Nexus

Gestão de Ativos

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

Sumário

1. Objetivo

A presente Política de Prevenção à Lavagem de Dinheiro, ao Financiamento do Terrorismo e ao Financiamento da Proliferação de Armas de Destruição em Massa ("Política de PLD/FTP") tem por objetivo estabelecer as diretrizes, regras, procedimentos e controles internos adotados pela Nexus Tech Gestão de Ativos Ltda. ("Nexus Tech" ou "Gestora") para prevenção, identificação, análise e reporte de eventos que apresentem características de lavagem de dinheiro, financiamento do terrorismo ou financiamento da proliferação de armas de destruição em massa ("LD/FTP"), em linha com a regulamentação da CVM e as regras de autorregulação da ANBIMA.

A prevenção da utilização dos ativos e sistemas da Nexus Tech para fins ilícitos é dever de todos os sócios, administradores, colaboradores, estagiários e prestadores de serviço da Gestora (em conjunto, "Colaboradores"), que devem reportar ao Diretor de PLD/FTP qualquer proposta ou atividade suspeita de LD/FTP, bem como violações ou possíveis violações das normas aqui dispostas.

1.1 O Crime de Lavagem de Dinheiro e suas Fases

O crime de lavagem de dinheiro, tipificado pela Lei nº 9.613/1998, consiste na ocultação ou dissimulação da natureza, origem, localização, disposição, movimentação ou propriedade de bens, direitos ou valores provenientes, direta ou indiretamente, de infração penal. Trata-se de processo dinâmico, cujas fases colocação, ocultação e integração podem ocorrer de forma sequencial ou simultânea: (i) colocação, quando recursos de origem ilícita são inseridos no sistema econômico por meio de depósitos, aquisição de ativos ou fracionamento de valores; (ii) ocultação, quando se busca dificultar o rastreamento dos recursos por meio de movimentações eletrônicas, transferências a terceiros ou estruturas societárias complexas; e (iii) integração, quando os recursos são incorporados à economia formal sob aparência de licitude, frequentemente por meio de investimentos. A compreensão dessas fases orienta a atuação de todos os Colaboradores na identificação de operações e situações atípicas no âmbito desta Política.

2. Base Legal

Esta Política está fundamentada nos seguintes normativos:

- Lei nº 9.613/1998, alterada pela Lei nº 12.683/2012;
- Resolução CVM nº 50, de 31 de agosto de 2021, conforme alterada ("RCVM 50");
- Resolução CVM nº 175/2022 e respectivos Anexos Normativos;

- Resolução CVM nº 21/2021;
- Lei nº 13.260/2016 (Lei Antiterrorismo);
- Lei nº 13.810/2019 (Cumprimento de Sanções do CSNU);
- Guia ANBIMA de PLD/FTP (versão vigente); e
- Ofícios e deliberações da CVM sobre a matéria.

3. Governança e Responsabilidades

3.1 Diretoria de PLD/FTP

O responsável pela implementação e manutenção desta Política é o Diretor de Risco, Compliance e PLD/FTP da Nexus Tech, nomeado perante a CVM nos termos da RCVM 50 ("Diretor de PLD"). O Diretor de PLD contará com o apoio da Área de Compliance para o exercício de suas atribuições, nos termos do Manual de Compliance e Controles Internos da Gestora.

O Diretor de PLD deve ter acesso irrestrito a todas as informações relativas ao gerenciamento do risco de LD/FTP, sendo vedada qualquer restrição, ainda que sob alegação de sigilo, proteção de dados pessoais (LGPD) ou segregação de atividades (chinese wall). Na hipótese de impedimento por prazo superior a 30 (trinta) dias, a Nexus Tech deverá indicar substituto, comunicando a CVM no prazo de 7 (sete) dias úteis.

