FÉNIX Pensões
SOCIEDADE GESTORA DE FUNDOS DE PENSÕES

POLÍTICA DE PREVENÇÃO E COMBATE AO BRANQUEAMENTO DE CAPITAIS E DO FINANCIAMENTO AO TERRORISMO E PROLIFERAÇÃO DE ARMAS DE DESTRUIÇÃO EM MASSA

2024

V 2.0

1. INTRODUÇÃO

Considerando que o desenvolvimento da actividade financeira e das tecnologias de informação e da comunicação proporcionaram o crescimento da economia, e ainda, o aumento do risco associado ao Branqueamento de Capitais e ao Financiamento do Terrorismo (BC/FT) e a proliferação de armas de Destruição em massa.

Com o intuito de implementar uma forte cultura e princípios de prevenção e combate ao branqueamento de capitais e cumprimento da legislação nacional, internacional e tendo em conta as melhores práticas em termos de actuação nos mercados, a Fénix, Sociedade Gestora de Fundos de Pensões implementou políticas, práticas e procedimentos cumprindo elevados padrões de ética e profissionalismo, de forma a evitar que a Sociedade possa ser utilizada ou sujeita, intencionalmente ou não, a práticas criminosas e de outra natureza que o possam sujeitar a níveis de risco operacional ou reputacional significativo, contribuindo assim, para a manutenção de elevados padrões de ética profissional e no equilíbrio do Sistema Financeiro Angolano.

A aplicação dessas práticas inclui regras de controlo e gestão dos riscos mais relevantes e, especificamente, no que respeita ao relacionamento com os Clientes, e respectivos representantes ou operações, abrange programas de conhecimento dos seus Clientes (*Know Your Customer - KYC*) e transacções.

Em consonância com as actividades desenvolvidas pela Fénix e que a presente política visa disciplinar, a expressão «cliente» abrange, também, os participantes e beneficiários efectivos dos Fundos de Pensões, bem como os seus Associados.

Assim sendo, a Fénix:

- Define o tipo de Clientes que está disposto a aceitar em termos de risco de Branqueamento de Capitais e Financiamento ao Terrorismo (BC/FT);
- Recolhe com objectividade e rigor a sua identificação e mantém actualizados os elementos de identificação e de informação que obtém no decurso da relação de negócio.

2. OBJECTIVO

No âmbito das metodologias de combate ao Branqueamento de Capitais e Financiamento ao Terrorismo (BC/FT) e no cumprimento dos normativos regulamentares e das recomendações das entidades relevantes, a Fénix desenvolveu políticas e procedimentos claros de aceitação de Clientes, incluindo a caracterização dos tipos de Clientes que possivelmente podem envolver um risco mais elevado para a instituição. No âmbito destas metodologias e procedimentos são tomadas em consideração factores relevantes para a definição do nível de risco dos Clientes.

Neste sentido, esta política tem como principal objectivo elencar os princípios adoptados pela Fénix para se precaver face aos diversos riscos a que se encontra exposto, no âmbito de BC/FT.

3. ÂMBITO

Esta Política obedece ao âmbito definido na "Prevenção e Combate ao Branqueamento de [illegible] em Massa", Aviso 3/21 de 06 de Dezembro da ARSEG - Regras sobre a implementação Efectiva das obrigações previstas na Lei n.º 5/20 de 27 de Janeiro, aplicada aos Clientes, pensionistas, participantes, representantes, beneficiários efectivos, outros intervenientes na operações e a todos os Colaboradores da Fénix

4. . TERMOS E DEFINIÇÕES

- **Relação de Negócio**: relação de natureza comercial ou profissional entre as entidades sujeitas e os seus Clientes que, no momento em que esta, efectivamente, se estabelece, se prevê que venha a ser ou seja duradoura.
- **Pessoas Politicamente Expostas (PPE´s)**: indivíduos nacionais ou estrangeiros que desempenham ou desempenharam funções públicas proeminentes em Angola ou em qualquer outro país ou jurisdição ou em qualquer outra organização internacional.
- **Unidade de Informação Financeira (UIF)**: unidade central nacional de natureza pública, autónoma e independente com competência para receber, analisar e difundir a informação suspeita de Branqueamento de Capitais, de Financiamento do Terrorismo e de Proliferação de Armas de Destruição em Massa, bem como cooperar com os congéneres internacionais e as demais entidades competentes para a prevenção e combate ao branqueamento de capitais, do financiamento do terrorismo e da proliferação de armas de destruição em massa, cuja organização e funcionamento é definida em diploma próprio.

5. MODELO DE GOVERNO (RESPONSABILIDADES)

A Fénix considera que todos os seus Colaboradores são intervenientes no programa de prevenção de branqueamento de capitais e financiamento do terrorismo.

Para efeitos de aplicação da presente política, os intervenientes relevantes, suas respectivas atribuições, suas responsabilidades no processo de prevenção ao branqueamento de capitais e financiamento do terrorismo, relativamente à aprovação, implementação e monitorização, são os seguintes:

5.1 CONSELHO DE ADMINISTRAÇÃO

São obrigações do Conselho de Administração (CAD):

a) Identificar e gerir efectivamente o risco do negócio;

b) Aprovar as políticas da Fénix;

c) Nomear um *Compliance Officer* com um conjunto de responsabilidades, entre as quais a divulgação do processo de prevenção de branqueamento de capitais e financiamento do terrorismo na Fénix;

d) Definir, implementar e aprovar os processos relacionados com as principais funções do *Compliance Officer;*

e) Disponibilizar recursos adequados e dedicados à prevenção do Branqueamento de Capitais e Financiamento ao Terrorismo.

