



---

**POLÍTICA DE PREVENÇÃO AO BRANQUEAMENTO DE CAPITAIS E  
FINANCIAMENTO AO TERRORISMO**

---

**Março | 2024  
Versão 08**

**ÍNDICE**

1	APROVAÇÃO E DIVULGAÇÃO .....	2
2	HISTÓRICO .....	3
3	INTRODUÇÃO .....	4
3.1	SUMÁRIO .....	4
3.2	OBJECTIVOS .....	5
3.3	ÂMBITO .....	5
3.4	ENQUADRAMENTO LEGAL E REGULAMENTAR .....	5
3.5	ENQUADRAMENTO INTERNO .....	6
4	CONCEITOS .....	7
5	MODELO DE GOVERNAÇÃO DO RISCO OPERACIONAL .....	9
5.1	RESPONSABILIDADE DO ÓRGÃO DE ADMINISTRAÇÃO .....	9
5.2	ESTRUTURA DO GABINETE DE COMPLIANCE .....	10
5.3	PRINCIPAIS RESPONSABILIDADES DO COMPLIANCE OFFICER .....	10
6	POLÍTICAS DE PREVENÇÃO .....	12
6.1	POLÍTICA DE ACEITAÇÃO E RECUSA DE CLIENTES .....	12
6.2	POLÍTICA DE IDENTIFICAÇÃO DE CLIENTES E APLICAÇÃO DE MEDIDAS DE DILIGÊNCIAS ....	14
6.3	POLÍTICA DE GESTÃO DE CONFLITOS DE INTERESSES E TRANSAÇÕES COM PARTES RELACIONADAS .....	16
6.4	POLÍTICA DE SANÇÕES FINANCEIRAS .....	17
6.5	POLÍTICA DE CONGELAMENTO E DESCONGELAMENTO DE FUNDOS .....	18
7	FERRAMENTAS E APLICATIVOS INFORMÁTICOS .....	19
8	MECANISMOS DE IDENTIFICAÇÃO DO BENEFICIÁRIO EFECTIVO .....	20
9	TRANSAÇÕES OCASIONAIS .....	21
10	PESSOAS POLITICAMENTE EXPOSTAS .....	22
11	PROCEDIMENTOS DE DILIGÊNCIAS .....	24
11.1	DILIGÊNCIA SIMPLIFICADA .....	24
11.2	DILIGÊNCIA REFORÇADA .....	24
12	DEVER DE MONITORIZAÇÃO CONTÍNUA .....	25
13	COMUNICAÇÃO DE IRREGULARIDADES .....	26
14	REGIME TRANSGRESSIONAL .....	27
15	COMUNICAÇÃO DE OPERAÇÕES SUSPEITAS .....	28
16	COLABORAÇÃO COM O REGULADOR E OUTRAS ENTIDADES DE SUPERVISÃO .....	29
17	CONTRATAÇÃO DE COLABORADORES .....	30
18	FORMAÇÃO DE COLABORADORES .....	31
19	RELAÇÃO DE CORRESPONDÊNCIA BANCÁRIA .....	32
20	AUDITORIA EXTERNA .....	33
21	DECLARAÇÃO DE PREVENÇÃO DO BC/FT .....	34
22	DISPOSIÇÕES FINAIS .....	35
23	ANEXOS .....	36
23.1	ANEXO 1 - LISTA DO CONJUNTO DE CATEGORIAS DE CRIMES SUBJACENTES AO CRIME DE BC 36	
23.2	ANEXO 2 - TIPOLOGIA DE OPERAÇÕES OU ACTIVIDADES SUSPEITAS IDENTIFICADAS PELA UIF PARA OS BANCOS E INSTITUIÇÕES FINANCEIRAS NÃO BANCÁRIAS LIGADAS À MOEDA E CRÉDITO .....	37

**1 | APROVAÇÃO E DIVULGAÇÃO**

	<b>Órgão</b>	<b>Data</b>
<b>Elaborado</b>	Direcção de Organização e Qualidade	25.02.2024
<b>Validado</b>	Comissão Executiva	05.03.2024
<b>Aprovado</b>	Conselho de Administração	07.03.2024
<b>Divulgado</b>	Direcção de Organização e Qualidade	

## 2| HISTÓRICO

Versão	Título	Alteração desde a Última versão	Data:	Aprovado
01	Política de AML	– N/A	18.09.2015	Conselho de Administração
02	MNP Sobre a Política de Prevenção ao Branqueamento de Capitais e Financiamento ao Terrorismo	– Revisão geral e adaptação a nova estrutura interna dos normativos.	18.12.2017	Conselho de Administração
03	MNP044_Política de Prevenção ao Branqueamento de Capitais e Financiamento ao Terrorismo	– Revisão no âmbito da Lei nº 34/11, de 12 de Dezembro.	30.08.2019	Conselho de Administração
04	Política de Prevenção ao Branqueamento de Capitais e Financiamento ao Terrorismo	– Revisão no âmbito da Lei nº 05/20, de 27 Janeiro e do Aviso Nº 14/20, de 22 de Junho.	23.12.2020	Conselho de Administração
05	Política de Prevenção ao Branqueamento de Capitais e Financiamento ao Terrorismo	– Revisão geral.	06.02.2022	Conselho de Administração
06	Política de Prevenção ao Branqueamento de Capitais e Financiamento ao Terrorismo	– Revisão geral e no âmbito do Aviso 01/22 – Código do Governo Societário das Instituições Financeiras Bancárias.	06.07.2022	Conselho de Administração
07	Política de Prevenção ao Branqueamento de Capitais e Financiamento ao Terrorismo	– Revisão geral da Política sem alterações ao conteúdo.	29.09.2022	Conselho de Administração
08	Política de Prevenção ao Branqueamento de Capitais e Financiamento ao Terrorismo	– Revisão geral da Política sem alteração do conteúdo	07.03.2024	Conselho de Administração

### 3| INTRODUÇÃO

#### 3.1| SUMÁRIO

Como resposta à crescente preocupação da comunidade internacional relativamente ao problema do Branqueamento de Capitais e Financiamento ao Terrorismo (BC/FT), numerosos países no mundo têm vindo a aprovar ou a rever as suas leis sobre esta matéria.

As instituições financeiras estão sujeitas a normas rígidas destinadas a evitar o BC/FT e a definir os parâmetros de colaboração com entidades reguladoras, de supervisão e de fiscalização, nesta matéria. O não cumprimento destas regras implica responsabilidades, o que pode resultar em penalizações ou consequências legais.

O Banco YETU identifica-se com a sociedade e com as autoridades, ao reconhecer a importância da luta ao BC/FT, por afectar aspectos essenciais da vida em sociedade.

O Banco YETU considera que a melhor forma de atingir o seu compromisso consiste no estabelecimento de normas e procedimentos internos eficazes que permitam:

- Desenvolver a actividade financeira de acordo com rigorosas regras deontológicas e respeitando a legislação em vigor;
- Implementar normas de actuação e sistemas de controlo interno e de comunicação com o objectivo de impedir que o Banco seja utilizado no BC/FT;
- Garantir que todos os seus Colaboradores cumprem as políticas e os procedimentos de Know Your Customer (KYC);
- Cumprir estritamente as leis contra o BC/FT, assim como as recomendações emitidas sobre este assunto pelo Grupo de Acção Financeira Internacional (GAFI) e pelas autoridades nacionais e internacionais;
- Assegurar a formação adequada que visa assegurar um conhecimento pleno, permanente e actualizado aos seus gestores, trabalhadores e demais prestadores.

