



PROA GESTORA DE RECURSOS LTDA – CNPJ: 62.200.538/0001-05

POLÍTICA DE PREVENÇÃO À LAVAGEM DE DINHEIRO

SUMÁRIO DO DOCUMENTO	Estabelece diretrizes sobre a prevenção à lavagem de dinheiro, ao financiamento do terrorismo e ao financiamento da proliferação de armas de destruição em massa (PLD/FT)
Referência	Setembro/2025
Confidencialidade	Público
Versão	1
Estado	Aprovado
Emissor	Risco e Compliance
Autor	Andressa Vianna Santos Viceconti
Cargo do Autor	Diretora de Risco e Compliance
Data de Criação	01/09/2025
Última Atualização	19/09/2025
Data de Publicação	19/09/2025

POLÍTICA DE PREVENÇÃO À LAVAGEM DE DINHEIRO

1. INTRODUÇÃO

A Política de Prevenção à Lavagem de Dinheiro (“Política”), visa estabelecer diretrizes com o objetivo de promover a adequação das atividades e incorporar ao negócio as melhores práticas de mercado e os requerimentos legais e regulamentares, referentes à prevenção e combate aos crimes de lavagem de dinheiro, ocultação de bens, direitos e valores, ao financiamento do terrorismo e ao financiamento da proliferação das armas de destruição em massa (“PLD/FTP”).

A **PROA GESTORA DE RECURSOS LTDA.** (“PROA”) tem estrito compromisso para com a integridade do sistema financeiro, buscando prevenir quaisquer práticas, que a firam. Nesse sentido, é tido como fundamental o respeito para com todas as leis, regulamentações, princípios e diretrizes relacionadas à PLD/FTP.

Todos os sócios, diretores, funcionários, estagiários, prestadores de serviços e agentes autônomos devem agir com diligência ao iniciar um relacionamento e no Cadastro de Clientes/contraparte da operação, evitando realizar negócios que apresentem indícios de relação a crimes de LD/FTP, ou que possam facilitá-las.

No cadastramento dos Clientes, deve-se mensurar os riscos de LD/FTP, adotando as melhores práticas e atendo-se aos procedimentos e controles implementados pela empresa.

O mesmo cuidado deve ser dado no monitoramento das operações realizadas pelos Clientes.

Adicionalmente são descritos os critérios utilizados para a identificação, registro e comunicação de operações financeiras cujas características sejam excepcionais no que se refere às partes envolvidas, forma de realização, e/ou instrumentos utilizados; ou para as quais falte, objetivamente, fundamento econômico ou legal, havendo assim a possibilidade de constituir indícios de crimes de LD/FTP, conforme previsto na Lei n.º 12.683/2012.

A implementação de um programa adequado de PLD/FTP tem o escopo de assegurar que, a instituição diligenciou e buscou tomar as precauções cabíveis para evitar o envolvimento de sua estrutura com práticas delitivas. O programa de PLD/FTP tem por objetivo proporcionar à Alta Administração uma visão geral dos esforços da instituição na PLD/FTP.

A Política de PLD/FTP, procura alinhar-se aos critérios estabelecidos na ANR da GTANR, para aprimoramento contínuo da avaliação de riscos da **PROA**.

2. ABRANGÊNCIA

A Política dispõe sobre as normas e procedimentos a serem observados pelos administradores, diretores, empregados, estagiários, prestadores de serviços, e demais Pessoas Vinculadas (“Colaboradores”).

É de responsabilidade de todos os Colaboradores conhecer e cumprir todas as obrigações decorrentes da presente Política, observar os mais altos padrões de conduta profissional ao conduzir suas atividades, bem como, informar e reportar inconsistências em procedimentos e práticas definidas neste documento, seja para o seu superior direto, seja pela ferramenta Compiasset ao Compliance.

3. GOVERNANÇA

A **PROA** possui uma estrutura de governança para identificação, prevenção, detecção da utilização de seus Recursos para lavagem de dinheiro, conforme os requerimentos legais e regulatórios, constituída, pelo:

- Comitê Diretivo: órgão máximo referente a gestão e controle do programa PLD/FTP, sendo responsável pela adoção de Políticas corporativas, supervisão do cumprimento das leis e regulamentações, e das medidas para atendimento de apontamentos e solicitações dos órgãos governamentais e de regulação, decorrentes das atividades de supervisão;

- Comitê de Risco e *Compliance*: órgão responsável pela avaliação de riscos e da eficácia do programa de PLD/FTP, e do sistema de controles internos. As vulnerabilidades e incidentes apresentados, podem gerar recomendações ao Comitê Diretivo, para mudanças na estratégia do negócio e do nível de aceitação de riscos;

- Comitê de Políticas: Subcomitê de Risco e Compliance, responsável pela aprovação das políticas, normas e procedimentos de PLD/FTP;

- Áreas geradoras de risco, são as áreas responsáveis pelas atividades comerciais, de consultoria, de gestão e demais atividades que geram exposição a riscos, como primeira linha de defesa, essas áreas devem realizar a gestão desses riscos, de acordo com a estratégia e os níveis de aceitação de risco definidos pelo Comitê Diretivo;

- Área de Riscos e *Compliance*, é uma área independente, que reporta diretamente ao Comitê Diretivo, responsável pela supervisão das atividades de gestão de riscos, realizadas pelas áreas geradoras de risco, assegurando que estas estejam em cumprimento com a legislação e a regulamentação, compatível com a natureza, o porte, a complexidade, a estrutura, o perfil de risco e o modelo de negócio da empresa; e

- Área de Auditoria Interna ou Controle Interno (*Compliance Test*) é a função de Controle de Qualidade, realizada pela área de *Compliance*, sendo responsável pela certificação da efetividade das políticas, metodologias e procedimentos implementados, e controle da efetividade do sistema de PLD/FTP.

O Comitê Diretivo constitui outros órgãos colegiados, para deliberação de outros programas e processos da PROA, onde, entre outros temas, são considerados aspectos e riscos de conformidade e PLD/FTP.

4. AVALIAÇÃO INTERNA DE RISCO (AIR)

Nos procedimentos de avaliação prévia de novos clientes, produtos e serviços, e da utilização de novas tecnologias, devem ser consideradas a AIR, com o objetivo de identificar e mensurar o risco de utilização de seus produtos e serviços na prática da lavagem de dinheiro, do financiamento ao terrorismo e da proliferação de armas de destruição em massa.

Os riscos em relação a LD/FTP, são categorizados conforme a AIR, em baixo risco, médio risco e alto risco para: (i) clientes e suas respectivas cadeias de relacionamento; (ii) produtos e serviços e seus respectivos canais de distribuição, bem como ambientes de negociação e registro; e (iii) avaliação do risco relativo ao relacionamento da instituição com outras pessoas submetidas à regulação de PLD/FTP da CVM.

No processo de identificação e avaliação do risco de LD/FTP aos quais a empresa está exposta, devem ser considerados vários fatores, como: a cultura de confidencialidade, dificuldade para identificação dos beneficiários finais, ocultação da origem do dinheiro - uso de empresas e contas bancárias abertas em territórios onde há menor tributação (Paraísos Fiscais) ou supervisão (Paraísos Jurídicos) - sigilo bancário, produtos e serviços financeiros complexos, PEP, transações de grande valor, múltiplas jurisdições, entre outros.

