a todas as condutas e/ou actividades cujos elementos caracterizadores possam agravar o risco ou susceptibilidade de relacionamento com os crimes de BC/FT/FP, devendo ser recolhidas informações e evidências documentais, da conformidade e do racional económico das transacções submetidas a análise;
- i) A actividade de monitorização e controlo, tem início nos balcões, que num 1º momento analisam as transacções de limiar legal ou superior para posterior validação pelos elementos que integram o COFF, os quais têm acesso a qualquer tipo de informação do Millennium Bim. Na sequência das acções de monitorização e controlo são emitidas, sempre que se revele apropriado, recomendações dirigidas às unidades orgânicas do Millennium Bim, as quais merecem o devido acompanhamento para efeitos de controlo de execução.

8. DEVER DE ABSTENÇÃO

No âmbito de dever de abstenção, sempre que se constate que uma determinada operação evidencia fundada suspeita de constituir crime, nos termos do disposto na Lei nº 14/2023, de 28 de Agosto, o Banco, deve abster-se de executar quaisquer operações relacionadas com o pedido do cliente. O Banco, deve informar de imediato ao Ministério Público (PGR - Procuradoria-Geral da República) e ao GIFiM (Gabinete de Informação Financeira de Moçambique) de que se absteve de executar a operação, podendo o Ministério Público determinar a suspensão da execução da operação suspeita, notificando, para o efeito, o Banco.

As entidades acima referidas têm a prerrogativa de determinar a suspensão da execução da operação suspeita, notificando ao Banco no prazo de 5 dias uteis para o efeito.

No caso do Banco, após consulta à PGR e ao GIFiM, considerar que a abstenção pode prejudicar a prevenção e futura investigação dos crimes previstos na Lei acima mencionada, a operação pode ser realizada, devendo o Banco, fornecer, de imediato, as entidades consultadas (PGR/GIFiM), as informações respeitantes à operação.

Nos casos do cumprimento do dever de abstenção, não poderá, em caso algum, ser revelada ao cliente a comunicação de operação suspeita à PGR e ao GIFiM.

O Millennium Bim cumprirá qualquer instrução emitida pelas entidades competentes, nomeadamente a PGR e o GIFiM por se mostrarem mandatarias.

9. DEVER DE RECUSA

No cumprimento do dever de recusa imposto pela legislação nacional vigente³, o Millennium Bim recusa o estabelecimento de uma relação de negócio, ou cessa uma relação de negócio já existente, sempre que:

1. Não sejam declarados pelo cliente todos os elementos de identificação requeridos por Lei⁴;
2. Não sejam entregues todos os documentos comprovativos dos elementos de identificação declarados⁵;
3. Existam dúvidas sobre a autenticidade dos documentos apresentados e nas diligências efectuadas não se consiga certificar a autenticidade dos mesmos⁶;
4. Não sejam declarados os beneficiários efectivos ou dados os mesmos elementos de identificação e documentos que o comprovem sobre estes⁷;
5. Existam suspeitas de que as operações, independentemente do seu valor, ou finalidade da conta,

³ Artigos 41.º da Lei nº 14/2023, de 28 de Agosto, artigo 21 do Decreto 53/2023, de 31 de Agosto, e, artigo 44 do Aviso 10/GBM/2024, de 30 de Agosto;

⁴ Definidos no artigo 10.º do Decreto nº 53/2023, de 31 de Agosto;

⁵ Definidos no artigo 11.º do 53/2023, de 31 de Agosto

⁶ Conforme artigo 12.º do Decreto nº 53/2023, de 31 de Agosto

⁷ Conforme artigos 15º, 18º, 19º da Lei 14/2023, de 28 de Agosto, 13.º do Decreto nº 53/2023, de 31 de Agosto e 36º do Aviso 10/GBM/2024, de 30 de Agosto;

estejam relacionadas como crime de BC/FT/FP⁸.

Sempre que exerce o dever de Recusa, é obrigatório o envio de comunicação ao GIFiM⁹.

10. POLÍTICA DE NÃO-ACEITAÇÃO

O estabelecimento de qualquer relação de negócio no Millennium bim obedece estritamente aos requisitos legais e regulamentares em vigor.