Compete ao Diretor de PLD, com apoio da Área de Compliance:

- implementar, manter atualizada e fiscalizar o cumprimento desta Política;
- desenvolver e aprimorar ferramentas e sistemas de monitoramento de operações ou situações atípicas;
- promover a disseminação da cultura de PLD/FTP por meio de treinamentos periódicos;
- analisar informações coletadas, monitorar operações suspeitas e providenciar comunicações aos órgãos competentes;
- elaborar o Relatório Anual de PLD/FTP e encaminhá-lo às Diretorias da Nexus Tech; e
- coordenar ações disciplinares decorrentes de descumprimentos das normas de PLD/FTP.

3.2 Sócios e Diretores

Os sócios e diretores da Nexus Tech, integrantes de suas respectivas Diretorias (Diretoria de Gestão e Diretoria de Risco, Compliance e PLD/FTP), têm os seguintes deveres:

- aprovar esta Política e garantir sua revisão periódica;
- assegurar que o Diretor de PLD tenha independência, autonomia e conhecimento técnico suficiente, bem como pleno acesso a todas as informações necessárias;
- assegurar a alocação de recursos humanos, financeiros e tecnológicos suficientes; e
- comprometer-se integralmente com a cultura de PLD/FTP, garantindo que se estenda a todas as áreas da Gestora, com especial destaque àquelas com relacionamento direto com clientes e operações de maior potencial de LD/FTP.

3.3 Comitê de Compliance

Nos termos do Manual de Compliance e Controles Internos, o Comitê de Compliance é órgão de apoio à Diretoria de Compliance, competindo-lhe, no âmbito de PLD/FTP: (i) apreciar casos relevantes encaminhados pelo Diretor de PLD; (ii) deliberar sobre a aceitação ou recusa de clientes, prestadores de serviço ou contrapartes classificados como alto risco; e (iii) analisar o Relatório Anual de PLD/FTP.

3.4 Colaboradores

Todos os Colaboradores devem conhecer e cumprir integralmente esta Política, participar dos treinamentos obrigatórios e comunicar tempestivamente ao Diretor de PLD qualquer situação, operação ou proposta suspeita de envolvimento com LD/FTP. As comunicações poderão ser realizadas por e-mail institucional à Área de Compliance (compliance@nexustech.ia.br) ou pelo Canal de Denúncias previsto no Código de Ética e Conduta da Nexus Tech, assegurada a proteção ao denunciante de boa-fé. É vedado, em qualquer hipótese, dar ciência ao cliente ou a terceiros sobre comunicações efetuadas.

4. Programa de PLD/FTP

4.1 Abordagem Baseada em Risco (ABR)

Nos termos da RCVM 50, a Nexus Tech adota uma Abordagem Baseada em Risco (“ABR”) para identificar, analisar, compreender e mitigar os riscos de LD/FTP inerentes às suas atividades no mercado de valores mobiliários, garantindo que as medidas de prevenção e mitigação sejam proporcionais aos riscos identificados.

A Nexus Tech classifica em baixo, médio e alto risco de LD/FTP os seguintes elementos, conforme critérios detalhados na Avaliação Interna de

Risco: (i) serviços prestados; (ii) produtos oferecidos; (iii) clientes; (iv) prestadores de serviços relevantes; (v) colaboradores; e (vi) contrapartes, ativos e ambientes de negociação. A ABR é revisada periodicamente, considerando mudanças no ambiente regulatório, no perfil de risco da instituição e nos resultados dos indicadores de efetividade.

Serviços e Produtos:

A Nexus Tech atua exclusivamente na gestão de recursos de terceiros (fundos de investimento e carteiras administradas), atividade regulada e supervisionada pela CVM e ANBIMA. Os recursos são provenientes de contas mantidas em instituições financeiras que já possuem controles de PLD/FTP. A gestão é realizada de forma discricionária e os ativos são negociados majoritariamente em mercados organizados (bolsa de valores e mercado de balcão organizado da B3). Por esses motivos, os serviços e produtos são classificados, de maneira geral, como de Baixo Risco, sem prejuízo da reclassificação de produtos específicos conforme a ABR, notadamente aqueles que envolvam ativos fora de mercados organizados, operações com partes relacionadas ou estruturas com interferência de terceiros na decisão de investimento.

