

**POLÍTICA DE PREVENÇÃO À LAVAGEM DE DINHEIRO,
FINANCIAMENTO DO TERRORISMO E DA PROLIFERAÇÃO DE
ARMAS DE DESTRUIÇÃO EM MASSA (PLD/FTP)**



Versão 2025.1

Editada em novembro de 2025

SUMÁRIO

| | |
|---|----|
| 1. INTRODUÇÃO..... | 3 |
| 2. DEFINIÇÕES..... | 3 |
| 3. LAVAGEM DE DINHEIRO | 5 |
| 4. TERRORISMO E SEU FINANCIAMENTO | 7 |
| 5. PROLIFERAÇÃO DE ARMAS DE DESTRUIÇÃO EM MASSA | 7 |
| 6. COMPROMETIMENTO DA ALTA ADMINISTRAÇÃO | 7 |
| 7. ESTRUTURA ORGANIZACIONAL – RESPONSABILIDADES..... | 8 |
| 8. PROGRAMA DE PLD/FTP | 10 |
| 9. AVALIAÇÃO INTERNA DE RISCO (AIR) | 11 |
| 10. AVALIAÇÃO DE EFETIVIDADE..... | 12 |
| 11. MONITORAMENTO, SELEÇÃO E ANÁLISE DE OPERAÇÕES E SITUAÇÕES SUSPEITAS . | 12 |
| 12. COMUNICAÇÃO DE OPERAÇÕES E SITUAÇÕES SUSPEITAS..... | 13 |
| 13. SANÇÕES IMPOSTAS POR RESOLUÇÕES DO CONSELHO DE SEGURANÇA DAS NAÇÕES UNIDAS (CSNU)..... | 13 |
| 14. ANÁLISE PRÉVIA DE NOVOS PRODUTOS, SERVIÇOS E TECNOLOGIAS | 14 |
| 15. TREINAMENTO..... | 14 |
| 16. CANAIS DE COMUNICAÇÃO | 14 |
| 17. MANUTENÇÃO DE INFORMAÇÕES E REGISTROS | 15 |
| 18. SANÇÕES APLICÁVEIS | 15 |
| 19. VIGÊNCIA E APROVAÇÃO..... | 15 |

1. INTRODUÇÃO

A Política de Prevenção à Lavagem de Dinheiro, Financiamento do Terrorismo e da Proliferação de Armas de Destruição em Massa (“PLD/FTP”) tem como objetivo orientar e definir diretrizes quanto à prevenção da utilização do sistema financeiro para a prática dos crimes de “lavagem” ou ocultação de bens, direitos e valores, e de financiamento do terrorismo e da proliferação de armas de destruição em massa, aos Administradores, Funcionários, Estagiários, Jovens Aprendizes e quaisquer terceiros e prestadores de serviço (“Colaboradores”) do Grupo da Oliveira Trust S.A. (“Oliveira Trust” ou “Companhia”), sendo complementar ao Código de Ética.

2. DEFINIÇÕES

ABR - Abordagem Baseada em Risco – ABR aplicada à PLD/FTP é a metodologia própria da Oliveira Trust que tem por objetivo identificar, avaliar e entender os riscos de LD/FTP a que a instituição está exposta, além de buscar as medidas preventivas proporcionais a esses riscos, a fim de garantir uma mitigação efetiva, em linha com o apetite a riscos da Oliveira Trust;

AIR – Avaliação Interna de Risco – É a metodologia própria da Oliveira Trust que tem por objetivo estruturar uma base conceitual e definir os critérios para diagnóstico, avaliação e compreensão dos riscos de Lavagem de Dinheiro, Financiamento ao Terrorismo e Proliferação de Armas de Destruição em Massa (LD/FTP) inerentes à execução de suas atividades.

Alta Administração – Para fins desta Política, entende-se por Alta Administração os membros do Conselho de Administração e da Diretoria da Oliveira Trust.

Beneficiário Final - De acordo com as definições da Receita Federal do Brasil, entende-se por Beneficiário Final a pessoa natural que, em última instância, de forma direta ou indireta, possui, controla ou influencia significativamente a entidade; ou a pessoa natural em nome da qual uma transação é conduzida.

Cliente – Sob o viés de PLD/FTP, considera-se Cliente toda e qualquer pessoa natural ou jurídica, atuando em nome próprio ou de terceiros, que mantenha relacionamento ativo com a Oliveira Trust com o objetivo de utilizar os serviços disponibilizados pela Companhia.

