

## BANCO INTERNACIONAL DE MOÇAMBIQUE

**Ordem de Serviço:** OS0202 - Versão nº 09 - Em vigor desde 01-08-2023

**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 AML é autonomizada das Políticas de *Compliance* ([OS0110-Políticas de Compliance](#)).

### Alterações à versão anterior

As alterações à versão anterior foram motivadas pela necessidade de acautelar a recomendação da KPMG referente a manutenção do registo das formações e participantes, de 5 para 7 anos.

- I. **Na página 13**, no Ponto 12. **Dever de Formação**, alínea i), alteração atinente ao período de conservação da documentação relativa as formações, de 5 para **7 anos**.

**Índice**

1.ENQUADRAMENTO .....	3
2. OBJECTIVO, AMBITO E PROCESSO DE REVISÃO.....	3
3. DEVER DE IDENTIFICAR.....	4
3.1. Customer Due Diligence / Know your Customer (KYC) .....	4
3.2. Abordagem Baseada no Risco ( <i>Risk Based Approach</i> ) .....	5
4. DEVER DE VIGILANCIA CONTÍNUA.....	6
5. DEVER DE EXAME .....	6
6. DEVER DE ABSTENÇÃO.....	9
7. DEVER DE RECUSA.....	10
8. DEVER DE COMUNICAR OPERAÇÕES SUSPEITAS.....	10
9. DEVER DE SIGILO PROFISSIONAL .....	11
10.DEVER DE CONSERVAÇÃO .....	12
11.DEVER DE COLABORAÇÃO .....	12
12.DEVER DE FORMAÇÃO.....	12
13.BANCOS CORRESPONDENTES .....	13
14.AUDITORIA INTERNA .....	13
15.DISPOSIÇÕES FINAIS .....	14
ANEXO I - MODELOS DE ATRIBUIÇÃO DO RISCO AML.....	16
ANEXO II - GLOSSÁRIO .....	18

---

## 1. ENQUADRAMENTO

---

A presente ordem de serviço tem por objectivo, a transmissão das principais linhas de orientação e directrizes de política geral aplicada ao Millennium Bim.

A globalização da actividade financeira e o rápido desenvolvimento das tecnologias de informação são factores que proporcionam novas oportunidades de crescimento da economia e ao mesmo tempo aumentam o risco associado ao branqueamento de capitais.

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 branqueamento de capitais 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 (BC/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 branqueamento de capitais, 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 branqueamento de capitais e financiamento ao terrorismo, que possam prejudicar a sua reputação e estabilidade.

Assim sendo, o Millennium Bim adopta medidas internas, procedimentos e programas de formação e controlo destinados a garantir a conformidade de todos os seus colaboradores, com o enquadramento legal existente sobre a matéria.

---

## 2. OBJECTIVO, AMBITO E PROCESSO DE REVISÃO

---

- a) Prevenir o uso dos serviços e produtos fornecidos pelo banco para efeitos do branqueamento de capitais, financiamento do terrorismo, e financiamento da proliferação de armas de destruição em massa (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 branqueamento de capitais, financiamento do terrorismo e financiamento da proliferação de armas de destruição em massa 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 branqueamento de capitais 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 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 branqueamento de capitais, em conformidade com legislação em vigor, a par, designadamente, com as definições e conceitos resultantes da Lei n.º 11/2022 de 7 de julho, do Decreto n.º 66/2014, de 29 de Outubro;
- 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 nº 4/GBM/2015 de de 17 de Junho. O Conselho de Administração é o órgão competente para aprovação do presente normativo e subsequentes alterações/revisões.