Devido aos últimos grandes “eventos judiciais” do nosso país, apresentados pelo ANR de 2021 da PLD Brasil, deve ser dada especial atenção, às acusações e condenações referentes aos crimes de (i) corrupção; (ii) tráfico de drogas; (iii) organizações criminosas; (iv) crimes financeiros; (v) sonegação fiscal; quando da classificação de risco de clientes, parceiros e ativos (ex.: análise do passivo tributário de uma empresa, pode ser um indício de o quanto ela representa de risco de crime fiscal e sua venda um ato de lavagem).

O risco é dinâmico e deve ser monitorado, testado e reavaliado de forma contínua, assim como, a aplicação das formas de mitigação, e necessitam de reclassificação de risco, à medida que surjam novos produtos ou serviços, clientes, ou elementos no contexto de relacionamento da PROA, ou na ocorrência de qualquer fato novo que possa alterar a classificação.

Mudanças no arcabouço legal e regulatório, e os resultados dos relatórios sobre a AIR, ANR, entre outros, devem ser considerados e analisados, e podem requerer correções ou aprimoramentos da metodologia de ABR, da Política de PLD/FTP e seus procedimentos e controles.

4.1. AVALIAÇÃO DE CLIENTES DIRETOS

São considerados Clientes Diretos, sujeitos a esta Política, os investidores, pessoas naturais ou jurídicas, com os quais a PROA mantenha relacionamento comercial direto.

A classificação dos Clientes Diretos por grau de risco tem como objetivo destinar maior atenção aos clientes que demonstrem maior probabilidade de apresentar envolvimento com LD/FTP.

Enquanto gestora de fundos de investimentos e carteiras administradas, a PROA é responsável por analisar quaisquer indícios de tais práticas na negociação de Ativos e valores mobiliários. Este procedimento baseia-se nas boas práticas de PLD/FTP de uma ótica mais voltada ao ativo, uma vez que a empresa não realiza a atividade de administração fiduciária nem de distribuição de cotas de fundos de investimentos.

Os Clientes são determinados pelos seguintes graus de risco:

a) Alto Risco:

A atualização cadastral destes Clientes Diretos, deve ser realizada anualmente ou no período máximo de 24 (vinte e quatro) meses, a partir da data do Cadastro ou da última atualização cadastral.

Clientes que sejam: (i) investidores não residentes, quando constituídos sob a forma de *trusts* e sociedades com títulos ao portador ("INR"); (ii) Pessoas Expostas Politicamente, conforme definidas no Anexo A da Resolução CVM n.º 50; e (iii) organizações não governamentais e/ou sem fim lucrativos, são classificados como de alto risco.

A Equipe de *Compliance* destinará especial atenção para aqueles Clientes Diretos classificados como de Alto Risco, devendo monitorar continuamente e de maneira diferenciada a relação de negócio e as propostas de início de relacionamento. Os clientes de alto risco, podem ser submetidos a diligências adicionais.

A área de *Compliance* pode determinar a adoção de diligências adicionais a clientes com outros níveis de risco, caso, estes estejam expostos a fatores, que podem "aumentar" o risco em relação à LD/FTP ("clientes com risco aumentado ou de risco crescente").

O Comitê de Risco e *Compliance* pode determinar a proibição ou a adoção de medidas especiais para determinados tipos de clientes e/ou ocupações/atividades econômicas, até mesmo o encerramento ou finalização das relações com clientes por motivos de LD/FTP.

b) Médio Risco

Atualização cadastral destes Clientes Diretos, deve ser realizada no período máximo de 36 (trinta e seis) meses, a partir da data do Cadastro ou da última atualização cadastral.

Clientes que sejam: (i) Investidores com grandes fortunas, geridas por área de instituições financeiras voltadas para clientes com este perfil ("*Private Banking*"), são classificados como de médio risco.

c) Baixo Risco - Clientes Diretos não listados acima.

A atualização cadastral destes Clientes Diretos, deve ser realizada no período máximo de 60 (sessenta) meses, a partir da data do Cadastro ou da última atualização cadastral.

As características para a classificação destes clientes seguem as definições contidas no AIR, e podem ser obtidas no Manual de Prevenção à Lavagem de Dinheiro ("Manual PLD/FTP").

O processo de avaliação é contínuo, alterações no Cadastro, perfil do negócio, estrutura societária, cadeia relacional, entre outras, identificadas pelas áreas de Operações, Middle ou pelos agentes comerciais,

devem ser informados a área de *Compliance*, que avaliará e realizará a reclassificação do risco de PLD/FT, caso necessário.

As listas de atividades terroristas, sanções e contramedidas financeiras, emitidas por programas nacionais e internacionais (COAF, ONU, EU, OFAC, entre outros) devem sempre ser consultadas para a análise e reclassificação dos clientes.

4.2. AVALIAÇÃO DE PRODUTOS E SERVIÇOS E SEUS RESPECTIVOS CANAIS DE DISTRIBUIÇÃO, BEM COMO AMBIENTE DE NEGOCIAÇÃO E REGISTRO

A **PROA** adota a mesma classificação da ANR para seus produtos carteiras administradas e fundos de investimento exclusivos, classificados como de risco médio, devendo estabelecer controles que busquem aprimorar o processo de identificação dos beneficiários finais e de contratação dos prestadores de serviços (KYP).

Considerando que a **PROA**:

- não possui relacionamento comercial direto com cotistas de fundos de investimento com múltiplos cotistas, sob sua gestão;
- não realiza distribuição de cotas de fundos de investimento sob sua gestão;
- não trabalha com fundos de investimentos que possuem como cotistas entidades de Regimes Próprios de Previdência Social;
- atua em um mercado altamente regulado e supervisionado pela CVM e ANBIMA;
- realiza negociação dos Ativos de suas carteiras em mercados organizados dentro do país; e
- trabalha somente com administradores fiduciários e distribuidores devidamente registrados e supervisionados pelo BCB, CVM e ANBIMA.

A Gestora classifica os produtos fundos de investimento restritos, de múltiplos cotistas e não exclusivos, como de risco médio, porém, deve previamente à aquisição destes produtos e continuamente durante o relacionamento, realizar a avaliação de risco de LD/FTP, dos emissores dos Ativos a serem adquiridos, as contrapartes da operação, os intermediários ou distribuidores do ativo, seus escrituradores e outros agentes envolvidos.

4.3. AVALIAÇÃO DO RISCO RELATIVO AO RELACIONAMENTO DA GESTORA COM OUTRAS PESSOAS SUBMETIDAS À REGULAÇÃO DE PLD/FTP DA CVM

Considerando que:

- os fundos sob gestão da **PROA**, contam com administradores fiduciários e distribuidores devidamente registrados e supervisionados pelo BCB, CVM e ANBIMA;
- realiza em nome do fundo, a contratação de prestadores de serviços de: (i) intermediação de operações; (ii) distribuição de cotas; (iii) consultoria de crédito; (iv) agência de classificação de risco de crédito; (v) formador de mercado de classe fechada; e (vi) cogestão de carteira de Ativos, somente com terceiros habilitados e autorizados pela CVM, e avalia tais prestadores previamente à sua contratação; e
- contrata serviços de auditoria de suas demonstrações financeiras com terceiros habilitados e autorizados pela CVM.

A Gestora classifica como baixo o risco de LD/FTP relativo aos relacionamentos com outras pessoas submetidas à regulação de PLD/FTP da CVM.

