



POLÍTICA DE PREVENÇÃO À LAVAGEM DE DINHEIRO E FINANCIAMENTO AO TERRORISMO E À PROLIFERAÇÃO DE ARMAS DE DESTRUIÇÃO EM MASSA

fevereiro de 2024

Sumário

1 - OBJETIVO	2
2 - ABRANGÊNCIA	2
3- CONCEITOS E DEFINIÇÕES.....	3
4 – DIRETRIZES	4



5 - RESPONSABILIDADES	12
5 - VIOLAÇÕES DA POLÍTICA	14
6 - POLÍTICAS RELACIONADAS	14
7 - REFERÊNCIAS A LEIS/REGULAMENTAÇÕES.....	14
8 - INFORMAÇÕES DE CONTROLE	14
9 - HISTÓRICO DE REVISÃO	15

1 - OBJETIVO

Esta Política visa estabelecer conceitos, regras e procedimentos, bem como descrever os responsáveis e os controles internos a serem implementados e observados no desempenho das atividades da **Forteseq**, a fim de prevenir, detectar e comunicar operações ou transações que apresentem característica atípicas, com a finalidade de combater os crimes de lavagem de dinheiro, financiamento do terrorismo e da proliferação de armas de destruição em massa.

2 - ABRANGÊNCIA

Esta Política se aplica a quaisquer sócios, administradores, diretores, funcionários, estagiários e terceiros da Forte Securitizadora S.A. (“Forte Securitizadora” ou “**Forteseq**”).



3- CONCEITOS E DEFINIÇÕES

Cliente: qualquer pessoa física ou jurídica que utiliza um produto ou serviço financeiro.

Colaborador(es): pessoa que mantém vínculo estatutário ou empregatício com a Fortesec.

Conselho de Controles de Atividades Financeiras (COAF): Órgão criado no âmbito do Ministério da Fazenda, foi instituído pela Lei nº 9.613/98 e atua eminentemente na prevenção e combate à lavagem de dinheiro e ao financiamento ao terrorismo e da proliferação de armas de destruição em massa.

Financiamento ao Terrorismo: Configura-se quando alguém, direta ou indiretamente, por qualquer meio, prestar apoio financeiro, fornecer ou reunir fundos com a intenção de serem utilizados ou sabendo que serão utilizados, total ou parcialmente, por grupos terroristas para a prática de atos terroristas.

Financiamento da Proliferação de Armas de Destruição em Massa: Configura-se quando alguém, direta ou indiretamente, por qualquer meio, prestar apoio financeiro, fornecer ou reunir fundos com a intenção de serem utilizados ou sabendo que serão utilizados, total ou parcialmente na proliferação de armas de destruição em massa.

Armas de Destruição em Massa: Pode-se entender arma de destruição em massa como o dispositivo capaz de promover danos intencionais em grande escala, a exemplo de armas nucleares, químicas e biológicas.

GAFI/FATF: Grupo de Ação Financeira Internacional / *Financial Action Task Force*.

Lavagem de Dinheiro: consiste na ocultação ou dissimulação da natureza, origem, localização, disposição, movimentação ou propriedade de bens, direitos ou valores provenientes, direta ou indiretamente da infração penal.

Pessoas Expostas Politicamente (PEP): são consideradas Pessoas Expostas Politicamente (**PEP**), pessoas que desempenham ou tenham desempenhado, nos últimos 5 (cinco) anos, cargos, empregos ou funções públicas relevantes, no Brasil ou em outros países, territórios e dependências estrangeiras, assim com seus representantes, familiares e outras pessoas de seu relacionamento próximo.

PLDFTP: Prevenção à Lavagem de Dinheiro e ao Financiamento do Terrorismo e da Proliferação de Armas de Destruição em Massa.

Terceiro(s): é todo aquele que fornece direta ou indiretamente, bens e serviços à Fortesec.

Beneficiário Final: é a pessoa física que detém, em última instância, o controle da pessoa jurídica ou em nome da qual uma transação está sendo conduzida. É também considerado beneficiário final o representante, inclusive o procurador e o preposto, que exerçam o comando de fato sobre as atividades do cliente Pessoa Jurídica.