COAF - Conselho de Controle de Atividades Financeiras – Unidade de Inteligência Financeira do Brasil, criado através da Lei 9.613 de 1998, conforme alterada, tem a finalidade de disciplinar, aplicar penas administrativas, receber, examinar e identificar as ocorrências suspeitas de atividades ilícitas, relacionadas a lavagem de dinheiro, previstas em Lei, sendo um órgão administrativo vinculado ao Banco Central do Brasil.

Colaboradores – Para fins desta política, entende-se por todos os administradores, funcionários, estagiários, jovens aprendizes e quaisquer terceiros e prestadores de serviço da Oliveira Trust.

CSNU – Conselho de Segurança da Organização das Nações Unidas – Órgão da Organização das Nações Unidas (ONU) que tem por principal objetivo a manutenção da paz mundial. Atua ativamente na prevenção de financiamento ao terrorismo através a imposição de sanções e divulgação de listas restritivas.

CVM – Comissão de Valores Mobiliários – Autarquia federal com poderes para disciplinar, normatizar e fiscalizar a atuação dos diversos integrantes do mercado de valores mobiliários, inclusive em assuntos relacionados à PLD/FTP.

KYC - Know Your Customer - Termo em inglês que, no contexto de PLD/FPT, significa “Conheça seu cliente”.

KYE - Know Your Employee - Termo em inglês que, no contexto de PLD/FPT, significa “Conheça seu colaborador”.

KYS - Know Your Supplier - Termo em inglês que, no contexto de PLD/FPT, significa “Conheça seu fornecedor/parceiro”.

PEP – Pessoas Expostas Politicamente – São todas as pessoas que, nos últimos cinco anos, exercem ou exerceram, no Brasil ou no exterior, algum cargo, emprego ou função pública relevante ou se têm, nessas condições, familiares, representantes ou ainda pessoas de seu relacionamento próximo.

3. LAVAGEM DE DINHEIRO

A expressão “lavagem de dinheiro” consiste na ação destinada a ocultar ou dissimular a natureza, origem, localização, disposição, movimentação ou propriedade de bens, direitos ou valores provenientes, direta ou indiretamente, de infração penal. As etapas, são, respectivamente:

- **Colocação** – a primeira etapa do processo é a colocação do dinheiro no sistema econômico. Objetivando ocultar sua origem, o criminoso procura movimentar o dinheiro em países com regras mais permissivas e naqueles que possuem um sistema financeiro liberal. A colocação se efetua 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 e a utilização de estabelecimentos comerciais que usualmente trabalham com dinheiro em espécie.
- **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 abertas em nome de "laranjas" ou utilizando empresas fictícias ou de fachada.
- **Integração** – nesta 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 o dinheiro ilegal.

O Brasil, em linha com os organismos internacionais, vem editando normas no sentido de combater sistematicamente os ilícitos previstos nessa política, estabelecendo diretrizes a serem observadas na identificação de clientes, análise de movimentações financeiras, detecção de transações que possam configurar indícios da ocorrência dos crimes previsto em lei.

3.1. DO CRIME DE LAVAGEM DE DINHEIRO

Os crimes de Lavagem de Dinheiro ou Ocultação de Bens, Direitos e Valores estão definidos na Lei 9.613/98, conforme alterada, como sendo o ato de ocultar ou dissimular a natureza, origem, localização, disposição, movimentação ou propriedade de bens, direitos ou valores provenientes, direta ou indiretamente, de infração penal.

Abaixo, exemplos, não exaustivos:

- tráfico de drogas;
- terrorismo e seu financiamento;
- contrabando ou tráfico de armas, munições ou material destinado à sua produção;
- extorsão mediante sequestro;
- contra a Administração Pública, inclusive a exigência, para si ou para outrem, direta ou indiretamente, de qualquer vantagem, como condição ou preço para a prática ou omissão de atos administrativos;
- contra o sistema financeiro nacional;
- praticado por organização criminosa;
- praticado por particular contra a administração pública estrangeira; ou
- quaisquer infrações caracterizadas como crime no Código Penal Brasileiro.

Incorre no mesmo crime quem, para ocultar ou dissimular a utilização de bens, direitos ou valores provenientes de quaisquer infrações penais:

- os converte em ativos lícitos;
- os adquire, recebe, troca, negocia, dá ou recebe em garantia, guarda, tem em depósito, movimenta ou transfere;
- importa ou exporta bens com valores não correspondentes aos verdadeiros.