4.4. AVALIAÇÃO DE EFETIVIDADE DO PROGRAMA

Mensalmente, a área de Risco e *Compliance*, deve apresentar ao Comitê de Risco e *Compliance*, um relatório apresentando as deficiências, vulnerabilidades e ocorrências, para definição de um plano de ação, para correção e/ou aprimoramento do programa, ou em convocação extraordinária do Comitê, tempestivamente, quando da ocorrência ou identificação de deficiência ou vulnerabilidade, caso seja considerado de alta criticidade.

Anualmente a área de Compliance deve apresentar um relatório ao Comitê Diretivo e o Comitê de Risco e *Compliance*, contendo o resultado dos testes de controle de qualidade ("*Compliance Test*") realizados, nos processos de: **a)** classificação e avaliação de riscos; **b)** verificação, validação, registro e adequação dos dados cadastrais; **c)** monitoramento, seleção, análise e comunicação ao COAF; **d)** vulnerabilidades, deficiências e ocorrências registradas e as medidas adotadas para sua correção; **e)** governança das políticas e do programa de PLD/FTP; **f)** treinamento, capacitação, e ações para disseminação da cultura de PLD/FTP dentro da empresa; e **g)** incorporação da prática de análise de riscos nos negócios.

5. POLÍTICA DE "CONHEÇA SEU CLIENTE" (KNOW YOUR CUSTOMER - KYC)

5.1. IDENTIFICAÇÃO DO CLIENTE

O procedimento de identificação do cliente deve assegurar a real identidade dos Clientes, certificar que possuem, de fato, um número de documento válido de identidade ou respectiva inscrição no Cadastro Nacional de Pessoa Jurídica. No caso de investidores não residentes, independentemente do uso do cadastro simplificado, tal informação também deverá contemplar o número do registro atribuído pela CVM ("código CVM").

O contato com o Cliente, poderá ser realizado "*in loco*" ou presencialmente, desde que não impacte a classificação de riscos, durante a continuidade do relacionamento com esse Cliente.

O contato inicial é o momento em que os procedimentos de qualificação devem possibilitar uma primeira abordagem na coleta preliminar e validação de algumas informações relevantes desse Cliente, necessárias ao adequado monitoramento futuro de suas transações, como, por exemplo, identificar se um Cliente pessoa natural é um PEP, ou se um Cliente pessoa jurídica é uma ONG.

5.2. CADASTRO

O processo de coleta de todas as informações cadastrais, deve satisfazer aos requerimentos das normas vigentes, e passível de verificação, seja por meio tradicional ou por meio alternativo eletrônico.

Em caso de sistema alternativo, este deve atender às funções mínimas descritas no Manual de PLD.

Os procedimentos para coleta, validação, avaliação e registro das informações dos Clientes, devem ser definidos aos Clientes, conforme aplicável:

a) Carteira administrada:

O Gestor deve realizar a coleta, validação, avaliação, registro e manutenção do Cadastro do investidor da carteira administrada. Deve-se conhecer o Beneficiário Final até a pessoa natural.

b) Fundo de investimento ou veículo de investimento exclusivo:

O Distribuidor é responsável pelo Cadastro do cotista do fundo ou veículo de investimento exclusivo. Mesmo não tendo a obrigatoriedade, a Gestora deve manter Cadastro conforme sua ABR e conhecer o Beneficiário Final do cotistas, até a pessoa natural, porém, somente se, a Gestora mantiver relacionamento comercial direto com o cotista, sendo capaz de obter as informações requeridas junto ao distribuidor, diretamente junto ao próprio cotista e/ou por meio de fontes públicas confiáveis.

c) Fundo de patrimônio:

A Gestora deve realizar a coleta, validação, avaliação, registro e manutenção do Cadastro do titular do patrimônio. Deve-se conhecer o Beneficiário Final até a pessoa natural.

d) Fundo com múltiplos cotistas:

Neste caso o cliente da Gestora é o próprio fundo, e deve colher, junto ao distribuidor, as informações cadastrais do fundo, e realizar o registro. A Gestora não conhecerá o Beneficiário Final.

Obs.: Caso a Gestora desempenhe simultaneamente, a atividade de distribuição dos fundos sob sua gestão, neste caso, deve realizar a coleta, validação, registro e manutenção do Cadastro do cotista do fundo, bem como deve adotar as diligências para controlar e monitorar o risco de LD/FTP referente às atividades como distribuidor.

Para fins desta Política, não configura relacionamento comercial direto, o mero repasse pela **PROA**, de ordens de aplicação e resgate enviadas pelos distribuidores aos administradores ("boletagem"), tendo em vista que, nesses casos, o relacionamento comercial direto com o Cliente continua sendo desempenhado pelo distribuidor.

Note-se que, em qualquer das hipóteses do item anterior, as informações serão declaradas pelo próprio cliente, devendo passar por um processo de validação pela empresa, por meio de bases de dados públicas ou privadas de reconhecida confiabilidade, podendo tal consulta ser realizada nos dois ambientes.

As divergências eventualmente apontadas durante o processo de análise e validação dos dados cadastrais fornecidos deverão ser dirimidas pelos agentes comerciais, junto aos clientes e tratadas pelas respectivas áreas e instâncias hierárquicas responsáveis pela aprovação e manutenção do relacionamento com clientes.

5.3. CONDUÇÃO DE DILIGÊNCIAS DEVIDAS

A condução contínua de diligências, deve vigorar ao longo de todo o relacionamento comercial com o cliente, visando: **a)** reforçar a verificação da veracidade das informações coletadas; **b)** coletar informações adicionais, quando for o caso; assim como **c)** mantê-las atualizadas, na hipótese de detecção de fato novo que justifique a antecipação do prazo estabelecido pela instituição para a atualização cadastral.

Na condução dessas diligências contínuas devem ser envidados e evidenciados esforços para a busca de informações adicionais visando a devida classificação e gerenciamento de riscos de LD/FTP desse cliente. A busca por dados adicionais deve inicialmente compreender todas as áreas da instituição, assim como outras informações eventualmente disponíveis em outras empresas que podem fazer parte do mesmo conglomerado financeiro. As áreas de *Compliance* das empresas do conglomerado ao qual a **PROA** faz parte, realizam intercâmbio de informações, pois estão sob a gestão do mesmo diretor estatutário de *Compliance*.

A **PROA** solicitará as informações adicionais de administradores e distribuidores de fundos, aos quais a **PROA** é gestora, e não sejam do mesmo conglomerado financeiro, mediante contrato específico ou cláusula contratual de prestação de serviços, para intercâmbio de informações específicas para cumprimento das obrigações de PLD/FTP previstas na legislação.

5.4. IDENTIFICAÇÃO DE BENEFICIÁRIO FINAL

Assim, quando for aplicável a condução do processo de identificação do Beneficiário Final, deve ser notado o valor mínimo de referência, que foi definido em 25% (vinte e cinco por cento) do capital social das pessoas jurídicas ou do patrimônio líquido dos fundos de investimento e demais entidades, sem prejuízo da utilização eventual de cadastro simplificado. Tal parâmetro deve estar alinhado com os resultados da avaliação interna de risco e pode ser inferior a esse percentual em situações de maior risco.