4 – DIRETRIZES

O crime de lavagem de dinheiro usualmente é cometido mediante um conjunto de operações comerciais ou financeiras que buscam a incorporação na economia, de modo transitório ou permanente, de recursos, bens e valores de origem ilícita. Essa incorporação ocorre por meio de um processo dinâmico que envolve, teoricamente, três etapas independentes que, com frequência, ocorrem simultaneamente.

- **Colocação:** a primeira etapa do processo é a colocação do dinheiro no sistema econômico. Com o objetivo de ocultar sua origem, os criminosos procuram movimentar o dinheiro em países com regras mais permissivas e naqueles que possuem um sistema financeiro menos regulado. A colocação se concretiza por meio de depósitos, compra de instrumentos negociáveis ou compra de bens. Para dificultar a identificação da procedência do dinheiro, os criminosos aplicam técnicas sofisticadas e cada vez mais dinâmicas, tais como o fracionamento dos valores que transitam pelo sistema financeiro, utilização de estabelecimentos comerciais que usualmente trabalham com dinheiro em espécie etc.
- **Ocultação:** a segunda etapa do processo consiste em dificultar o rastreamento contábil dos recursos ilícitos. O objetivo é quebrar a cadeia de evidências ante a possibilidade da realização de investigações sobre a origem do dinheiro. Os criminosos buscam movimentá-lo de forma eletrônica, transferindo os ativos para contas anônimas, preferencialmente, em países amparados por lei de sigilo bancário, ou realizando depósitos em contas em nome de terceiros, geralmente por meio de apresentação de documentação falsa, quando do cadastro.
- **Integração:** nessa última etapa, os ativos são incorporados formalmente ao sistema econômico. As organizações criminosas buscam investir em empreendimentos que facilitem suas atividades, podendo tais sociedades prestarem serviços entre si. Uma vez formada a cadeia, torna-se cada vez mais fácil legitimar os recursos de origens ilícitas.

O financiamento do terrorismo e da proliferação de armas de destruição em massa podem ser definidos como o apoio financeiro, por qualquer meio, ao terrorismo e à proliferação de armas de destruição em massa, ou àqueles que incentivam, planejam ou cometem tais atos.

Assim, o financiamento do terrorismo e a proliferação de armas de destruição em massa têm como objetivo fornecer fundos ou capital para atividades terroristas e outras práticas análogas e conexas. Essa arrecadação pode acontecer de diversas formas, até mesmo por meios legais, tais como contribuições associativas, doações ou lucros de atividades comerciais diversas, bem como a partir de fontes criminosas, como por exemplo tráfico de drogas.



A atuação da Securitizadora se dá na condição de emissora de valores mobiliários (CRI /CRA) ofertados publicamente com a contratação obrigatória de instituição intermediária.

Visto que o relacionamento com os clientes é formalmente estabelecido por tais instituições intermediárias, e que estas devem observar a Resolução CVM N° 50, as ameaças e/ou vulnerabilidades e riscos internos da **Fortesec** estão mitigados por eventuais atos de prevenção à lavagem de dinheiro e financiamento ao terrorismo adotados por tais instituições.

Vale lembrar que a **Fortesec** repudia atos de lavagem de dinheiro, financiamento ao terrorismo, corrupção ou quaisquer atos ilícitos.

A **Fortesec** estabelece a presente política com o objetivo de impedir a sua participação em atividades ilícitas, bem como zelar e proteger a sua imagem e reputação ilibada perante os: (i) colaboradores, (ii) clientes, (iii) sociedade, e, (iv) potenciais parceiros, terceiros, prestadores de serviços, contrapartes e tomadores de recursos ("Parceiros").

É dever de todos os colaboradores da **Fortesec**, bem como aos Parceiros por ela contratados, denunciar totalmente à área de Riscos & *Compliance*, situações suspeitas de envolvimento ou prática de crimes de lavagem de dinheiro ou financiamento ao terrorismo envolvendo clientes, parceiros de negócios, fornecedores ou colaboradores, sendo a área responsável por aprofundar a análise e, caso seja aplicável, reportar ao COAF.