Incorre, ainda, no mesmo crime quem:

- utiliza na atividade econômica ou financeira, bens, direitos ou valores que sabe serem provenientes de quaisquer infrações penais;
- participa de grupo, associação ou escritório tendo conhecimento de que sua atividade principal ou secundária é dirigida à prática dos crimes mencionados;
- participa da tentativa ou facilita a prática dos crimes citados.

4. TERRORISMO E SEU FINANCIAMENTO

De acordo com a Lei nº 13.260/16, o terrorismo consiste na prática por um ou mais indivíduos dos atos previstos na Lei, por razões de xenofobia, discriminação ou preconceito de raça, cor, etnia e religião, quando cometidos com a finalidade de provocar terror social ou generalizado, expondo a perigo pessoa, patrimônio, a paz pública ou a incolumidade pública. Ele se configura quando alguém, direta ou indiretamente, por qualquer meio, presta: (i) apoio financeiro, (ii) fornece ou reúne fundos com a intenção de serem utilizados; (iii) sabe que serão utilizados, total ou parcialmente, por grupos terroristas para a prática de atos terroristas.

5. PROLIFERAÇÃO DE ARMAS DE DESTRUIÇÃO EM MASSA

Pode-se entender arma de destruição em massa (ADM) como o dispositivo capaz de promover danos intencionais em grande escala, a exemplo de armas nucleares, químicas e biológicas ou tóxicas. Mísseis e veículos aéreos não tripulados, também denominados vetores, com capacidade de transportar ADM, não são assim considerados, embora despertem idênticas preocupações do ponto de vista da segurança internacional.

O Decreto Nº 7.722 de 20 de abril de 2012 dispõe sobre a execução no Brasil das Resoluções nº 1540 (2004) e nº 1977 (2011), adotadas pelo Conselho de Segurança das Nações Unidas, as quais dispõem sobre o combate à proliferação de armas de destruição em massa.

6. COMPROMETIMENTO DA ALTA ADMINISTRAÇÃO

O Conselho de Administração e a Diretoria se comprometem com a disponibilização de recursos financeiros, materiais e humanos para implementação, manutenção, efetividade e a

melhoria contínua da política, dos procedimentos e dos controles internos relacionados com a prevenção à lavagem de dinheiro e financiamento do terrorismo.

7. ESTRUTURA ORGANIZACIONAL – RESPONSABILIDADES

7.1. Conselho de Administração

O Conselho de Administração é responsável por revisar, aprovar e acompanhar o cumprimento das diretrizes desta política.

7.2. Diretor responsável PLD/FTP e demais ilícitos

O diretor responsável pelas atividades de PLD/FTP deve, anualmente, revisar a Política, assim como assegurar o cumprimento desta Política, demais normas aplicáveis e as determinações dos órgãos reguladores para atuação na PLD/FTP.

Além disso, é de sua responsabilidade elaborar, até o último dia útil de abril de cada ano, o relatório anual de avaliação interna de risco de LD/FTP a ser encaminhado para os órgãos da alta administração especificados nesta política.

7.3. Demais Diretores

Sem prejuízo da responsabilidade do diretor de PLD/FTP, os demais Diretores são responsáveis pela adequação e implementação desta política, da avaliação interna de risco, assim como das regras, dos procedimentos e dos controles internos.

7.4. Comitê de Compliance e Riscos

As operações com indícios de suspeita de lavagem de dinheiro são levadas a este Comitê, que analisa a situação e, por meio de voto eletrônico, seus membros decidem se devem ser comunicadas ao COAF.

O Comitê de Compliance e Riscos é composto por Diretores e Gerentes, se reunindo presencialmente ou através de vídeo conferência, a cada 02 (dois) meses ou sempre que houver necessidade através da abertura de fórum eletrônico.

