

# MONEYTRUST SERVIÇOS DIGITAIS LTDA

CNPJ: 48.399.308/0001-88

---

## POLÍTICA DE PREVENÇÃO À LAVAGEM DE DINHEIRO E AO FINANCIAMENTO DO TERRORISMO

(POLÍTICA PLD/FT)

*Versão: 1.1*

*Data de aprovação: 15 de abril de 2026*

*Próxima revisão: 15 de abril de 2027*

---

**APROVADO POR:**

---

**Alexandr Naryshev**

Representante Legal e Diretor de Compliance

CPF: 061.315.407-05

*Rio de Janeiro/RJ, 15 de abril de 2026*

## 1. APRESENTAÇÃO E OBJETIVO

A Moneytrust Serviços Digitais EPP ("Moneytrust" ou "Empresa"), inscrita no CNPJ sob o nº 48.399.308/0001-88, é empresa constituída nos termos da legislação brasileira, com sede no Município do Rio de Janeiro/RJ, que atua como intermediadora de ativos virtuais (Virtual Asset Service Provider — VASP), realizando operações de troca entre pares (P2P) e operações de balcão (OTC) com criptoativos, bem como com moeda fiduciária (BRL e RUB).

A presente Política de Prevenção à Lavagem de Dinheiro e ao Financiamento do Terrorismo ("Política PLD/FT") tem por objetivo estabelecer os princípios, procedimentos e controles internos adotados pela Empresa para prevenir, detectar e comunicar a prática de crimes de lavagem de dinheiro, financiamento do terrorismo e de proliferação de armas de destruição em massa, em conformidade com a legislação e regulamentação aplicáveis.

## 2. FUNDAMENTOS LEGAIS E REGULATÓRIOS

Esta Política é elaborada em conformidade com os seguintes instrumentos normativos:

- a) **Lei nº 9.613, de 3 de março de 1998**, que 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; cria o Conselho de Controle de Atividades Financeiras (COAF), e dá outras providências;
- b) **Lei nº 13.260, de 16 de março de 2016**, Lei Antiterrorismo, que regulamenta o disposto no inciso XLIII do art. 5º da Constituição Federal, disciplinando o terrorismo, tratando de disposições investigatórias e processuais e reformulando o conceito de organização terrorista;
- c) **Lei nº 14.478, de 21 de dezembro de 2022**, Marco Legal dos Ativos Virtuais, que dispõe sobre diretrizes a serem observadas na prestação de serviços de ativos virtuais e na regulamentação das prestadoras de serviços de ativos virtuais;
- d) **Resolução BCB nº 277, de 31 de dezembro de 2022**, que regulamenta a Lei nº 14.286/2021 em relação ao mercado de câmbio e ao ingresso e saída de valores do País;
- e) **Instrução Normativa RFB nº 1.888, de 3 de maio de 2019**, que institui e disciplina a obrigatoriedade de prestação de informações relativas às operações

realizadas com criptoativos à Secretaria Especial da Receita Federal do Brasil (RFB);

- f) **Resoluções COAF: Resolução nº 31, de 7 de junho de 2019** (procedimentos para cumprimento de sanções e comunicações sobre terrorismo) e a **Resolução Coaf nº 36, de 10 de março de 2021** (forma de adoção de políticas, procedimentos e controles internos de PLD/FT);
- g) **Recomendações do GAFI/FATF: Padrões Internacionais de Combate à Lavagem de Dinheiro e ao Financiamento do Terrorismo e da Proliferação.**

### 3. ÂMBITO DE APLICAÇÃO

Esta Política aplica-se a:

- Todos os sócios, administradores e colaboradores da Moneytrust;
- Prestadores de serviços terceirizados que atuem em nome ou para a Empresa;
- Todos os clientes, parceiros e contrapartes que realizem operações com a Empresa;
- Todas as operações realizadas em plataformas digitais e físicas sob controle da Moneytrust, incluindo operações P2P, OTC e intermediações com ativos fiduciários.

### 4. AVALIAÇÃO DE RISCO

#### 4.1 Fatores de Risco Considerados

A Empresa adota uma abordagem baseada em risco (Risk-Based Approach — RBA), avaliando os seguintes fatores:

- **Perfil do cliente:** residência, nacionalidade, exposição política (PEP), histórico transacional;
- **Natureza da operação:** volume, frequência, tipo de ativo, jurisdição de origem/destino;
- **Canais utilizados:** plataformas digitais, operações remota ou presencial;

- **Países e territórios envolvidos:** jurisdições de alto risco conforme listas GAFI e OFAC;
- **Origem dos fundos** declarada *versus* **Padrão transacional** observado.