O Conselho de Administração está totalmente comprometido na decisão de realizar processos e assumir o domínio da Abordagem Baseada no Risco ``ABR´´ (*RBA – Risk Based Approach*).

5.2. GABINETE DE GESTÃO DE RISCO E *COMPLIANCE*

O Gabinete de Gestão de Risco e Compliance (GGRC) é responsável pela implementação do programa de prevenção de BC/FT, pela centralização de informação e comunicação de operações suspeitas, pessoas designadas e comunicações espontâneas à UIF (Unidade de Informação Financeira) e outras entidades competentes, competindo-lhe:

a) A obtenção da aprovação do programa de Prevenção de Branqueamento de Capitais, do Financiamento do Terrorismo e da Proliferação de Armas de Destruição em Massa da Fénix;

b) A monotorização da conformidade da Fénix com as obrigações de BC/FT;

c) A supervisão da comunicação e da formação para os restantes Colaboradores;

d) A centralização e análise das comunicações internas sobre o tema do BC/FT;

e) Comunicação das operações susceptíveis de configurar a prática de crime de BC/FT à UIF;

f) Recepção de pedidos da UIF e outras entidades e quando aplicável facultar a informação solicitada;

g) Assegurar que as Declarações de Operações Suspeitas (DOS) e Declarações de Pessoas Designadas (DIPD) a enviar para a Unidade de Informação Financeira (UIF), estão devidamente preenchidas;

h) Prestação de informação relevante e regular ao Conselho de Administração.

5.2.1. Designação do *COMPLIANCE OFFICER* (Representante de Conformidade) da Fénix e Suas Funções

O Conselho da Administração da Fénix, Sociedade Gestora de Fundos de Pensões, S.A., designou como seu representante de conformidade, com total responsabilidade sobre o Programa de Prevenção do Branqueamento de Capitais, do Financiamento do Terrorismo e da Proliferação de Armas de Destruição em Massa o Responsável do Gabinte de Gestão de Risco e Compliance.

O Gabinete de Gestão de Risco e Compliance está investido com plena responsabilidade, autoridade e independência para aplicar e fazer cumprir o programa de Prevenção do BC/FT e da Proliferação de Armas de Destruição em Massa da Fénix, tendo para tal o apoio do Conselho de Administração.

5.3 ÁREAS DE NEGÓCIO E OPERACIONAIS

Cada área de negócio e operacional tem como obrigação, realizar os controlos estabelecidos pelo Gabinte de Gestão de Risco e Compliance, enquanto parte da sua actividade normal, comunicando as operações susceptíveis de configurar a prática de crime de BC/FT.

5.4 COMITÉ DE RISCO E COMPLIANCE

O Comité de Risco e Compliance é responsável pela monitorização do programa de Prevenção do Branqueamento de Capitais, do Financiamento do Terrorismo e da Proliferação de Armas de Destruição em Massa.

6. DIRECTRIZES

A Fénix estabelece orientações para identificar e exigir os controlos de *Compliance* que visam proteger, detectar e responder quaisquer procedimentos e riscos, tendo como base os seguintes princípios e políticas, processos e controlos, aqui enunciados e nos pontos subsequentes.

É política da Fénix, Sociedade Gestora de Fundos de Pensões, S.A., proibir e activamente prevenir qualquer actividade que facilite o branqueamento de capitais ou o financiamento do terrorismo ou actividades criminosas, através do cumprimento de todos os requisitos legais e regulamentares.

A Fénix, Sociedade Gestora de Fundos de Pensões, S.A., na eventualidade de ser usada para branqueamento de capitais e financiamento do terrorismo, incorre em risco operacional, risco de compliance, risco reputacional, riscos legais e regulatórios.

Assim, o Conselho de Administração tem a responsabilidade de assegurar que os seus processos de controlo e procedimentos, estão desenhados e implementados e são operados de modo efectivo, para reduzir o risco da Fénix ser conectada com o branqueamento de capitais e financiamento do terrorismo.

As políticas de prevenção contra o BC e FT, bem como os procedimentos de controlo interno estão desenhados para assegurar a conformidade com as Leis do Estado Angolano e os regulamentos da Agência Angolana de Regulação e Supervisão de Seguros (ARSEG), assim como dos padrões internacionais, sendo revistas e actualizadas numa base regular para garantir políticas apropriadas, procedimentos de controlos internos que estão implementados para registar tanto as alterações verificadas na componente legislativa como nas actividades realizadas pela Fénix.

A Fénix, partindo de uma abordagem baseada no risco, tem como premissa inicial, de que, a maioria dos seus Clientes, não são branqueadores de capitais ou financiadores do terrorismo. Contudo, entende igualmente que deve munir-se de mecanismos e procedimentos que permitam detectar e acompanhar os Clientes que apresentam risco elevado.

Nestes termos, o Conselho de Administração da Fénix assume o compromisso de efectuar uma verificação satisfatória da identidade do Cliente, antes da sua aceitação como Cliente, por via dos processos KYC- Conheça o Seu Cliente"Know Your Customer´´ e KYB- Conheça o Seu Negócio "Know your Business´´.

É também assumido o compromisso de que tudo será feito para que os Colaboradores da Fénix tenham a formação adequada e estejam cientes da lei e das suas obrigações, estabelecendo procedimentos para a implementação destes requisitos, sendo reconhecida a importância de que os Colaboradores transmitam prontamente as suas suspeitas internas.

6.1 POLÍTICA DE DILIGÊNCIAS

6.1.1 CDD (Diligência Simples)

Define as medidas que devem ser tomadas em relação à identificação dos Clientes, bem como, na obtenção de informação sobre o propósito e natureza da relação de negócio pretendida.

Estas acções são feitas com base nos documentos de identificação válidos e necessários que o Cliente deve apresentar, em função da natureza da operação que pretender realizar.