Só através do compromisso de todos os Colaboradores se pode garantir que os produtos que se comercializam e os serviços que se prestam não são utilizados para o BC/FT.

### 3.2| OBJECTIVOS

A Política de Prevenção ao Branqueamento de Capitais e Financiamento ao Terrorismo insere-se no âmbito dos mecanismos de prevenção de combate ao BC/FT, tendo em conta os princípios gerais de prevenção e combate ao BC/FT, em cumprimento a legislação, a regulamentação nacional e internacional, e as boas práticas nos termos de actuação nos mercados, o Banco YETU entende como fundamental a avaliação dos possíveis riscos dos seus Clientes e potenciais Clientes, para garantir a prevenção eficaz do BC/FT.

### 3.3| ÂMBITO

Esta Política aplica-se a todos Colaboradores, Accionistas, Clientes, Contrapartes e Parceiros do Banco YETU, devendo ser garantido pelos responsáveis das Unidades de Negócio (U.N.) a disseminação da mesma junto dos Colaboradores adstritos às respectivas U.N.

Cabe à Direcção de Organização e Qualidade (DOQ) garantir a publicação e divulgação desta Política, sendo a iniciativa para a actualização e revisão do responsável pela Política, sem prejuízo de haver iniciativa por parte do Gabinete de Compliance (GCO), da Comissão Executiva (CE) e/ou Conselho de Administração (CA).

### 3.4| ENQUADRAMENTO LEGAL E REGULAMENTAR

A Política de Prevenção ao Branqueamento de Capitais e Financiamento ao Terrorismo está alinhada com as disposições legais e regulamentares a que o Banco YETU está obrigado, nomeadamente:

- Lei n.º 05/2020 – Lei de Prevenção e Combate ao Branqueamento de Capitais, do Financiamento ao Terrorismo e da Proliferação de Armas de Destruição em Massa.
- Aviso n.º 14/2020 – Regras de Prevenção e Combate ao Branqueamento de Capitais e Financiamento do Terrorismo.
- Aviso n.º 01/2022 – Código do Governo Societário das Instituições Financeiras Bancárias.

### 3.5| ENQUADRAMENTO INTERNO

O Banco YETU estabeleceu regras e procedimentos rigorosos para o cumprimento das normas de BC/FT alinhados com as orientações previstas na legislação e normativos em vigor.

Em termos de combate ao BC/FT, o Banco YETU cumpre a obrigação de comunicar às entidades de supervisão e de fiscalização quaisquer transacções suspeitas, que apresentem indícios de BC/FT, de forma a obter informação suficiente dos Clientes e Contrapartes sobre a sua identidade ou sobre a sua actividade económica ou profissional, com o objectivo de aplicar o controlo interno e procedimentos de notificação, e formar os seus Colaboradores relativamente a questões relacionadas com a prevenção do BC/FT.

Os efeitos negativos que o BC/FT tem na reputação do Banco YETU, obrigam a tomada de medidas e estabelecimento de regras e procedimentos a fim de assegurar:

- Que todas as operações do Banco YETU estejam de acordo com as melhores práticas e em estrita conformidade com as leis e normas vigentes;
- Que não seja efectuada nenhuma transacção ilegal;

Que todos Colaboradores do Banco YETU conheçam e sigam as regras estabelecidas, a fim de conhecer os Clientes e contrapartes e identificar eventuais operações suspeitas.

## 4| CONCEITOS

Para efeitos da presente Política considera-se:

**Branqueamento de Capitais:** É a participação em qualquer actividade que tenha como finalidade adquirir, deter, utilizar, converter, transferir, ocultar ou disfarçar a natureza, a origem, a localização, a disposição, o movimento ou a propriedade efectiva de bens ou direitos sobre bens, sabendo que os ditos bens têm origem numa actividade ilícita ou da participação numa actividade ilícita.

**Financiamento do Terrorismo:** Consiste no fornecimento, no depósito, na distribuição ou na recolha de fundos, por qualquer meio, de forma directa ou indirecta, com a intenção de os utilizar ou com o conhecimento de que serão utilizados integralmente ou em parte, para a execução de qualquer acto terrorista.

**Proliferação de Armas de Destruição em Massa:** Transferência e exportação de armas nucleares, químicas ou biológicas, materiais relacionados e os seus meios de entrega.

**Pessoas Politicamente Expostas:** Indivíduos nacionais ou estrangeiros que desempenham ou desempenharam funções públicas proeminentes em Angola, ou em qualquer outro País ou jurisdição ou em qualquer organização internacional.

**Compliance Officer:** Responsável pela coordenação e monitorização da implementação do Sistema de prevenção de Branqueamento de Capitais, Financiamento do Terrorismo e da Proliferação de Armas de Destruição em Massa, incluindo dos respectivos procedimentos de Controlo Interno, bem como pela centralização da informação e comunicação de operações susceptíveis de BC/FT e Proliferação de Armas de Destruição em Massa à Unidade de Informação Financeira (UIF) e outras autoridades competentes.

**Colaborador:** Qualquer pessoa singular que, em nome ou interesse do Banco e sob a sua autoridade ou na sua dependência, participe na execução de quaisquer operações, actos ou procedimentos próprios da actividade prosseguida por aquele, independentemente de ter com a mesma um vínculo de natureza laboral (Colaborador Interno) ou não (Colaborador Externo).

**Colaborador Relevante:** Qualquer Colaborador, interno ou externo, do Banco, que preencha, pelo menos, uma das seguintes condições:

- Ser membro do respectivo órgão de administração;
- Exercer funções que impliquem o contacto directo, presencial ou à distância, com os Clientes do Banco;
- Estar afecto às áreas funcionais de controlo do cumprimento do quadro normativo, de gestão de riscos ou de auditoria interna;
- Ser qualificado como tal pelo Banco.

**Operações Suspeitas:** Operações que suscitem indícios à prática do crime de BC/FT e Proliferação de Armas de Destruição em Massa.

**Beneficiário efectivo:** Pessoa ou pessoas singulares que detém, em última instância, uma participação no capital de uma pessoa colectiva ou a controlam e/ou a pessoa singular em cujo nome a operação está sendo realizada.

**Cliente:** Pessoa singular ou colectiva, grupo de pessoas singulares ou colectivas, públicas ou privadas, coligadas ou não, agindo em conjunto, vinculadas contratualmente ao Banco a quem este coloca à disposição, produtos ou serviços.

Geralmente, do processo de branqueamento de capitais, muito vinculado com o financiamento do terrorismo, constam 3 (três) fases:

- **Colocação:** Introduzir o numerário proveniente de actividades ilícitas em instituições financeiras ou não financeiras;



- **Diversificação:** A desvinculação dos rendimentos procedentes de uma actividade ilícita, através da utilização de diversas operações financeiras ou não financeiras complexas;
- **Integração:** O retorno dos rendimentos branqueados no sector da economia de onde procediam ou outro sector diferente, com uma aparência de legitimidade.