O agente comercial da Gestora em cada processo de Cadastro, assim entendido como aquele colaborador da Gestora que possua relacionamento ou contato direto com o Cliente Direto e Contraparte, caso

a caso, (“Agente Comercial”) será responsável pela coleta de documentos e informações, bem como pelo preenchimento do Relatório Interno de *Know Your Customer* relativamente a cada Cliente Direto e Contraparte

O Agente Comercial deve realizar visita pessoal aos Clientes Diretos e Contrapartes, durante o processo de coleta de informações cadastrais, somente quando entender necessário, ou quando for solicitado pela área de *Compliance*, em especial no caso de o Cliente ser considerado de “Alto Risco” e/ou no caso de inconsistências relativamente aos documentos e informações ordinariamente obtidos.

A área de *Compliance* deve analisar as informações e documentação e, após a análise, o Diretor de *Compliance* poderá aprovar o respectivo Cliente Direto ou Contraparte, bastando que comunique o Agente Comercial por e-mail.

As alterações das informações constante do Cadastro, realizado com base nas informações e documentos definidos nesta Política, dependem de ordem escrita do Cliente Direto ou Contraparte, por meio físico ou eletrônico (e-mail), acompanhadas dos respectivos comprovantes.

O Cadastro de Clientes Diretos e Contrapartes pode ser efetuado e mantido em sistema eletrônico, e deve abranger, todas as pessoas naturais autorizadas a representá-los, e se for o caso, todos seus controladores, diretos e indiretos, e as pessoas naturais que sobre eles tenham Influência Significativa, até alcançar a pessoa natural caracterizada como Beneficiário Final ou qualquer das entidades, aos quais não se obriga a verificação do Beneficiário Final.

Tratando-se de Beneficiário Final *trust* ou veículos assemelhados, a Gestora envidará e evidenciará esforços para identificar: (i) a pessoa que instituiu o *trust* ou veículo assemelhado (*settlor*); (ii) o supervisor do veículo de investimento, se houver (*protector*); (iii) o administrador ou gestor do veículo de investimento (curador ou *trustee*); e (iv) o beneficiário do *trust*, seja uma ou mais pessoas naturais ou jurídicas.

5.5. CADASTRO E FISCALIZAÇÃO DO ATIVO (CONTRAPARTE)

Nas operações ativas (investimentos), o “cliente” deve ser entendido como o emissor do ativo a ser adquirido, a contraparte da operação, o intermediário ou distribuidor do ativo, seu escriturador, entre outros agentes envolvidos. A Gestora é responsável pelo seu Cadastro e monitoramento, se for o caso, devendo observar o disposto no item a seguir, ressalvadas as exceções aqui previstas (“Contrapartes”).

Neste contexto, para as carteiras sob gestão, dentro do princípio da razoabilidade e agindo com bom senso, a Gestora deverá se utilizar das seguintes práticas, conforme estabelecido no Guia ANBIMA de PLD/FTP:

5.5.1. Processo de Identificação de Contrapartes

A negociação de Ativos financeiros para as carteiras de fundos e/ou carteiras administradas, sob gestão da **PROA** deve, assim como os Clientes Diretos (passivo), ser igualmente objeto de análise, avaliação e monitoramento para fins de prevenção e combate à lavagem de dinheiro, aplicando-se as mesmas diretrizes previstas nos itens 5.1. e 6.1. acima, no que aplicável.

A Gestora deve estabelecer processo de identificação de Contraparte adequado às características e especificidades dos negócios. Tal processo visa a prevenir que a Contraparte utilize as carteiras sob gestão para atividades de LD/FTP.

Os Ativos e valores mobiliários elencados a seguir, em função do tipo de emissão e da forma de negociação, passaram por processo de verificação, o que, em princípio, acabaria por eximir a Gestora de diligência adicional em relação ao controle da Contraparte, a saber: **a)** Ativos que tenham sido objeto de ofertas públicas iniciais e secundárias registradas de acordo com as normas emitidas pela CVM; **b)** Ativos que tenham sido objeto de ofertas públicas com esforços restritos, dispensadas de registro de acordo com as normas emitidas pela CVM; **c)** Ativos emitidos ou negociados por instituição financeira ou equiparada; **d)** Ativos emitidos por emissores de valores mobiliários registrados na CVM; e, **e)** Ativos de mesma natureza econômica dos listados acima, quando negociados no exterior, desde que (a) sejam admitidos à negociação em bolsas de valores, de mercadorias e futuros, ou registrados em sistema de registro, custódia ou de liquidação financeira, devidamente autorizados em seus países de origem e supervisionados por autoridade

local reconhecida pela CVM, ou (b) cuja existência tenha sido assegurada por terceiros devidamente autorizados para o exercício da atividade de custódia em países signatários do Tratado de Assunção ou em outras jurisdições, ou supervisionados por autoridade local reconhecida pela CVM.

No entanto, a Gestora sempre diligenciará no processo de identificação da contraparte, caso seja possível tal diligência em razão das circunstâncias e características do ativo a ser investido.

Para os demais Ativos, como títulos e valores mobiliários objeto de distribuição privada (renda fixa ou ações), direitos creditórios, empreendimentos imobiliários etc., é recomendável que a Gestora, além dos procedimentos de Identificação de Contrapartes, adote também outros procedimentos (como visita de diligência) e controles internos, ou verificar se a contraparte dispõe de mecanismos mínimos para análise para fins de prevenção e combate à lavagem de dinheiro.

6. PROCESSO DE “CONHEÇA SEU COLABORADOR” (KNOW YOUR EMPLOYEE - KYE)

O processo de seleção e contratação de colaboradores deve considerar regras, procedimentos e controles, para certificar a idoneidade e a integridade de seus contratados, evitando vínculos com pessoas com envolvimento em atos ilícitos.

Os novos colaboradores devem ser igualmente objeto de análise, avaliação e monitoramento para fins de prevenção e combate à lavagem de dinheiro, aplicando-se as mesmas diretrizes previstas no item 6.1. acima, no que for aplicável.

As medidas devem ser aplicadas durante todo o período de vínculo com a empresa.

Dentre as medidas a serem adotadas a área responsável pela contratação do colaborador deve: **a)** coletar, verificar, validar e atualizar as informações cadastrais obrigatórias, conforme as regulamentações e as políticas corporativas; **b)** aplicar controles e medidas voltadas à LD/FTP nos processos de seleção, contratação, e durante todo o período do vínculo contratual com o colaborador, a fim de prevenir e detectar falhas nos sistemas, e atuações negligentes ou irregulares; **c)** acompanhar e identificar quaisquer mudanças de conduta, na situação econômico-financeiras dos colaboradores ou outras mudanças que indiquem uma fragilidade na estrutura moral do colaborador que, possam conduzir ao cometimento de, ou ser um indício do envolvimento em um ato ilícito; e, **d)** garantir que todos os colaboradores recebam capacitação e treinamento permanente, sobre o código de conduta e as regras de *Compliance*.

7. PROCESSO DE “CONHEÇA SEU PRESTADOR DE SERVIÇO E PARCEIRO COMERCIAL” (KNOW YOUR PARTNER - KYP)

O processo de seleção e aceitação de fornecedores, prestadores de serviços e parceiros comerciais, deve prever regras e procedimentos para a contratação de empresas idôneas, sem restrições legais ou suspeitas de envolvimento em atividades ilícitas, e deve ainda, avaliar que eles possuem procedimentos adequados de PLD/FTP, quando aplicável.