A **Fortesec** estabelece uma cultura em seu Código de Conduta e Ética, com a finalidade de proteger a sua reputação e a sua marca, e, por esse motivo, é importante que todos os nossos clientes e Parceiros, estejam de acordo com as nossas diretrizes.

Não é tolerada a prática de lavagem de dinheiro e financiamento ao terrorismo em quaisquer transações de que a **Fortesec** seja parte.

4.1 - Método de Prevenção à Lavagem de Dinheiro, ao Financiamento do Terrorismo e da Proliferação de Armas de Destruição em Massa

A **Fortesec** tem como boa prática fazer diligência ou pedir evidências de Parceiros em sua rotina de PLD/FTP, com análises de todos os beneficiários finais (denominada internamente como *Due Diligence* – DD), no momento do início do relacionamento

Em síntese a nossa atuação em Prevenção à Lavagem de Dinheiro, ao Financiamento do Terrorismo e da Proliferação de Armas de Destruição em Massa, está baseada em:

- I. Analisar e monitorar os parceiros de cada operação;
- II. Identificação do beneficiário final de todas as empresas que estão envolvidas na possível Operação da **Fortesec**;
- III. Observar a origem dos recursos patrimoniais dos parceiros e a compatibilidade destes em relação à operação;



- IV. Reportar qualquer movimentação suspeita à CVM/COAF, conforme a Resolução CVM nº 50;
- V. Analisar lista OFAC e sanções da ONU; e
- VI. Pesquisar e identificar Pessoas Expostas Politicamente (“PEP”);

Todas as operações suspeitas que forem identificadas são devidamente reportadas ao COAF por meio de sistema específico na forma aplicável. Na hipótese de inoccorrência de suspeitas, é feita uma Declaração Negativa Anual ao COAF, conforme a Resolução 50 da CVM.

Excepcionalmente, a critério da Diretoria, o processo de diligência pode ser realizado: (i) de forma simplificada e/ou (ii) em relação a investidores que tenham iniciado relacionamento com a **Fortesec** antes do investimento efetivo em valores mobiliários de sua emissão, sem prejuízo das auditorias eventualmente realizadas pelas instituições intermediárias que atuarem no âmbito das ofertas públicas e/ou emissões da **Fortesec**.

4.1.1 - Conheça seu Cliente (Know Your Client – KYC)

Trata-se de um conjunto de ações que devem ser adotadas para assegurar a identificação e qualificação dos clientes, bem como a origem e a constituição de seu patrimônio e recursos financeiros. Também inclui procedimentos específicos para identificação de beneficiários finais e de Pessoas Expostas Politicamente (PEP).

Essas ações têm o propósito de identificar, também, se os clientes possuem mídias negativas, se figuram em alguma lista restritiva, exercem profissão de risco e se residem em cidade de fronteira.

A área de Riscos e *Compliance* é responsável pela análise, registro das informações e documentos de identificação de clientes com os quais a **Fortesec** mantém relacionamento.

Quanto mais precisas forem as informações coletadas e registradas tempestivamente no início do relacionamento, maior será a capacidade de identificação de riscos de ocorrência da prática de atos ilícitos e maior segurança para a instituição.

A **Fortesec** atua em operações de securitização, com a finalidade de emitir certificados de recebíveis imobiliários (CRI) e certificados de recebíveis do agronegócio (CRA), observados os parâmetros regulatórios instituídos pela Comissão de Valores Mobiliários (CVM). Antes da operação de securitização ser estruturada e ocorrer a emissão dos Títulos de CRI ou CRA, os nossos clientes são os tomadores de recursos, cedentes e/ou devedores.

Em ambos os casos, há: (i) a manutenção do histórico de dados e informações enviadas; (ii) foco na análise de dados relativos à origem dos recursos do cliente (de modo a comprovar a licitude desta e a compatibilidade dos recursos com o valor envolvido na operação); e (iii) acompanhamento das pesquisas reputacionais, se houver algum apontamento negativo.



4.1.2 - Conheça seu Parceiro e Fornecedor (Know Your Partner – KYP e Know Your Supplier – KYS)

Conforme a descrição do nosso Método de Prevenção à Lavagem de Dinheiro, ao Financiamento do Terrorismo e da Proliferação de Armas de Destruição em Massa da **Fortesec**, analisamos todos os nossos Parceiros e Fornecedores de acordo com o nosso Manual de *Due Diligence* interno.