## 5| MODELO DE GOVERNAÇÃO DO RISCO OPERACIONAL

### 5.1| RESPONSABILIDADE DO ÓRGÃO DE ADMINISTRAÇÃO

1. Aprovar e aplicar as políticas e os procedimentos e controlos internos proporcionais ao risco identificado;
2. Ter conhecimento adequado dos riscos de BC/FT e da proliferação de armas de destruição em massa a que o Banco YETU se encontra a todo o tempo exposta, bem como dos processos utilizados para identificar, avaliar, acompanhar e controlar esses riscos;
3. A implementar políticas e procedimentos e controlos internos, de modo a prevenir situações de conflitos de interesse;
4. Promover uma cultura de prevenção do BC/FT e da proliferação de armas de destruição em massa que abranja todos os Colaboradores do Banco YETU cujas funções sejam relevantes neste âmbito, sustentada em elevados padrões de ética e de integridade e, sempre que necessário, na definição e aprovação de códigos de conduta apropriados;
5. Acompanhar a actividade dos demais membros da direcção de topo, na medida em que estes tutelem áreas de negócio que estão ou possam vir a estar expostas a riscos de branqueamento de capitais, financiamento do terrorismo e da proliferação de armas de destruição em massa;
6. Avaliar periodicamente à eficácia das políticas e dos procedimentos e controlos internos, assegurando a execução das medidas adequadas à correcção das deficiências detectadas;
7. Abster-se de qualquer interferência no exercício do dever de comunicação, sempre que se conclua a existência de potenciais suspeitas;
8. Garantir que o *Compliance Officer* exerça as suas funções de modo independente, permanente, efectivo e com autonomia decisória necessária a tal exercício;
9. Garantir que o *Compliance Officer* dispõe da idoneidade, qualificação profissional e responsabilidade adequadas ao exercício da função, sendo os resultados desta avaliação disponibilizados ao Banco Nacional de Angola (BNA) sempre que solicitado;
10. Garantir que o *Compliance Officer* dispõe de meios e recursos técnicos, matérias e humanos adequados, incluindo os Colaboradores necessários ao bom desempenho da função;
11. Garantir que o *Compliance Officer* tem acesso sem restrição e atempado a toda informação referente à execução do dever de identificação e diligência e aos registos das operações efectuadas e não se encontra sujeita a potenciais conflitos funcionais, em especial quando não se verifique a segregação das suas funções.

## 5.2| ESTRUTURA DO GABINETE DE COMPLIANCE

O Banco YETU designou, de acordo com a natureza, dimensão e complexidade da sua actividade, um *Compliance Officer* e garante que:

1. Exerce as suas funções com autoridade e independência permanente, efectiva e com autonomia decisória, com o apoio do Órgão de Gestão;
2. Dispõe de meios e recursos técnicos, materiais e humanos adequados;
3. Não se encontra sujeito a potenciais conflitos funcionais, em especial quando não se verifique a segregação de funções;
4. Dispõe de idoneidade, da qualificação profissional e da disponibilidade adequada ao exercício da função;
5. Tem acesso irrestrito e atempado a toda a informação interna relevante para o exercício da função, em particular a informação referente à execução do dever de identificação e diligência e aos registos das operações efectuadas.

## 5.3| PRINCIPAIS RESPONSABILIDADES DO COMPLIANCE OFFICER

São consideradas como principais responsabilidades do *Compliance Officer*:

1. Coordenar e monitorar a aplicação efectiva das políticas e dos procedimentos e controlos adequados à gestão eficaz dos riscos de branqueamento de capitais, financiamento do terrorismo e da proliferação de armas de destruição em massa a que a entidade financeira esteja ou venha a estar exposta;
2. Participar na definição e emitir parecer prévio sobre as políticas e os procedimentos e controlos destinados a prevenir o branqueamento de capitais, financiamento do terrorismo e da proliferação de armas de destruição em massa;
3. Acompanhar, em permanência, a adequação, a suficiência e a actualidade das políticas e dos procedimentos e controlos em matéria de prevenção do branqueamento de capitais, financiamento do terrorismo e da proliferação de armas de destruição em massa, propondo as necessárias actualizações;
4. Participar na definição, acompanhamento e avaliação da política de formação interna do Banco;
5. Assegurar a centralização de toda a informação relevante que provenha das diversas áreas de negócio do Banco YETU;
6. Comunicar, sem interferências internas ou externas, as operações à Unidade de Informação Financeira (UIF);
7. Acompanhar e avaliar os processos e procedimentos de controlo interno em matéria de prevenção e detecção de actividades criminosas, incluindo a prevenção do BC/FT, assim como assegurar a centralização da informação e a comunicação legalmente devidas, neste âmbito, com as autoridades competentes, designadamente à UIF;
8. Apoiar na preparação e execução das avaliações previstas no artigo 9.º da Lei n.º 05/20, de 27 de Janeiro e no artigo 9.º do Aviso n.º 14/2020, de 25 de Junho;
9. Coordenar a elaboração dos reportes, relatórios e demais informações a enviar ao BNA em matéria de prevenção do BC/FT.
10. Estabelecer processos para detectar e avaliar o risco decorrente do incumprimento das obrigações legais e dos deveres da Instituição, bem como para correcção das deficiências detectadas;

11. Estabelecer e manter um registo permanente e actualizado dos normativos internos e legislação vigente a que o Banco está sujeito, com identificação dos responsáveis pelo seu cumprimento e pelos incumprimentos detectados;
12. Monitorar o cumprimento das políticas de governança corporativa do Banco YETU, nomeadamente, conflito de interesses e código de conduta;
13. Elaborar relatórios periódicos para o órgão de administração em matérias de compliance, designadamente, indícios ou situações concretas de incumprimento das regras de conduta, incluindo no relacionamento com os Clientes, bem como as situações em que o Banco YETU ou os seus Colaboradores estejam ou possam estar sujeitos à processos de transgressão;

## 6| POLÍTICAS DE PREVENÇÃO

Como elementos fundamentais das políticas do Banco YETU foram inseridas Normas de controlo e gestão dos riscos e, especificamente no que respeita ao relacionamento com os Clientes, respectivos representantes ou transacções, incluindo programas de conhecimento dos seus Clientes (Know Your Customer). Neste domínio estão incluídas 05 (cinco) políticas fundamentais:

- Política de Aceitação e Recusa de Clientes;
- Política de Identificação e Verificação de Clientes e Aplicação de Medidas de Diligência;
- Política de Gestão de Conflitos de Interesses e Transacções com Partes Relacionadas;
- Política de Sanções Financeiras;
- Política de Congelamento e Descongelamento de Fundos.

### 6.1| POLÍTICA DE ACEITAÇÃO E RECUSA DE CLIENTES

No âmbito dos procedimentos de combate ao BC/FT, e no cumprimento dos normativos regulamentares e das recomendações das entidades relevantes, o Banco adopta políticas e procedimentos claros de aceitação de Clientes, incluindo a caracterização dos tipos de Clientes que implicam um risco mais elevado.