Os novos prestadores de serviços e parceiros comerciais devem ser igualmente objeto de análise, avaliação e monitoramento para fins de prevenção e combate à lavagem de dinheiro, aplicando-se as mesmas diretrizes previstas nos itens 5.1.e 6.1. acima, no que for aplicável.

As medidas devem ser aplicadas durante todo o período de vínculo com a empresa.

Para aqueles que representarem um risco de PLD/FTP maior, devem ser adotados procedimentos adicionais e diligências aprofundadas de avaliação e alçadas específicas de aprovação, de acordo com a criticidade dos apontamentos.

8. MONITORAMENTO, SELEÇÃO E ANÁLISE DE OPERAÇÕES

As operações realizadas pelos seus fundos de investimento e carteiras administradas, devem ser monitoradas continuamente, de modo a identificar eventuais atipicidades que possam configurar indícios de LD/FTP. Em especial,

ao monitoramento de atipicidades envolvendo operações dos fundos de investimentos e carteiras administradas, com destaque para: **a)** recorrência ou concentração de ganhos ou perdas; **b)** mudança de padrão em termos de volume de negócios e de modalidade operacional; **c)** variação dos preços dos Ativos negociados pelos fundos em comparação aos preços praticados no mercado; **d)** reincidência de contraparte; **e)** transferências injustificadas; e, **f)** incompatibilidade patrimonial e sem fundamento econômico.

O monitoramento é realizado por meio de coleta diária das informações cadastrais, operacionais e movimentação financeira dos Clientes. As informações que apresentarem incompatibilidade com as regras definidas (cenários) gerarão alertas. Além destas ocorrências, algumas circunstâncias requerem especial atenção, como: **a)** operações envolvendo PEP; **b)** mudança atípica de endereço ou titularidade de conta bancária ou procurador; **c)** identificação em Listas de Sanções; **d)** possui residência, conta ou procurador em locais de fronteira; **e)** operações em que não seja possível identificar o Beneficiário Final; e, **f)** operações de câmbio em que o país de destino/origem seja Paraíso Fiscal.

A área de *Compliance* deve analisar os alertas gerados para confirmar a existência ou não de indícios de LD/FTP. Os casos em que houver a confirmação de indícios são apresentados ao Comitê de Risco e *Compliance* para a deliberação das ações de comunicação ao COAF, solicitação de bloqueio da conta do Cliente, encerramento do relacionamento, entre outras ações cabíveis.

8.1. MONITORAMENTO: CONTROLE DE PREÇO DOS ATIVOS E VALORES MOBILIÁRIOS NEGOCIADOS

Devem ser adotados procedimentos com vistas a controlar e monitorar a faixa de preços dos Ativos negociados para as carteiras sob sua gestão, de modo que eventuais operações efetuadas fora dos padrões praticados no mercado, de acordo com as características do negócio, sejam identificadas e, se for o caso, comunicadas aos órgãos competentes.

Neste sentido, a faixa de preço para títulos públicos, verifica se o preço negociado está abaixo ou acima de um percentual dos preços máximo e mínimo divulgado pela ANBIMA. A faixa de preço para ações, verifica se o preço negociado está dentro de um percentual sobre a amplitude de preço do dia anterior. Por fim, a faixa de preço para os demais Ativos líquidos, verifica se o preço está abaixo ou acima de um percentual do preço de mercado.

No caso de Ativos que não possuam mercado ativo, o valor deve ser suportado por laudo de avaliação elaborado pela Gestora, por terceiro independente e especializado e/ou por quem o regulamento do respectivo fundo indicar.

As empresas terceirizadas responsáveis pela emissão dos laudos de avaliação, devem ser submetidas ao processo de KYP.

8.2. COMUNICAÇÃO DE OPERAÇÕES AO COAF

Todas as situações e operações detectadas ou propostas de operações que possam constituir em indícios de LD/FTP devem ser comunicadas ao COAF, no prazo de 24 horas a contar da conclusão da análise que caracterizou a atipicidade da operação, respectiva proposta ou mesmo da situação atípica detectada.

As informações sobre as comunicações realizadas ao COAF, bem como toda a documentação e informação analisada no processo e apresentada no Comitê de Risco e *Compliance*, devem ser restritas e mantidas em sigilo, e não deve ser compartilhada ou disponibilizada a Clientes, terceiros e demais pessoas não autorizadas.

A **PROA** deve comunicar à CVM, se for o caso, a não ocorrência, no ano anterior, de situações, operações ou propostas de operações passíveis de serem comunicadas, com periodicidade anual, até o último dia útil do mês de abril.

8.3. CUMPRIMENTO DE SANÇÕES

A **PROA** deverá identificar Clientes Diretos que sejam alcançados pelas determinações de indisponibilidade de Ativos, nos termos da Lei n.º 13.810/2019 e do artigo 27 da Resolução CVM n.º 50/2021, bem como deverá cumprir imediatamente e sem aviso prévio aos eventuais Clientes Diretos eventualmente sancionados, as medidas estabelecidas nas resoluções sancionatórias do Conselho de Segurança das Nações Unidas ("CSNU") ou as designações de seus comitês de sanções que determinem a indisponibilidade de Ativos de titularidade, direta ou indiretamente de Clientes Diretos que eventualmente sofram as referidas sanções, sem prejuízo do dever de cumprir determinações judiciais de indisponibilidade, nos termos da regulamentação em vigor.

A **PROA** monitorará, direta e permanentemente, as determinações de indisponibilidade, bem como eventuais informações a serem observadas para o seu adequado atendimento, inclusive o eventual levantamento total ou parcial de tais determinações em relação ao Cliente Direto sancionado ou Ativos, visando ao cumprimento imediato do quanto determinado, acompanhando para tanto, sem prejuízo da adoção de outras providências de monitoramento, as informações divulgadas na página do CSNU na rede mundial de computadores.

A **PROA** deverá, ainda: **a)** informar, sem demora, ao Ministério da Justiça e Segurança Pública ("MJSP") e à CVM, a existência de pessoas e Ativos sujeitos às determinações de indisponibilidade a que deixaram de dar o imediato cumprimento, justificando as razões para tanto; **b)** comunicar imediatamente a indisponibilidade de Ativos e as tentativas de sua transferência relacionadas aos Clientes Diretos sancionados ao MJSP, à CVM e ao COAF; **c)** manter sob verificação a existência ou o surgimento, em seu âmbito, de Ativos alcançados pelas determinações de indisponibilidade, para efeito de pôr tais Ativos imediatamente, tão logo detectados, sob o regime de indisponibilidade; e **d)** proceder ao imediato levantamento da indisponibilidade de Ativos, na hipótese de exclusão dos Clientes Diretos eventualmente sancionados das listas do CSNU ou de seus comitês de sanções.

9. DESCUMPRIMENTO DA POLÍTICA

Todos os Colaboradores devem ter ciência de que o uso das informações e dos sistemas de informação da **PROA** podem ser monitorados, e que os registros, assim obtidos, poderão ser utilizados para detecção de violações desta Política e, conforme o caso, servir como evidência para aplicação das sanções cabíveis.

As sanções podem implicar desde advertência, suspensão ou demissão/distrato por justa causa, conforme a gravidade e a reincidência na violação, sem prejuízo das penalidades civis e criminais, caso haja descumprimento das disposições legais e regulamentares sob a ótica de LD/FTP.