---

### **3. DEVER DE IDENTIFICAR**

---

O Millennium Bim adopta todos os procedimentos necessários no sentido de determinar a verdadeira identidade dos seus clientes, representantes e/ou beneficiários efectivos (Política de Identificação de Clientes), assim como de obter toda a informação relevante e pertinente nas seguintes situações:

- a) No estabelecimento de uma relação de negócio;
- b) Previamente à realização de transacções ocasionais de montante igual ou superior a 900.000 MZN (novecentos mil Meticais);
- c) Na existência de suspeitas de que as operações, independente do seu valor, estejam relacionadas com o crime de branqueamento de capitais financiamento do terrorismo e financiamento da proliferação de armas de destruição em massa;
- d) Quando existem dúvidas quanto a veracidade ou adequação dos dados de identificação do cliente;
- e) No acompanhamento da relação de negócio através dos processos de actualização dos dados de identificação dos clientes.

#### **3.1. Customer Due Diligence / Know your Customer (KYC)**

No âmbito do processo de identificação e conhecimento do cliente, o Millennium Bim avalia necessariamente, sem prejuízo de outros aspectos que possam ser considerados relevantes:

- a) A finalidade e o propósito da conta que se pretende abrir;
- b) Beneficiários Efectivos, verificando a sua identidade;

- c) Existência do estatuto de Pessoa Politicamente Exposta (PPE) nos seus clientes, representantes ou beneficiários efectivos;
- d) A natureza e o racional dos negócios, fontes de rendimento da actividade económica principal e/ou emprego do cliente;
- e) A fonte da riqueza e outras fontes de fundos do cliente envolvidos no relacionamento comercial, para garantir que são legítimos;
- f) O objectivo da transacção, incluindo, quando apropriado, o destino dos fundos do cliente (nomeadamente a sua recorrência ou atipicidade);
- g) Informações sobre quaisquer associações que o cliente possa ter com outras jurisdições (sede, instalações operacionais, filiais, etc.) e os indivíduos que podem influenciar nas suas operações; quando o cliente estiver sediado em outro país, qual a natureza da relação pretendida e a razão para se procurarem serviços bancários fora da sua jurisdição local.
- h) O perfil transaccional expectável;
- i) A estrutura de propriedade e controlo do cliente quanto este é uma pessoa colectiva;
- j) A coerência e consistência de toda a informação existente.

No caso do estabelecimento de relações de negócio com as entidades que tenham estatuto referido na alínea c) o Millennium Bim tem um processo desenho que:

1. Requer a autorização superior para estabelecer a relação de negócio;
2. Determina a origem do património e dos fundos envolvidos na relação de negócio ou transacções ocasionais;
3. Acompanha de forma contínua a relação.

### **3.2. Abordagem Baseada no Risco (*Risk Based Approach*)**

- a) O Millennium Bim desenvolve um sistema de classificação de risco de branqueamento de capitais (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, 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 branqueamento (*AML*);
- c) Embora as orientações acerca da matéria de branqueamento de capitais e financiamento do terrorismo 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 dilligence*;

- 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 branqueamento de capitais e ao financiamento do terrorismo, 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

---

#### 4. DEVER DE VIGILANCIA CONTÍNUA

Os princípios de *Due Diligence* são aplicados não só 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.

Como parte da monitorização e actualização contínuas do perfil de risco de *AML* dos seus clientes, o *KYC* é periodicamente actualizado de acordo com o perfil de risco, anual para clientes com grau de risco *AML* Alto, até 3 anos para clientes com grau de risco *AML* Médio e até 5 anos para clientes com grau de risco *AML* baixo.

O Millennium Bim tem ao seu dispor várias fontes de informação sobre os seus clientes, tanto internas como externas e actualiza com regularidade essa informação, mantendo o registo de transacções recentes, contrapartes nelas envolvidas e sua relação com o cliente.

