# POLÍTICA INSTITUCIONAL DE PREVENÇÃO À LAVAGEM DE DINHEIRO, AO FINANCIAMENTO AO TERRORISMO E À PROLIFERAÇÃO DE ARMAS DE DESTRUIÇÃO EM MASSA (PLD/FTP)

---

Empresa: TKB ASSET
Razão Social: TOKENIZACAO MANAGEMENT GESTAO DE NEGOCIOS, PATRIMONIO E INVESTIMENTOS LTDA.
CNPJ: 45.933.866/0001-93

Documento: POL-PLDFTP-001
Versão: 2.0
Data de Aprovação: Outubro/2025
Classificação: Confidencial – Uso Interno

Aprovado por: Diretoria Executiva da TKB ASSET
Responsável: Compliance Officer

---

## 1. OBJETIVO E ABRANGÊNCIA

### 1.1. OBJETIVO

Esta Política Institucional formaliza o compromisso inabalável e irrevogável da alta administração da TKB ASSET ("Empresa" ou "TKB ASSET") com a integridade, a transparência e a conformidade legal no sistema financeiro nacional e internacional.

Seu propósito é estabelecer as diretrizes estratégicas, os procedimentos operacionais e os controles internos essenciais e obrigatórios para evitar, detectar, prevenir e mitigar o risco de que os serviços prestados pela Empresa sejam utilizados, direta ou indiretamente, consciente ou inconscientemente, para:

a) Lavagem de dinheiro ou ocultação de bens, direitos ou valores (Lei nº 9.613/98 e

alterações);
b) Financiamento ao terrorismo ou a organizações terroristas (Lei nº 13.260/2016);
c) Financiamento da proliferação de armas de destruição em massa;
d) Evasão de divisas ou burla a controles de capitais;
e) Crimes contra o sistema financeiro nacional;
f) Sonegação fiscal ou crimes tributários;
g) Corrupção ativa ou passiva;
h) Quaisquer outras atividades ilícitas que violem a legislação brasileira ou internacional.

1.2. ABRANGÊNCIA

A presente Política é aplicável, sem exceções, a:

a) Todos os sócios, administradores, diretores e membros da alta administração da TKB ASSET;
b) Todos os colaboradores, prestadores de serviços, consultores e terceiros contratados que atuem em nome ou por conta da TKB ASSET;
c) Todos os parceiros comerciais, fornecedores de liquidez, exchanges, instituições financeiras e demais entidades com as quais a TKB ASSET mantenha relacionamento de negócios;
d) Todas as operações, transações e interações com clientes realizadas pela TKB ASSET, independentemente de valor, frequência ou jurisdição envolvida.

1.3. VIGÊNCIA E ATUALIZAÇÃO

Esta Política entra em vigor na data de sua aprovação pela Diretoria e permanecerá válida por prazo indeterminado, sendo revisada e atualizada, no mínimo, anualmente, ou sempre que houver:

a) Alterações na legislação brasileira ou internacional aplicável;
b) Mudanças no modelo de negócios ou na estrutura operacional da TKB ASSET;
c) Identificação de novas tipologias de lavagem de dinheiro ou financiamento ao terrorismo;
d) Recomendações de autoridades regulatórias (COAF, Banco Central, CVM, Receita Federal);
e) Resultados de auditorias internas ou externas que indiquem necessidade de aprimoramento.

---

2. MARCO LEGAL E REGULATÓRIO

A TKB ASSET fundamenta seu programa de PLD/FTP nas seguintes normas legais e regulatórias:

LEGISLAÇÃO NACIONAL:

• Lei nº 9.613/98 (Lei de Lavagem de Dinheiro) e suas alterações posteriores;
• Lei nº 13.260/2016 (Lei Antiterrorismo);
• Lei nº 14.478/2022 (Marco Legal dos Ativos Virtuais);
• Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – LGPD);
• Código Penal Brasileiro (crimes contra o sistema financeiro);
• Resoluções e Circulares do Conselho de Controle de Atividades Financeiras (COAF);
• Instruções Normativas da Receita Federal do Brasil (especialmente IN 1.888/2019);
• Resoluções do Conselho Monetário Nacional (CMN) e do Banco Central do Brasil (BCB).