1. A Fénix pode, nos termos do artigo 13.º da Lei n.º 05/20, de 27 de Janeiro, aplicar 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:

a) Estado, ou uma pessoa colectiva de direito público, de qualquer natureza, integrada na administração central ou local; e

b) Autoridade ou organismo público sujeito a práticas contabilísticas transparentes e objecto de fiscalização;

c) Pessoas singulares que não se enquadram no conceito de Pessoas Politicamente Expostas e que realizem transações em nome próprio ou por conta própria.

1. A Fénix deve demonstrar à Agência Angolana de Regulação e Supervisão de Seguros (ARSEG), caso este assim o entenda, a verificação do enquadramento dos Clientes nas categorias acima mencionadas.

2. A demonstração indicada no número anterior, é feita com base em critérios definidos 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.

6.1.2 EDD (Diligência Reforçada)

A *EDD* é um processo que fornece um nível maior de análise e destaca riscos que não podem ser detectados pela *CDD*, ou seja, é efectuada sempre que estivermos em presença de Clientes/operações classificados na categoria de Alto Risco ou susceptível de enquadrar num tipo legal de crime, tais como:

a) Cliente PEP (Pessoa Exposta Politicamente), seus familiares ou associados conhecidos;

b) Jurisdição de Alto risco;

c) Banca privada;

d) Banca correspondente;

e) ONG´s;

f) Casinos;

g) Clientes que exercem a profissão de contabilistas e juristas;

h) Cliente que apresente um perfil transacional alterado de forma repentina;

i) Negócios com uso intensivo de dinheiro, pedras preciosas e obras de arte.

Nestes termos, para além das informações solicitadas numa *CDD*, as acções da Fénix consubstanciam-se em:

Analisar a fonte da riqueza e origem dos fundos/patrimônio;

a) Identificar os representantes legais, o(s) beneficiário(s) efectivo(s) bem como todos os intervenientes na operação/transacção/processo;

b) Constatar a localização real do Cliente – confrontando assim com os documentos apresentados;

c) Acompanhar as transacções do Cliente durante um determinado período, observando assim o perfil transacional do mesmo;

d) Obter informações adicionais de identificação, por outras vias de informação, quando possível.

A obrigação de diligência, seja na modalidade de *CDD* ou *EDD*, é feita no inicio da relação negocial, isto é, no momento da celebração do contrato de gestão ou de adesão, ou no momento da realização de uma transacção ou ainda quando exista alguma suspeita sobre aquele Cliente.

Porém, se os dados solicitados ao Cliente, não garantir o conforto para a Fénix proceder com a transacção ou continuar com a relação de negócio, de acordo com o artigo 25.º do Aviso da ARSEG n.º 03/2021 de 06 de Dezenbro, a Fénix deve recusar o início da relação de negócio ou de realizar a transacção ou ainda extinguir a referida relação, e comunicar à UIF.

A Fénix aplica estas obrigações a todos os novos Clientes, bem como aos Clientes já existentes e suas contrapartes, de acordo com os riscos que eles representem, e exerce o seu dever de diligência em momentos adequados relativamente às relações existentes.

6.2 POLÍTICA DE IDENTIFICAÇÃO E VERIFICAÇÃO DA IDENTIDADE DO CLIENTE

Define os elementos de identificação dos seus Clientes, seus representantes e beneficiários efectivos, que permitirão criar condições para a correcta aplicação da Política de Aceitação de Clientes e sua subsequente monitorização.

6.2.1 Princípios Básicos sobre a Verificação de Identidade

No relacionamento com os Clientes, a Fénix procede à identificação dos mesmos tendo como um dos aspectos fundamentais a criação e manutenção de uma relação de negócio continuada e estável, nos termos da legislação em vigor.

Neste sentido, os elementos fornecidos pelos Clientes, têm como suporte documentos necessários e suficientes para criar a prova efectiva da veracidade do processo.

Tanto no início da relação comercial, como no decorrer da mesma, os documentos que servem de prova dos elementos constantes do processo de identificação do Cliente, devem ser redigidos e obtidos em tempo oportuno, o mais próximo possível do acto e das informações que procuram comprovar.

6.2.2 Elementos à Obter

A Fénix nos seus normativos internos e em consonância com a legislação em vigor, estabelece os elementos fundamentais a observar no início do relacionamento de negócio com cada uma das naturezas de Clientes com quem se relaciona e a manter na continuação dessa relação.

Para o fim identificado no parágrafo anterior, estão criados diferentes requisitos para pessoas individuais e colectivas e, dentro destas naturezas, para nacionais e estrangeiros, para pessoas com situações especiais (expostas politicamente, por exemplo, para entidades colectivas com capitais abertos ao público, ou com natureza fechada, para entidades colectivas com natureza fiduciária, residentes ou não em jurisdições offshore) e para o conhecimento dos beneficiários efectivos das entidades colectivas, quando aplicável o requisito, numa descrição não exaustiva.

Deste modo, a seguir se enunciam os elementos fundamentais do acto de identificação das diversas categorias, detalhados de forma exaustiva nas normas e procedimentos em vigor:

6.2.2.1 Pessoas Singulares

No caso das pessoas individuais, a Fénix deverá obter do Cliente todas as informações relevantes para aferir da sua identidade e idoneidade na manutenção de relacionamento de negócio, designadamente:

a) Nome completo e assinatura;

b) Data de nascimento;

c) Nacionalidade;

d) Morada completa de residência;

e) Profissão e entidade patronal;

f) Cargos públicos que exerça; e

g) Tipo, número, data e entidade emitente do documento de identificação.