São tomados em atenção factores relevantes para a definição do nível de risco dos Clientes, designadamente, o país de origem, o perfil profissional e a sua eventual participação em actividades políticas, o ramo de negócio do Cliente e as transacções que pretende realizar.

Tendo como objectivo proteger o Banco YETU de práticas que possam colocar em risco a sua actividade e de forma a proteger a sua reputação, o Banco YETU recusa quaisquer potenciais Clientes que se enquadrem em alguma das seguintes categorias:

- Pessoas cuja informação disponível sugere que estes possam estar relacionados com actividades ilícitas, nomeadamente as incluídas em alguma das listas oficiais de sanções;
- Pessoas cuja actividade ou fonte de rendimento seja, directa ou indirectamente, o comércio de armas, ou outros equipamentos de natureza ou finalidade bélica;
- Pessoas relativamente às quais o Banco disponha de informação que as associe a actividades criminosas;
- Clientes ou beneficiários efectivos que residam em paraísos fiscais ou outros territórios de Risco identificados pelo GAFI;
- Clientes que realizem negócios nos quais não é possível verificar a legitimidade das actividades ou a origem dos fundos;
- Pessoas que recusem fornecerem informações ou a documentação necessária;
- Pessoas cuja actividade ou modo de vida torne inviável ou difícil o conhecimento, pelo Banco, da origem do respectivo património;
- Casas de câmbio, prestadores de serviço de transferências de dinheiro ou outras entidades similares, não autorizadas pelos organismos com competências para tal;
- Bancos de fachada.

O Banco YETU tem um processo de aprovação de potenciais Clientes, fazendo depender da autorização do *Compliance Officer* (que por sua vez pode decidir a necessidade de autorização por parte do CE), a aceitação de Clientes que se enquadrem em alguma das seguintes categorias:

- Pessoas qualificadas com nível elevado de risco de branqueamento de capitais;
- Pessoas Politicamente Expostas (PEP's);
- PEP's que pretendam ser Clientes no país ou fora do país de que são nacionais;
- Membros próximos da família dos PEP's, incluindo as pessoas que com estes convivam em situação de facto;
- Outras pessoas, singulares ou colectivas, que reconhecidamente tenham com os PEP's ou respectivos familiares com estreitas relações de natureza comercial ou societária;
- Outras pessoas titulares de outros cargos públicos relevantes.

**Para estes casos devem ser aplicadas medidas de diligência reforçada, nomeadamente:**

- Uma autorização da Comissão Executiva para que seja iniciada uma relação de negócio, que será registada (sempre que o Compliance Officer considerar necessário obter esta autorização);
- Acompanhamento reforçado e permanente da relação de negócio;
- No que diz respeito a pessoas singulares, corroborar informação sobre a actividade do Cliente, consultando as suas fontes ou outras fontes externas;
- No caso de pessoas colectivas, um certificado sobre a titularidade da transacção (pessoas singulares com participação directa ou indirecta ou controlo de 25% ou mais da pessoa colectiva);

No caso de pessoas colectivas, é verificada a veracidade das informações fornecidas pelo Cliente na sua actividade profissional ou empresarial, facto que pode ser evidenciado Relatório e Contas do ano anterior.

## **6.2| POLÍTICA DE IDENTIFICAÇÃO DE CLIENTES E APLICAÇÃO DE MEDIDAS DE DILIGÊNCIAS**

O Banco YETU recolhe e conserva a informação relativa aos Clientes, aos seus representantes e beneficiários efectivos, antes do início da relação de negócio, solicitando os seguintes elementos:

### **Pessoas singulares**

1. Nome completo e assinatura;
2. Data de Nascimento;
3. Nacionalidade;
4. Morada completa da residência ou, caso não seja possível, quaisquer outros contactos considerados como válidos pela instituição financeira bancária;
5. Profissão e entidade patronal, quando existam;
6. Nome do documento de identificação utilizado, número de identificação, data de expiração e entidade emissora;
7. Natureza e montante do rendimento;
8. Número de Identificação Fiscal (facultativo).

Os presentes elementos são verificados da seguinte forma:

- No que concerne aos elementos de identificação mencionados nos pontos 1), 2) e 3):
  - a) Pelos residentes cambiais mediante apresentação do bilhete de identidade ou cartão de residente emitido pelo órgão competente, onde conste fotografia, nome completo, data de nascimento e nacionalidade;
  - b) Pelos não residentes cambiais mediante apresentação do passaporte, à excepção de não residentes cambiais de nacionalidade angolana mediante apresentação de bilhete de identidade, onde conste fotografia, nome completo, data de nascimento e nacionalidade.
- O elemento de identificação mencionado no ponto 8) é verificado mediante a apresentação de cartão de identificação fiscal ou equivalente emitido pela Direcção Nacional de Impostos do Ministério das Finanças.

**Pessoas colectivas**

1. Denominação social completa da pessoa colectiva;
2. Objecto social e finalidade do negócio;
3. Endereço da sede;
4. Número de Identificação fiscal (NIF);
5. Número de matrícula do registo comercial;
6. Identidade dos titulares de participações no capital e dos direitos de voto da pessoa colectiva de valor igual ou superior a 20%;
7. Identidade dos procuradores da pessoa colectiva e respectivo mandato;
8. Relativamente aos comerciantes em nome individual, são solicitados o NIF, a denominação social, a sede e o objecto social, para além dos elementos de identificação referidos na alínea 1).

Os presentes elementos são verificados da seguinte forma:

- Em relação às pessoas colectivas residentes, os elementos de identificação mencionados nos pontos 1), 2), 3) e 4) são verificados mediante a apresentação da certidão do registo comercial emitida pela Conservatório do Registo Comercial ou outro documento público comprovativo, nomeadamente o exemplar do Diário da República contendo a publicação dos estatutos ou certidão notarial de escritura da constituição;
- Em relação às pessoas colectivas não residentes, os elementos de identificação mencionados nos pontos 1), 2) e 3) são verificados mediante a apresentação de comprovativo do registo comercial ou outro documento público válido, devidamente certificado pelas entidades competentes do país de residência, e autenticado pela representação consular de Angola no país de origem;
- O elemento de identificação mencionado no ponto 4) é verificado mediante a apresentação do Cartão de Identificação Fiscal ou equivalente emitido pela Direcção Nacional de Impostos do Ministério das Finanças;
- Os elementos de identificação mencionados no ponto 6) são comprovados mediante apresentação da Acta da Assembleia-Geral Constituinte assim como a acta de alteração à estrutura accionista ou de sócios;
- O elemento de identificação mencionado no ponto 7) é comprovado mediante declaração escrita emitida pela própria pessoa colectiva, contendo o nome dos titulares do órgão de gestão, procuradores e representantes.

No estabelecimento da relação de negócio em nome de menores que, em razão da sua idade, não sejam titulares de quaisquer dos documentos referidos no ponto 1), a comprovativo dos respectivos elementos de identificação do menor é efectuada mediante exibição de cédula pessoal se for residente cambial ou no caso de não residente cambial, por documento público equivalente, a apresentar por quem demonstre legitimidade enquanto seu representante legal para o estabelecimento da relação de negócio sendo verificada a respectiva identidade do mesmo aquando do início da relação de negócio.