A negligência e a falha voluntária são consideradas descumprimento desta Política e do Código de Ética e Conduta, sendo passíveis de aplicação de medidas disciplinares previstas nas diretrizes internas. Colaboradores encontram-se sujeitos às cominações previstas no Código Penal Brasileiro, na Lei n.º 9.613/1998, Lei n.º 13.260/2016 e demais normas aplicáveis no ordenamento jurídico brasileiro.

10. TREINAMENTO E CULTURA

Treinamentos para capacitação dos colaboradores são disponibilizados no início e durante todo o período do relacionamento com a **PROA**. O treinamento de PLD/FTP é composto por uma parte conceitual e por outra dedicada à avaliação da assimilação do conhecimento adquirido, e abrange todo o conteúdo da Política.

A área de *Compliance* avalia anualmente o treinamento, e pode definir novos treinamentos ou revisões dos já aplicados. Os treinamentos de PLD/FTP são mandatórios para todos os colaboradores e exige um percentual mínimo de acertos. Os colaboradores que não atingem este percentual, devem realizar o treinamento e a avaliação novamente.

A área de *Compliance* deve manter controle atualizado dos treinamentos, contendo as informações dos colaboradores que realizaram e os que não realizaram o treinamento, bem como o percentual de aprovação determinado (percentual mínimo de assimilação).

Podem ser definidos treinamentos específicos de reforço para as áreas consideradas sensíveis para LD/FTP como, *front office*, Cadastro, financeiro, *middle* e *backoffice*, entre outras.

11. RESPONSABILIDADES

a) Alta Administração

- i. Estar tempestivamente ciente dos riscos de conformidade referente às práticas de PLD/FTP;
- ii. Assegurar que o Diretor de Riscos e *Compliance*, tenha a independência e o pleno acesso às informações que este, julgar necessário, e o conhecimento necessário para o pleno cumprimento dos seus deveres;
- iii. Assegurar que os sistemas responsáveis pela coleta, atualização e guarda das informações relacionadas a identificar os Clientes, são adequados para o fim a que se destinam;
- iv. Assegurar que os sistemas de monitoramento das operações estão alinhados com os objetivos e estratégias do negócio, as situações atípicas identificadas e as tipologias empregadas na lavagem de Ativos, divulgadas pelo COAF.
- v. Aprovar Relatório Relativo à Avaliação Interna de Risco de LD/FTP;
- vi. Engajar e garantir que a empresa tenha Recursos adequados para implementar o programa de PLD/FTP; e
- vii. Promover a divulgação da Política para seus colaboradores, disseminar e incentivar a cultura de conformidade e gestão de riscos.

b) Comitê de Produtos, Investimentos e Crédito

- i. Avaliar e aprovar novos negócios pelos veículos de investimento dos quais a gestão seja realizada pela **PROA**, e deliberar sobre os riscos apresentados, inclusive os riscos de LD/FTP;
- ii. Verificar a viabilidade de novos produtos ou serviços em determinado segmento de mercado; e
- iii. Avaliar o dossiê de *Compliance* pertinente aos riscos de LD/FTP, emitido para fins de novos negócios pelos veículos de investimento geridos pela **PROA** ou novos produtos/serviços em outros segmentos de mercado.

c) Comitê de Risco e *Compliance*

- i. Analisar as avaliações realizadas pela área de *Compliance* e decidir sobre a comunicação ao COAF e demais órgãos competentes;
- ii. Aprovação da avaliação de riscos, que deve ser revista e atualizada regularmente;
- iii. Definir as ações disciplinares a Colaboradores que venham a descumprir os procedimentos de PLD/FTP;
- iv. Avaliar o programa de PLD/FTP, e deliberar sobre possíveis alterações das estratégias de negócio e dos níveis de aceitação riscos, assegurando a efetividade do programa;
- v. Deliberar sobre o reporte das situações atípicas e suspeitas para o COAF;
- vi. Deliberar sobre as medidas a serem adotadas com relação as ocorrências e atipicidades;
- vii. Revisar e avaliar a efetividade dos processos e controles implementados pela **PROA**, para cumprimento da Política; e
- viii. Aprovação das políticas, assegurando que estão consistentes com as avaliações de riscos aprovadas, e que as políticas e procedimentos de mitigação do risco de LD/FTP, refletem o apetite de risco da empresa e o nível de aceitação ao risco.

d) Diretor de Risco e *Compliance*

- i. Implementar, acompanhar e zelar pelo cumprimento da Política, das novas práticas, resoluções e alterações;
- ii. Garantir o cumprimento das determinações dos órgãos reguladores e autorreguladores em atendimento a PLD/FTP;
- iii. Assegurar a devida alocação dos recursos humanos e financeiros a área de *Compliance*, permitindo suporte necessário, inclusive, investimentos em novos sistemas, quando cabível;

- iv. Responsável pela elaboração do relatório relativo a Avaliação Interna de Risco de LD/FTP a ser encaminhado para aprovação da Alta Administração, Comitê de Risco e *Compliance*, nos termos previstos na regulação vigente;
- v. Aprovar o início e a manutenção do relacionamento com PEP, podendo submeter ao crivo do Comitê de Risco e *Compliance*, quando necessário;
- vi. Recomendar as áreas de negócios especial atenção quanto ao estabelecimento ou manutenção de contrato ou relação de negócio com Clientes classificados como Clientes de alto risco;
- vii. Difundir a cultura de PLD/FTP entre os colaboradores; e
- viii. Atuar como responsável de PLD/FTP no Comitê de Risco e *Compliance* e outros fóruns de discussão equivalentes.