Complementarmente, no âmbito da constituição do processo de KYC - *Know Your Customer*, a Fénix deve ainda obter informação clara e verdadeira sobre:

a) A finalidade da relação de negócio que se pretende estabelecer;

b) A origem e o destino dos fundos que se quer movimentar;

c) As fontes de rendimento e de património do Cliente, criando a convicção da sua licitude;

d) O perfil transaccional expectável, de forma a aferir o respectivo grau de risco de branqueamento de capitais ou o enquadramento do Cliente na Política de Aceitação de Clientes.

A verificação, em sentido estrito, da identidade deve ser realizada através de documento de identificação original válido, pré-assinado e com fotografia, do qual deve constar o seu nome completo, data de nascimento e nacionalidade.

No caso de tal ser entendido relativamente aos Clientes e às transacções, que pela sua natureza ou características, possam suscitar um maior risco de branqueamento de capitais ou financiamento ao terrorismo, a Fénix promove um conjunto de procedimentos especiais e prepara um processo de KYC e acompanhamento reforçados. Estão nesta situação, designadamente, o estabelecimento de relações de negócio ou operações realizadas à distância, assim como as relações estabelecidas com Pessoas Politicamente Expostas (PEP).

6.2.2.2 Pessoas Colectivas (independentemente da sua natureza)

No caso das pessoas colectivas, para além das informações relativas à identidade do Cliente, a Fénix deverá obter todas as informações relevantes para aferir a sua idoneidade na manutenção de relacionamento de negócio e, ao mesmo tempo, obter as informações e documentos probatórios que permitam identificar o beneficiário último da entidade e as relações de domínio que a mesma detém com outros Clientes da Fénix, nomeadamente:

a) Denominação Social;

b) Objecto;

c) Endereço da Sede;

d) Número de Identificação de Pessoa Colectiva;

e) Identidade dos titulares de participacções no capital e nos direitos de voto de valor igual ou superior a 20%;

f) Identidade dos titulares dos órgãos de gestão.

Acresce, nestes casos, a necessidade de identificar e comprovar documentalmente os seus beneficiários efectivos, tanto através da documentação societária, como individualmente, segundo procedimentos semelhantes aos aplicados às pessoas singulares.

Igualmente, no âmbito da constituição do processo de *KYC – Know Your Customer*, a Fénix deve ainda obter informação clara e verdadeira sobre:

a) A finalidade da relação de negócio que se pretende estabelecer;

b) A origem e o destino dos fundos que se quer movimentar;

c) As fontes de rendimento e de património do Cliente, criando a convicção da sua licitude;

d) O perfil transaccional expectável, de forma a aferir o respectivo grau de risco de branqueamento de capitais ou o enquadramento do Cliente na Política de Aceitação de Clientes.

No caso de tal ser entendido relativamente aos Clientes e às transacções, que pela sua natureza ou características, possam suscitar um maior risco de branqueamento de capitais ou financiamento ao terrorismo, a Fénix promove um conjunto de procedimentos especiais e prepara um processo de KYC e ferramentas reforçados.

6.2.2.3 Mecanismos de identificação do Beneficiário Efectivo

Ao beneficiário efectivo, a Fénix deve exigir os mesmos elementos e documentos comprovativos da identificação que exigiria ao Cliente, nos termos da alínea a) do número 2 do artigo 9° e do n° 2 do artigo 10° do Aviso 3/21 da ARSEG.

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

a) Documento autenticado que confirme a identidade do beneficiário efectivo;

b) Cópia do acordo fiduciário ou acordo de parceria, ou outro documento equivalente;

c) Acta da assembleia-geral constituinte assim como a acta de alteração à estrutura accionista ou de sócios; e

d) Outra informação fidedigna, e que a instituição financeira considere relevante.

6.2.3 Procedimento Excepcional

A verificação da identidade do Cliente deve ser realizada no momento do estabelecimento da relação de negócio, ou na pendência de uma transacção.

Em situações excepcionais, nomeadamente naquelas em que comprovadamente não resultem riscos de branqueamento ou de financiamento ao terrorismo, ou estes riscos sejam limitados, a Fénix admite a possibilidade da celebração do Contrato sem que o processo de identificação esteja completo, dentro dos limites previstos na lei.

Nestas situações, os contratos serão realizados de forma provisória, sem a possibilidade não sendo aceite contribuições adicionais, após contribuição inicial, sem a possibilidade de reembolso, nem permitidas alterações na titularidade.

Estas restrições só serão levantadas após boa conclusão do processo de identificação, nomeadamente, *due diligence* e *Know Your Customer*, o que deve ser realizado no mais curto prazo de tempo.

6.2.4 Qualidade dos Documentos Exigíveis

Os documentos e elementos de confirmação das informações de identificação definidos pelas leis, pelos regulamentos e pelos normativos internos aplicáveis devem ter sempre a natureza de documentos originais, quer porque foram emitidos originariamente pelas entidades com capacidade para tal, quer porque resultam de cópias devidamente autenticadas com força pública.

Para a identidade das pessoas singulares, pelo menos um documento de identificação oficial, com fotografia e assinatura clara, deve ser apresentado e comprovado pelos Colaboradores da Fénix que os recebem.

Em caso algum, serão aceites documentos que apresentem rasuras, estragos ou danos visíveis em partes fundamentais ou, por qualquer razão, possam sugerir a suspeita de falsificação ou violação de elementos.

Em geral, existindo dúvidas sobre a veracidade ou qualidade dos documentos apresentados, deve o acto de identificação do Cliente ser considerado não válido, salvo se o Gabinete de Risco e *Compliance* emitir Parecer Favorável à continuação do processo.