4.2 Conheça seu Cliente (KYC)

A Nexus Tech não realiza a distribuição de cotas dos fundos sob sua gestão, tampouco possui, na data desta Política, fundos exclusivos ou carteiras administradas com relacionamento comercial direto. A responsabilidade de KYC recai sobre os distribuidores contratados, que devem ser devidamente registrados e supervisionados pela CVM e, conforme o caso, pelo Banco Central do Brasil.

Caso a Nexus Tech venha a ter relacionamento comercial direto com clientes (carteiras administradas ou fundos exclusivos), deverá: (i) identificá-los e manter cadastro atualizado conforme o Anexo B da RCVM 50; (ii) classificá-los por nível de risco (alto, médio e baixo); (iii) adotar periodicidades de revisão cadastral diferenciadas 12 meses para alto risco, 24 meses para médio risco e 36 meses para baixo risco; e (iv) identificar o beneficiário final até a pessoa natural, ressalvadas as exceções previstas na RCVM 50.

Nessa hipótese, a diligência de KYC deverá compreender, no mínimo:

- identificação do beneficiário final até a pessoa natural, inclusive mediante procedimentos que assegurem identificar quem, isolada ou conjuntamente, possua, controle ou influencie significativamente o cliente;

- levantamento da origem dos recursos e do patrimônio do cliente (Source of Wealth), suas fontes de renda, residência fiscal e atividade profissional exercida;
- consulta à situação cadastral de CPF/CNPJ perante a Receita Federal e emissão das respectivas certidões negativas;
- pesquisas reputacionais em fontes públicas (mídia, tribunais, órgãos de proteção ao crédito e cadastros de distribuidores), voltadas à identificação de indícios de corrupção, fraude, desvio de recursos públicos, sonegação fiscal, lavagem de dinheiro ou financiamento do terrorismo;
- verificação de classificação como Pessoa Politicamente Exposta (PEP), mediante consulta a bases oficiais (CVM, COAF) ou fontes idôneas; e
- diligência contínua ao longo de todo o relacionamento, com atualização cadastral nas periodicidades definidas nesta Política.

Constatado qualquer apontamento impeditivo ou indício de associação a atividades ilícitas, o caso deve ser submetido ao Comitê de Compliance, a quem cabe deliberar pela aprovação, reprovação ou manutenção do relacionamento.

PEPs (Pessoas Expostas Politicamente), nos termos da regulamentação vigente, seus familiares até o segundo grau, cônjuges, companheiros, enteados, estreitos colaboradores e pessoas jurídicas de que participem serão automaticamente classificados como alto risco, exigindo análise e monitoramento reforçados.

4.3 Conheça seu Colaborador (KYE)

A Nexus Tech aplica regras, procedimentos e controles internos para a contratação e o acompanhamento do comportamento dos Colaboradores, conforme previsto no Código de Ética e Conduta. O processo de KYE é realizado antes da contratação e reavaliado de acordo com a classificação de risco, em periodicidade não superior a 36 meses. São avaliados, entre outros critérios: existência de condenações judiciais relevantes, irregularidade de CPF, classificação como PEP e existência de mídias negativas. Mudanças repentinas no padrão econômico do Colaborador, sem respaldo lícito, são passíveis de investigação e medidas disciplinares.