### 6.3| POLÍTICA DE GESTÃO DE CONFLITOS DE INTERESSES E TRANSAÇÕES COM PARTES RELACIONADAS

O Banco YETU mantém, por um período mínimo de 10 (dez) anos, todos os registos necessários, estes registos incluem:

1. Cópias dos documentos comprovativos do cumprimento da obrigação de identificação e de diligência;
2. Registo de transacções nacionais e internacionais que sejam suficientes para permitir a reconstituição de cada operação, de modo a fornecer, se necessário, provas no âmbito de um processo criminal; toda a documentação relacionada com transacções realizadas com Bancos correspondentes;
3. Registos dos resultados de investigações internas, assim como registo da cópia das comunicações efectuadas pelo Banco YETU à UIF e a outras autoridades competentes;
4. Fundamentação da decisão de não comunicação à UIF e outras autoridades competentes pelo Banco YETU.

O Banco YETU garante que todos os registos relativos a transacções e a Clientes se encontram disponíveis atempadamente, para que a autoridade competente, de acordo com a legislação aplicável, os possa consultar caso considere necessário. Os registos são conservados em documentos originais, na forma de documentos físicos.

O Banco YETU realiza periodicamente a monitorização e controlo de operações realizadas por Clientes através de:

1. Manutenção regular da actualização da informação disposta;
2. Análise regular das transacções efectuadas pelos Clientes do Banco e registadas em sistema;
3. Verificação do risco dos Clientes com base na monitorização manual regular da base de dados de Clientes face a listas de *Anti-Money Laundering* (AML) e identificação de indícios de situações de branqueamento de capitais;
4. Emissão de parecer sobre operações suspeitas por parte do *Compliance Officer*.

A posterior avaliação de risco de BC/FT tem em conta os seguintes factores:

1. Natureza do Cliente;
2. Natureza da actividade do Cliente;
3. Forma de estabelecimento da relação de negócio;
4. Localização geográfica do Cliente e da sua actividade, se aplicável;
5. Transacções efectuadas;
6. Histórico do Cliente;
7. Produtos e serviços adquiridos.

## 6.4 | POLÍTICA DE SANÇÕES FINANCEIRAS

**Sanções financeiras** são medidas restritivas de natureza financeira implementadas por organizações internacionais ou por países (a título individual) aplicáveis a jurisdições, pessoas ou entidades com o propósito de combater o terrorismo e manter ou restaurar a paz e a segurança internacional.

De entre os países ou organizações internacionais que mantêm listas de pessoas, grupos ou entidades designadas destaca-se, entre outros o *Office for Foreign Assets and Control (OFAC)*, *Her Majesty's Treasury (HMT)*, o *European Union's Common Foreign and Security Policy (CFSP)* e o Comité de Sanções de acordo com as diferentes Resoluções do Conselho de Segurança das Nações Unidas (CSNU).

**Pessoas, grupos ou entidades designadas:** são as pessoas, grupos ou entidades designadas:

1. Pelo Comité de Sanções das Nações conforme a Resolução do Conselho de Segurança das Nações Unidas N.º 1267, mediante a Lista actualizada pelo referido Comité de Sanções;
2. Pelo Comité de Sanções conforme a Resolução do Conselho de Segurança das Nações Unidas N.º 1988, que mantém uma Lista actualizada de pessoas, grupos e entidades associados com os Talibã, que constituam uma ameaça para a paz, estabilidade e segurança do Afeganistão;
3. Por qualquer outro Comité de Sanções criado pela Organização das Nações Unidas ou outro organismo da Organização das Nações Unidas que mantenha listas de pessoas, grupos ou entidades associadas ao terrorismo, incluindo o financiamento do terrorismo, a terroristas ou a organizações terroristas, com vista à aplicação de medidas restritivas de natureza financeira; e
4. Pela autoridade nacional competente pela designação nacional e aplicação de medidas restritivas, mediante Lista nacional, conforme a Lei n.º 1/12, de 12 de Janeiro - Lei sobre a Designação e Execução de Actos Jurídicos Internacionais, sempre que a designação for relativa a pessoas, grupos ou entidades associadas ao terrorismo, incluindo o financiamento do terrorismo, a terroristas ou a organizações terroristas, com vista à aplicação de medidas restritivas de natureza financeira.

Caso algum Cliente apresente indícios, o Gabinete de Compliance contacta o titular de conta para identificar a justificação para a realização da operação suspeita e emitir parecer sobre operação suspeita, caso se confirmem as suspeitas este segrega a operação suspeita e comunica a ocorrência e o seu parecer ao CA para análise final e comunicação à UIF.

## **6.5| POLÍTICA DE CONGELAMENTO E DESCONGELAMENTO DE FUNDOS**

### **6.5.1| Obrigação de Congelamento de Fundos**

O Banco YETU deve congelar de forma imediata e sem qualquer aviso prévio, todos os fundos ou recursos económicos pertencentes, possuídos ou detidos, directa ou indirectamente, individualmente ou em conjunto.

O congelamento de fundos consiste num bloqueio operacional realizado na(s) conta(s) bancária(s) identificada(s), de forma que não seja permitido o lançamento da(s) conta(s) bancária (s) a débito seja em que circunstância for.

### **6.5.2| Descongelamento de Fundos**

Sempre que o Banco YETU receber da autoridade competente instruções claras que indiquem o levantamento da medida de restrição financeira, relativamente a uma entidade designada, deve proceder imediatamente ao levantamento dos bloqueios operacionais existentes e à libertação dos fundos congelados.

## 7 | FERRAMENTAS E APLICATIVOS INFORMÁTICOS

Encontra-se implementada uma aplicação tecnológica que permite a avaliação, gestão e mitigação do risco e reporte, tais como:

1. Avaliar o perfil de risco associado aos Clientes, relações de negócio, transacções ocasionais e operações em geral;
2. Monitorar Clientes e operações face aos riscos identificados, incluindo a detecção atempada de alterações relevantes ao padrão operativo de um dado Cliente ou conjunto de Clientes relacionados entre si e operações ou conjunto de operações que denotem elementos caracterizadores de suspeição;
3. Detectar a aquisição da qualidade de pessoa politicamente exposta ou de titular de outro cargo político ou público, bem como de qualquer outra qualidade específica que deva motivar a intervenção de um membro da direcção de topo ou de outro elemento de nível hierárquico superior;
4. Detectar pessoas ou entidades identificadas em medidas restritivas, designadamente as que decorram de resolução do Conselho de Segurança das Nações Unidas, ou outras;
5. Bloquear ou suspender o estabelecimento ou prosseguimento de uma relação de negócio, bem como da realização de uma transacção ocasional ou operação em geral, sempre que dependam da intervenção de um membro da direcção de topo ou de outro elemento de nível hierárquico superior;
6. A extracção tempestiva de informação fiável e compreensível que suporte a análise e a tomada de decisões pelas estruturas internas relevantes, bem como o exercício das obrigações de comunicação e de colaboração legalmente previstos.