6.2.5 Períodos de Actualização e Arquivo dos Documentos

A Fénix promove a actualização periódica da informação e respectivos documentos comprovativos, no máximo, a cada 5 anos e sempre que tenha conhecimento:

a) Da caducidade de um documento;

b) Do facto ou ocorrência que altere a realidade do Cliente, comprovada pelos documentos até então em sua posse;

c) Sempre que surjam dúvidas sobre a exactidão dos dados em sua posse.

6.3 POLÍTICA DE ACEITAÇÃO DE CLIENTES

A politica de aceitação de Clientes, define critérios que devem orientar a Fénix da aceitação ou recusa de relacionamento com potenciais Clientes, na definição de critérios de aceitação condicionada de Clientes e na definição de critérios de classificação do nível de risco dos Clientes, no momento da sua aceitação.

6.3.1 Clientes Cuja Aceitação Deve Ser Recusada

Tendo como objectivo proteger a Fénix de práticas que possam colocar em risco a sua actividade e de forma a proteger a sua reputação, a Fénix recusa quaisquer Clientes que se enquadrem em algumas das seguintes categorias:

a) Pessoas/Entidades cuja reputação, na comunicação social ou no mercado, surge habitualmente associada a actividades criminosas;

b) Pessoas/Entidades cuja actividade ou fonte de rendimento seja, directa ou indirectamente, o comércio de armas, ou outros equipamentos de natureza ou finalidade bélica, com violação as leis em vigor;

c) Pessoas/Entidades relativamente às quais a Fénix disponha de convicção que as associe a actividades criminosas;

d) Pessoas/Entidades que não colaborem com a Fénix na disponibilização da informação requerida;

e) Bancos de fachada.

6.3.2 Clientes Cuja Aceitação Deve Ser Condicionada a Processo Especial de Autorização

Carecem de especial autorização a aceitação de Clientes que se enquadrem em alguma das seguintes categorias:

a) Pessoas relativamente às quais a Fénix tenha classificado com nível elevado de risco de branqueamento de capitais;

b) Pessoas cuja actividade ou modo de vida torne inviável ou difícil o conhecimento, pela Fénix, da origem do respectivo património;

c) Casinos, estabelecimentos de jogo de fortuna e azar ou outros de natureza afim, desde que autorizados pelo Estado em matéria de branqueamento de capitais e de financiamento do terrorismo;

d) Casas de Câmbio ou quaisquer outros estabelecimentos que efectuem o comércio, interno ou transfronteiriço, de divisa;

e) Pessoas Politicamente Expostas (PEP´s).

6.3.3 Critérios para atribuição de grau de risco elevado no momento da aceitação de Clientes

A atribuição de grau elevado de risco na aceitação de potencial Cliente é efectuada pelo *Gabinete de Risco e Compliance*, considerando os seguintes factores relevantes:

a) A geografia de residência/actividade do potencial Cliente, ou a origem/destino dos fundos da transacção for:

- Jurisdições objecto de embargos ou de sanções decretados por quaisquer entidades de Direito Internacional com competência na matéria;
- Aquelas susceptíveis de serem qualificadas, em matéria de branqueamento de capitais ou de financiamento de terrorismo.

b) Clientes cuja aceitação deve ser condicionada a processo especial de autorização;

c) A actividade/profissão do potencial Cliente estar sujeita à aplicação da legislação preventiva de branqueamento de capitais;

d) A presença de outros factores ou circunstâncias, definidos pelo Gabinte de Risco e *Compliance*.

6.4. POLÍTICA DA RELACÇÃO COM PESSOAS POLITICAMENTE EXPOSTAS - PEP´S

Em relação às pessoas politicamente expostas (PEP´s), na qualidade de Clientes ou de beneficiários efectivos, além da aplicação das medidas de diligência normais, são aplicadas as seguintes medidas de diligência reforçadas:

a) Consulta a listas electrónicas internacionais no sentido de determinar se o Cliente ou o beneficiário efectivo é uma pessoa politicamente exposta;

b) Sempre que se confirme que o Cliente é uma pessoa politicamente exposta é submetido ao Conselho de Administração um pedido para o estabelecimento ou manutenção de relações de negócio com tais Clientes ou beneficiários efectivos;

c) São adoptadas medidas razoáveis para determinar a origem do património e dos fundos;

d) É assegurada uma vigilância, de forma reforçada e contínua, da relação de negócio.

As obrigações relativas a pessoas politicamente expostas aplicam-se igualmente aos membros da família ou a pessoas muito próximas dessas pessoas.

A aceitação de PEP como Cliente da Fénix depende no mínimo de um Parecer Favorável do Gabinete de Risco e *Compliance* e posterior aprovação do Conselho de Administração do Banco.

6.5 POLÍTICA DE FONTES DE INFORMAÇÃO

Para efeitos de identificação, avaliação e mitigação dos riscos concretos de Branqueamento de Capitais e de Financiamento ao Terrorismo e da proliferação de armas de destruição em massa, a Instituição deverá recorrer as fontes de informação idóneas, credíveis e diversificadas relativamente a sua origem e natureza, de entre as quais destacam-se:

a) Agência Angolana de Regulação e Supervisão de Seguros (ARSEG), relacionadas com as tipologias e os métodos de identificação de riscos específicos ou emergentes ou com riscos de suspeição;

b) Unidade de Informação Financeira (UIF) ou autoridades de aplicação da Lei, relacionadas com as tipologias e os métodos de identificação de riscos específicos ou emergentes ou com indicadores de suspeição;

c) Governo, através da emissão de informações, orientações ou alertas;

d) Sociedade Civil ou Organizações Internacionais (GAFI e outras) por intermédio de informações independentes e credíveis;

e) *Internet* e de órgãos de comunicação social, desde que de fonte independente e credível;

f) A informação constante de bases de dados, listas, relatórios de risco e outras análises provenientes de fontes comerciais disponíveis no mercado, bem como informações disponibilizadas por outras Instituições Financeiras ou Instituições de natureza semelhante, na medida em que tal seja legalmente admissível.

g) Informação resultante da Avaliação Nacional de Risco.