O nosso maior objetivo é que nada que contratamos ou que escolhemos para ser Parceiros ou prestadores de serviços tenham atividades ligadas ao crime de lavagem de dinheiro, financiamento ao terrorismo e da proliferação de armas de destruição em massa e prevenir o envolvimento da **Fortesec** em situações que possam acarretar riscos legais e à sua reputação perante o mercado e aos órgãos reguladores.

Os nossos parceiros comerciais com quem mantemos relações contratuais ou comerciais, geralmente são ligadas ao *core business*, como por exemplo, agentes fiduciários, coordenadores e distribuidores, e passam pelo processo de *due diligence* pela área de Riscos e *Compliance*.

Antes do início do relacionamento com parceiros de negócios, a área solicitante deverá seguir com o processo de Cadastro do Terceiro, que preencherá a ficha cadastral e passará pela análise de Riscos e *Compliance* para realização de *Due Diligence*.

A área de Riscos e *Compliance* fará pesquisas sobre a reputação e outras informações relevantes de terceiros, por meio das informações disponíveis em mecanismos de busca online e demais fontes de informação pública e/ou privada, adotando um conjunto de regras, procedimentos e controles para identificação, qualificação e aceitação de terceiros que devem ser compatíveis com essa política, visando prevenir a contratação de pessoas físicas ou pessoas jurídicas inidôneas ou suspeitas de envolvimento em atividades ilícitas.

A **Fortesec** faz diligências prévias e pede evidências de contrapartes dos negócios a fim de confirmar se estas cumprem, adequadamente, as obrigações regulatórias que lhes cabem no contexto de operações ou relacionamento com a **Fortesec**.

Os procedimentos serão proporcionais aos riscos identificados pela companhia em cada contratação e para aqueles que representarem maior risco, serão adotados procedimentos complementares e diligências aprofundadas de avaliação e alçadas específicas de aprovação, de acordo com a criticidade dos apontamentos ou exceções.

4.1.4 - Conheça seu Colaborador (know your employee - KYE)

Os procedimentos de “Conheça seu Colaborador” têm por objetivo fornecer à **FORTESEC** informações detalhadas sobre seus Colaboradores, os quais incluem critérios para a sua contratação e verificação de suas condutas em conformidade com a presente Política e com o Código de Conduta e Ética da **FORTESEC**.



O procedimento adotado deve garantir o conhecimento do colaborador, com sua identificação e qualificação, e estar compatível com essa Política e com o Código de Conduta e Ética da **FORTESSEC**.

A **FORTESSEC** tem a prerrogativa de realizar análises de background check, no âmbito do processo de Conheça seu Funcionário (Know your Employee).

Devem ser avaliadas as atividades desenvolvidas pelos funcionários tendo como base a classificação interna de riscos a ela associada e a relevância das informações envolvidas

Os procedimentos devem garantir o conhecimento do funcionário, com sua identificação e qualificação, e devem ser compatíveis com essa Política, bem como alinhado a avaliação interna de riscos.

O processo de conheça seu funcionário deve promover ainda a cultura organizacional de risco englobando o risco de LDFTP, por meio de treinamentos permanentes, bem como destinar treinamentos específicos as áreas consideradas sensíveis para o processo de gestão do risco de LDFTP.

4.2 - Pessoa Exposta Politicamente (PEP)

São considerados PEP Titulares os agentes públicos que desempenham ou tenham desempenhado, nos últimos cinco anos, no Brasil ou em países, territórios e dependências estrangeiras, cargos, empregos ou funções públicas relevantes, assim bem como a verificação da condição de representante, familiar ou estreito funcionário dessas pessoas (Relacionados).

Entende-se por estreito funcionário:

- a) pessoa natural conhecida por ter qualquer tipo de estreita relação com pessoa exposta politicamente, inclusive por: (i) ter participação conjunta em pessoa jurídica de direito privado; (ii) figurar como mandatária, ainda que por instrumento particular da pessoa mencionada ou (iii) ter participação conjunta em arranjos sem personalidade Jurídica;
- b) pessoa natural que tem o controle de pessoas jurídicas ou de arranjos sem personalidade Jurídica, conhecidos por terem sido criados para o benefício de pessoa exposta politicamente.