## 4.2 Classificação de Risco dos Clientes

Os clientes são classificados nas seguintes categorias:

Nível de Risco	Crterios Indicativos	Revisão Cadastral
Baixo Risco	Cliente com perfil compatível com atividade declarada, sem ocorrências em listas restritivas, transações dentro do padrão esperado.	A cada 24 meses
Mdio Risco	Algumas inconsistências de perfil, jurisdições com risco moderado, volumes acima da média, ou ausência de histórico verificável.	A cada 12 meses
Alto Risco	PEP ou familiar de PEP, jurisdição de alto risco (FATF), histórico de ocorrências, volumes atípicos elevados, inconsistência na origem dos fundos.	A cada 6 meses

## 5. CONHEÇA SEU CLIENTE (KYC)

### 5.1 Identificação e Verificação

Todo cliente deve ser identificado e ter sua identidade verificada antes do início das operações. Os documentos e informações mínimas exigidas são:

#### Para Pessoas Físicas:

- Documento de identidade com foto (RG, CNH, passaporte ou carteira profissional);
- CPF (para residentes no Brasil);
- Comprovante de residência atualizado (emitido nos últimos 90 dias);
- Selfie com documento (verificação biométrica via plataforma KYCAID);
- Declaração de origem dos fundos;
- Para clientes estrangeiros: passaporte, documentos equivalentes aceitos.

### **Para Pessoas Jurídicas:**

- Contrato Social ou Estatuto atualizado;
- CNPJ e comprovante de regularidade fiscal;
- Documentos de identificação dos sócios administradores com poderes de representação;
- Comprovante de endereço da sede;
- Declaração de beneficiários finais (conforme Resolução BCB nº 277/2022).

### **5.2 Verificação Biométrica e Documental**

A empresa utiliza a plataforma KYCAID.com para a verificação facial (liveness detection) e autenticidade dos documentos apresentados pelos clientes. O processo inclui:

- Captura e análise de documento de identidade (frente e verso);
- Verificação facial com prova de vida;
- Validação automática de dados e verificação de adulteração documental;
- Consulta automática a listas de sanções e PEPs internacionais.

### **5.3 Triagem contra Mídia Adversa (Adverse Media Screening)**

A Empresa realiza triagem de mídia adversa como parte integrante do processo de KYC e do monitoramento contínuo, abrangendo:

- Pesquisa de notícias negativas e publicações em fontes públicas sobre o cliente no momento do onboarding;
- Monitoramento contínuo de mídia adversa para clientes ativos, com frequência proporcional ao nível de risco:
  - Baixo risco: a cada 24 meses;
  - Médio risco: a cada 12 meses;
  - Alto risco: a cada 6 meses.
- Consulta a bases de dados especializadas integradas à plataforma KYC, incluindo listas de envolvidos em crimes financeiros, corrupção, tráfico e outras infrações precedentes;

- Registro dos resultados e das medidas adotadas em caso de resultado positivo;
- Resultado positivo na triagem de mídia adversa enseja reclassificação de risco e, conforme o caso, due diligence reforçada ou encerramento do relacionamento.

#### **5.4 Pessoas Politicamente Expostas (PEPs)**

São considerados PEPs os agentes públicos que desempenham ou tenham desempenhado funções públicas relevantes, conforme definição da Resolução CVM nº 50/2021 e demais normas aplicáveis. Para clientes identificados como PEPs:

- A classificação de risco é automaticamente elevada para Alto Risco;
- Aplica-se o procedimento de Due Diligence Reforçada (EDD), descrito no item 6;
- Exige-se aprovação do representante legal para onboarding e manutenção do relacionamento;
- Monitoramento transacional reforçado com revisão semestral.