6.6 POLÍTICA DE FERRAMENTAS E APLICATIVOS INFORMÁTICOS

Para o cumprimento escrupuloso das obrigações e deveres previstos na Lei nº 05/20, de 27 de Janeiro, regulamentada pelo Aviso da ARSEG n.º 03/2021, a Fénix implementa ferramentas ou aplicativos informáticos instrumentais ou auxiliares que permitam:

a) Fazer registo dos dados identificados e demais elementos relativos aos Clientes;

b) A detecção de circunstâncias susceptíveis de parametrização que devam fundamentar a actualização daqueles dados identificativos e elementos;

c) A definição e actualização do perfil de risco associado aos Clientes, relações de negócio, transacções ocasionais e operações em geral;

d) A monitorização de Clientes e operações em face dos riscos identificados;

e) A detecção da aquisição da qualidade de pessoa politicamente exposta (PEP´s), 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;

f) O bloqueio ou a suspensão do 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 in line.

6.7 POLÍTICA PARA A IDENTIFICAÇÃO E COMUNICAÇÃO DE OPERAÇÕES POR EXIGÊNCIA DAS ENTIDADES A SER COMUNICADAS

A Fénix cria canais específicos, independentes e confidenciais que internamente assegurem, de forma adequada, a recepção, o tratamento e o arquivo das comunicações de irregularidades relacionadas com eventuais violações à Lei n.º 05/20, de 27 de Janeiro e ao Aviso 03/2021, e irregularidades relacionadas a integridade da organização.

6.7.1Declaração de Operações Suspeitas

Se a Fénix estiver na posse de indicadores subjectivos de uma operação suspeita, conhecimento, ou motivos razoáveis por suspeitar que certos fundos são provenientes de uma actividade de natureza criminosa, ou que estão relacionados com o financiamento do terrorismo, efectua logo que seja razoavelmente possível uma declaração de operação suspeita (DOS) à Unidade de Informação Financeira (UIF).

6.7.2 Alerta ao Cliente e Confidencialidade

A Fénix considera estar eximido pela lei, de responsabilidade criminal ou civil por quebra das regras de confidencialidade, impostas por contrato ou por qualquer disposição legislativa, regulamentar ou administrativa, quando declarar, de boa-fé, as suas suspeitas à UIF, ainda que não conhecendo, com precisão, qual é a actividade criminosa em questão e mesmo que a actividade ilegal de que suspeitava não tenha realmente ocorrido; e reconhece a proibição de divulgar o facto de ter sido feita à UIF uma declaração de operação suspeita (DOS) ou de ter sido transmitida à UIF uma informação conexa com essa declaração.

6.7.3 Relatório de Prevenção do BC/FT e da Proliferação de Armas de Destruição em Massa

A Fénix deve preencher, anualmente, formulários específicos sobre os elementos informativos, para a Prevenção do Branqueamento de Capitais, Financiamento do Terrorismo e da Proliferação de Armas de Destruição em Massa;

Os formulários em causa devem ser enviado à Agência Angolana de Regulação e Supervisão de Seguros até dia 31 de janeiro de cada ano, reportando-se ao período compreendido entre 1 de janeiro e 31 de dezembro do ano anterior, de acordo com o modelo de prestação de informação obrigatória e periódica, aprovado em diploma próprio pela ARSEG;

Toda informação a ser integrada no relatório encontra-se plasmada no nº 3 do artigo 36.º do Aviso 03/21.

6.8. POLÍTICA DE FORMAÇÃO, CONSCIENCIALIZAÇÃO E ALERTA PARA OS RISCOS DE BC/FT

Define critérios de formação para os Colaboradores em termos de riscos de BC/FT.

6.8.1 Principais Obrigações

Os Colaboradores da Fénix que procedam à execução das obrigações de identificação e diligência, nomeadamente à recolha, registo e verificação dos meios comprovativos apresentados, devem fazer constar nos registos internos de suporte àqueles actos, mencionando claramente a sua identificação e a data em que os praticaram;

Todos os Colaboradores da Fénix devem ser alertados para os riscos de BC/FT, para a legislação relevante, para as suas obrigações decorrentes dessa legislação e terem conhecimento da identidade e responsabilidades do *Compliance Officer*.

Devem ser treinados nos procedimentos da Fénix e em como reconhecer e gerir transacções ou actividades potenciais de branqueamento de capitais, ou financiamento do terrorismo.

A formação aos Colaboradores ocorre em intervalos regulares trimestrais e sempre que entrar um novo colaborador, procede-se ao registo dos detalhes.

O Compliance Officer é o responsável pela supervisão da adequação da formação em termos de requisitos, no que respeita à formação dos Colaboradores da Fénix, bem como do estabelecimento e manutenção dos preparativos para uma formação efectiva.

6.8.2 Acções Implementadas a Serem Mantidas Sob Revisão Regular

Providenciar formação apropriada para alertar os Colaboradores para as questões de branqueamento de capitais incluindo como estes crimes ocorrem e de como eles podem ter lugar através da Fénix.

Assegurar que é fornecida aos Colaboradores a informação e compreender, a posição legal da Fénix e de cada um dos Colaboradores e das alterações nestas posições legais.

Fornecer aos Colaboradores casos de estudo e exemplos relacionados com o negócio da Fénix.

Treinar os Colaboradores em como operar numa abordagem baseada no risco ao BC/FT.