As transações que envolvam PEP como tomadoras de recursos, cedentes, avalistas, e/ou garantidoras não são vedadas, mas devem contar com análise mais aprofundada dessas contrapartes no processo de *due dilligence*, bem como com a aprovação da Diretoria e com informações levantadas área de Riscos & *Compliance*.

Na tomada de decisão da Diretoria sobre a manutenção do relacionamento com PEP, a **Fortesec** deve levantar maiores detalhes sobre a PEP e a origem dos recursos financeiros de modo a permitir uma análise mais adequada ao respectivo risco.



As operações de clientes PEP são consideradas de alto risco e por esse motivo são analisadas com especial atenção pelo área de Riscos & *Compliance*.

Portanto a **Fortesec** empreende esforços específicos na análise de início de relacionamento e operações que possua pessoa considerada como expostas politicamente (“PEP”) ou PEP relacionado nos termos da legislação vigente. A manutenção da condição de PEP é realizada através de monitoramento contínuo através de sistemas.

4.3 - Identificação e Cadastro de Clientes e Terceiros

Nosso propósito, como Securitizadora, é adquirir créditos do agronegócio ou imobiliários a fim de lastrear valores mobiliários, como Certificados de Recebíveis Imobiliários (CRI) e Certificados de Recebíveis do Agronegócio (CRA).

Os nossos CRI e CRA são distribuídos por instituições financeiras autorizadas a distribuir referidos papéis. O nosso cliente é cedente ou devedor dos créditos lastro dos nossos valores mobiliários ofertados e que temos relacionamento comercial direto (“Cliente”). Para realizamos a aprovação desse cadastro, partimos para o KYC e para a manutenção deste cadastro sempre atualizado.

O cadastro de clientes e terceiros deverá ser realizado pela área de Riscos e *Compliance*, Novos Negócios, pela área responsável pelo prestador de serviço ou pelo próprio cliente dentro do sistema de cadastro KN1 e aprovado pela área de Riscos e *Compliance*. É importante salientar que nenhuma operação poderá ser realizada com este cliente antes de sua aprovação e cadastramento na base de dados da **Fortesec**.

No caso específico para adequação da base de cadastro de clientes à Resolução CVM nº 50, a **Fortesec** tomará as seguintes providências levando em consideração a metodologia de Abordagem Baseada em Riscos (ABR).

Para realizar a identificação e qualificação do cliente, devem ser seguidos os procedimentos de obtenção de informações, que permitam dentre outros apontamentos, verificar a condição de Pessoa Exposta Politicamente (PEP), bem como de análise da cadeia de participação societária até a identificação da pessoa natural caracterizada como beneficiário final nos termos da legislação vigente.

Caso necessário, a área de Riscos e *Compliance* poderá desempenhar atividades complementares de pesquisa em relação ao cliente, por meio de solicitação de documentação adicional para clientes em situações de risco.

O cadastro de clientes aprovados terá validade de 12 meses. Após esse período, o cliente deverá atualizar seu cadastro a fim de realizar qualquer operação com a **Fortesec**. Os documentos apresentados pelo cliente deverão ser arquivados pela área de *Compliance* por pelo menos 5 anos a contar da data de sua aprovação.



Vale Ressaltar que é proibido o início ou a manutenção de relacionamento com indivíduos ou entidades mencionadas nas listas de sanções impostas por resoluções do Conselho de Segurança das Nações Unidas - CSNU, US Office of Foreign Assets Control (OFAC) e União Europeia.

4.4 - Controle e Monitoramento de Operações

A **Fortesec** utiliza sistema específico como ferramenta para identificar indícios de lavagem de dinheiro, práticas não equitativas e atipicidades no que diz respeito às exigências regulatórias, para analisar todas as operações e situações que podem, após detecção e respectiva análise, configurar indícios de LDFT.

As hipóteses que, a critério da área de Riscos e *Compliance* e do Diretor responsável por PLD/FTP, configurem indícios de LDFTP, serão analisadas e notificadas ao COAF.