Nestes termos, o Millennium bim deve rejeitar, sem prejuízo e em articulação com os deveres de prevenção consagrados na legislação em vigor, sempre que se verifique:

- a) Contrapartes cuja reputação, segundo fontes credíveis, que esteja associada a actividades de natureza criminal ou cuja actividade torne inviável ou de difícil comprovação, o conhecimento da origem do património injustificado;
- b) Contrapartes que, no processo negocial, recusem a entrega de informação ou documentação considerada necessária para o cumprimento cabal das obrigações legais e regulamentares;
- c) Entidades culturais de fachada, ou entidades que exerçam actividade própria ou equivalente à de uma entidade cultural, constituídas em país ou jurisdição onde não disponham de presença física que envolva uma efectiva direcção e gestão, não sendo considerada presença física a mera existência de um agente local ou funcionários subalternos.

11. DEVER DE CUMPRIMENTO DE MEDIDAS RESTRITIVAS

Uma medida restritiva consiste numa restrição temporária do exercício de um determinado direito, através da imposição de uma proibição ou de uma obrigação, aprovada pelo Conselho de Segurança da Organização das Nações Unidas - ONU (Lista Internacional), Procurador-Geral da República (Lista Nacional) ou outras entidades competentes para o efeito. As medidas restritivas devem ser implementadas de imediato e sem demora¹⁰.

As Sanções Financeiras Específicas (SFE) da ONU abrangem o congelamento de activos e as proibições. Estas sanções visam impedir que fundos ou outros activos sejam disponibilizados, directa ou indirectamente, em benefício de pessoas e entidades designadas associadas ao terrorismo ou a actividades terroristas. O principal objectivo das Nações Unidas quando impõem sanções à terroristas é interromper as actividades financeiras de terroristas e organizações terroristas. Ao congelar activos e impor proibições (sanções), estas impedem a sua capacidade de levar a cabo ataques, adquirir armas ou operar eficazmente.¹¹

De acordo com o artigo 117 do Aviso 10/GBM/2024:

⁸ Conforme o artigo 24 do Decreto 53/2023, de 31 de Agosto;

⁹ Nos termos da al. d) do artigo 41 da Lei nº 14/2023, de 28 de Agosto.

¹⁰ Vide anexo 2 (Glossário).

¹¹ Despacho nº 1 /GIFiM-GDG/120.1/2025, de 22 de Agosto.

1. Para cumprimento do disposto na legislação relativa ao BC/FT/FP, o Banco deve dispor de mecanismos permanentes, rápidos e seguros que garantam a execução imediata, plena e eficaz das medidas restritivas, permitindo, pelo menos:
 - a) A detecção de quaisquer pessoas ou entidades identificadas em medidas restritivas;
 - b) O bloqueio ou a suspensão da realização de operações ou conjunto de operações, quando a instituição financeira deva dar cumprimento às obrigações de congelamento decorrentes das sanções financeiras; e
 - c) A existência de canais de comunicação e procedimentos fiáveis, seguros e eficazes, que garantam a adequada execução do dever de comunicação e assegurem a existência de uma estreita cooperação com as autoridades competentes nacionais.
2. O Banco deve monitorar, através de avaliações periódicas e independentes, o correcto funcionamento dos meios e mecanismos implementados, destinados a assegurar o cumprimento das medidas restritivas.
3. Compete ao Oficial de Comunicação de Operações Suspeitas (OCOS) Coordenador:
 - a) Garantir o conhecimento imediato e pleno e a actualização permanente das listas de pessoas e entidades, emitidas ou actualizadas ao abrigo das medidas restritivas;
 - b) Acompanhar, em permanência, a adequação, a suficiência e a actualidade dos meios e mecanismos destinados a assegurar o cumprimento das medidas restritivas;
 - c) Cumprir as obrigações de notificar previamente, de comunicar e de realizar pedidos prévios de autorização para a execução de transferências de fundos;
 - d) Monitorar à execução das medidas de congelamento e o registo das mesmas;
 - e) Cumprir o dever de comunicação;
 - f) Denunciar as situações que configurem violação; e
 - g) Desempenhar o papel de interlocutor com as autoridades competentes nacionais, assegurando o cumprimento do dever de colaboração.
4. O cumprimento dos deveres previstos nas alíneas c) a f) do número anterior deve constar de documento ou registo escrito e estão sujeitas ao dever de conservação;
5. Sempre que o Banco decida não proceder à execução das medidas restritivas, devem fazer constar de documento ou registo escrito, em conformidade com o disposto no número anterior:
 - a) Os fundamentos da decisão de não execução; e
 - b) A referência a quaisquer eventuais contactos informais que, no processo de tomada de decisão, tenham sido estabelecidos com as autoridades competentes, com indicação das respectivas datas e meios de comunicação utilizados.

12. DEVER DE COMUNICAR OPERAÇÕES SUSPEITAS

A monitorização e controlo apropriados de clientes e transacções é uma actividade fundamental utilizada pelo Millennium Bim na detecção, identificação e acompanhamento de transacções ou actividades atípicas

e/ou potencialmente suspeitas.