## **8| MECANISMOS DE IDENTIFICAÇÃO DO BENEFICIÁRIO EFECTIVO**

O Banco YETU solicita ao beneficiário efectivo os mesmos elementos e documentos comprovativos da identificação que exigiria ao Cliente.

Os meios apropriados de determinação da identidade do beneficiário efectivo devem incluir, nomeadamente:

- Documento autenticado que confirme a identidade do beneficiário efectivo;
- Cópia do acordo fiduciário ou acordo de parceria, ou outro documento equivalente;
- Acta da Assembleia Geral constituinte assim como a acta de alteração à estrutura accionista ou de sócios;
- Outra informação fidedigna, e que a instituição financeira considere relevante.

## 9| TRANSAÇÕES OCASIONAIS

O Banco YETU recolhe e conserva a informação sempre que, presencialmente ou à distância, um Cliente pretenda efectuar transacções ocasionais, cujo montante seja superior em moeda nacional ou outra, ao equivalente a USD 15.000,00 (Quinze Mil Dólares Americanos), independentemente da transacção ser realizada mediante uma única operação ou através de várias operações que aparentem estar relacionadas.

Consideram-se operações relacionadas, entre outras, as que observam uma das seguintes condições:

1. Vários remetentes para um mesmo beneficiário;
2. Um remetente para vários beneficiários.

Caso seja solicitada a realização de transacções ocasionais em nome de menores a comprovação dos respectivos elementos de identificação do menor deve ser efectuada mediante exibição de cédula pessoal caso seja residente cambial ou documento público equivalente caso seja residente não cambial, a apresentar por quem demonstre legitimidade enquanto seu representante legal, para realizar a transacção ocasional devendo ser verificada a respectiva identidade do mesmo aquando da realização da transacção ocasional.

## 10 | PESSOAS POLITICAMENTE EXPOSTAS

São consideradas PEP's os indivíduos nacionais ou estrangeiros que desempenham ou desempenharam funções públicas proeminentes em Angola, ou em qualquer outro país ou jurisdição ou em qualquer organização internacional:

Consideram-se altos cargos de natureza política ou pública, de entre outros, os seguintes:

1. Presidente da República ou Chefe de Estado;
2. Vice-Presidente da República;
3. Primeiro-Ministro ou Chefe de Governo;
4. Órgãos Auxiliares do Presidente da República, ou membros do Governo, designadamente Ministros de Estado, Ministros, Secretários de Estado e outros cargos ou funções equiparadas;
5. Deputados, membros de Câmaras Parlamentares e equiparados;
6. Magistrados judiciais dos tribunais superiores e da Relação, cujas decisões não possam ser objecto de recurso, salvo em circunstâncias excepcionais;
7. Magistrados do Ministério Público de escalão equiparado aos Magistrados Judiciais referidos no número anterior;
8. Provedor de Justiça e Provedor de Justiça Adjunto;
9. Membros do Conselho da República, do Conselho de Segurança Nacional e demais Conselheiros de Estado;
10. Membros da Comissão Nacional Eleitoral;
11. Membros dos Conselhos Superiores da Magistratura Judicial e do Ministério Público;
12. Membros de Órgãos de Administração e fiscalização dos Bancos Centrais e outras autoridades de regulação e supervisão do sector financeiro;
13. Chefes de missões diplomáticas e de postos consulares;
14. Oficiais Gerais das Forças Armadas e Oficiais Comissários das Forças de Segurança e Ordem Interna;
15. Membros de órgãos de administração e de fiscalização de empresas públicas e de sociedades de capitais exclusiva ou maioritariamente públicos, institutos públicos, associações e fundações públicas, estabelecimentos públicos, qualquer que seja o modo da sua designação, incluindo os órgãos de gestão das empresas integrantes dos sectores empresariais locais;
16. Membros do Conselho de Administração, Directores, Directores Adjuntos e ou pessoas que exercem funções equivalentes numa organização internacional;
17. Membros dos órgãos executivos de Direcção de partidos políticos;
18. Membros das administrações locais e do poder autárquico;
19. Líderes de confissões religiosas.

São também tratadas como PEP's, os membros da família e as pessoas muito próximas dos indivíduos acima mencionados, nomeadamente:

1. O cônjuge ou companheiro de união de facto;
2. Os parentes, até ao 3.º Grau da linha colateral, os afins até ao mesmo grau, os respectivos cônjuges ou companheiros de união de facto;
3. Pessoas com reconhecidas e estreitas relações de natureza pessoal;
4. Pessoas com reconhecidas e estreitas relações de natureza societária ou comercial, nomeadamente:
  - a) Qualquer pessoa singular, que seja notoriamente conhecida como proprietária em conjunto de uma pessoa colectiva com o titular do alto cargo de natureza política ou pública ou que com ele tenha relações comerciais próximas;
  - b) Qualquer pessoa singular que seja proprietária do capital social ou dos direitos de voto de uma pessoa colectiva ou do património de um centro de interesses colectivos sem personalidade jurídica, que seja notoriamente conhecido, tendo como único beneficiário efectivo o titular do alto cargo de natureza política ou pública.



## 11 | PROCEDIMENTOS DE DILIGÊNCIAS

### 11.1 | DILIGÊNCIA SIMPLIFICADA

O Banco YETU aplica procedimentos de diligência simplificada, desde que disponha de informação suficiente para o efeito de uma avaliação de risco consistente, devendo igualmente o Cliente estar enquadrado numa das seguintes categorias:

1. Estado, ou uma pessoa colectiva de direito público, de qualquer natureza, integrada na administração central ou local;
2. Autoridade ou organismo público sujeito a práticas contabilísticas transparentes e objecto de fiscalização;
3. Pessoas singulares titulares de conta bancária simplificada;
4. O Banco YETU deve demonstrar ao BNA, caso este assim o entenda, a verificação do enquadramento dos Clientes nas categorias acima mencionadas;
5. O Banco YETU deve definir critérios para determinar se a informação recolhida é suficiente para verificar que o Cliente se enquadra numa das categorias ou profissões acima referidas, nomeadamente, a existência de informação pública disponível que confirme a sua identidade.

### 11.2 | DILIGÊNCIA REFORÇADA

Atendendo às suas características, determinados Clientes e operações apresentam um risco acrescido de BC/FT, pelo que o Banco YETU adoptou medidas reforçadas, nomeadamente:

1. Entidades sem fins lucrativos;
2. Relações de correspondência Bancária;
3. Pessoas politicamente expostas (PEP's);
4. Pessoas de perfis de risco elevado (PPER's);
5. Clientes ou operações relacionadas com países de risco elevado de BC;
6. Quando a avaliação de risco do Banco indica que a relação de negócio ou transacção ocasional tem um risco elevado de BC/FT;
7. Quando previsto legalmente.