e) Risco e *Compliance*

- i. Elaborar e submeter a Política de PLD para aprovação do Comitê de Políticas, Subcomitê de Risco e *Compliance*;
- ii. Garantir o cumprimento da política, regras, procedimentos e controles de PLD/FTP;
- iii. Avaliar regularmente o programa de PLD/FTP, de modo a garantir sua eficiência e efetividade, assim como incorporar novos fatores de risco, quando aplicável;
- iv. Monitorar e realizar *Compliance Test* dos processos e controles, de forma a assegurar a efetividade do programa de PLD/FTP;
- v. Emitir relatório com as vulnerabilidades e recomendar aprimoramentos no programa de PLD/FTP, bem como, apontar os incidentes, casos de descumprimento de colaboradores e levar os casos de indícios de LD/FTP para deliberação do Comitê de Risco e *Compliance*;
- vi. Analisar as informações coletadas pelas equipes responsáveis na empresa e monitorar as operações dos Clientes, avaliando os alertas e reportando os casos de atipicidade, ao Comitê de Risco e *Compliance*, à Alta Administração e a autoridades competentes, de acordo com a Política;
- vii. Desenvolver e aprimorar ferramentas e sistemas de monitoramento de operações ou situações atípicas;
- viii. Elaborar programas periódicos de treinamento, capacitação e conscientização dos Colaboradores, conforme aplicável;
- ix. Analisar novos produtos e serviços sob a ótica de PLD/FTP, corrupção e outros ilícitos previstos na legislação vigente;
- x. Definir em conjunto com as áreas responsáveis, eventuais planos de ação para implantação de medidas voltadas ao combate à LD/FTP;
- xi. Interagir com órgãos reguladores e autorreguladores em atendimento a PLD/FTP;
- xii. Assegurar que o início do relacionamento com Clientes, prestadores de serviço e parceiros comerciais ou a entrada de novos produtos e serviços, sejam submetidos à avaliação das alçadas competentes para aprovação e de áreas responsáveis sempre que identificadas informações consideradas relevantes sob a ótica de PLD/FTP, nos termos da Política;
- xiii. Acompanhar as notícias divulgadas na mídia relacionadas a LD/FTP verificando se há impactos na lista de Clientes e parceiros;
- xiv. Registrar e informar a Diretoria responsável, nos casos aplicáveis ao Comitê de Produtos, Investimentos ou Crédito, as situações identificadas e que possuam indícios de LD/FTP ou quaisquer outras práticas ilícitas, disponibilizando também, as informações necessárias para a tomada de decisão;
- xv. Reunir e arquivar toda a documentação referente às análises realizadas, bem como da decisão de arquivamento ou comunicação aos reguladores;
- xvi. Comunicar ao COAF as situações, propostas ou operações suspeitas, de acordo com os critérios estabelecidos pela regulamentação;
- xvii. Avaliar as notas atribuídas pelo COAF para aprimoramento das comunicações de indícios através do Siscoaf, caso ocorra.
- xviii. Requerer aprovação das alçadas competentes, para início de relacionamento ou investimentos com Clientes ou parceiros identificados como PEP;
- xix. Identificar os controles chaves para assegurar o cumprimento desta Política;
- xx. Realizar os testes dos controles chaves, para assegurar a eficiência do processo de PLD/FTP;
- xxi. Elaborar relatório relativo a Avaliação Interna de Risco de LD/FTP a ser encaminhado para aprovação da Alta Administração, Comitê de Risco e *Compliance*, nos termos previstos na regulação vigente;
- xxii. Organizar e coordenar os treinamentos;

- xxiii. Assegurar que os Colaboradores realizem os treinamentos referentes à PLD/FTP, conforme periodicidade definida na regulamentação vigente;
- xxiv. Garantir a aderência dos Colaboradores a Política, por meio de assinatura, no ingresso do relacionamento com a **PROA**;
- xxv. Disponibilizar as informações sobre treinamentos e a sua realização, quando solicitado, inclusive para fins de auditoria;
- xxvi. Aplicar as sanções aos Colaboradores, de acordo com a violação cometida, em relação as obrigações estabelecidas pela Política; e
- xxvii. Adotar procedimento de avaliação reputacional durante o processo de contratação dos Colaboradores;

f) Colaboradores

- i. Todos os Colaboradores devem estar cientes da política, regras, procedimentos e controles internos de PLD/FTP, assim como de suas respectivas responsabilidades, de acordo com suas atribuições;
- ii. Agir com diligência ao iniciar um relacionamento e no Cadastro de Clientes/contraparte da operação, evitando realizar negócios que apresentem indícios de estarem relacionados a crimes de LD/FTP ou que possam facilitá-los;
- iii. Efetivar a leitura e aderir aos termos desta Política, por meio de assinatura
- iv. Realizar os treinamentos de PLD/FTP;
- v. Comunicar toda situação ou suspeita de envolvimento com algum ato ilícito para a área de *Compliance*;
- vi. Responder, de forma tempestiva, as solicitações da área de *Compliance*; e
- vii. Atuar como multiplicador da cultura de prevenção e combate aos crimes de LD/FTP.

12. VALIDADE DESTE DOCUMENTO

Este documento, “Política de Prevenção à Lavagem de Dinheiro”, entra em vigor na data de publicação que consta na sua capa, e com prazo de validade indeterminado. Deverá, no entanto, ser revisto em períodos não maiores que 12 (doze) meses.

13. REFERÊNCIAS

Associação Brasileira das Entidades dos Mercados Financeiro e de Capitais (ANBIMA), Código de Administração e Gestão de Recursos de Terceiros, 2025;

Associação Brasileira das Entidades dos Mercados Financeiro e de Capitais (ANBIMA), Guia ANBIMA de PLD/FTP, edição IV, 2022;

Comissão de Valores Mobiliários (CVM), Diretrizes da CVM atualizadas acerca dos riscos de LD/FTP identificados no mercado de capitais de 2023;

BSM Supervisão de Mercados (BSM), Comunicado Externo 004/2020-DAR-BSM;

Comissão de Valores Mobiliários (CVM), Resoluções n.º 21/2021; 50/2021 e 175/2022;

Conselho de Controle de Atividades Financeiras (COAF), Resoluções n.º 36/2021 e 40/2021;

Decreto 10.270/2020;

Leis 9.613/1998, 12.683/2012 e 13.260/2016;

Grupo de Ação Financeira (GAFI), As Recomendações do GAFI, 2012, Padrões internacionais de combate à lavagem de dinheiro e ao financiamento do terrorismo e da proliferação; e

Grupo de Trabalho de Avaliação Nacional de Riscos de Lavagem de Dinheiro, Financiamento do Terrorismo e Financiamento da Proliferação de Armas de Destruição em Massa - Avaliação Nacional de Risco, 2021.

14. CONCEITOS E DEFINIÇÕES

Above the wall ou “Acima da muralha”: são as situações, pessoas ou áreas que podem ter acesso à informação livremente, diante da necessidade de acesso e controle da informação que transitam em diferentes áreas, que lidam com informações privadas. Como, Compliance, Jurídico e Riscos;

ABR ou Abordagem Baseada em Risco: metodologia que permite que as medidas de prevenção à lavagem de dinheiro, financiamento ao terrorismo sejam aplicadas de proporcional à natureza dos riscos, de modo a tornar mais eficientes os procedimentos implementados;

Alta Administração: órgão decisório máximo ou indivíduos integrantes da administração e/ou diretoria que seja responsável pela condução de assuntos estratégicos conforme previsto na política de PLD/FTP;

ANBIMA: Associação Brasileira das Entidades dos Mercados Financeiro e de Capitais;

ANR ou Avaliação Nacional de Risco: avaliação nacional de risco, conforme definida no Decreto n.º 10.270/2020 pelo Grupo de Trabalho de Avaliação Nacional de Riscos de Lavagem de Dinheiro, Financiamento do Terrorismo e Financiamento da Proliferação de Armas de Destruição em Massa;

Ativos: Ativos Financeiros e Ativos Imobiliários quando considerados em conjunto;

BCB: Banco Central do Brasil;

Beneficiário final: pessoa natural ou pessoas naturais que, em conjunto, possuam, controlem ou influenciem significativamente, direta ou indiretamente, um cliente em nome do qual uma transação esteja sendo conduzida ou dela se beneficie. Equivalem ao beneficiário final, para fins da presente política, os seus prepostos, procuradores ou representantes legais;

Cadastro: registro, em meio físico ou eletrônico, das informações e dos documentos de identificação de clientes com os quais a instituição mantém relacionamento comercial direto em função da prestação de serviços no mercado de valores mobiliários;

Cadeia de relacionamento: Entidades que representem os Clientes no fluxo entre a emissão da ordem até a sua execução, exemplo: gestores de recursos e administradores fiduciários;

Chinese Wall (muralha da China): é um termo presente no mundo dos negócios, que se refere a uma série de medidas, cuja função é impedir a circulação de informações que possam gerar conflito de interesses. É uma barreira que garante que, dentro de uma mesma empresa, as áreas que detém informações privilegiadas sobre o mercado (prestando assessoria corporativa em caso de fusões e aquisições, por exemplo) não tenham contato com quem de fato opera nele;