Havendo a suspeita fundada de que um cliente ou potencial cliente está a usar ou pretende usar os produtos ou serviços fornecidos pelo Millennium Bim para branquear fundos provenientes de actividade ilícita, financiamento ao terrorismo **ou financiamento da proliferação de armas de destruição em massa**, o Millennium Bim tomará todas as medidas necessárias para assegurar o integral cumprimento da legislação existente sobre a matéria.

O normativo interno do Millennium Bim ([NP0009 - Medidas de Prevenção do Crime de Branqueamento de Capitais e Financiamento ao Terrorismo](#)), define os procedimentos a serem adoptados pelas várias Unidades Orgânicas, no caso de serem detectadas transacções ou actividades que se devam considerar suspeitas. Estas transacções ou actividades serão sempre reportadas pelos colaboradores ou respectivas áreas ao OCOS **Coordenador através da Equipa de Reporte (OCOS)**, órgão ao qual compete a sua análise de forma aprofundada.

A conferência *AML do Compliance*, constituído no seio do “*AML/CFT & Transaction Monitoring*” avalia os processos analisados e decide a existência de fundamento para a comunicação de possíveis transacções suspeitas.

Neste contexto, as transacções alvo de dever de exame nas quais:

- a) Existam suspeitas ou motivos razoáveis para suspeitar que fundos ou bens são produtos de actividade criminosa, ou com esta estão relacionados;
- b) Existam indícios de os referidos fundos serem utilizados para o financiamento do terrorismo;
- c) Exista o conhecimento de um facto ou de uma actividade que possa indiciar o crime de BC/FT/FP são comunicadas pelo Millennium Bim às autoridades competentes de acordo com os procedimentos legalmente instituídos e de acordo com os procedimentos descritos na [NP0009 - Medidas de Prevenção do crime de Branqueamento de Capitais](#).

Adicionalmente, o Millennium Bim comunica todas as transacções em numerário, sejam realizadas de forma única ou de forma fraccionada:

- A. Todas as transacções em numerários iguais ou superiores a 250.000,00 MZN (duzentos e cinquenta mil meticais) ou equivalente contravalor;
- B. Todas as transacções de valor igual ou superior a 750.000,00 MZN (setecentos e cinquenta mil meticais) ou equivalente contravalor.

13. DEVER DE SIGILO PROFISSIONAL

É expressamente proibido a qualquer colaborador do Millennium Bim, titular de órgão directivo ou de gestão, bem como a qualquer outra pessoa que exerça funções ao serviço do Banco revelar ao cliente ou a terceiros, seja a que título for, a comunicação de transacções suspeitas referidas no ponto anterior, qualquer facto ou dado relativo às contas que se encontram sob monitoramento para determinar as transacções suspeitas bem como qualquer informação de que se encontra em curso uma investigação

criminal.

Esta obrigação também se aplica a qualquer troca de correspondência entre as autoridades de supervisão e o Millennium Bim.

A violação deste dever é punível nos termos previstos na lei. Não constitui violação do dever enunciado acima, a divulgação de informações legalmente devidas às autoridades de supervisão.

14. DEVER DE CONSERVAÇÃO

Todos os registos e evidências documentais cuja conservação é exigida por imposição legal são mantidos em diversos suportes, pelo prazo legalmente estipulado de 10 (dez) anos, contados a partir da data do término da relação de negócio e do encerramento da conta, no que respeita aos registos de diligência relativos à clientela.

15. DEVER DE COLABORAÇÃO

O Millennium Bim presta colaboração às autoridades judiciais competentes, entidade responsável pela Segurança do Estado, bem como ao GIFiM, sempre que solicitada a sua colaboração, fornecendo informações sobre operações realizadas, pelos seus clientes ou apresentando documentos relacionados com as respectivas operações, bens, depósitos ou quaisquer outros valores à sua guarda.