O Formulário de Conheça seu Colaborador (KYE) deve conter, no mínimo, as seguintes declarações do Colaborador:

- confirmação de reputação ilibada;
- certificação de que não está inabilitado ou suspenso para o exercício de cargo em instituições autorizadas a funcionar pela CVM, pelo Banco Central do Brasil, pela SUSEP ou pela PREVIC;

- declaração de que não foi condenado por crimes falimentares, contra o sistema financeiro nacional, a administração pública, a ordem econômica, as relações de consumo ou por lavagem de dinheiro;
- declaração quanto à sua eventual condição de Pessoa Politicamente Exposta (PEP);
- confirmação de inexistência de impedimentos legais para administrar os próprios bens;
- adesão à Política de Segurança da Informação e Cibernética da Gestora, com autorização para monitoramento de comunicações no âmbito corporativo;
- compromisso de participação nos treinamentos obrigatórios de PLD/FTP;
- compromisso de comunicar, de imediato, qualquer alteração relevante nas informações prestadas; e
- autorização para que a Nexus Tech realize verificações independentes com base em informações publicamente disponíveis.

4.4 Conheça seu Prestador de Serviço (KYP/KYS)

A Nexus Tech adota procedimentos para conhecer e monitorar seus prestadores de serviços relevantes (administradores fiduciários, custodiantes, distribuidores, escritórios de advocacia, consultorias, entre outros), visando prevenir a realização de negócios com pessoas ou entidades inidôneas ou suspeitas de envolvimento em atividades ilícitas.

Os prestadores são classificados por nível de risco, considerando: (i) existência e qualidade de políticas de PLD/FTP; (ii) existência de programa de treinamento; (iii) histórico perante a CVM e ANBIMA; (iv) aceitação de cláusula contratual de observância da RCVM 50; e (v) respostas ao Questionário de Due Diligence ANBIMA (QDD), quando aplicável. A periodicidade de reavaliação segue a classificação: anual (alto risco), a cada 3 anos (médio risco) e a cada 5 anos (baixo risco). Para prestadores de alto risco, a deliberação de início ou manutenção do relacionamento é submetida ao Comitê de Compliance.

4.5 Conheça sua Contraparte e Ativos Negociados

A Nexus Tech adota procedimentos de identificação e classificação de risco das contrapartes das operações realizadas para as carteiras sob sua gestão, notadamente as corretoras intermediárias, quando a Gestora não tiver conhecimento direto da contraparte compradora ou vendedora. A análise considera o histórico da contraparte perante a CVM e a ANBIMA, sua situação em listas restritivas, incluindo as do Conselho de Segurança das Nações Unidas (CSNU) e, quando disponível, do OFAC e sua exposição a jurisdições de maior

risco de LD/FTP, sendo revisada periodicamente ou sempre que identificadas mudanças relevantes no perfil de risco.

A Nexus Tech monitora, ainda, a compatibilidade dos preços praticados nas operações das carteiras sob gestão com os padrões de mercado, reportando ao Administrador Fiduciário e, se for o caso, aos órgãos competentes eventuais operações executadas fora da faixa de preços usualmente praticada. A adoção de novas tecnologias ou produtos pelas carteiras sob gestão é precedida de análise, pelo Diretor de PLD, do respectivo risco de LD/FTP, privilegiando-se soluções já validadas por agências ou instituições reconhecidas e compatíveis com a complexidade das atividades da Nexus Tech.

4.6 Monitoramento de Operações e Situações Atípicas

A Nexus Tech mantém registro e monitoramento das operações realizadas pelas carteiras sob gestão, de forma a observar atipicidades que possam configurar indícios ou suspeita de LD/FTP. Devem ser dispensadas especial atenção, entre outras, às seguintes situações:

- operações realizadas entre mesmas partes com seguidos ganhos ou perdas para algum dos envolvidos;
- oscilação significativa no volume ou frequência de negócios;
- operações fora dos padrões de preço praticados no mercado;
- operações sem fundamento econômico ou legal aparente;
- mudança repentina e injustificada de modalidade operacional;
- impossibilidade de identificar o beneficiário final;
- envolvimento de PEPs, jurisdições classificadas pelo GAFI como não cooperantes ou de alto risco, ou listas de sanções do CSNU;
- transferências privadas de recursos ou valores mobiliários sem motivação aparente; e
- operações envolvendo ativos de emissores com sede em jurisdições offshore sem acordo de cooperação com a CVM ou signatárias do memorando multilateral da OICV/IOSCO.
- operações que envolvam sociedades ou contrapartes recentemente constituídas, sem histórico ou propósito econômico aparente compatível com o volume negociado;
- pagamento de comissões, remunerações ou vantagens a intermediários em valores desproporcionais aos serviços efetivamente prestados; e
- operações liquidadas, ainda que parcialmente, em espécie ou por meios que dificultem a identificação da origem ou do destino dos recursos.