A área de Riscos e *Compliance* é responsável por analisar as ocorrências identificadas no que diz respeito a indícios de Lavagem de Dinheiro, Financiamento ao Terrorismo e da Proliferação de Armas de Destruição em Massa.

A comunicação deve obedecer ao prazo máximo de vinte e quatro horas contadas a partir da finalização do processo de análise e constatação.

Toda e qualquer reunião realizada para discussão de casos com indícios de lavagem de dinheiro deve ser formalizada por meio de ata.

Todos os casos levados para reunião são arquivados no diretório da área de Riscos e *Compliance*, sendo utilizados para identificação de recorrência, independentemente de ter sido ou não reportada a situação. A avaliação de recorrência é utilizada como um dos pilares do processo decisório de comunicação aos reguladores.

Cabe ressaltar que, desde que não tenha sido prestada nenhuma comunicação ao COAF durante o ano, a **Fortesec** comunicará até o último dia útil do mês de janeiro a não ocorrência no ano civil anterior das transações ou propostas de transações passíveis de serem comunicadas, bem como emitirá um “Relatório de Avaliação Interna de Risco de Lavagem de Dinheiro, Financiamento ao Terrorismo e da Proliferação de Armas de Destruição Em Massa – PLD/FT”, conforme a Resolução CVM nº 50.

A “declaração negativa”, caso cabível, será encaminhada ao COAF através do segmento da CVM, SFN-Atípicas e SFN-Espécie no Sistema Siscoaf.

4.5 – Treinamentos

A área de Riscos e *Compliance* é responsável por elaborar e ministrar o treinamento interno de Prevenção à Lavagem de Dinheiro, ao Financiamento do Terrorismo e da Proliferação de Armas de Destruição em Massa.

Este treinamento é realizado na admissão e no mínimo anualmente para todos os



nossos colaboradores. O comparecimento ao treinamento na admissão e periodicamente é obrigatório.

O treinamento tem por objetivo apresentar os principais conceitos, operações e situações que podem configurar indícios e procedimentos a serem adotados na prevenção e combate às atividades relacionadas com o crime de lavagem de dinheiro.

Cabe ressaltar que, caso ocorra qualquer mudança em processos que envolvam questões relacionadas à controles de prevenção à lavagem de dinheiro, poderão ser realizados treinamentos pontuais para alinhamento do conhecimento técnico.

Os treinamentos ministrados para os Colaboradores internos, nos termos da Política de Treinamento, devem atender aos seguintes critérios:

- Ser aplicado no ingresso de todo novo Colaborador;
- Ser ministrado anualmente a todos os Colaboradores;
- Ter aproveitamento mínimo de 70% (setenta por cento) do conteúdo aplicado, passível de evidência;
- Prover insumos para reciclagem das áreas e pessoas com deficiência de aprendizado;
- Ser passível de evidência, a qual deve ser mantida em arquivo pelo prazo mínimo de 5 (cinco) anos.

4.6 - Abordagem Baseada em Risco (ABR)

Nos termos da Resolução CVM 50, a **Fortesec** deve, no limite de suas atribuições, identificar, analisar, compreender e mitigar os riscos de LDFTP inerentes às suas atividades desempenhadas no mercado de valores mobiliários, adotando uma abordagem baseada em risco (“ABR”) para garantir que as medidas de prevenção e mitigação sejam proporcionais aos riscos identificados, conforme detalhado em nossa Norma de Avaliação Interna de Risco.

Todos os novos serviços serão analisados pelo Time de Riscos & Compliance, a fim de identificar vulnerabilidades sob a ótica de prevenção à lavagem de dinheiro.

Buscando continuamente conhecer a outra parte, anualmente é realizada revisão da classificação de risco de cada produto, serviço e tipos de clientes e da forma e critérios de monitoramento.

4.7 - Avaliação de Efetividade

Anualmente até o último dia útil do mês de abril, o Diretor de Riscos e *Compliance* deve apresentar ao Comitê de Riscos e *Compliance* relatório de avaliação interna de riscos de LD/FTP, contendo o gerenciamento dos eventos relativos ao ano anterior, levando em consideração os aspectos estipulados na Resolução CVM n.º 50.