#### As diligências reforçadas consistem:

1. Na obtenção de informação do Cliente sobre e destino dos seus fundos bem como na elaboração de um relatório sobre as medidas adoptadas;
2. Na monitorização contínua e reforçada da relação de Negócio;
3. Na obtenção de documentação adicional, sobre a estrutura organizacional, localização geográfica, destino dos fundos, incluindo informação básica dos beneficiários, caso seja necessário;
4. Origem dos rendimentos;
5. Na exigência de autorização expressa do órgão de Gestão do Banco YETU para o estabelecimento/ ou manutenção da relação de negócios, sempre que necessário;
6. Na solicitação de informações suplementares de forma a compreender a natureza de sua actividade.

## 12 | DEVER DE MONITORIZAÇÃO CONTÍNUA

O Banco YETU mantém um acompanhamento contínuo da relação de negócio, bem como dos perfis de risco do mesmo, e deve ser solicitada a seguinte informação:

1. Natureza e detalhes do negócio, da ocupação ou do emprego;
2. Registo de mudanças de domicílio;
3. Origem e destino dos fundos a serem usados na relação de negócio;
4. Origem dos rendimentos iniciais e contínuos;
5. As várias relações entre signatários e os respectivos beneficiários efectivos, em função das transacções efectuadas pelos Clientes e do resultado da avaliação de risco, o Banco YETU, pode, sempre que considere necessário, solicitar informação adicional aos Clientes, tais como comprovativo de origem de fundos, o Relatório Anual e Contas e outros documentos complementares.

### **13 | COMUNICAÇÃO DE IRREGULARIDADES**

O Banco YETU implementou canais específicos, independentes e confidenciais que internamente asseguram, de forma adequada, a recepção, o tratamento e o arquivo das comunicações de irregularidades relacionadas a sua integridade e com eventuais violações à Lei n.º 05/20, de 27 de Janeiro - Lei de Prevenção e Combate ao Branqueamento de Capitais, do Financiamento do Terrorismo e da Proliferação de Armas de Destrução em Massa e nos termos do Aviso n.º 14/2020, de 22 de Junho - Regras de Prevenção e Combate ao Branqueamento e Capitais e Financiamento do Terrorismo.

## 14 | REGIME TRANSGRESSIONAL

As informações prestadas de boa-fé pelas entidades sujeitas no âmbito de uma determinada operação que evidencia fundada suspeita e, que seja susceptível de constituir crime não constitui violação do dever de segredo, nem implica a responsabilização de quem efectue a comunicação.

Sem prejuízo da responsabilidade penal pelo crime de branqueamento a que podem estar sujeitas tanto as pessoas singulares como as pessoas colectivas ou de outras disposições sancionatórias conexas aplicáveis a cada caso concreto, estão tipificadas contra-ordenações pelo incumprimento dos deveres e obrigações impostos pela Lei n.º 5/20, de 27 de Janeiro - Lei de Prevenção e Combate ao Branqueamento de Capitais, do Financiamento do Terrorismo e da Proliferação de Armas de Destruição em Massa e o Aviso n.º 14/20, de 22 de Junho - Regras de Prevenção e Combate ao Branqueamento e Capitais e Financiamento do Terrorismo, pelas quais podem ser responsabilização as entidades financeiras.

O Banco YETU é responsável pelas infracções quando os factos tenham sido praticados, no exercício das respectivas funções ou em seu nome ou por sua conta, pelos titulares dos seus Órgãos Sociais, Representantes ou qualquer Colaborador, permanente ou ocasional.

A responsabilidade da pessoa colectiva não exclui a responsabilidade individual dos respectivos agentes.

## 15| COMUNICAÇÃO DE OPERAÇÕES SUSPEITAS

O Banco YETU sempre que saiba, suspeite ou tenha razões suficientes para suspeitar que teve lugar, está em curso ou foi tentada uma operação susceptível de estar associada à prática do crime de BC/FT ou de qualquer outro crime tomará a iniciativa própria de informar, de imediato à UIF.

Ao reportar uma actividade suspeita à UIF, o Banco YETU preenche o formulário relativo à Declaração de Operação Suspeita (DOS). Este documento assegura que toda a informação necessária à sua análise está incluída no mesmo.

O Banco YETU compromete-se a facultar informação relativa aos seus Clientes ou transacções suspeitas, sempre que for solicitada pelas autoridades competentes.

## **16| COLABORAÇÃO COM O REGULADOR E OUTRAS ENTIDADES DE SUPERVISÃO**

O *Compliance Officer* do Banco YETU assegura a prestação de toda a assistência requerida pela autoridade responsável pela condução dos processos de investigação, ou pelas autoridades competentes de supervisão e fiscalização, garantindo o acesso directo e transparente às informações e apresentando os documentos ou os registos solicitados pelas mesmas.

Os pedidos de informação relativamente ao branqueamento de capitais de origem criminosa, dirigidos ao Banco YETU emitidos por Tribunais ou Juízes ou qualquer outra autoridade, são enviados directamente pelo Representante nomeado, que responde à autoridade.

## 17 | CONTRATAÇÃO DE COLABORADORES

No que diz respeito à contratação de novos Colaboradores, é reunida toda a informação referente ao percurso profissional e ao registo criminal do candidato e caso não se verifique histórico de actividades ilícitas e que não apresentam nível de risco elevado (e.g. dificuldade de obtenção de informação sobre o candidato) o candidato estará apto a integrar a equipa do Banco YETU.

Candidatos que tenham residência em países de riscos indicados pelo GAFI ou que sejam estrangeiros com cargos públicos são alvo de análise aprofundada.

O Banco YETU, no acto de contratação dos Colaboradores (Seleccção e Obrigação de Identificação), deve efectuar uma avaliação fundamentada da confiabilidade e credibilidade de Colaboradores que pretenda indicar para funções de maior sensibilidade e risco na realização integral da sua actividade bem como da sua integridade.

## 18 | FORMAÇÃO DE COLABORADORES

O Banco YETU providencia periodicamente aos Colaboradores, conforme as suas diferentes necessidades, em particular, aos recém-admitidos, do front office, de supervisão ou com funções de Compliance, Auditoria, Gestão de Risco e Gestão Comercial para que estes estejam informados sobre:

- Legislação aplicável em sede de prevenção e repressão do branqueamento de capitais, combate ao financiamento do terrorismo e da Proliferação de Armas de Destruição em Massa;
- Os riscos de branqueamento de capitais, do financiamento do terrorismo e da Proliferação de Armas de Destruição em Massa;
- Procedimentos de identificação e comunicação das operações suspeitas às entidades de supervisão e outras afins;
- O Sistema de Controlo Interno e de avaliação de risco no âmbito da prevenção de branqueamento de capitais, do financiamento do terrorismo e da Proliferação de Armas de Destruição em Massa;
- Os riscos reputacionais, legais e prudenciais e as consequências de natureza transgracional decorrentes da inobservância das obrigações preventivas de BC/FT.

O Banco YETU realiza periodicamente acções de formação em matéria de BC/FT aos Colaboradores, conforme as suas diferentes necessidades, em particular, aos recém-admitidos, Colaboradores de front office, de supervisão ou com funções de Compliance, Auditoria, Gestão de Risco e Gestão Comercial para que estes estejam informados sobre:

- Risco de BC/FT;
- Legislação aplicável em sede de prevenção e repressão do branqueamento de capitais e combate ao financiamento do terrorismo;
- Procedimentos de identificação e comunicação das operações suspeitas às entidades adequadas;
- Sistema de controlo interno e de avaliação de risco no âmbito da prevenção de BC/FT.