16. DEVER DE FORMAÇÃO

- a) O objectivo da formação do Millennium Bim em BC/FT/FP é, não só, assegurar a conformidade do Millennium Bim com o enquadramento legal, garantindo formação adequada e periódica aos seus gestores e colaboradores, para melhorar o conhecimento de operações e acções que possam estar ligadas ao BC/FT/FP, instruí-los sobre os procedimentos que devem adoptar, mas também desenvolver uma cultura de *compliance* aumentando o sentido de responsabilidade de todos os colaboradores relativamente às políticas, procedimentos e abordagem baseada no risco (*risk based approach*) que o Millennium Bim preconiza;
- b) Neste contexto, tem vindo a implementar, para todos os colaboradores, um programa contínuo de formação sobre prevenção de BC/FT/FP, que prevê igualmente cursos de reciclagem anuais. Este programa abrange as medidas e procedimentos necessários para assegurar que fundos decorrentes de actividades ilícitas não sejam canalizados para contas do Millennium Bim;
- c) A formação é ministrada a todos os colaboradores do Millennium Bim, sendo que é dada prioridade de formação a todos os colaboradores que asseguram contacto directo com clientes, bem como a todos os recém-admitidos, no âmbito do programa de “Formação de Integração”;
- d) O programa de formação inclui formação em sala, *on-job* e *e-learning*. A formação em sala e *on-job* é assegurada essencialmente por formadores internos, nomeadamente pessoas com elevada experiência e formação na matéria, que integram o *Compliance Office*;
- e) O programa, entre outros conteúdos, inclui as seguintes matérias:

- (i) Risco de BC/FT/FP;

- (ii) Legislação aplicável em sede de prevenção e combate do BC/FT/FP;
 - (iii) Identificação e os procedimentos de verificação da identidade dos clientes;
 - (iv) Procedimentos de identificação, verificação, diligência e comunicação das operações suspeitas às entidades competentes;
 - (v) Controlo interno e avaliação de risco.
- f) No âmbito da formação em BC/FT/FP, é dada especial atenção aos Deveres de Identificação de clientes, diligência e exame de transacções e aos métodos de movimentação de contas que, face aos montantes envolvidos, natureza ou complexidade, aparentem inconsistência com a actividade/perfil do cliente;
- g) O objectivo último é a sensibilização de todos os colaboradores por forma a permitir que quando em presença de uma situação suspeita e com forte probabilidade de configurar crime de BC/FT/FP, sejam cumpridos todos os deveres que ao Millennium Bim incumbem, solicitando aconselhamento às respectivas hierarquias e ao *Compliance Office*, sobre os procedimentos a observar, agindo em conformidade com os mesmos e no rigoroso cumprimento das disposições legais a que o Millennium Bim se encontra obrigado;
- h) É ainda ministrada a formação aos Agentes Bancários e aos *brokers* contratados pelo Millennium Bim sobre os procedimentos de prevenção de branqueamento de capitais, financiamento do terrorismo e financiamento da proliferação de armas de destruição em massa;
- i) As evidências das formações e participantes delas são mantidas por um período de 5 anos.

17. BANCOS CORRESPONDENTES

O Millennium Bim toma as medidas consideradas necessárias de acordo com as boas práticas existentes, quando está em causa o estabelecimento ou a manutenção de relações com Bancos correspondentes, desenvolvendo procedimentos especificamente definidos, no sentido de assegurar a *Due Diligence* necessária relativamente a estas entidades.

Toda a informação relevante, nomeadamente no que diz respeito a políticas de BC/FT/FP, *Corporate Governance* e enquadramento regulamentar, é reunida no sentido de permitir uma decisão fundamentada sobre o estabelecimento ou manutenção de uma relação de correspondência.

Neste âmbito, o Millennium Bim desenvolve os mecanismos necessários à definição de um modelo de risco específico para este tipo de clientes, tendo sempre presente princípios de *Risk Based Approach* que a legislação consagra.

Os princípios orientadores da aprovação, monitoria e controlo aplicáveis ao estabelecimento ou manutenção de relações de banca de correspondência encontra-se devidamente descrita na [OS0234 - Política de Selecção e Relacionamento com Bancos Correspondentes](#).

18. AUDITORIA INTERNA

- a) A auditoria interna é responsável pela realização de uma avaliação independente, pela eficácia e

eficiência do sistema de prevenção do BC/FT/FP, devendo nomeadamente:

- (i) Verificar a adequação das políticas internas;
 - (ii) Adoptar procedimentos e sistema de suporte para detectar potenciais operações suspeitas de BC/FT/FP;
 - (iii) Avaliar se cada linha de defesa desempenha adequadamente as tarefas e funções atribuídas;
 - (iv) Rever o funcionamento do sistema para garantir um desempenho adequado;
 - (v) Assegurar o cumprimento, a nível de todo Banco, dos procedimentos preventivos ao BC/FT/FP;
 - (vi) Rever, em especial, os processos de *due diligence* e de *KYC* realizados para clientes, produtos, serviços ou canais de distribuição identificados como de alto risco;
 - (vii) Verificar o tratamento diligente dos alertas de BC/FT/FP, e se os alertas gerados são prontamente encerrados com uma avaliação de risco adequada.
- b) O relatório de auditoria interna deve ser elaborado, pelo menos uma vez ao ano, e remetido ao Conselho da Administração assim como as suas principais conclusões remetidas à Comissão de Auditoria;
- c) O programa de auditoria interna deve estar alinhado com a avaliação do risco efectuada pelo Banco;
- d) O Millennium Bim procura que as políticas e procedimentos de gestão corporativa sejam revistos e inspeccionados com regularidade, usando uma abordagem baseada no risco, no sentido de determinar:
- (i) Se a política de risco é adequada e eficaz;
 - (ii) Se a gestão de risco, actividades de monitorização e controlo assim como actividades de formação são adequadas e eficazes, e;
 - (iii) Se as transacções são executadas em concordância com o enquadramento legal, políticas e procedimentos do Grupo.