O relatório de avaliação interna de riscos de LD/FTP e os documentos relativos à análise, inclusive a ata de reunião do Comitê que aprovou o relatório, devem ficar à disposição de órgãos reguladores e fiscalizadores pelo prazo mínimo de 5 (cinco) anos.



Todos os registros e documentos relativos às conclusões das análises de LD/FTP e comunicações realizadas devem ser armazenados por prazo não inferior a 5 (cinco) anos, podendo ser estendido por solicitação das autoridades legais e reguladoras.

5 - RESPONSABILIDADES

Diretor de *Compliance*/PLDFTP

- Definir a Política de Prevenção à Lavagem de Dinheiro e ao Financiamento do Terrorismo (PLDFTP) em consonância com as Leis e regulamentações aplicáveis; (Governança de PLDFTP)
- Assegurar a elaboração da Avaliação Interna de Risco visando definir a abordagem de risco a ser aplicada nos processos e controles de PLDFTP;
- Assegurar a elaboração de procedimentos que definam os processos e controles de PLDFTP nos relacionamentos com Clientes, Colaboradores, Parceiros e Prestadores de Serviço Terceirizado, no monitoramento, seleção e análise de operações e situações suspeitas, e na comunicação dos fatos ao Coaf;
- Assegurar a elaboração de Relatório de Efetividade para identificar deficiências nos processos e controles de PLDFTP e definir a correção tempestivas das deficiências identificadas, com planos de ação, datas e responsáveis pela regularização;
- Acompanhar por meio de métrica e indicadores de gestão a efetividade das atividades e das ações relacionadas à PLDFTP;
- Promover a disseminação da cultura de Prevenção à Lavagem de Dinheiro e ao Financiamento do Terrorismo;
- Assegurar recursos adequados e suficientes para o exercício das atividades de Prevenção à Lavagem de Dinheiro e ao Financiamento do Terrorismo;
- Submeter à Diretoria Executiva proposta para o estabelecimento ou alterações de políticas e procedimentos;
- Apreciar os relatórios e comunicações emitidos pelos Órgãos Supervisores competentes, pelas áreas de *Compliance* e Auditoria, determinando as ações e providências que se fizerem necessárias;
- Deliberar sobre a contratação de serviços profissionais especializados, quando julgar conveniente;
- Deliberar a respeito de suspensão bloqueio ou encerramento de relacionamento com clientes, parceiros ou prestadores de serviços em decorrência de atipicidades que podem configurar indícios de lavagem de dinheiro ou de financiamento ao terrorismo;
- Deliberar quanto a definição do detentor de alçada para aprovação de pessoa exposta politicamente no início ou manutenção de relacionamento.
- Deliberar quanto aos critérios de risco e percentuais que serão adotados para identificação de beneficiário final, obedecendo os requisitos estipulados na Circular BCB 3978/20;
- Deliberar sobre situações excepcionais não claramente previstas em políticas e procedimentos internos ou externos;
- Manter registros de suas deliberações e decisões.