PADRÕES INTERNACIONAIS:
• Recomendações do FATF/GAFI (Financial Action Task Force / Grupo de Ação Financeira);
• Convenção de Viena (1988) – Tráfico de Drogas;
• Convenção de Palermo (2000) – Crime Organizado Transnacional;
• Resoluções do Conselho de Segurança das Nações Unidas (CSNU) sobre sanções e terrorismo;
• Diretrizes da OFAC (Office of Foreign Assets Control) – Sanções dos EUA;
• Regulamentações da União Europeia sobre sanções e PLD/FT.

---

## 3. GOVERNANÇA E ESTRUTURA DE COMPLIANCE

### 3.1. ALTA ADMINISTRAÇÃO – RESPONSABILIDADE FINAL

A Diretoria Executiva da TKB ASSET é a responsável última e final pela efetividade do programa de PLD/FTP, cabendo-lhe:

a) Aprovar esta Política e todas as suas atualizações;
b) Garantir recursos humanos, tecnológicos e financeiros adequados para a implementação do programa;
c) Fomentar uma cultura organizacional de integridade, ética e conformidade;
d) Revisar periodicamente relatórios de compliance e tomar decisões estratégicas com base em análises de risco;
e) Responder perante autoridades regulatórias pelo cumprimento das obrigações de PLD/FTP.

### 3.2. COMPLIANCE OFFICER – AUTORIDADE OPERACIONAL

Um Compliance Officer é formalmente designado pela Diretoria, reportando-se diretamente à alta administração, e investido de autonomia técnica, autoridade decisória e recursos necessários para o pleno exercício de suas funções, que incluem:

a) Supervisionar a implementação, o funcionamento e o cumprimento integral desta Política;

b) Desenvolver, propor e implementar procedimentos, controles e atualizações no programa de PLD/FTP;
c) Atuar como ponto focal de contato para o Conselho de Controle de Atividades Financeiras (COAF), Receita Federal, Banco Central, Ministério Público, Polícia Federal e demais autoridades regulatórias e investigativas;
d) Liderar a análise técnica de casos de operações suspeitas, atípicas ou inconsistentes com o perfil de clientes;
e) Tomar a decisão final, de forma fundamentada e documentada, sobre a comunicação ou não de operações suspeitas ao COAF;
f) Coordenar e ministrar programas obrigatórios de treinamento e capacitação em PLD/FTP para toda a equipe da TKB ASSET;
g) Elaborar relatórios gerenciais periódicos (mensais, trimestrais, anuais) sobre o desempenho do programa de PLD/FTP, indicadores de risco, casos reportados e lições aprendidas;
h) Interagir com fornecedores de tecnologia, parceiros comerciais e consultores externos especializados em compliance e PLD/FT;
i) Manter-se atualizado sobre novas tipologias de lavagem de dinheiro, tendências de fraude no mercado de criptoativos, e alterações regulatórias nacionais e internacionais.

### 3.3. LINHA DE REPORTE E INDEPENDÊNCIA

O Compliance Officer possui independência funcional e não pode sofrer retaliação, pressão ou interferência indevida no exercício de suas atribuições. Suas decisões técnicas de compliance, quando fundamentadas em análise de risco e em conformidade com esta Política e com a legislação aplicável, são soberanas e vinculantes para toda a organização.

Em situações excepcionais de divergência entre o Compliance Officer e a Diretoria, a decisão final caberá à Diretoria, mas deverá ser formalmente documentada, com justificativa fundamentada, e arquivada para eventual auditoria ou fiscalização.

---

## 4. PILARES DO PROGRAMA DE PLD/FTP

O programa de PLD/FTP da TKB ASSET é estruturado em uma Abordagem Baseada em Risco (ABR – Risk-Based Approach), em conformidade com as melhores práticas internacionais recomendadas pelo FATF/GAFI, e se sustenta nos seguintes pilares fundamentais:

---

### 4.1. PILAR I – DUE DILIGENCE DE CLIENTES (CUSTOMER DUE DILIGENCE – CDD)

4.1.1. Identificação e Qualificação Obrigatória

Nenhum relacionamento comercial será estabelecido com qualquer cliente (pessoa física ou jurídica) sem a completa identificação, qualificação e validação de sua identidade e de seu perfil de risco.