---

#### 5. 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 branqueamento de capitais e financiamento do terrorismo e financiamento da proliferação de armas de destruição em massa, 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 nos normativos legais<sup>1</sup> 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/*Office of Foreign Assets Control*), com o objectivo de verificar a “coincidência” ou não, com as entidades constantes naquelas listas. No 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

---

<sup>1</sup> Dentre os quais se destacam a Lei nº11/2022 de 7 de Julho (lei de prevenção e Combate ao Branqueamento de Capitais, Financiamento do Terrorismo e Financiamento da Proliferação de Armas de Destruição em Massa); o Decreto nº66/2014 de 29 de Outubro (Aprova o regulamento da lei 14/2013 de 12 de Agosto); e o Aviso nº 5/GBM/2022 de 17 de Novembro (Aprova as Directrizes sobre Prevenção e repressão do Branqueamento de Capitais, Financiamento do Terrorismo e Financiamento da Proliferação de Armas de Destruição em Massa).

- verdadeiro repositório de normativos legais, 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 15 do Decreto 66/2014 de 29 de Outubro. 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 branqueamento de capitais, financiamento do terrorismo e financiamento da proliferação de armas de destruição em massa;
  - 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 branqueamento de capitais ou financiamento do terrorismo.

Todas as análises têm de ser reduzidas a escrito e relevam especialmente os seguintes elementos<sup>2</sup>:

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. Meios de pagamento utilizados;
5. Natureza, actividade, padrão operativo e perfil dos intervenientes;
6. Tipo de transacção ou produto que possa favorecer especialmente o anonimato

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

- (i) Monitorização e controlo de clientes e transacções com nível de risco *AML* elevado;
- (ii) Monitorização e controlo de transacções envolvendo países de risco *AML* elevado;
- (iii) Monitorização e controlo de transacções complexas e/ou extraordinárias;
- (iv) 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);
- (v) 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;

---

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

- (vi) Monitorização e controlo de transacções pontuais relacionadas que, no seu todo, excedam o limite legal requerido;
  - (vii) Monitorização de transacções fraccionadas que no seu conjunto representam valores iguais ou superiores a 900.000,00 MT (novecentos mil Meticais);
  - (viii) Monitorização de transacções ocasionais ou depósitos realizados por terceiros;
  - (ix) 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;
  - (x) 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;
  - (xi) 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 branqueamento de capitais, financiamento do terrorismo e financiamento da proliferação de armas de destruição em massa, 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.

---

## 6. DEVER DE ABSTENÇÃO

---

No âmbito de dever de abstenção, sempre que se constate que uma determinada operação evidencia fundada suspeita de constituir crime ao abrigo do disposto na Lei nº 11/2022 de 7 de Julho, o Banco, deve abster-se de executar quaisquer operações relacionadas com o pedido do cliente. O Banco, deve informar de imediato ao Ministério Público e ao GIFiM de que se absteve de executar a operação.

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. Entretanto, após o Banco consultar a

PGR e ao GIFiM, considerar que a abstenção pode prejudicar a prevenção e futura investigação dos crimes previstos na presente Lei, a operação pode ser realizada, devendo o Banco, fornecer, de imediato, as entidades consultadas (PGR/GIFiM), as informações respeitantes à operação.

O Millennium Bim atenderá a qualquer instrução emitida por estas entidades (Procuradoria Geral da República e GIFiM) por se mostrarem mandatórias.

Caso a ordem de suspensão não seja confirmada pelo juiz de instrução criminal, no prazo estabelecido (5 dias úteis a contar da data de comunicação), a operação poderá ser realizada, com autorização do *Compliance Officer*.

---

## **7. DEVER DE RECUSA**

---

No cumprimento do dever de recusa imposto pela legislação nacional vigente<sup>3</sup> 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 Lei<sup>4</sup>;
2. Não sejam entregues todos os documentos comprovativos dos elementos de identificação declarados<sup>5</sup>;
3. Existam dúvidas sobre a autenticidade dos documentos apresentados e nas diligências efectuadas não se consiga certificar a autenticidade dos mesmos<sup>6</sup>;
4. Não sejam declarados os beneficiários efectivos ou dados os mesmos elementos de identificação e documentos que o comprovem sobre estes<sup>7</sup>;
5. Existam suspeitas de que as operações, independentemente do seu valor, ou finalidade da conta, estejam relacionadas como crime de branqueamento de capitais de financiamento do terrorismo e financiamento da proliferação de armas de destruição em massa

Sempre que exerce o dever de Recusa, é obrigatório o envio de comunicação ao GIFiM<sup>8</sup>.