O Banco YETU tem também como política a conservação durante um período de 05 (cinco) anos cópia dos documentos relativos à formação efectuados aos empregados e aos Colaboradores.



## 19 | RELAÇÃO DE CORRESPONDÊNCIA BANCÁRIA

O Banco YETU deve definir, implementar e controlar medidas de diligência específicas e apropriadas para a identificação e mitigação de riscos de branqueamento de capitais, financiamento do terrorismo e da proliferação de armas de destruição em massa que ocorram através das suas contas correspondentes, nomeadamente:

1. Entender a natureza da actividade da Instituição correspondente;
2. Identificação do país de origem da instituição correspondente e verificação do risco do país, nomeadamente embargos ou sanções impostas por Organizações Internacionais, níveis de criminalidade e corrupção, legislação no âmbito de branqueamento de capitais, financiamento do terrorismo e proliferação de armas de destruição em massa;
3. Verificação das políticas internas do Banco correspondente relativamente às normas internacionais de combate ao branqueamento de capitais e ao financiamento do terrorismo e da implementação efectiva de processos e procedimentos de controlos internos nesta matéria;
4. Verificação de que o Banco correspondente não permite que sejam mantidas contas anónimas nem contas sob nomes fictícios.

## 20 | AUDITORIA EXTERNA

As medidas de controlo interno descritas nesta Política são revistas anualmente por uma entidade externa competente.

Os resultados dos testes são registados em relatório escrito, que documenta as actuais medidas de controlo interno, avaliar a sua eficácia operacional e propor, se necessário, as devidas correcções ou melhorias.

O relatório, em qualquer caso, estará disponível às entidades de supervisão e fiscalização, durante os cinco (05) anos subsequentes à data de emissão, em caso de necessidade das mesmas.

## **21| DECLARAÇÃO DE PREVENÇÃO DO BC/FT**

O Banco YETU declara que conduz a sua actividade bancária em conformidade com os mais altos padrões éticos e põe em prática métodos de actuação e comportamento que permitem assegurar que os serviços do Banco não são usados como plataforma para operações de branqueamento de capitais, financiamento ao terrorismo ou outro tipo de actividade criminosa.

O Banco YETU compromete-se com os seguintes princípios presentes nesta Política:

1. Conduzir a sua actividade de acordo com a legislação e regulamentos vigentes;
2. Criar e aplicar normas de actuação e sistemas de controlo com o intuito de prevenir ou impedir que o Banco YETU seja usado como plataforma para actividades consideradas ilegais;
3. Garantir o conhecimento e alinhamento de todos os Colaboradores com as Políticas e procedimentos do Banco.

O Conselho de Administração aprova e realiza o acompanhamento desta Política, e qualquer alteração do seu conteúdo será levada ao conhecimento e validação do Conselho de Administração, mais informa que esta Política tem carácter obrigatório e é transversal a todos os elementos de todas as U.N. do Banco YETU.

## 22| DISPOSIÇÕES FINAIS

1. A manutenção desta Política é da responsabilidade do Gabinete de Compliance, ou seja, compete ao Gabinete de Compliance realizar quaisquer propostas para alteração e actualização que se revelem necessárias e apresentar à Comissão Executiva numa base anual para aprovação.
2. A Política deve ser anualmente revista pelo Gabinete de Compliance, tomando designadamente em consideração os contributos e propostas de melhoria sugeridos.
3. É responsabilidade do Conselho de Administração a ratificação desta Política antes da sua publicação.

## 23| ANEXOS

### 23.1| ANEXO 1 - LISTA DO CONJUNTO DE CATEGORIAS DE CRIMES SUBJACENTES AO CRIME DE BC

#### LISTA SOBRE O CONJUNTO DE CATEGORIAS DE CRIMES SUBJACENTES AO CRIME DE BRANQUEAMENTO DE CAPITAIS (40 RECOMENDAÇÕES GAFI)

- Participação num grupo criminoso organizado e em acções ilegítimas para obtenção de fundos, nomeadamente através de chantagem, intimidação ou outros meios;
- Terrorismo, incluindo o financiamento do terrorismo;
- Tráfico de seres humanos, incluindo tráfico de órgãos ou tecidos humanos e tráfico ilícito de migrantes;
- Exploração sexual, incluindo a exploração sexual de crianças;
- Tráfico de estupefacientes e de substâncias psicotrópicas;
- Tráfico de bens roubados e de outros bens;
- Corrupção;
- Suborno;
- Fraude;
- Contrafacção de moeda;
- Contrafacção;
- Pirataria de produtos;
- Crimes contra o ambiente, incluindo tráfico de espécies protegidas;
- Homicídio;
- Ofensas corporais graves;
- Rapto;
- Sequestro;
- Tomada de reféns;
- Roubo ou furto;
- Contrabando;
- Extorsão;
- Falsificação;
- Pirataria;
- Utilização abusiva de informação privilegiada e manipulação do mercado;
- Crimes fiscais;
- Lenocínio;
- Peculato.

## **23.2| ANEXO 2 - TIPOLOGIA DE OPERAÇÕES OU ACTIVIDADES SUSPEITAS IDENTIFICADAS PELA UIF PARA OS BANCOS E INSTITUIÇÕES FINANCEIRAS NÃO BANCÁRIAS LIGADAS À MOEDA E CRÉDITO.**

Neste sector, podemos encontrar as seguintes tipologias de operações ou actividades suspeitas ou indicadores de operações susceptíveis de estarem relacionadas com o Branqueamento de Capitais, financiamento do Terrorismo e Proliferação de Armas de Destruição em Massa:

- Um potencial cliente tem claramente um montante elevado em numerário na sua posse e abre várias contas ou adquire vários produtos com variações nos nomes das contas e o potencial cliente tem na sua posse várias moedas diferentes e pretende efectuar operações cambiais como parte da transacção;
- O cliente estrutura uma operação de forma a fraccionar o valor total em várias operações de montante mais reduzido, de modo a evitar que os limites estabelecidos sejam ultrapassados (*smurfing*);
- Um cliente estrangeiro utiliza Serviços de Remessas Alternativos (ARS) para transferir montantes significativos de dinheiro, sob a falsa finalidade de transferir dinheiro para a família no país estrangeiro;
- O cliente adquiriu vários produtos financeiros similares e movimenta fundos entre os mesmos, efectuando como suplemento pagamentos em numerário;
- O alto valor patrimonial de um cliente não é compatível com as informações a seu respeito nem com o respectivo negócio;
- Um cliente utiliza repetidamente um endereço, mas altera frequentemente os nomes envolvidos;
- O número de telefone profissional ou da residência do cliente foi desconectado ou é detectado que os mesmos são inexistentes aquando da tentativa de efectuar o primeiro contacto num curto espaço de tempo após a abertura da conta;
- O cliente encontra-se envolvido numa actividade pouco usual para o tipo de pessoa ou o tipo de negócio.