Todo cliente, antes de realizar sua primeira operação, deverá preencher e fornecer, de forma completa e verídica, o Dossiê de Qualificação Cadastral e Avaliação de Perfil de Risco (KYC/CDD), desenvolvido pela TKB ASSET, que inclui:

a) Dados cadastrais completos (nome, CPF/CNPJ, endereço, atividade econômica);
b) Documentos de identificação oficial (RG, CNH, Contrato Social, Cartão CNPJ);
c) Comprovante de residência atualizado;
d) Estrutura societária e identificação de Beneficiários Finais (UBOs – Ultimate Beneficial Owners);
e) Declaração de origem dos recursos e finalidade das operações;
f) Informações sobre perfil transacional esperado (volume, frequência, jurisdições envolvidas);
g) Declaração de Pessoa Politicamente Exposta (PEP);
h) Autorização para validação de dados e consulta a bases públicas e privadas.

4.1.2. Validação de Documentos e Informações

A TKB ASSET realizará procedimentos de validação para confirmar a autenticidade e a veracidade das informações e documentos fornecidos, incluindo:

a) Consulta ao CNPJ/CPF na base da Receita Federal do Brasil;
b) Verificação de regularidade fiscal e cadastral;
c) Consulta a bureaus de crédito e bases de dados públicas;
d) Validação de endereços e contatos fornecidos;
e) Pesquisa em fontes abertas de informação (OSINT – Open Source Intelligence);
f) Contato com referências comerciais fornecidas pelo cliente (quando aplicável);
g) Análise de compatibilidade entre o perfil declarado e o comportamento transacional esperado.

4.1.3. Classificação de Risco

No momento do onboarding (integração do novo cliente), cada cliente será submetido a uma Matriz de Classificação de Risco, desenvolvida pela TKB ASSET com base em critérios objetivos e mensuráveis, que considera, dentre outros fatores:

a) Tipo de cliente: Pessoa Física (PF) ou Pessoa Jurídica (PJ);
b) Ramo de atividade econômica e compatibilidade com operações em criptoativos;
c) Volume transacional projetado (mensal e anual);

d) Frequência esperada de operações;
e) Jurisdição de residência, domicílio ou operação do cliente;
f) Jurisdições de destino dos recursos convertidos em USDT;
g) Exposição a atividades de alto risco (câmbio, remessas, comércio internacional, etc.);
h) Relacionamento com Pessoas Politicamente Expostas (PEPs);
i) Histórico de relacionamento com a TKB ASSET (cliente novo vs. cliente recorrente);
j) Resultados de consultas a listas restritivas e bases de sanções.

Com base na Matriz de Risco, o cliente será classificado em uma das seguintes categorias:

• RISCO BAIXO: Clientes com perfil conhecido, atividade compatível, volumes moderados, jurisdições de baixo risco, sem exposição a PEPs ou listas restritivas.

• RISCO MÉDIO: Clientes com algum fator de risco moderado (volumes elevados, atividades com maior exposição a riscos de PLD, jurisdições com controles regulatórios menos desenvolvidos).

• RISCO ALTO: Clientes com múltiplos fatores de risco elevado (PEPs, estruturas societárias complexas, jurisdições de alto risco, atividades sensíveis, histórico de inconsistências).