---

## **8. 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

---

<sup>3</sup> Artigo 40.º da Lei nº 11/2022 de 7 de Julho

<sup>4</sup> Definidos no artigo 4.º do Decreto nº 66/2014

<sup>5</sup> Definidos no artigo 5.º do Decreto nº 66/2014

<sup>6</sup> Conforme artigo 6.º do Decreto nº 66/2014

<sup>7</sup> Conforme artigo 7.º do Decreto nº 66/2014

<sup>8</sup> Nos termos da al. d) do artigo 40 da Lei nº 11/2022 de 7 de Julho

ou serviços do Millennium Bim para branquear fundos provenientes de actividade ilícita ou financiamento ao terrorismo, o Millennium Bim toma 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, 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 branqueamento de capitais ou de financiamento de terrorismo 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 MZN ou equivalente contravalor;
- B. Todas as transacções de valor igual ou superior a 750.000 MZN ou equivalente contravalor.

---

## **9. 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.

---

## **10. DEVER DE CONSERVAÇÃO**

---

Todos os registos e evidências documentais são mantidos em vários suportes, pelo prazo legalmente definido de 10 anos (dez anos depois do término da relação de negócio e encerramento da conta com relação aos registos de diligência relativa à clientela).

---

## **11. DEVER DE COLABORAÇÃO**

---

O Millennium Bim presta colaboração às autoridades judiciais competentes, 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.

---

## **12. 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 branqueamento de capitais, financiamento do terrorismo e financiamento da proliferação de armas de destruição em massa, 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 branqueamento de capitais, financiamento do terrorismo e financiamento da proliferação de armas de destruição em massa, 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 branqueamento de capitais, financiamento do terrorismo e financiamento da proliferação de armas de destruição em massa;
  - (ii) Legislação aplicável em sede de prevenção e combate do branqueamento de capitais, financiamento do terrorismo e financiamento da proliferação de armas de destruição em massa;
  - (iii) Identificação e os procedimentos de verificação da identidade dos clientes;

- (iv) Procedimentos de identificação 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 branqueamento de capitais, financiamento do terrorismo e financiamento da proliferação de armas de destruição em massa, 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 **7 anos**.

---

### 13. 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 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.

---

### 14. AUDITORIA INTERNA

---

- a) A auditoria interna é responsável pela realização de uma avaliação independente, pela eficácia e eficiência do sistema de prevenção do branqueamento de capitais, financiamento do terrorismo e financiamento da proliferação de armas de destruição em massa, devendo nomeadamente:
- (i) verificar a adequação das políticas internas;
  - (ii) Adoptar procedimentos e sistema de suporte para detectar potenciais operações suspeitas;

- (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 branqueamento de capitais, financiamento do terrorismo e financiamento da proliferação de armas de destruição em massa;
  - (vi) Rever, em especial, os processos de *due diligence* e de *KYC*.
- 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.

---

**15. 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 a utilização da voz corporativa.

	<b>COFF - COMPLIANCE OFFICE</b>
TELEFONE FAX	21 351594
VOZ CORPORATIVA	7011594
E-MAIL	BIM Compliance Office <Complianceoffice@millenniumbim.co.mz>