### **6. DUE DILIGENCE REFORÇADA (EDD)**

#### **6.1 Casos de Aplicação**

A Due Diligence Reforçada (Enhanced Due Diligence — EDD) é aplicada obrigatoriamente nos seguintes casos:

- Clientes classificados como Alto Risco;
- Clientes identificados como PEPs ou familiares e associados próximos de PEPs;
- Clientes provenientes de jurisdições identificadas como de alto risco pelo GAFI/FATF ou sujeitas a sanções;
- Operações cujo volume ou frequência sejam incompatíveis com o perfil declarado do cliente;
- Clientes com ocorrências em listas de sanções ou em pesquisa de mídia adversa;

- Qualquer caso em que o operador de compliance identifique indicadores de risco elevado.

## **6.2 Procedimentos de EDD**

O procedimento de EDD compreende, adicionalmente à diligência padrão:

- Coleta aprofundada de informações sobre a origem dos fundos e do patrimônio do cliente;
- Verificação da natureza e propósito da operação com maior detalhe;
- Entrevista ou contato direto com o cliente para esclarecimentos;
- Verificação em bases de dados adicionais (PEP, sanções, mídia adversa);
- Aprovação expressa do representante legal para onboarding ou continuidade do relacionamento;
- Monitoramento transacional reforçado com relatório semestral;
- Registro detalhado de todas as etapas da EDD e das conclusões obtidas.

## **7. MONITORAMENTO DE TRANSAÇÕES**

### **7.1 Programa de Monitoramento**

A Moneytrust mantém programa contínuo de monitoramento de transações, destinado a identificar operações suspeitas e aquelas que possam configurar lavagem de dinheiro ou financiamento do terrorismo. O programa contempla:

- Análise individual das transações pelo operador responsável de compliance;
- Verificação de consistência entre o perfil do cliente e o padrão transacional observado;
- Aplicação de regras de alerta baseadas em tipologias do COAF e GAFI/FATF;
- Avaliação dos endereços de carteiras de criptoativos envolvidos nas operações;

- Identificação de operações fracionadas (smurfing) ou estruturadas para evitar limites de reporte.

## **7.2 Alertas e Red Flags**

Constituem indicadores de suspeita (red flags), dentre outros:

- Transações incompatíveis com o perfil econômico ou atividade declarada do cliente;
- Resistência do cliente em fornecer documentos ou informações exigidas;
- Uso de intermediários sem justificativa plausível;
- Transações em horários incomuns ou com velocidade atípica;
- Operações envolvendo jurisdições de alto risco sem justificativa econômica;
- Endereços de carteiras cripto com histórico de associação a atividades ilícitas (identificados via ferramentas KYT);
- Múltiplas transações de valores próximos ao limite de comunicação obrigatória ao COAF;
- Solicitação de anonimato ou recusa em identificar o beneficiário final.

## **7.3 Ferramentas de KYT (Know Your Transaction)**

A Empresa encontra-se em processo de implementação de ferramenta especializada de monitoramento de carteiras de criptoativos (KYT), visando:

- Análise de risco de endereços de carteiras e transações em blockchain;
- Identificação de endereços associados a atividades ilícitas, darknet, ransomware ou sanções;
- Cumprimento do Travel Rule do GAFI para transferências de criptoativos acima dos limites aplicáveis;
- Integração com o fluxo de onboarding e monitoramento contínuo.

A plataforma a ser adotada será indicada neste documento por aditamento, após contratação. As plataformas em avaliação incluem Regcheq ([regcheq.com.br](https://regcheq.com.br)) e

equivalentes especializadas. Enquanto a ferramenta automatizada não for implementada, o monitoramento é realizado manualmente pelo responsável de compliance, com registro de todas as análises efetuadas.

## **8. COMUNICAÇÃO DE OPERAÇÕES SUSPEITAS**

A Empresa tem a obrigação legal de comunicar ao COAF — Conselho de Controle de Atividades Financeiras — as transações suspeitas identificadas, nos termos do art. 11 da Lei nº 9.613/1998. O procedimento adotado é:

- Identificação pelo operador de compliance de operação que configure red flag ou padrão suspeito;
- Análise e documentação da suspeita, com registro dos elementos que a fundamentam;
- Deliberação do responsável de compliance sobre a necessidade de comunicação ao COAF;
- Envio da comunicação via sistema SISCOAF, observando o prazo de 24 horas contadas da confirmação da suspeita para casos urgentes;
- Manutenção de sigilo absoluto em relação ao cliente investigado sobre a comunicação realizada (proibição de tipping off, conforme art. 11, §1º, da Lei nº 9.613/1998);
- Registro da comunicação e arquivamento dos documentos que embasaram a decisão.