A conclusão do tratamento dos alertas oriundos do monitoramento deverá ocorrer em até 45 (quarenta e cinco) dias da data de geração do alerta, ressalvadas as situações de urgência.

4.7 Comunicação ao COAF

Caso a Área de Compliance, após análise final do Diretor de PLD, entenda pela existência de materialidade nos indícios identificados, será realizada comunicação formal ao COAF no prazo de 24 (vinte e quatro) horas a contar da conclusão da análise. As comunicações de boa-fé não acarretam responsabilidade civil ou administrativa à Nexus Tech nem a seus Colaboradores.

A comunicação ao COAF não pressupõe certeza ou prova quanto à ocorrência de crime, bastando a identificação consistente e fundamentada de indícios de atipicidade, cabendo às autoridades competentes o exame conclusivo da matéria.

Cada comunicação deverá ser trabalhada individualmente e fundamentada de maneira detalhada, contendo: (i) data de início do relacionamento; (ii) explicação fundamentada dos sinais de alerta; (iii) descrição e detalhamento das operações; (iv) informações obtidas por meio das diligências, inclusive se a pessoa é PEP; e (v) conclusão da análise com relato fundamentado.

A Nexus Tech deve abster-se de dar ciência de comunicações a qualquer pessoa, inclusive àquela a quem se refira a informação. Toda documentação deve ser arquivada pelo prazo mínimo de 5 (cinco) anos. Anualmente, até o último dia útil de abril, caso não tenha sido efetuada comunicação no ano civil anterior, a Nexus Tech enviará declaração negativa por meio dos mecanismos estabelecidos entre a CVM e o COAF.

4.8 Prevenção ao Financiamento do Terrorismo e Sanções CSNU

A Nexus Tech monitora continuamente as listas obrigatórias divulgadas pelo Conselho de Segurança das Nações Unidas (“CSNU”), pelo Grupo de Ação Financeira (“GAFI”) e pela CVM, acompanhando as informações divulgadas na página do CSNU na internet.

A Gestora deve cumprir, imediatamente e sem aviso prévio aos sancionados, as medidas estabelecidas nas resoluções sancionatórias do CSNU que determinem a indisponibilidade de ativos, nos termos da Lei nº 13.810/2019. A indisponibilidade refere-se à proibição de transferir, converter, trasladar, disponibilizar ativos ou deles dispor, direta ou indiretamente, incidindo sobre juros, frutos civis e rendimentos.

Caso identificada a situação, a Nexus Tech deverá: (i) comunicar imediatamente a indisponibilidade ao Ministério da Justiça e Segurança Pública (“MJSP”), à CVM e ao COAF; (ii) informar, sem demora, a existência de pessoas e ativos sujeitos às determinações de indisponibilidade a que não tenha dado

imediato cumprimento, justificando as razões; e (iii) proceder ao imediato levantamento da indisponibilidade na hipótese de exclusão dos sancionados das listas do CSNU.

4.9 Anticorrupção

Todos os Colaboradores estão proibidos de receber, oferecer, prometer, fazer, autorizar ou proporcionar direta ou indiretamente qualquer vantagem indevida, pagamento, presente ou transferência de valor a agente público ou privado, para influenciar ou recompensar qualquer ação oficial ou decisão em benefício da Nexus Tech, dos Colaboradores ou de terceiros a eles relacionados, nos termos do Código de Ética e Conduta da Gestora e da legislação anticorrupção vigente.