19. DISPOSIÇÕES FINAIS

Quaisquer dúvidas ou solicitação de esclarecimentos adicionais, necessários para a correcta aplicação dos procedimentos ora definidos, deverão ser encaminhadas ao **COFF- Compliance Office**, através dos meios de comunicação habituais, devendo dar-se preferência à utilização da voz corporativa.

	COFF - COMPLIANCE OFFICE
TELEFONE FAX	21 351594
VOZ CORPORATIVA	7011059 / 7011126 / 7011310
E-MAIL	BIM Compliance Office <Complianceoffice@millenniumbim.co.mz>

BANCO INTERNACIONAL DE MOÇAMBIQUE
O CONSELHO DE ADMINISTRAÇÃO

Senhor Dr. Moisés Jorge

Senhor Dr. Nuno Manuel da Silva Amado

Senhor Dr. Rui Manuel Pereira Pedro

Senhor Dr. Miguel Maya Dias Pinheiro

Senhor Dr. Manuel Alfredo de Brito Gamito

Senhor Eng.º Jacinto Zacarias Uqueio

Senhora Dr.ª Liliana Marisa Catoja da Costa Lemos

Senhor Dr. José Artur Gouveia Coelho Caetano

Senhor Dr. João Nuno Oliveira Jorge Palma

Senhor Dr. José Miguel Bensliman S. da Silva Pessanha

Senhora Dr.ª Anabela Júlia Chamluca Pinho

Senhor Dr. Rui Nelson Moreira de Carvalho Maximino

Senhor Eng.º Sérgio Quintas Vieira da Silva Magalhães

Senhora Dr.ª Ana Maria J. F. Torres Marques Tavares

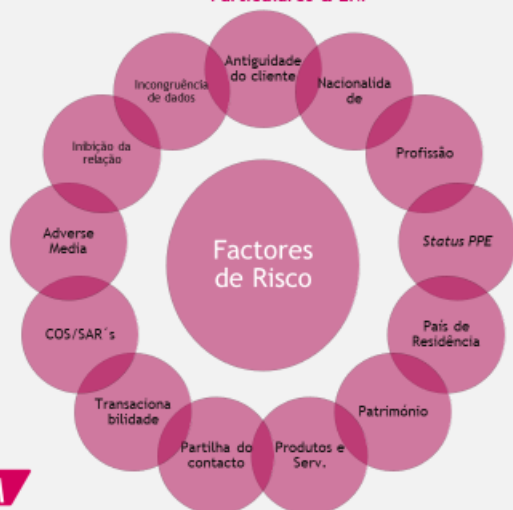
Senhor Dr. Januário da Costa Valente Júnior

ANEXO I - MODELOS DE ATRIBUIÇÃO DO RISCO AML

Modelo de Atribuição de Risco

O **modelo actual de cálculo de risco** tem como objectivo atribuir um perfil de risco de AML aos Clientes. Este processo é desencadeado de forma automática (1) no momento de estabelecimento e (2) durante a relação de negócio, e envolvem os seguintes factores:

Particulares & ENI



Pessoas Colectivas & Bancos Correspondentes



Modelo de Atribuição de Risco

Particulares

Cliente possui 10 ou mais produtos no banco	-10
Antiguidade do cliente no banco > 10 anos	-10
Cliente possui pelo menos entre 5 e 9 produtos no banco	-5
Classificação de transações mensais a crédito em intervalos de montante (0-6)	6
Antiguidade do cliente no banco 12 a < 24 meses	10
Classificação de transações mensais em cash em intervalos de montante (0-6)	11
Cliente faz parte de um grupo de mais de 10 pessoas com o mesmo número de telemóvel	15
Cliente que fez Onboarding digital	15
Antiguidade do cliente no banco <12 meses	20
Transações realizadas de ou para países de risco (último mês)	55
Dados Incongruentes	31
Património financeiro 25 000 000	55
Nacionalidade de um país com sanções ou embargos	60
Cliente com profissão ou atividade profissional de risco	150
Cliente tem 1 convidado para aceder ao cofre de aluguer	150
Residência fiscal num país de risco	200
Cliente possui 1 cofre de aluguer	200
Inibição Relação (risco AML 5)	210
PEP	210
Adverse Media	220
UIF/DCIAP flag- Supervisão (risco AML 9)	220
Cliente Participado (risco AML 55 ou 95)	225