4.1.4. Due Diligence Intensificada (Enhanced Due Diligence – EDD)

Clientes classificados como de RISCO ALTO, bem como clientes que, durante o relacionamento, apresentem comportamento atípico ou suspeito, serão obrigatoriamente submetidos a um processo de Due Diligence Intensificada (EDD), que inclui:

a) Análise aprofundada e documentada da origem do patrimônio e dos recursos a serem transacionados;
b) Solicitação de documentos adicionais (extratos bancários, declarações de Imposto de Renda, contratos comerciais, notas fiscais);
c) Entrevistas ou reuniões com o cliente para esclarecimentos;
d) Validação de informações junto a terceiros (bancos, fornecedores, clientes do cliente);
e) Consulta a bases de dados especializadas em inteligência financeira;
f) Análise on-chain de endereços de carteiras digitais (wallets) para identificação de histórico transacional e associações com atividades ilícitas;
g) Avaliação de reputação do cliente e de seus sócios em fontes abertas de informação (notícias, processos judiciais, redes sociais corporativas);
h) Aprovação final pela Diretoria, em conjunto com o Compliance Officer, para o estabelecimento ou continuidade do relacionamento.

4.1.5. Ongoing Due Diligence (Monitoramento Contínuo)

A TKB ASSET adota uma abordagem de monitoramento contínuo de seus clientes,

reconhecendo que o risco não é estático, mas dinâmico e evolutivo. Assim:

a) Clientes de RISCO BAIXO serão revisados anualmente;
b) Clientes de RISCO MÉDIO serão revisados semestralmente;
c) Clientes de RISCO ALTO serão revisados trimestralmente, ou sempre que houver eventos relevantes (mudança de sócios, alteração de atividade, operações atípicas).

A atualização cadastral poderá incluir solicitação de novos documentos, confirmação de informações anteriores, e reavaliação da classificação de risco.

---

4.2. PILAR II – MONITORAMENTO TRANSACIONAL (KNOW YOUR TRANSACTION – KYT)

4.2.1. Análise Off-Chain (Sistema Financeiro Tradicional)

A TKB ASSET monitora todas as transferências bancárias (TED, PIX) recebidas de clientes, verificando:

a) Compatibilidade entre o valor transferido e a operação solicitada;
b) Identidade do ordenante da transferência (deve ser o próprio cliente, não terceiros);
c) Histórico de relacionamento bancário do cliente;
d) Padrões de transferências (horários, valores, frequência);
e) Instituições financeiras de origem (bancos tradicionais vs. fintechs vs. instituições de menor porte).

Transferências com indícios de triangulação, fracionamento (smurfing), ou oriundas de terceiros não previamente autorizados serão automaticamente bloqueadas e devolvidas, com comunicação ao cliente.

4.2.2. Análise On-Chain (Redes Blockchain)

A TKB ASSET emprega ferramentas e procedimentos para o monitoramento e análise de transações registradas em redes blockchain (análise on-chain), visando identificar:

a) Histórico transacional de endereços de carteiras (wallets) de destino fornecidos pelos clientes;
b) Associações de carteiras com atividades ilícitas conhecidas (darknet, ransomware, exchanges hackeadas, mixers/tumblers);
c) Pontuação de risco (risk score) de endereços de carteira, utilizando bases de dados especializadas;
d) Fluxos de fundos suspeitos ou incompatíveis com o perfil declarado pelo cliente;

e) Transferências para jurisdições de alto risco ou para entidades sob sanções internacionais.

Carteiras com alta pontuação de risco ou associações com atividades ilícitas poderão resultar na recusa de operações, bloqueio do cliente, e comunicação ao COAF.

4.2.3. Sinais de Alerta (Red Flags)

A TKB ASSET monitora ativamente um conjunto abrangente de tipologias e sinais de alerta (red flags), que incluem, mas não se limitam a:

COMPORTAMENTO TRANSACIONAL:
• Operações com volume ou frequência incompatíveis ou desproporcionais em relação ao perfil econômico-financeiro declarado pelo cliente;
• Operações realizadas de forma aparentemente fracionada (smurfing), em valores logo abaixo de limites de reporte obrigatório, visando iludir controles;
• Alterações súbitas, significativas e não justificadas no padrão transacional do cliente (aumento repentino de volume ou frequência);
• Operações que não fazem sentido econômico ou comercial aparente, considerando a atividade declarada do cliente;
• Cancelamentos frequentes de operações após a trava de cotação, sem justificativa razoável;
• Tentativas de realizar operações fora do horário comercial ou em condições atípicas.