7.5. Compliance e Controles Internos

A área de Compliance e Controles Internos deve, dentre suas atribuições, garantir a conformidade com a legislação, normas, regulamentos e políticas internas que disciplinam a prevenção à LD/FTP. Além disso, são suas responsabilidades:

- Elaborar e atualizar as políticas e normas internas voltadas a crimes relacionados à LD/FTP, incluindo a definição de procedimentos como KYC, KYP, KYS e KYE;
- Disseminar e atuar como multiplicador da cultura de PLD/FTP;
- Implementar procedimentos para identificação, monitoramento e comunicação ao COAF das operações enquadradas nos critérios de comunicação estabelecidos nas regulamentações aplicáveis;
- Providenciar comunicação ao COAF de operações ou situações que possam configurar indício de lavagem de dinheiro, após aprovação do Comitê de Compliance e Riscos, mantendo a confidencialidade sobre o processo;
- Implementar melhorias recomendadas pela Auditoria Interna durante sua avaliação anual dos processos de PLD/FTP.

7.6. Auditoria Interna

Como terceira linha de defesa, o escopo da Auditoria Interna abrange a revisão e avaliação da implementação dos controles da Política de PLD/FTP. A Auditoria Interna é independente e responde diretamente à Diretoria, tendo como principal função o exame dos processos internos, verificando, anualmente, conforme seu planejamento, a adequação e validação dos processos, das informações e registros, recomendando melhorias quando necessário.

7.7. Cadastro

Responsável pela execução dos processos de “Conheça seu Cliente” (KYC), “Conheça seu Parceiro/Prestador de Serviço” (KYP), “Conheça seu Fornecedor” (KYS), por parte do “Conheça seu Funcionário” (KYE), e por realizar a análise e verificação de regularidade dos documentos cadastrais dos clientes / investidores, bem como pela manutenção da atualização dos dados e documentos cadastrais.

Se identificado algum indício de ocorrência de lavagem de dinheiro ou financiamento do terrorismo, a área de Cadastro deverá encaminhar o caso para avaliação da área de Compliance e Controles Internos.

7.8. Todos os Colaboradores

É disciplinado a todos os colaboradores o conhecimento e cumprimento das normas, internas e externas, relativas à PLD/FTP, bem como a disseminação da cultura relacionada ao tema. Além disso, é papel coletivo comunicar, de forma tempestiva, à área de Compliance e Controles

Internos toda e qualquer proposta, operação ou situação considerada atípica ou suspeita que possa configurar indícios de LD/FTP.

8. PROGRAMA DE PLD/FTP

8.1. Conheça seu Cliente (KYC)

O processo conheça seu cliente é um dos mais importantes pilares na PLD/FTP, compreendendo um conjunto de regras e procedimentos, que tem por objetivo identificar e conhecer a origem e constituição do patrimônio e dos recursos financeiros do cliente.

Visam assegurar a identidade e a atividade econômica dos clientes, bem como a origem e a constituição de seu patrimônio e seus recursos financeiros. A coleta destas informações deve permitir a avaliação da capacidade financeira do cliente.

Com base em uma abordagem baseada no risco de LD/FTP, para os clientes classificados com maior risco e para os casos que requerem Especial Atenção, como o relacionamento com Pessoa Exposta Politicamente (PEP) e clientes onde não foi possível identificar o beneficiário final, são adotados procedimentos rigorosos específicos de análise.

É obrigatória a avaliação sobre o interesse no início ou na manutenção do relacionamento com pessoas físicas ou pessoas jurídicas classificadas como PEPs por um detentor de cargo ou função de nível hierárquico superior ao do responsável pela autorização do relacionamento, conforme definido em regra interna.

Por fim, esse processo visa direcionar e padronizar procedimento para o início, manutenção e monitoramento do relacionamento com aqueles que utilizam ou que pretendam utilizar seus produtos e/ou serviços, de modo a prevenir qualquer forma de colaboração com a lavagem de dinheiro e ao financiamento do terrorismo ou quaisquer outras atividades ilícitas.

8.1.1. Identificação do Beneficiário Final

“Beneficiário final” é a pessoa natural que, em última instância, de forma direta ou indireta, possui, controla ou influencia significativamente a entidade; ou a pessoa natural em nome da qual uma transação é conduzida. Presume-se influência significativa, quando a pessoa natural possui mais de 25% (vinte e cinco por cento) do capital da entidade, direta ou indiretamente; ou direta ou indiretamente, detém ou exerce a preponderância nas deliberações sociais e o poder de eleger a maioria dos administradores da entidade, ainda que sem controlá-la.

8.2. Conheça seu Colaborador (KYE)

O processo “Conheça seu Colaborador”, consiste na aplicação de procedimentos e controles para identificar e qualificar adequadamente os colaboradores e/ou candidatos, a fim de subsidiar a sua seleção e contratação, bem como acompanhar situações que possam caracterizar algum tipo de risco ou desvio, para fins de LD/FTP e demais atos ilícitos.