6.8.3 Sensibilização e Formação

É entendimento da Fénix que um dos controlos mais importantes na prevenção e detecção de branqueamento de capitais é ter os Colaboradores em alerta para o risco de BC/FT, e bem treinados na identificação de actividades e transacções não usuais que possam ser suspeitas.

A aplicação efectiva do mais bem desenhado sistema de controlo pode ser comprometida se os Colaboradores que os utilizam não estão adequadamente formados. A eficácia da formação é importante para a estratégia de BC/FT da Fénix.

É essencial para a Fénix implementar uma política clara e bem articulada no sentido de assegurar que os Colaboradores estejam conscientes das suas obrigações no que respeita à prevenção do BC/FT e para os treinar na identificação e reporte de qualquer coisa que levante suspeitas. Isto é particularmente importante para os Colaboradores que tratem de transacções e instruções de Clientes.

6.8.4 Penalização Criminal dos Colaboradores

Os Colaboradores da Fénix estão sujeitos a penalizações criminais, se estiverem envolvidos no branqueamento de capitais ou financiamento do terrorismo, se não reportarem o seu conhecimento ou suspeitas sobre branqueamento de capitais ou financiamento ao terrorismo, onde existam bases razoáveis para o seu conhecimento ou suspeita de tal actividade. É importante, por isso, que os Colaboradores estejam conscientes destas obrigações e lhes seja proporcionado, formação de como evitá-las.

6.8.5 Obrigações Gerais, Legais e Regulamentares

Os compromissos da Fénix para a formação dos Colaboradores, tendem alcançar os seguintes objectivos:

a) Os seus Colaboradores sejam competentes;

b) Os seus Colaboradores permaneçam competentes no trabalho que executem;

c) Os seus Colaboradores são apropriadamente supervisionados;

d) A competência dos seus Colaboradores é regularmente revista;

e) O nível de competência é apropriado à natureza do negócio.

A regulamentação requer que o *Compliance Officer* tenha a responsabilidade de supervisionar os sistemas e controlos de BC/FT da Fénix, os quais incluem formação adequada para os Colaboradores no relacionado com BC e FT constatado igualmente. É preocupação da Fénix não só saber que os seus Colaboradores receberam a formação necessária, mas também, que são tomadas medidas para avaliar a sua efetividade.

6.8.6 Formação sobre os Procedimentos de Prevenção ao Branqueamento de Capitais ou Financiamneto do Terrorismo e Proliferação de Armas de Destruição em Massa

A Fénix forma os seus Colaboradores, em particular, em como os seus produtos e serviços podem ser usados como veículos para o branqueamento de capitais ou financiamento do terrorismo e proliferação de armas de destruição em massa, bem como nos procedimentos de gestão deste risco. Os Colaboradores também são informados em como a própria Fénix pode ser penalizada, se processar transacções indevidas.

Os Colaboradores da Fénix são formados naquilo que efectivamente precisam de saber, de modo a poderem desempenhar a sua função particular. Os Colaboradores envolvidos na área comercial, ou na área de liquidação de operações, não têm o mesmo tipo de formação, sendo esta ministrada à medida.

Os Colaboradores da Fénix são alertados das circunstâncias particulares, de Clientes que apresentam um elevado risco de branqueamento de capitais ou financiamento ao terrorismo, ou de quem seja financeiramente excluído. A formação inclui como a identidade deve ser verificada nesses casos e que passos adicionais devem ser dados.

6.8.7 Estado de Alerta dos Colaboradores Para Situações Específicas

É ministrada formação suficiente aos Colaboradores para os capacitar no reconhecimento de quando uma transacção não é usual ou é suspeita, ou quando eles devem ter bases razoáveis para saberem ou suspeitarem que branqueamento de capitais ou financiamento do terrorismo está a acontecer.

O alerta e a formação dos Colaboradores devem também incluir a natureza do financiamento do terrorismo e a actividade terrorista, de modo a que estejam de atentos para as transacções dos Clientes que possam estar relacionadas com o terrorismo, tais como:

a) Depósitos redondos seguidos de transferências electrónicas de igual montante;

b) Fonte desconhecida de rendimento;

c) Mudanças frequentes de endereço;

d) Compra de bens ou tecnologia militar; e

e) Notícias sobre suspeita, prisão de terroristas ou grupos.

É importante que os Colaboradores da Fénix estejam apropriadamente alertas para as mudanças de comportamento e de práticas entre os branqueadores de capitais e os que financiam o terrorismo.

É importante a utilização de exemplos, baseados em casos reais de como indivíduos e organizações podem obter fundos e usarem os produtos e serviços para BC/FT.

6.8.8 Métodos de Treino e Avaliação

A Fénix considera que não existe uma única solução para determinar como deve ser ministrada esta formação, estando, no entanto, focado na formação em sala, para as áreas de maior risco, por considerar mais efectivo.

Manuais de procedimentos, quer em papel ou na *intranet*, são úteis para aumentar o estado de alerta dos Colaboradores e em complementar formas mais dedicadas de formação, mas o seu principal propósito é fornecer referência contínua e, geralmente, não estão escritos como manual de formação

A formação contínua é dada a Colaboradores relevantes em intervalos apropriados, assumindo a forma de programa contínuo.

De formas a monitorizar quem foi formado, seja qual for a forma de formação de Colaboradores, a Fénix deve estabelecer registos compreensivos, relativos as acções de formação, interna ou externa que tenham sido realizadas, onde podemos destacar:

a) Denominação e objecto da formação;

b) Data de realização;

c) Entidade formadora;

d) Duração (em horas);

e) Natureza (formação interna ou externa);

f) Ambiente (formação presencial ou à distância);

g) Material didáctico de suporte;

h) Nome e função dos formandos (internos e externos); e

i) Avaliação final dos formandos, quando exista.