Cliente: pessoa natural ou jurídica, fundo de investimento, clube de investimento ou INR, que mantém relacionamento comercial direto com a **PROA**, em nome dos quais são efetuadas operações com Ativos e valores mobiliários;

COAF: Conselho de Controle de Atividades Financeiras, a Unidade de Inteligência Financeira brasileira;

CSNU: Conselho de Segurança das Nações Unidas;

CVM: Comissão de Valores Mobiliários;

Decreto n.º 10.270/2020: que institui o Grupo de Trabalho de Avaliação Nacional de Riscos de Lavagem de Dinheiro, Financiamento do Terrorismo e Financiamento da Proliferação de Armas de Destruição em Massa;

GAFI: Grupo de Ação Financeira contra a LD/FTP, a organização internacional multilateral intergovernamental cujo propósito é desenvolver e promover políticas de PLD/FTP e de combate à LD/FTP;

GTANR: Grupo de Trabalho de Avaliação Nacional de Riscos de Lavagem de Dinheiro, de Financiamento do Terrorismo e de Financiamento da Proliferação das Armas de Destruição em Massa;

Informação Privilegiada: são informações relevantes, que ainda não foram divulgadas aos investidores e ao público em geral, e que, por esse motivo, torna a pessoa que as possui, em posição indevidamente favorecida;

Influência Significativa: situação em que uma pessoa natural, seja o controlador ou não, exerça influência de fato nas decisões ou seja titular de mais de 25% (vinte e cinco por cento) do capital social ou mais, das pessoas jurídicas ou do patrimônio líquido dos fundos de investimento;

INR: investidor não residente, nos termos estabelecidos pela Resolução CVM nº 13/2020, e suas alterações posteriores;

KYC (Know your Customer) ou Conheça seu Cliente: é um conjunto de ações e estratégias dentro das políticas de Compliance, para evitar que uma empresa mantenha relações comerciais com clientes (pessoas naturais ou jurídicas) capazes de cometer crimes como fraude, corrupção, lavagem de dinheiro, e outras atividades ilícitas;

As mesmas ações e estratégias devem ser utilizadas para outros *Stakeholders*: **KYP (Know your Partner) ou Conheça seu Parceiro**, **KYE (Know your Employee) ou Conheça seu Funcionário**, **KYS (Know your Supplier) ou Conheça seu Fornecedor**;

LD/FTP: lavagem de dinheiro, financiamento do terrorismo e financiamento da proliferação de armas de destruição em massa;

Lei n.º 9.613/1998: dispõe sobre os crimes de "lavagem" ou ocultação de bens, direitos e valores; a prevenção da utilização do sistema financeiro para os ilícitos previstos nesta Lei e cria o COAF;

Lei n.º 12.683/2012: altera a Lei n.º 9.613/1998, para tornar mais eficiente a persecução penal dos crimes de lavagem de dinheiro;

Lei n.º 13.260/2016: dispõe sobre o crime de terrorismo, organizações terroristas e sobre o crime de financiamento do terrorismo;

Listas de Sanções: sanções e contramedidas financeiras, de programas internacionais emitidos pela Organização das Nações Unidas (ONU), União Europeia (UE) e da Agência de Controle de Ativos Estrangeiros dos EUA ("OFAC"), entre outros;

Offshores: centros financeiros de jurisdições cujas transações financeiras são realizadas por pessoas físicas e/ou jurídicas não residentes no local e, as instituições financeiras envolvidas não são manejadas por residentes. São semelhantes aos Paraísos Fiscais, pois podem também dotar de baixa tributação, regulamentações falhas, controles inexistentes e com legislações extremamente protecionistas ao que envolve sigilo bancário e identificação dos clientes, tornando difícil o reconhecimento dos clientes e valores transferidos;

Paraísos Fiscais: são locais que oferecem alíquotas tributárias baixas ou inexistentes, que atraem agentes e Recursos estrangeiros, tais como agentes expostos publicamente e remessas de altos valores para o exterior. Esses paraísos dificilmente possuem qualquer controle sobre a identidade dos clientes, contudo, possuem alta proteção quanto à identidade destes, com sigilo máximo;

Paraísos Jurídicos: são países que não colaboram com investigações, não respondem cartas rogatórias, por exemplo, que não possuem tratados envolvendo extradição ou até combate à lavagem de capitais e financiamento ao terrorismo, não participam de atos de cooperação, ao todo, são países foco de agentes que pretendem lavar dinheiro, pois, caso haja a descoberta, a investigação e a punição tornam-se difíceis;

PEP ou Pessoa Exposta Politicamente: é um indivíduo que tenha exercido cargos, funções ou empregos públicos nos últimos cinco anos. O exercício pode ter sido no Brasil ou no exterior, assim como se referir a políticos, servidores públicos, militares ou magistrados;

Pessoas Vinculadas: a) Diretores, administradores, empregados, operadores e demais prepostos da **PROA**; b) Agentes autônomos que prestem serviços a **PROA**; c) Demais profissionais que mantenham com a **PROA**, contrato de

prestação de serviços diretamente relacionados à atividade principal ou de suporte operacional; d) Pessoas naturais que sejam, direta ou indiretamente, controladoras ou participem do controle societário da **PROA Capital**; e) Sociedades controladas, direta ou indiretamente, pela **PROA** ou por pessoas a ela vinculadas; f) Cônjuge ou companheiro e filhos menores das pessoas mencionadas nos itens a) até d) dessa lista;

PLD/FTP: prevenção à lavagem de dinheiro, ao financiamento do terrorismo e ao financiamento da proliferação de armas de destruição em massa;

Recursos: qualquer ativo, tangível ou intangível, pertencentes a serviço ou sob responsabilidade da **PROA**, que possua valor para a empresa. Podem ser considerados recursos: pessoas, ambientes físicos, tecnologias, serviços contratados, sistemas e processos;

Stakeholder: parte interessada de uma empresa, um agente que exerce influência ou é influenciado direta ou indiretamente pelo resultado da empresa (ex.: sócios, acionistas, investidores, colaboradores, clientes, fornecedores, governos, concorrentes, mídia, entre outros).

ANEXO I

TERMO DE CIÊNCIA E COMPROMISSO À POLÍTICA DE PREVENÇÃO A LAVAGEM DE DINHEIRO

Por meio deste instrumento, DECLARO para os devidos fins:

- i. Ter recebido, na presente data, a Política de Segregação de Atividades (“Política”) atualizada, da **PROA GESTORA DE RECURSOS LTDA.** (“PROA”), inscrita no CNPJ sob o nº 62.200.538/0001-05;
- ii. Ter lido, sanado todas as minhas dúvidas e entendido integralmente as disposições constantes nesta Política;
- iii. Estar ciente de que esta Política, como um todo, passa a fazer parte dos meus deveres como Colaborador(a) da PROA, incorporando-se às demais regras internas adotadas; e
- iv. Estar ciente do meu compromisso de comunicar a Diretoria de Risco e Compliance da PROA, qualquer situação que chegue ao meu conhecimento que esteja em desacordo com as regras definidas nesta Política.

São Paulo, [=] de [=] de 2025.

Assinatura do Colaborador