Além das comunicações de suspeitos, a Empresa observa as obrigações de comunicação automática ao COAF para operações com criptoativos de valor igual ou superior a R\$ 10.000,00 (dez mil reais), conforme normativos aplicáveis.

## **9. RETENÇÃO DE REGISTROS**

A Moneytrust mantém registros completos e organizados de todas as suas operações e procedimentos de compliance, observando os seguintes prazos e critérios:

<b>Tipo de Registro</b>	<b>Prazo Mínimo de Guarda</b>	<b>Fundamento Legal</b>
Documentos de identificação de clientes (KYC)	5 anos após encerramento do relacionamento	Art. 10, II, Lei 9.613/1998
Registros de transações realizadas	5 anos a contar da data da operação	Art. 10, II, Lei 9.613/1998
Comunicações ao COAF e documentos de suporte	5 anos após a comunicação	Art. 11, Lei 9.613/1998
Relatórios de análise de risco e EDD	5 anos	Resolução BCB 277/2022
Registros de treinamento de colaboradores	5 anos	Boas práticas GAFI/FATF
Resultados de triagem AML e mídia adversa	5 anos	Resolução BCB 277/2022

Os registros são mantidos em formato digital seguro, com backup periódico. Ao final do prazo legal de guarda, os documentos são descartados de forma segura, garantindo a proteção de dados pessoais conforme a Lei Geral de Proteção de Dados (LGPD — Lei nº 13.709/2018). O responsável pela gestão do arquivo de compliance é o representante legal da Empresa.

## **10. TREINAMENTO E CAPACITAÇÃO**

O responsável de compliance receberá treinamento anual sobre:

- Legislação e regulamentação aplicável (PLD/FT, Marco Legal de Ativos Virtuais);
- Tipologias de lavagem de dinheiro e financiamento do terrorismo relevantes para VASPs;
- Uso das plataformas de KYC e KYT adotadas pela Empresa;
- Procedimentos internos desta Política;
- Atualização sobre listas de sanções e alertas internacionais.

O registro dos treinamentos realizados será arquivado pelo prazo mínimo de 5 (cinco) anos.

## **11. RESPONSÁVEL DE COMPLIANCE**

O responsável pela implementação, monitoramento e revisão desta Política é o representante legal da Empresa, Alexandr Naryshev, que acumula as funções de Diretor de Compliance. Suas responsabilidades incluem:

- Supervisionar a aplicação desta Política e dos procedimentos internos de PLD/FT;
- Conduzir ou supervisionar os procedimentos de KYC e EDD;
- Analisar e decidir sobre comunicações ao COAF;
- Manter os registros de compliance atualizados;
- Promover ou participar de treinamentos periódicos;
- Revisar e atualizar esta Política anualmente ou quando houver alterações normativas relevantes;
- Interagir com autoridades regulatórias e plataformas parceiras (como a Binance) sobre questões de compliance.

## **12. REVISÃO E ATUALIZAÇÃO DA POLÍTICA**

Esta Política será revisada e atualizada:

- Anualmente, de forma ordinária, com data-limite na semana do aniversário de aprovação;
- Extraordinariamente, sempre que houver alteração legislativa, regulatória ou operacional relevante;
- Após qualquer evento de não conformidade identificado internamente ou por entidade externa.

A presente versão está devidamente revisada, atualizada, aprovada e assinada pelo representante legal, sendo submetida às plataformas parceiras que a exijam.

## **13. SANÇÕES E CONSEQUÊNCIAS**

O descumprimento desta Política por colaboradores, prestadores ou representantes da Empresa sujeitará os infratores às medidas cabíveis, incluindo advertência, rescisão contratual e comunicação às autoridades competentes.

A Moneytrust está ciente de que o descumprimento das obrigações de PLD/FT pode ensejar sanções administrativas, civis e penais previstas na Lei nº 9.613/1998, na Lei nº 13.260/2016 e nas normas aplicáveis às PSAVs.

---

#### **14. APROVAÇÃO**

Esta Política foi elaborada, revisada e aprovada por:

---

**Alexandr Naryshev**

Representante Legal e Diretor de Compliance

Moneytrust Serviços Digitais Ltda — CNPJ: 48.399.308/0001-88

*Rio de Janeiro, 14 de abril de 2026*