7. RESUMO DA AVALIAÇÃO DO RISCO DE BC/FT NA FÉNIX

A Fénix implementou este programa, de prevenção ao branqueamento de capitais ou financiamento do terrorismo e proliferação de armas de destruição em massa, de forma a conseguir identificar, monitorizar e impedir actividades de natureza criminosa, assente numa abordagem baseada no risco, através da identificação das áreas potencialmente vulneráveis a serem utilizadas para o BC e FT. Esta abordagem baseada no risco deverá ser suportada no documento Avaliação de Risco de BC/FT, na Fénix, Sociedade Gestora de Fundos de Pensões, onde constarão os respetivos fundamentos.

A Fénix deverá realizar as avaliações de risco nos termos do estabelecido nos artigos 9.º da Lei n.º 05/20, de 27 de Janeiro e actualizá-las numa periodicidade não inferior a 12 (doze) meses, excepto se existirem alterações legais e regulamentares.

7.1 ABORDAGEM BASEADA NO RISCO (ABR)

A Fénix adopta um modelo de classificação de risco de BC/FT, aplicável a todos os Clientes, que se baseia na atribuição em tempo real de um nível de risco com base nas características do Cliente, conhecidas no decurso do 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.

Para sustentar a antecipação e controlo do risco de BC/FT o Banco tem definido na Política de Aceitação de Clientes os princípios orientadores sobre a aceitação de Clientes com quem a Fénix está disposto a iniciar e manter relações comerciais. Adicionalmente, o Banco aplica a toda a sua carteira de Clientes as orientações, em matéria de BC/FT, aplicáveis a todos os novos Clientes. Neste sentido o processo de classificação de risco de BC/FT é aplicado a todos os Clientes, em sintonia com a legislação e regulamentação em vigor.

Embora as orientações acerca da matéria de branqueamento de capitais e financiamento ao 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.

Em consonância com o exposto, é necessário assegurar que as operações não presenciais e à distância, estejam sujeitas a normas ajustadas de KYC que permitam assegurar a obtenção da identidade dos seus beneficiários efectivos, bem como, o perfil transaccional das referidas contas.

7.2 CLASSIFICAÇÃO DE RISCO

Os mecanismos de prevenção do risco reputacional da Fénix e de combate ao BC/FT ganham maior robustez e eficácia com a aplicação de procedimentos de classificação, análise e monitorização do nível de risco do Cliente. Nesse sentido, todos os Clientes da Fénix são classificados tendo em conta os seguintes níveis de risco de BC/FT:

a) **Risco baixo**, se as entidades, fontes de riqueza ou origem de fundos são facilmente identificáveis ou cujas operações usualmente se apresentam adequadas e em aparente conformidade com o perfil conhecido do Cliente, seja um particular ou uma pessoa colectiva;

b) **Risco médio**, quando se verifica a existência de factores susceptíveis de conduzir ao agravamento de um risco considerado não negligenciável para o Banco, tais como:

- A profissão ou actividade do Cliente;
- O objecto do negócio da entidade;
- A inexistência de alguns dados de identificação e o perfil transaccional na utilização de produtos e serviços.

c) **Risco alto**, para todas aquelas entidades que se enquadrem nos critérios que a Fénix definiu para considerar a aceitação dos Clientes como condicionada, sempre que se esteja na presença de factores considerados como fortemente potenciadores de agravamento do risco, tais como:

- Critérios geográficos,
- Estatuto de pessoas expostas politicamente (PEP),
- Clientes cujo risco é objecto de afectação manual (em virtude de ocorrências concretas que indiciam elevado risco);
- Todas as situações em que se verifique que as fontes de financiamento, identidades e operações não se mostrem claras, sempre que os Clientes recusem ou não colaboram na prestação das informações requeridas ou ainda, aquelas que pela sua natureza possam revelar directa ou indirectamente, um maior risco para a prática de actos de ilícitos.

8. OBRIGAÇÃO DE CONTROLO – COMUNICAÇÃO DAS IRREGULARIDADES

Em respeito à orientação legal, a Fénix deverá conferir ao Gabinte de Gestão de Risco e Compliance as atribuições necessárias para a criação e gestão de um Canal de Denúncias, como um veículo fundamental para a detecção de situações consideradas suspeitas e que possam estar relacionadas com práticas de BC/FT ou crimes subjacentes ao BC.

A gestão do Canal de Denúncias supramencionado, deverá ser supervisionada directamente pelo Conselho Fiscal.

9. SANÇÕES E PENALIDADES

As violações, mesmo que por mera omissão ou tentativa não consumada, desta política, bem como as demais normas e procedimentos de *Compliance*, serão passíveis de penalidades.

As directrizes estabelecidas nesta política e nas demais normas e procedimentos de *Compliance*, não se limitam em razão da contínua actualização das leis, evolução tecnológica e constante surgimento de novos riscos. Desta maneira, não se constitui um inventário, sendo obrigação do utilizador da informação adoptar, sempre que possível, outras medidas de *Compliance* além das aqui previstas, com o objectivo de garantir o cumprimento da função *Compliance* da Fénix, Sociedade Gestora de Fundos de Pensões, S.A.

10. REVISÕES

Está política deve ser objecto de revisão por parte da Fénix, no mínimo, uma vez por ano e sempre que as alterações no enquadramento em que esta desenvolva as suas actividades assim o obrigue ou aconselhe.

~A elaboração e revisão da presente Política é da responsabilidade do Gabinete de Risco e *Compliance* (GRC).

11. APROVAÇÃO DA POLÍTICA

A Política é aprovada pelo Conselho de Administração da Fénix, Sociedades Gestora de Fundos de Pensões.