COMPORTAMENTO DO CLIENTE:
• Recusa, relutância, demora injustificada ou resistência em fornecer informações ou documentação solicitada pela TKB ASSET;
• Prestação de informações inconsistentes, contraditórias ou inverídicas;
• Solicitação de sigilo excessivo ou inadequado em relação às operações;
• Demonstração de desconhecimento incomum sobre a própria atividade empresarial ou sobre a origem dos recursos;
• Falta de interesse em questões comerciais normais (taxas, prazos, condições), focando apenas na celeridade da operação;
• Mudanças frequentes e não justificadas de endereços, telefones, representantes legais ou estrutura societária.

PERFIL DE RISCO:
• Envolvimento do cliente, de seus sócios, administradores ou beneficiários finais em investigações, processos judiciais, inquéritos policiais ou procedimentos administrativos relacionados a crimes financeiros, lavagem de dinheiro, corrupção, fraude, sonegação fiscal, ou crimes contra a ordem tributária;
• Inclusão do cliente ou de pessoas relacionadas em listas restritivas, listas de sanções, ou listas de Pessoas Politicamente Expostas (PEPs) com avaliação de risco desfavorável;
• Notícias negativas (adverse media) envolvendo o cliente ou seus representantes em fontes abertas de informação;

• Relacionamento do cliente com jurisdições consideradas de alto risco para lavagem de dinheiro ou financiamento ao terrorismo pelo FATF/GAFI.

TRANSAÇÕES EM BLOCKCHAIN:
• Transferências de USDT para endereços de carteiras (wallets) associados a mixers, tumblers, ou serviços de anonimização;
• Transferências para carteiras vinculadas a exchanges não regulamentadas, mercados darknet, ou plataformas de alto risco;
• Transferências para endereços constantes de listas de sanções (OFAC SDN List) ou de análises de risco on-chain com alta pontuação de ilicitude;
• Uso de carteiras novas (sem histórico transacional) para operações de grande volume;
• Múltiplas transferências para diferentes carteiras em sequência rápida (chain hopping), sugerindo tentativa de ofuscação de rastros.

4.2.4. Procedimento de Análise de Operações Suspeitas

Sempre que um sinal de alerta for identificado, seja por sistemas automatizados, seja por análise manual, o seguinte procedimento será adotado:

a) A operação suspeita será escalada imediatamente ao Compliance Officer;
b) O Compliance Officer conduzirá uma análise detalhada, documentada e fundamentada, considerando todos os dados disponíveis sobre o cliente e sobre a operação específica;
c) Poderão ser solicitados esclarecimentos adicionais ao cliente, mediante contato formal;
d) A operação poderá ser bloqueada cautelarmente enquanto a análise estiver em andamento;
e) Se, após análise, o Compliance Officer concluir que há fundados indícios de lavagem de dinheiro ou financiamento ao terrorismo, a operação será comunicada ao COAF, conforme procedimento descrito no Pilar III.

---

4.3. PILAR III – COMUNICAÇÃO AO COAF (CONSELHO DE CONTROLE DE ATIVIDADES FINANCEIRAS)

4.3.1. Obrigatoriedade Legal

Nos termos do Art. 11 da Lei nº 9.613/98, a TKB ASSET, na qualidade de prestadora de serviços relacionados a operações com ativos virtuais, está obrigada a comunicar ao COAF, de forma sigilosa e no prazo legal, todas as operações ou propostas de operação que, após análise técnica, apresentem fundados indícios de constituírem crime de lavagem de dinheiro, de ocultação de bens, direitos e valores, ou de financiamento ao terrorismo.

4.3.2. Critérios para Comunicação

A decisão de comunicar uma operação ao COAF é de natureza técnica, fundamentada em análise de risco, e compete exclusivamente ao Compliance Officer, observados os seguintes critérios:

a) Existência de um ou mais sinais de alerta (red flags) relevantes;
b) Incompatibilidade entre o perfil do cliente e a operação realizada;
c) Impossibilidade de o cliente fornecer explicação razoável, lógica e comprovável para a operação ou para a origem dos recursos;
d) Suspeita fundamentada de que a operação está sendo utilizada para lavagem de dinheiro, ocultação de patrimônio, ou financiamento ao terrorismo.