**BANCO INTERNACIONAL DE MOÇAMBIQUE**  
**O CONSELHO DE ADMINISTRAÇÃO**

*Rui Cirne Plácido de Carvalho Fonseca*

*Nuno Manuel da Silva Amado*

*João Manuel Rodrigues Tomé Cunha Martins*

*Miguel Maya Dias Pinheiro*

*Manuel Alfredo de Brito Gamito*

*Jacinto Zacarias Uqueio*

*Jorge Octávio Neto dos Santos*

*Moisés Jorge*

*Liliana Marisa Catoja da Costa Lemos*

*José Artur Gouveia Coelho Caetano*

*Albino António Carneiro de Andrade*

*João Nuno Oliveira Jorge Palma*

*José Miguel Bensliman S. da Silva Pessanha*

*Anabela Júlia Chambuca Pinho*

*Rui Nelson Moreira de Carvalho Maximino*

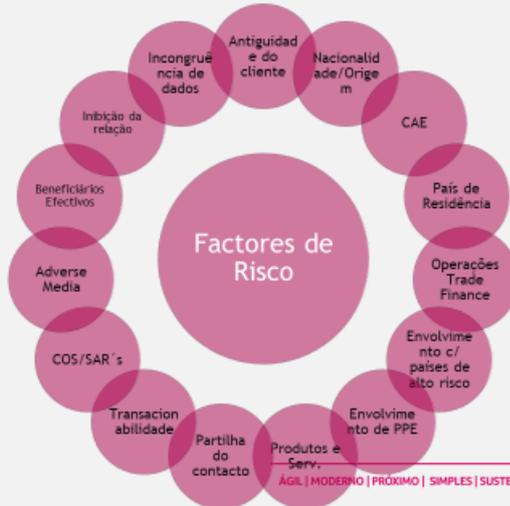
ANEXO I - MODELOS DE ATRIBUIÇÃO DO RISCO AML

# 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:

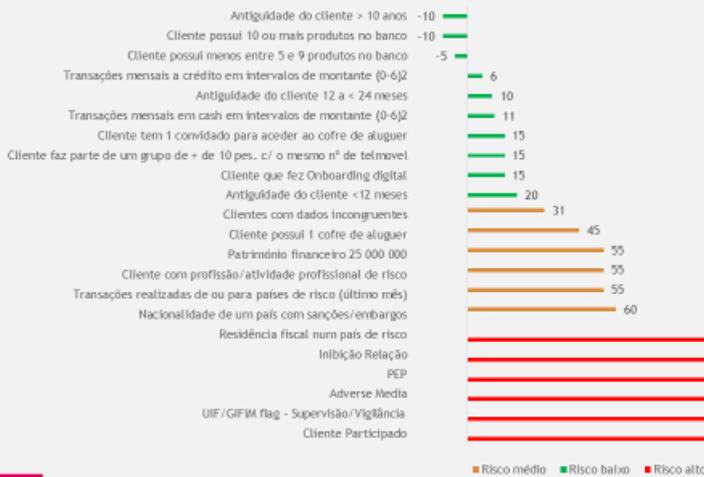
**Particulares & ENI**

**Pessoas Colectivas & Bancos Correspondentes**



# Modelo de Atribuição de Risco

**Particulares**

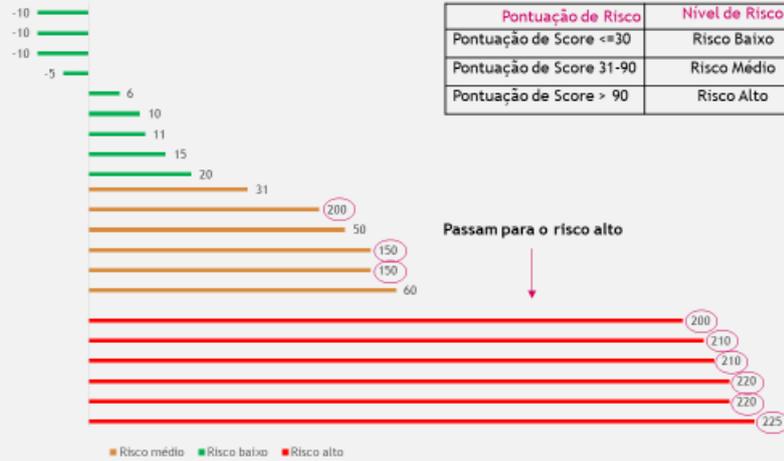


Pontuação de Risco	Nível de Risco
Pontuação de Score <=30	Risco Baixo
Pontuação de Score 31-90	Risco Médio
Pontuação de Score > 90	Risco Alto