5. Treinamento

O Diretor de PLD, com apoio da Área de Compliance, deve promover treinamento de PLD/FTP para todos os Colaboradores, adotando linguagem clara e acessível, compatível com as funções desempenhadas e com a sensibilidade das informações a que tenham acesso.

O treinamento é obrigatório no ingresso de novos Colaboradores e a reciclagem é realizada no mínimo anualmente, podendo ocorrer extraordinariamente a critério da Área de Compliance. As evidências de participação devem ser arquivadas por no mínimo 5 (cinco) anos, conforme previsto no Manual de Compliance e Controles Internos.

A participação nos treinamentos deve observar assiduidade mínima de 70% (setenta por cento) da carga horária oferecida, sendo de responsabilidade da Área de Compliance a manutenção de lista de presença ou de relatório equivalente emitido pela plataforma de treinamento utilizada.

6. Avaliação de Efetividade e Relatório Anual

A Nexus Tech realiza avaliações periódicas da efetividade de seu programa de PLD/FTP. Os resultados são formalizados no Relatório Anual de PLD/FTP, de responsabilidade do Diretor de PLD, encaminhado às Diretorias da Nexus Tech até o último dia útil de abril de cada ano, devendo conter, conforme o art. 6º da RCVM 50:

- identificação e análise das situações de risco de LD/FTP, considerando ameaças, vulnerabilidades e consequências;
- quando aplicável, análise da atuação de prepostos e prestadores de serviços relevantes contratados;

- tabela do ano anterior com: número consolidado de operações atípicas detectadas (segregadas por hipótese), análises realizadas, comunicações ao COAF e data da declaração negativa;
- medidas adotadas para conhecimento contínuo de clientes, colaboradores e prestadores de serviço, e para identificação do beneficiário final;
- indicadores de efetividade, incluindo tempestividade da detecção, análise e comunicação;
- recomendações para mitigação de riscos e cronogramas de saneamento; e
- indicação da efetividade das recomendações do relatório anterior, com individualização dos resultados.

O Relatório Anual de PLD/FTP poderá ser elaborado em documento único ou compor o Relatório Anual de Compliance, ficando disponível para consulta da CVM e, quando aplicável, da ANBIMA.

7. Penalidades

Nos termos do Manual de Compliance e Controles Internos e do Código de Ética e Conduta, o descumprimento desta Política poderá sujeitar o infrator à aplicação de sanções disciplinares internas, observados a gravidade da infração, a reincidência e o histórico do Colaborador. As sanções poderão compreender, isolada ou cumulativamente: (i) advertência verbal; (ii) advertência escrita; (iii) suspensão; e (iv) desligamento, inclusive por justa causa, sem prejuízo de eventual responsabilização civil, administrativa e criminal prevista na legislação aplicável.

8. Disposições Gerais

Esta Política foi aprovada pelos sócios e diretores da Nexus Tech e deve ser revisada e atualizada no mínimo anualmente, ou tempestivamente em caso de mudanças na regulamentação. A responsabilidade de revisão é do Diretor de PLD, com suporte do Comitê de Compliance.

Todos os Colaboradores devem firmar Termo de Recebimento e Adesão a esta Política no momento da contratação e a cada nova versão aprovada, atestando conhecimento e compromisso de cumprimento de seus termos. A versão vigente desta Política é divulgada a todos os Colaboradores e, quando aplicável, disponibilizada no website institucional da Nexus Tech.

As informações e registros relativos às operações, diligências e comunicações previstas nesta Política devem ser mantidos pelo prazo mínimo de 5 (cinco) anos, em conformidade com a regulamentação vigente.

Esta Política é parte integrante do arcabouço normativo interno da Nexus Tech, devendo ser interpretada em conjunto com o Manual de Compliance e Controles Internos, o Código de Ética e Conduta, a Política de Investimentos Pessoais, o Manual de Gestão de Riscos e as demais políticas internas da Gestora.