4.3.3. Sigilo Absoluto (Vedação de Tipping Off)

Todas as comunicações ao COAF são realizadas de forma absolutamente sigilosa. É terminantemente proibido informar o cliente, ou qualquer terceiro, sobre a existência de uma análise em andamento ou sobre a comunicação efetuada ao COAF.

A violação deste sigilo constitui crime de "tipping off", previsto no Art. 11, § 2º, da Lei nº 9.613/98, punível com pena de reclusão de 2 a 6 anos, além de multa.

4.3.4. Prazo de Comunicação

As comunicações ao COAF serão realizadas no prazo de até 24 (vinte e quatro) horas após a conclusão da análise pelo Compliance Officer, utilizando o sistema eletrônico SISCOAF (Sistema de Controle de Atividades Financeiras).

4.3.5. Documentação e Arquivamento

Todas as comunicações ao COAF, bem como as análises que as fundamentaram, serão documentadas de forma detalhada e arquivadas em local seguro, com acesso restrito, pelo prazo mínimo de 10 (dez) anos.

---

4.4. PILAR IV – FERRAMENTAS, TECNOLOGIAS E RECURSOS DE COMPLIANCE

A TKB ASSET reconhece que um programa de PLD/FTP eficaz exige não apenas políticas e procedimentos bem estruturados, mas também o emprego de tecnologias, ferramentas especializadas e recursos técnicos adequados para suportar as atividades de compliance.

4.4.1. Ferramentas de Análise de Blockchain (On-Chain Analysis)

A TKB ASSET utiliza, ou reserva-se o direito de utilizar, ferramentas especializadas de análise on-chain para monitoramento, rastreamento e avaliação de risco de endereços de carteiras digitais (wallets) e transações em redes blockchain, incluindo, mas não se limitando a:

• Chainalysis (plataforma líder mundial em análise de blockchain e compliance para criptoativos);
• Elliptic (ferramenta de screening de carteiras e identificação de atividades ilícitas);
• CipherTrace (análise de risco on-chain e inteligência sobre ameaças em cripto);
• TRM Labs (detecção de fraudes e lavagem de dinheiro em blockchain);
• Crystal Blockchain (rastreamento de transações e análise forense).

Estas ferramentas permitem à TKB ASSET:

a) Atribuir pontuações de risco (risk scores) a endereços de carteiras fornecidos por clientes;
b) Identificar associações de carteiras com atividades ilícitas conhecidas (darknet markets, ransomware, exchanges hackeadas, mixers/tumblers, fraudes);
c) Rastrear fluxos de fundos (flow of funds) e identificar a origem e o destino de criptoativos;
d) Detectar padrões de comportamento suspeito (fracionamento, chain hopping, uso de anonimizadores);
e) Gerar relatórios forenses para suporte a investigações internas ou para fornecimento a autoridades competentes, quando solicitado.

4.4.2. Ferramentas de Screening de Listas Restritivas e Sanções

A TKB ASSET realiza, de forma sistemática e regular, consultas e cruzamentos de dados de seus clientes (e de seus sócios, administradores e beneficiários finais) com listas restritivas nacionais e internacionais, utilizando ferramentas automatizadas de screening, incluindo:

LISTAS INTERNACIONAIS:
• OFAC SDN List (Office of Foreign Assets Control – Specially Designated Nationals and Blocked Persons);
• CSNU – Listas de Sanções do Conselho de Segurança das Nações Unidas;
• União Europeia – Listas de Sanções Consolidadas;
• HM Treasury (Reino Unido) – Listas de Sanções Financeiras;
• Interpol – Avisos Vermelhos (Red Notices).

LISTAS NACIONAIS:
• Lista de Pessoas Politicamente Expostas (PEPs) – COAF/Receita Federal;
• Cadastro Nacional de Empresas Inidôneas e Suspensas (CEIS) – CGU;
• Cadastro Nacional de Empresas Punidas (CNEP) – CGU;
• Lista de Trabalho Escravo – Ministério do Trabalho;
• Listas de Processos Criminais e Inquéritos (consultas públicas aos Tribunais).