Área de *Compliance*/PLDFTP

- Aplicar e atualizar as políticas e procedimentos relacionados a PLDFTP
- Disseminar e atuar como multiplicador da cultura de *Compliance* na **Fortesec**;
- Interagir com órgãos reguladores;
- Avaliar suspeitas de PLD/FTP quando da realização de Due Diligence de Fornecedores, Clientes e Parceiros;
- Monitorar e fiscalizar o cumprimento desta Política pelos Colaboradores, assim como a realização das comunicações previstas na lei e regulamentação em vigor;
- Elaborar dossiês de análise sobre transações suspeitas de LD/FTP;
- Elaborar e manter à disposição da alta administração, os relatórios e o registro das obrigações regulatórias referentes à PLF/FTP, observando a regulamentação;
- Garantir, com o auxílio da área de Recursos Humanos, a realização, anual, do treinamento aos Colaboradores sobre o tema PLD/FTP;
- Garantir a realização das devidas diligências nos processos cadastrais e, periodicamente, com base no nível de risco dos clientes, através das ferramentas disponibilizadas pela **Fortesec**.
- Encaminhar para análise da Diretora de *Compliance* os casos avaliados como médio-alto e para a análise do Comitê de Risco e *Compliance* os casos avaliados como risco alto;
- Estabelecer controles e o tratamento de clientes, pessoas físicas e jurídicas ou de entidades submetidas às sanções impostas por resoluções do Conselho de Segurança das Nações Unidas;
- Analisar novos produtos, juntamente com as demais áreas, observando sempre à aderência às regras e legislação vigente, os riscos inerentes a novos produtos, serviços e tecnologias, verificando com especial atenção os riscos de PLD/FTP;
- Recepcionar documentação societária e fichas cadastrais devidamente preenchidas através das ferramentas disponibilizadas pela **Fortesec**;
- Garantir a manutenção e pronta obtenção dos documentos cadastrais dos clientes, pelo prazo mínimo de 5 (cinco) anos a contar do fim do relacionamento;
- Observar a validade da documentação societária;
- Controlar a existência de pendências documentais e comunicá-las ao Cliente e às áreas com relacionamento direto;
- Desenvolver e implementar metodologia de Abordagem Baseada em Risco (ABR) de LD/FTP;
- Elaborar Relatório de Avaliação Interna de Risco (AIR) de LD/FTP, a ser encaminhado a Diretoria da **Fortesec**; e
- manter as informações da instituição atualizadas junto ao COAF, prestando esclarecimentos quando necessário;

Área de Recursos Humanos



- Viabilizar programas de treinamento periódicos para assegurar que todos os funcionários estejam devidamente orientados e atualizados quanto às suas obrigações e responsabilidades de acordo com a regulamentação aplicável; e
- Adotar controles quanto ao conhecimento dos funcionários, realizando a análise reputacional durante a fase de contratação destes.

5 - VIOLAÇÕES DA POLÍTICA

O descumprimento das disposições legais ou regulamentares internas pode acarretar sanções disciplinares e administrativas, no caso de Diretores e Colaboradores ou o encerramento do relacionamento comercial, no caso de parceiros, fornecedores ou prestadores de serviços. Quando a Departamento de *Compliance* tiver conhecimento de situações por parte do colaborador, que representem violação ao estabelecido nesta Política e demais normas internas, a equipe de *Compliance*, liderada por seu gestor ou Diretor, deverá analisar o caso e tomar as medidas disciplinares cabíveis, conforme abaixo descritas.

Os procedimentos adotados serão conduzidos pelo gestor ou Diretor da Departamento, a quem cabe também a recomendação final das respectivas penalidades para aprovação pela Diretoria Executiva. As penalidades aplicáveis resumem-se em advertência, suspensão temporária e afastamento definitivo.

6 - POLÍTICAS RELACIONADAS

- Código de Conduta e Ética;
- Política de *Compliance*;
- Política de Anticorrupção;

7 - REFERÊNCIAS A LEIS/REGULAMENTAÇÕES

- Lei 12.846 de 1º de agosto de 2013;
- Lei 9.613 de 03 de março de 1998;
- Resolução 60 de 12 de dezembro de 2021;
- Resolução 194 de 17 de novembro de 2023;
- Resolução 50 de 31 de agosto de 2021.
- Guia de Prevenção à Lavagem de Dinheiro e ao Financiamento ao Terrorismo no Mercado de Capitais Brasileiro ("Guia PLD") divulgado pela ANBIMA.

8 - INFORMAÇÕES DE CONTROLE

Vigência: Entra em vigor na data da sua publicação

Versão: 002

Data de Aprovação: _____

Frequência de Revisão: Anual

Departamento Emissor: Riscos e *Compliance*



Aprovador: Guilherme Zakalski

9 - HISTÓRICO DE REVISÃO

Versão	Modificação	Motivo	Data
001	N/A	Criação	22/12/2022
002	Template	Modificação do Template e adequação regulatória	08/02/2024

DocuSigned by:
Juliana Mello Esteves Pereira
F07A5B68D27C471...
Juliana Mello

Rodrigo Ribeiro

DocuSigned by:
Marilia Garcia
647BFDAA97FDD4C3...
Marilia Garcia

DocuSigned by:
Felipe Biscuola
EBE6BDA15AAB42A...
Felipe Biscuola

Pedro Mileti