■ Risco Alto ■ Risco Médio ■ Risco Baixo

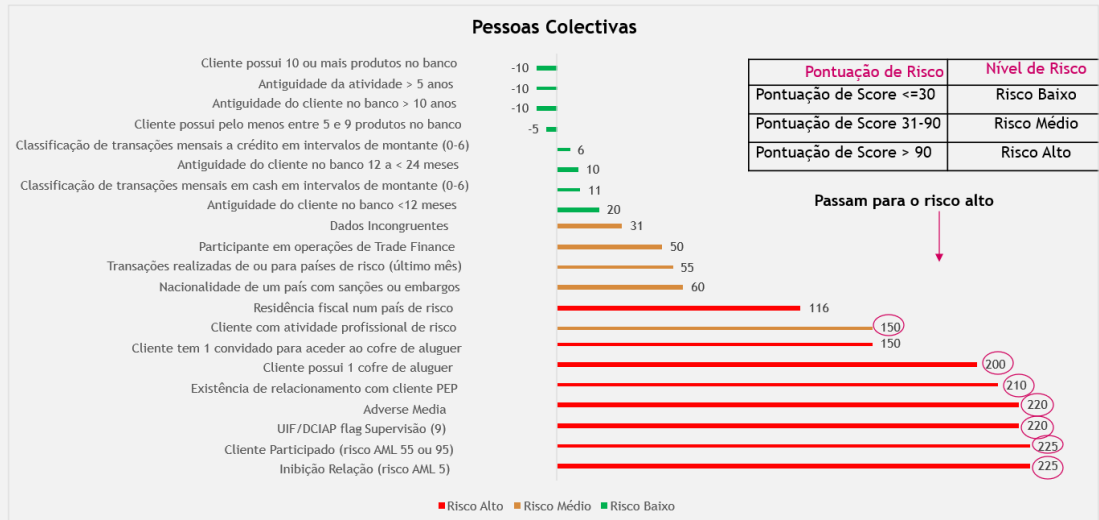
Pontuação de Risco	Nível de Risco
Pontuação de Score <=30	Risco Baixo
Pontuação de Score 31-90	Risco Médio
Pontuação de Score > 90	Risco Alto

ÁGIL | MODERNO | PRÓXIMO | SIMPLES | SUSTENTÁVEL

3

Modelo de Atribuição de Risco

78000078
Quando impresso, este documento constitui cópia não controlada.



M

ÁGIL | MODERNO | PRÓXIMO | SIMPLES | SUSTENTÁVEL

4

Modelo de Atribuição de Risco

Cada **factor de risco** apresentado no slide anterior é composto por uma pontuação que irá contribuir para o cálculo do score dos clientes, obedecendo as seguintes etapas:

- 1 Cada cliente deve receber uma classificação de score de base obtida através da soma das pontuações atribuídas a cada **factor de risco**.
- 2 Após o primeiro cálculo de score para todos os clientes **Particulares ou Eni** é necessário identificar todos os seus relacionamentos com outros clientes deste tipo.
- 3 Após o cálculo de score para **Pessoas Colectivas** é necessário identificar os seus BEFs.
- 4 O score final do cliente **Particular ou Eni** será influenciado com uma pontuação adicional de acordo com o pior score dos clientes consigo relacionados.
- 5 O score final do cliente para **Pessoas Colectivas** será influenciado com uma pontuação adicional de acordo com o pior score dos seus BEFs.
- 6 Para cada **score final** serão aplicados **Cut-offs** de pontuação de forma a atribuir o **Nível de Risco AML** adequado

78000078
Quando impresso, este documento constitui cópia não controlada.

M

ÁGIL | MODERNO | PRÓXIMO | SIMPLES | SUSTENTÁVEL

4

ANEXO II - GLOSSÁRIO

1. *Anti money laundering* (AML)

Procedimento, medidas contra o branqueamento de capitais;

2. Beneficiário Efectivo

Pessoa singular proprietária última ou que detém o controlo final de um cliente e/ou a pessoa no interesse da qual é efectuada uma operação. Inclui também as pessoas que controlam efectivamente uma pessoa colectiva ou uma entidade sem personalidade jurídica. **Deve abranger:**

a) No caso de cliente ser uma pessoa colectiva:

- (i) As pessoas singulares que, em última instância, detêm a propriedade ou o controlo, directo ou indirecto, igual ou superior a 10% 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 normas internacionais;
- (ii) As pessoas singulares que, de qualquer outro modo, exerçam o controlo da gestão da pessoa colectiva;
- (iii) As pessoas singulares que detêm a titularidade ou controlo, directo ou indirecto, igual ou superior a 10% de unidades de participação ou de titularização em circulação num organismo de investimento colectivo.

b) No caso de cliente ser uma entidade jurídica que administra e distribua fundos:

- (i) As pessoas singulares beneficiárias de pelo menos, 10% do seu património, quando os futuros beneficiários já tiverem sido determinados;
- (ii) 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;
- (iii) As pessoas singulares que exerçam controlo igual ou superior a 10% do património da pessoa colectiva.

c) No caso de fundos fiduciários (*trusts*) ou de outros centros de interesses colectivos sem personalidade jurídica:

- (i) Os fundadores (*settlers*);
- (ii) Os administradores fiduciários (*trustees*);
- (iii) Os curadores, se aplicável;
- (iv) Os beneficiários ou, se os mesmos não tiverem ainda sido determinados, a categoria de pessoas em cujo interesse principal o fundo fiduciário (*trust*) foi constituído ou exerce a sua actividade;
- (v) Qualquer outra pessoa singular que detenha o controlo final do fundo fiduciário (*trust*) através de participação directa ou indirecta ou através de outros meios.

3. *Counter terrorism financing* (CFT)

Procedimento, medidas de Combate de Financiamento ao Terrorismo.

4. *Due diligence*

Due diligence é um processo de investigação e auditoria às informações fornecidas pelos clientes às instituições, fundamental para confirmar os dados disponibilizados.

5. *Enhanced due diligence*

Diligência reforçada.

6. GAFI - Grupo de Acção Financeira Internacional

É um organismo intergovernamental global que estabelece padrões e promove a implementação de medidas para combater o BC/FT.

7. Imediato e sem demora (cumprimento de medidas restritivas)

Decisões tomadas num período máximo de 24 horas após a adição, emenda ou revogação de uma designação na Lista Internacional pelo órgão competente das Nações Unidas. Relativamente às designações nacionais, a obrigação de agir sem demora é desencadeada por uma designação a nível nacional, apresentada por iniciativa própria da República de Moçambique ou a pedido de outro Estado, logo que existam motivos ou razões razoáveis para crer que uma pessoa, grupo ou entidade preenche os critérios de inclusão na Lista Nacional. Em ambos casos, a palavra “imediato” deve ser interpretada no contexto da necessidade de evitar a evasão ou dissipação de fundos ou outros activos ligados a pessoas, grupos ou entidades designadas e da necessidade de uma acção global coordenada para interromper e desfazer rapidamente esse fluxo.

8. Lista Designada

Lista de pessoas, grupos, organizações e entidades designados pelas Resoluções de um órgão competente das Nações Unidas (lista Internacional) ou pela Procuradoria-Geral da República como terroristas, organizações terroristas, grupo terrorista, combatentes terroristas estrangeiros e financiadores de terroristas e/ou organizações terroristas (lista Nacional).

9. Lista Internacional

Lista de todas as pessoas, grupos, organizações e entidades sujeitas a sanções financeiras específicas, em conformidade com as resoluções do Conselho de Segurança das Nações Unidas, juntamente com todas as informações associadas.

10. Lista Nacional

Lista de todas as pessoas, grupos, organizações e entidades designadas pela Procuradoria-Geral da República como terroristas, organizações terroristas, grupo terrorista, combatentes terroristas estrangeiros e financiadores de terroristas e/ou organizações terroristas.

11. *Know your customer (KYC)*

Conheça o seu cliente, informação relevante da actividade e rendimentos do cliente, no seu aspecto quantitativo e qualitativo.

12. Pessoa Politicamente Exposta (PEP)

Pessoas Politicamente Expostas, conhecidas por *PEP* ou *PPE*, são indivíduos nacionais ou estrangeiros que desempenham ou desempenharam funções públicas proeminentes em Moçambique ou em qualquer outro país ou jurisdição ou ainda em qualquer organização internacional.

13. Proliferação de Armas de Destruição em Massa

Fabrico, aquisição, posse, desenvolvimento, exportação, transbordo, corretagem, transporte, transferência, armazenamento ou uso de energia nuclear, armas químicas ou biológicas, materiais relacionados e seus meios de entrega (incluindo tecnologias e produtos de dupla utilização usados para fins ilegítimos), em violação das leis nacionais ou, quando aplicável, das obrigações internacionais.