4.4.3. Bureaus de Crédito e Validação Cadastral

A TKB ASSET utiliza serviços de bureaus de crédito e bases de dados públicas e privadas para validação de informações cadastrais, verificação de idoneidade financeira e análise de perfil de risco de clientes, incluindo:

• Serasa Experian (consultas de crédito, score, protestos, processos, falências);
• Boa Vista SCPC (histórico de crédito e inadimplência);
• Receita Federal – Validação de CNPJ/CPF e situação cadastral;
• Juntas Comerciais – Validação de contratos sociais e estrutura societária;
• Cartórios de Protesto – Consulta de títulos protestados;
• Tribunais de Justiça – Pesquisa de processos judiciais cíveis e criminais.

4.4.4. Sistemas de Gestão de Compliance (GRC – Governance, Risk & Compliance)

A TKB ASSET poderá implementar, conforme necessidade e crescimento da operação, sistemas de gestão integrada de compliance (GRC platforms), que centralizam:

a) Cadastro completo de clientes e histórico de due diligence;
b) Registro de todas as transações e operações realizadas;
c) Alertas automatizados baseados em regras de detecção de sinais de alerta (red flags);
d) Workflow de análise e aprovação de casos suspeitos;
e) Gestão de comunicações ao COAF e registro de casos reportados;
f) Controle de treinamentos obrigatórios e certificações da equipe;
g) Geração de relatórios gerenciais e indicadores de desempenho (KPIs de compliance);
h) Auditoria de trilhas de decisões (audit trail) para fins de fiscalização ou investigação.

4.4.5. Inteligência de Fontes Abertas (OSINT – Open Source Intelligence)

A TKB ASSET adota práticas de inteligência baseada em fontes abertas (OSINT) para complementar suas análises de due diligence e monitoramento de clientes, incluindo:

a) Pesquisa em motores de busca (Google, Bing) sobre o cliente, seus sócios e administradores;
b) Análise de notícias negativas (adverse media) em portais de notícias, jornais e publicações especializadas;
c) Consulta a redes sociais corporativas (LinkedIn) e profissionais para validação de informações;
d) Verificação de websites, domínios e presença digital da empresa;
e) Pesquisa em fóruns, blogs e comunidades online relacionadas a criptoativos (para identificação de esquemas de fraude, golpes ou atividades ilícitas associadas a determinados atores).

4.4.6. Atualização e Aprimoramento Contínuo

A TKB ASSET compromete-se a manter-se atualizada sobre as mais recentes tecnologias, ferramentas e melhores práticas de compliance disponíveis no mercado, avaliando periodicamente a necessidade de adoção de novos recursos ou de upgrade das soluções existentes, sempre que justificado pela evolução da operação, pelo aumento da base de clientes, ou por recomendações de autoridades regulatórias.

---

4.5. PILAR V – TREINAMENTO E CAPACITAÇÃO

4.5.1. Programa de Treinamento Obrigatório

Todos os colaboradores, sócios e administradores da TKB ASSET, sem exceção, são obrigados a participar de treinamentos periódicos sobre PLD/FTP, que abordam:

a) Legislação brasileira e internacional aplicável;
b) Conceitos fundamentais de lavagem de dinheiro e financiamento ao terrorismo;
c) Tipologias e sinais de alerta específicos do mercado de criptoativos;
d) Procedimentos internos de due diligence, monitoramento transacional e comunicação ao COAF;
e) Ética, integridade e cultura de compliance;
f) Consequências legais e criminais do descumprimento das normas de PLD/FTP;
g) Casos práticos e estudos de casos reais (adaptados para preservar sigilo).

4.5.2. Frequência e Registro

Os treinamentos são realizados:

• No momento da admissão ou contratação (onboarding de novos colaboradores);
• Anualmente, de forma obrigatória e compulsória para todos;
• Sempre que houver alterações significativas na legislação, nas políticas internas, ou nas tipologias de risco.

Todos os treinamentos são registrados, documentados e arquivados, incluindo listas de presença, conteúdo ministrado, avaliações de aprendizado (quando aplicável), e certificados de conclusão.