## Modelo de Atribuição de Risco

### Pessoas Colectivas

- Cliente possui 10 ou mais produtos no banco
- Antiguidade do cliente no banco > 10 anos
- Antiguidade da atividade > 5 anos
- Cliente possui menos entre 5 e 9 produtos no banco
- Transações mensais a crédito em intervalos de montante (0-6)
- Antiguidade do cliente no banco 12 a < 24 meses
- Transações mensais em cash em intervalos de montante (0-6)
- Cliente tem 1 convidado para aceder ao cofre de aluguer
- Antiguidade do cliente no banco < 12 meses
- Cientes com dados incongruentes
- Cliente possui 1 cofre de aluguer
- Participante em operações de Trade Finance
- Cliente com atividade profissional de risco
- Transações realizadas de ou para países de risco (último mês)
- Nacionalidade de um país com sanções ou embargos
- Residência fiscal num país de risco
- Existência de relacionamento com cliente PEP
- Inibição Relação
- UIF/GIFIM flag- Supervisão (9)
- Adverse Media
- Cliente Participado



7000078 Quando impresso, este documento constitui cópia não controlada.



## Modelo de Atribuição de Risco

Cada **factor de risco** apresentado no slide anterior é composto por uma pontuação que irá contribuir para o calculo 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

7000078 Quando impresso, este documento constitui cópia não controlada.



---

## ANEXO II - GLOSSÁRIO

---

### 1. *Anti money laundering (AML)*

Procedimento, medidas contra o branqueamento de capitais e financiamento ao terrorismo

### 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.

### 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 - Group d'Action Financière*

Organismo internacional que investiga e promove estratégia de luta contra branqueamento de capitais e financiamento ao terrorismo.

### 7. *Insider information*

Informação privilegiada cujo uso antecipado distorce o mercado. Por exemplo, conhecimento da taxa de câmbio, alteração das taxas de juros.

### 8. *Know your customer (KYC)*

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

### 9. **Pessoa Politicamente Exposta (PEP)**

Pessoas Politicamente Expostas, conhecidas por *PEP* ou *PPE*, são aquelas pessoas detentoras de cargos públicos proeminentes em qualquer país. Ex. Membros do Governos, titulares de órgãos de soberania, Chefes de importantes repartições de finanças públicas, Executivos de empresas públicas e outros. A sua classificação e o *KYC* ajudam a melhorar a transparência dos seus actos.

### 10. **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.

### **11. 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.

### **12. 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.

### **13. 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.

**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 08).	26-04-2023

**2. Documentos relacionados:**

Referência	Título	Data de entrada em vigor
OS0110	Políticas de Compliance	
NP0009	Medidas de Prevenção e Combate ao crime de Branqueamento de Capitais e financiamento ao Terrorismo.	
NP0058	Abertura de Contas de Depósitos à Ordem	
Lei nº 11/2022	Lei de Prevenção e Combate ao Branqueamento de Capitais e Financiamento do Terrorismos e Financiamento da Proliferação de Armas de Destruição em Massa.	
Decreto nº 66/2014	Aprova o Regulamento da Lei n.º 14/2013, de 12 de Agosto, que estabelece o regime jurídico e as medidas de prevenção e repressão em relação à utilização do sistema financeiro e das entidades não financeiras para efeitos de branqueamento de capitais, financiamento ao terrorismo e de crimes conexos	

**3. Documentos referidos:**

Referência	Título	Data de entrada em vigor
OS0125	Gestão Documental	

**4. Informações adicionais:**

Elaborado por: COFF- Gestão Documental - X141731