Estes colaboradores devem ser classificados em categorias de risco considerando as atividades por eles exercidas junto à Oliveira Trust.

8.3. Conheça seu Parceiro/Fornecedor/Prestador de Serviço (KYS)

São considerados como “Parceiro(s)”, “Prestador(es) de serviços” e/ou “Fornecedor(es)” as Pessoas Jurídicas que firmam contratos de prestação de serviços e que atendam aos requisitos estabelecidos internamente.

É um conjunto de procedimentos e controles que devem ser adotados para identificar e qualificar adequadamente esses parceiros, para aceitação de fornecedores e prestadores de serviços, prevenindo a contratação de empresas inidôneas ou suspeitas de envolvimento em atividades ilícitas. Estes parceiros devem ser classificados em categorias de risco considerando as atividades por eles exercidas.

8.4. Vedações

A Oliveira Trust não inicia relacionamento com Pessoas Naturais ou Jurídicas presentes na lista de Sanções do CSNU (Conselho de Segurança das Nações Unidas) e com os denominados Bancos de Fachada (*Shell Banks*), ou seja, bancos constituídos em uma jurisdição onde não há qualquer presença física e que não se encontrem integrados a nenhum grupo financeiro regulamentado.

Adicionalmente, a Oliveira Trust opera apenas com bancos que possuam licenças para operar em seu país de origem e, dada a natureza de suas operações, não opera com bancos correspondentes

9. AVALIAÇÃO INTERNA DE RISCO (AIR)

A Oliveira Trust estrutura sua Avaliação Interna do Risco (AIR) adotando metodologia própria, com o objetivo de identificar, mensurar e mitigar os riscos de Lavagem de Dinheiro,

Financiamento ao Terrorismo e Proliferação de Armas de Destruição em Massa (LD/FTP) inerentes à execução de suas atividades.

Com base na AIR é aplicada a Abordagem Baseada em Risco (ABR), também confeccionada através de metodologia própria, com o objetivo de garantir medidas de prevenção e mitigação dos riscos identificados, conforme o nível de risco, medidas adotadas poderão ser mais reforçadas ou mais simplificadas.

10. AVALIAÇÃO DE EFETIVIDADE

A Oliveira Trust elabora anualmente Relatório de Efetividade, de modo a avaliar a efetividade das políticas, procedimentos e controles internos de PLD/FTP. Os planos de ação endereçados a solucionar as deficiências identificadas, por meio da referida Avaliação, deverão ser acompanhados por meio de um fórum eletrônico e reportados ao Comitê de Compliance e Riscos para fins de acompanhamento.

Adicionalmente, a Avaliação de Efetividade deverá conter, no mínimo, informações que descrevam a metodologia adotada; os testes aplicados; a qualificação dos avaliadores e as deficiências identificadas.

11. MONITORAMENTO, SELEÇÃO E ANÁLISE DE OPERAÇÕES E SITUAÇÕES SUSPEITAS

A Oliveira Trust possui sistema de monitoramento e seleção automática de operações, levando em consideração os parâmetros compatíveis à estrutura e complexidade dos serviços prestados, enquanto administrador, custodiante de fundos de investimento e escriturador. Nesse sentido, as transações e operações financeiras, inclusive as propostas, ficam registradas em sistemas, sendo passíveis de análise sob a ótica de PLD-FTP.

O período para a execução dos procedimentos de análise das operações e situações selecionadas não pode exceder o prazo de quarenta e cinco dias, contados a partir da data da seleção da operação

ou situação. A análise mencionada deve ser formalizada em dossiê, independentemente da comunicação ao COAF.

12. COMUNICAÇÃO DE OPERAÇÕES E SITUAÇÕES SUSPEITAS.

As operações, situações ou propostas que contêm indícios de lavagem de dinheiro ou de financiamento ao terrorismo devem ser comunicadas aos órgãos reguladores competentes, em cumprimento às determinações legais e regulamentares. Comunicações de boa-fé não acarretam responsabilidade civil ou administrativa à Oliveira Trust, nem a seus administradores e Colaboradores.

As comunicações ao COAF devem ser efetuadas sem que seja dada ciência aos envolvidos.