4.5.3. Responsabilidade pelo Treinamento

A coordenação e a execução dos treinamentos são de responsabilidade do Compliance Officer, que poderá contar com o apoio de consultores externos especializados, quando necessário.

---

4.6. PILAR VI – MANUTENÇÃO DE REGISTROS E ARQUIVAMENTO

4.6.1. Prazo de Retenção de Documentos

Todos os registros, documentos, informações e evidências obtidos no processo de due diligence de clientes, bem como todos os registros de transações, operações, análises de casos suspeitos, comunicações ao COAF, e demais documentos relacionados ao programa de PLD/FTP, serão arquivados de forma segura, organizada e acessível, por um período mínimo de 10 (dez) anos, contados a partir da data de conclusão da operação ou do encerramento do relacionamento com o cliente.

Este prazo está em conformidade com o Art. 10, II, da Lei nº 9.613/98.

4.6.2. Formato de Armazenamento

Os documentos poderão ser armazenados em formato físico ou digital, preferencialmente digital, desde que garantida:

a) Integridade dos arquivos (sem alterações ou adulterações);
b) Confidencialidade (acesso restrito a pessoal autorizado);
c) Disponibilidade (possibilidade de recuperação rápida para atendimento a requisições de autoridades);
d) Backup regular e seguro dos arquivos digitais.

4.6.3. Controle de Acesso

O acesso aos arquivos de PLD/FTP é restrito ao Compliance Officer, à Diretoria, e a colaboradores especificamente autorizados. Não é permitido o compartilhamento de informações sensíveis com terceiros, salvo mediante ordem judicial, requisição formal de autoridade competente, ou nos casos de comunicação obrigatória ao COAF.

---

5. RELACIONAMENTO COM AUTORIDADES E COOPERAÇÃO EM INVESTIGAÇÕES

5.1. A TKB ASSET compromete-se a cooperar plenamente com todas as autoridades competentes (COAF, Receita Federal, Banco Central, CVM, Ministério Público, Polícia Federal, Poder Judiciário), no âmbito de suas atribuições legais, fornecendo informações, documentos e esclarecimentos solicitados, no prazo e na forma determinados.

5.2. Requisições de autoridades serão tratadas com prioridade máxima, e o Compliance Officer será imediatamente notificado para coordenar a resposta.

5.3. A TKB ASSET não divulgará, publicará ou tornará pública qualquer requisição recebida de autoridades, respeitando o sigilo legal quando aplicável.

---

## 6. SANÇÕES INTERNAS POR DESCUMPRIMENTO

6.1. O descumprimento desta Política por qualquer colaborador, sócio, administrador ou parceiro de negócios da TKB ASSET será tratado com máxima severidade, podendo resultar em:

a) Advertência formal;
b) Suspensão temporária;
c) Demissão por justa causa (no caso de colaboradores);
d) Rescisão contratual imediata (no caso de parceiros);
e) Responsabilização civil por eventuais prejuízos causados à TKB ASSET;
f) Comunicação às autoridades competentes, quando o descumprimento configurar crime.

---

## 7. REVISÃO E ATUALIZAÇÃO DESTA POLÍTICA

7.1. Esta Política será revisada, no mínimo, anualmente, ou sempre que houver necessidade decorrente de:

a) Alterações na legislação;
b) Mudanças no modelo de negócios da TKB ASSET;
c) Identificação de novas tipologias de risco;
d) Recomendações de auditorias ou de autoridades regulatórias.

7.2. A versão atualizada será aprovada pela Diretoria e comunicada a todos os colaboradores e parceiros.

## 8. APROVAÇÃO E VIGÊNCIA

Esta Política Institucional de PLD/FTP foi aprovada pela Diretoria Executiva da TKB ASSET e entra em vigor na data de sua publicação, revogando quaisquer disposições em contrário.

São Paulo – SP, Outubro de 2025.

_____

TOKENIZACAO MANAGEMENT GESTAO DE NEGOCIOS, PATRIMONIO E INVESTIMENTOS LTDA.

Por: EGON JUNIOR GOTCHALK SANTANA
Sócio Administrador
CPF: 064.727.329-22