14. Terrorismo

Uso de ameaça ou uso de violência física ou psicológica com intuito de criar insegurança social, terror ou pânico na população ou de pressionar o Estado ou alguma organização de carácter económico, social ou político a realizar ou abster-se de realizar certa ou certas actividades.

15. Financiamento ao Terrorismo

Fornecimento, recolha ou detenção (de forma directa ou indirecta) de fundos ou bens de qualquer tipo, bem como de produtos ou direitos susceptíveis de serem transformados em fundos, destinados a serem utilizados ou sabendo que podem ser utilizados (total ou parcialmente) no planeamento, na preparação ou para a prática de actos terroristas.

A facilitação do financiamento de actos terroristas difere do processo de branqueamento de capitais, na medida em que, o financiamento ao terrorismo pode ter como fonte actividades criminosas e como também actividades legais, desde que o individuo ou organização tenha os mesmos ideais.

16. Financiamento da Proliferação de Armas de Destruição em Massa

Refere-se ao acto de fornecer fundos e bens, ou serviços financeiros que são usados, no todo ou em parte, para fabricação, aquisição, posse, desenvolvimento, exportação, transbordo, corretagem, transporte, transferência, armazenamento ou uso de energia nuclear, armas químicas ou biológicas e seus meios de entrega e materiais relacionados (incluindo tecnologias e produtos de dupla utilização usados para fins ilegítimos), em violação das leis nacionais ou, quando aplicável, das obrigações internacionais.

17. Sanções Financeiras Específicas (SFE)

Significa o congelamento de activos e proibições para impedir que fundos ou outros activos sejam disponibilizados, directa ou indirectamente, em benefício de pessoas e entidades designadas.

BANCO INTERNACIONAL DE MOÇAMBIQUE

Ordem de Serviço: OS0202 (09ª Versão) - Em vigor desde 18-11-2025

1. Documentos que revoga:

Referência	Título	Data de entrada em vigor
OS0202	Políticas de Combate ao Branqueamento de Capitais e Financiamento ao Terrorismo, (versão nº 10).	26-03-2025

2. Documentos relacionados:

Referência	Título	Data de entrada em vigor
NP0058	Abertura de Contas de Depósitos à Ordem	
Despacho nº 2 /GIFiM-GDG/120.1/2025	Directrizes Públicas para as Pessoas, Entidades e Organizações Designadas na República de Moçambique	22 de Agosto

3. Documentos referidos:

Referência	Título	Data de entrada em vigor
OS0125	Gestão Documental	
OS0203	Política de Identificação, Aceitação e Diligência de Clientes	
OS0234	Política de Selecção e Relacionamento com Bancos Correspondentes	
NP0305	Processo de Actualização Permanente (On Going) de Dados de Clientes	
NP0009	Medidas de Prevenção e Combate ao crime de Branqueamento de Capitais e financiamento ao Terrorismo	
Lei nº 14/2023	Lei que estabelece o Regime Jurídico e as Medidas de Prevenção e Combate ao Branqueamento de Capitais e Financiamento do Terrorismo	28 de Agosto
Lei nº 3/2024	Lei que altera os artigos 7, 8, 9, 13, 15, 23, 50, 52, 79 e 80 da Lei n.º 14/2023, de 28 de Agosto, que estabelece o Regime Jurídico e as Medidas de Prevenção e Combate ao Branqueamento de Capitais e Financiamento do Terrorismo	22 de Março
Decreto nº 53/2023	Aprova o Regulamento da Lei n.º 14/2023, de 28 de Agosto, que estabelece o Regime Jurídico e as Medidas de Prevenção e Combate ao Branqueamento de Capitais e Financiamento do Terrorismo e revoga o Decreto n.º 66/2014, de 29 de Outubro	31 de Agosto
Aviso 10/GBM/2024	Aprova as Directrizes sobre Prevenção e Combate ao Branqueamento de Capitais, Financiamento do Terrorismo e Financiamento da Proliferação de Armas de Destruição em Massa e revoga o Aviso n.º 5/GBM/2022, de 17 de Novembro.	30 de Agosto
Despacho nº 1 /GIFiM-GDG/120.1/2025	Directrizes para a Aplicação de Sanções Financeiras Específicas Relacionadas com o Terrorismo e o Financiamento do Terrorismo	22 de Agosto

4. Informações adicionais:

Elaborado por: COFF- Gestão Documental - X070470