12.1. Comunicação de não ocorrência a operações e situações suspeitas

No caso de não ocorrerem no ano civil registros de operações ou propostas de operações passíveis de comunicação ao COAF e à CVM, a Oliveira Trust deverá:

- Declarar ao BACEN, em até dez dias úteis do ano subsequente, a não ocorrência de situações passíveis de comunicação; e
- Declarar à CVM, até o último dia útil do mês de abril do ano subsequente, a não ocorrência de situações passíveis de comunicação;

13. SANÇÕES IMPOSTAS POR RESOLUÇÕES DO CONSELHO DE SEGURANÇA DAS NAÇÕES UNIDAS (CSNU)

Como sujeito obrigado, a Oliveira Trust deve cumprir, imediatamente e sem aviso prévio aos sancionados, as medidas estabelecidas nas resoluções sancionatórias do CSNU e as designações de seus comitês de sanções que determinem a indisponibilidade de ativos de pessoas naturais e jurídicas e de entidades, bem como a designação nacional de pessoas investigadas ou acusadas de atos correlacionados ao terrorismo (Sancionados), conforme termos da Lei nº 13.810, de 2019.

A indisponibilidade de ativos refere-se à proibição de transferir, converter, trasladar, disponibilizar ativos ou deles dispor, direta ou indiretamente, de bens, direitos, valores, fundos,

incidindo inclusive sobre os juros e outros frutos civis e rendimentos decorrentes do contrato, de qualquer natureza, financeiros ou não.

A comunicação da indisponibilidade de ativos deverá ser comunicada à CVM, Ministério da Justiça e Segurança Pública e COAF.

14. ANÁLISE PRÉVIA DE NOVOS PRODUTOS, SERVIÇOS E TECNOLOGIAS

Novos produtos e serviços, assim como utilização de novas tecnologias, deverão ser avaliados, obrigatoriamente, de forma prévia, sob a ótica de PLD/FTP e demais ilícitos, antes de serem negociados com clientes e/ou investidores.

15. TREINAMENTO

O programa de treinamento para assuntos relacionados à PLD/FTP promove a capacitação contínua e dissemina a cultura do tema, alcançando, assim, a aprendizagem e conscientização da sua importância, bem como o aprofundamento e reciclagem do conhecimento. O programa tem como objetivos:

- Aprofundar o conhecimento das exigências e responsabilidades legais e regulamentares;
- Capacitar sobre a melhor forma para a identificação, prevenção, tratamento e comunicação de situações de risco ou com indícios de ocorrência de LD/FTP nos negócios realizados; e
- Promover a cultura organizacional de prevenção à lavagem de dinheiro e ao financiamento do terrorismo, inclusive à proliferação de armas de destruição de massa.

As definições quanto as responsabilidades, aplicabilidade e periodicidade para treinamentos relacionados à PLD/FTP podem ser encontradas na Política de Treinamento e Capacitação.

16. CANAIS DE COMUNICAÇÃO

Os administradores, colaboradores, parceiros e clientes da Oliveira Trust devem comunicar imediatamente à área de Compliance, através de e-mail, ou pelo canal de denúncias, o qual se encontra disponível no site da companhia¹, as situações com indícios ou evidências de atos ilícitos relacionados à LD/FTP.

¹ <https://www.oliveiratrust.com.br/canal-de-denuncia/>

17. MANUTENÇÃO DE INFORMAÇÕES E REGISTROS

Os documentos referentes às operações, documentos cadastrais e dossiês de análise de operações e situações suspeitas devem ser arquivados pelo período mínimo de 10 (dez) anos a partir do encerramento do relacionamento ou da conclusão da última transação realizada pelo cliente.

18. SANÇÕES APLICÁVEIS

O descumprimento das disposições legais e regulamentares sujeita os Administradores e os Colaboradores a sanções que vão desde penalidades administrativas até criminais por lavagem de dinheiro, financiamento ao terrorismo e fraudes.

As sanções aplicáveis pelo descumprimento desta Política são as mesmas contidas no Código de Ética.

19. VIGÊNCIA E APROVAÇÃO

Esta Política deverá ser revisada e atualizada no mínimo anualmente.

| Versão | Data | Revisado/ Aprovado | Responsável |
|--------|------------|-----------------------|---------------------------|
| 2025.1 | 06/11/2025 | Revisado | Gerente de Compliance |
| 2025.1 | 06/11/2025 | Revisado | Diretoria de Compliance |
| 2025.1 | 06/11/2025 | Aprovado | Conselho de Administração |

OLIVEIRA TRUST