Política de Compliance, Prevenção à Lavagem de Dinheiro (PLD) e Combate ao Financiamento do Terrorismo (AML)

FF Soluções Digitais e Financeiras LTDA - FFS
CNPJ: 05.980.434/0001-19

São Paulo, 08 de Agosto de 2023
Versão 2.0.1

Índice

1. Introdução

1.1 Objetivo do Manual

O objetivo deste manual é estabelecer diretrizes, políticas e procedimentos para a implementação efetiva de um programa de Prevenção à Lavagem de Dinheiro (PLD) e Combate ao Financiamento do Terrorismo (AML) específico para atividades de intermediação de criptoativos. Ele visa garantir o cumprimento das regulamentações brasileiras e padrões internacionais aplicáveis, promovendo a transparência, integridade e segurança das operações, bem como a proteção da FFS (denominada como empresa neste manual) contra riscos associados à lavagem de dinheiro e financiamento do terrorismo.

Os principais objetivos deste Manual são:

- Estabelecer um programa de compliance robusto para garantir o cumprimento das legislações nacionais e internacionais aplicáveis à PLD e AML, bem como as normas específicas relacionadas à intermediação de criptoativos;
- Identificar, avaliar e mitigar os riscos de lavagem de dinheiro e financiamento ao terrorismo associados às operações com criptoativos, buscando assegurar a integridade do sistema financeiro e proteger os interesses dos clientes e da empresa;
- Definir procedimentos adequados para a identificação e conhecimento dos clientes (KYC), incluindo a verificação de sua identidade e informações relevantes;
- Estabelecer mecanismos de monitoramento contínuo das transações realizadas com criptoativos, a fim de detectar padrões suspeitos e operações atípicas;
- Assegurar a capacitação e conscientização dos colaboradores da empresa em relação às questões de PLD e AML, bem como a importância do cumprimento das políticas e controles internos estabelecidos;
- Estabelecer um canal eficiente de comunicação com as autoridades competentes para reportar operações suspeitas ou atípicas, conforme exigido pela legislação vigente;
- Promover a cultura de conformidade e ética empresarial, reforçando o compromisso da empresa com a prevenção à lavagem de dinheiro e ao combate ao terrorismo, fortalecendo sua reputação no mercado.

- Este Manual é parte integrante do Programa de Compliance da FFS e deve ser seguido por todos os colaboradores envolvidos nas atividades de intermediação de criptoativos, independentemente de sua posição hierárquica. Além disso, a alta administração da empresa compromete-se a revisar periodicamente este Manual, garantindo que esteja em conformidade com as regulamentações mais recentes e melhores práticas adotadas no setor.

1.2 O que é PLD e AML?

A Prevenção à Lavagem de Dinheiro (PLD) é um conjunto de medidas, procedimentos e controles implementados para evitar que recursos obtidos ilegalmente sejam legitimados através de transações financeiras, ocultando sua origem ilícita. Já o Combate ao Financiamento do Terrorismo (AML) refere-se às ações destinadas a impedir que ativos financeiros sejam utilizados para financiar atividades terroristas ou grupos terroristas.

As instituições financeiras, incluindo as que lidam com criptoativos, desempenham um papel crucial na prevenção dessas atividades ilícitas, pois podem ser exploradas por criminosos para movimentar e ocultar fundos. Portanto, é essencial que as empresas adotem políticas e procedimentos rigorosos de PLD e AML para garantir a detecção e prevenção de atividades suspeitas.

1.3 Importância da Prevenção à Lavagem de Dinheiro e Combate ao Financiamento do Terrorismo

A lavagem de dinheiro e o financiamento do terrorismo representam ameaças significativas à integridade do sistema financeiro e à sociedade em geral. Essas práticas podem ser utilizadas para sustentar atividades criminosas e desestabilizar a segurança global. A implementação de um programa eficiente de PLD e AML é essencial para proteger a reputação da empresa, cumprir com as obrigações legais e contribuir para a segurança e estabilidade do mercado financeiro.

1.4 Abrangência do Manual

Este manual é aplicável a todas as atividades de intermediação de criptoativos realizadas pela empresa, abrangendo desde a aquisição e negociação de criptomoedas até a prestação de serviços relacionados, como custódia e negociação em nome de clientes. Todas as áreas da empresa envolvidas com essas atividades devem aderir às políticas e procedimentos descritos neste documento, garantindo a conformidade com as diretrizes regulatórias e as melhores práticas nacionais e internacionais de PLD e AML. É importante que todos os colaboradores e

terceiros envolvidos nessas operações estejam cientes e engajados em promover a prevenção e combate às práticas ilícitas.

1.5 Criptoativos e intermediação

Criptoativos são ativos digitais que utilizam criptografia e tecnologia de registro distribuído (blockchain) para garantir a segurança das transações e a integridade dos dados. Esses ativos funcionam como um meio de troca, unidade de conta ou reserva de valor e podem ser usados para diversos fins, como investimentos, pagamentos e financiamento de projetos.

Os criptoativos mais conhecidos são as criptomoedas, como o Bitcoin, Ethereum e Algorand. No entanto, existem muitos outros tipos de criptoativos, incluindo tokens de utilidade (que representam acesso a um produto ou serviço) e tokens de segurança (que representam ações ou participações em empresas).

A intermediação de criptoativos é o processo pelo qual empresas e instituições financeiras facilitam a compra, venda, troca e armazenamento desses ativos digitais. Essa atividade pode ser realizada por meio de diferentes plataformas e serviços, como corretoras, casas de câmbio, carteiras digitais e plataformas de negociação.

Devido à natureza digital e descentralizada dos criptoativos, a intermediação desses ativos apresenta riscos específicos em relação à lavagem de dinheiro, financiamento ao terrorismo e fraudes financeiras. As transações com criptoativos podem ser realizadas rapidamente, atravessar fronteiras internacionais com facilidade e, em alguns casos, oferecer um certo grau de anonimato. Essas características podem atrair criminosos que buscam ocultar ou movimentar recursos ilícitos.

1.5.1 Características Principais

- Descentralização: As criptomoedas não são controladas por instituições financeiras ou governos centrais. Em vez disso, sua emissão e validação são realizadas por meio de protocolos criptográficos e de consenso, envolvendo uma rede de computadores distribuídos.

- Anonimato e Pseudonimato: As transações com criptoativos podem ser realizadas de forma relativamente anônima, pois os usuários não precisam revelar suas identidades reais. Em vez disso, utilizam endereços digitais (chaves públicas) para realizar transações, o que confere um nível de pseudonimato às operações.

- Segurança: As transações de criptoativos são protegidas por criptografia, o que torna as operações seguras e resistentes a fraudes e falsificações.

- Transparência: Todas as transações de criptoativos são registradas em um livro-razão público, conhecido como blockchain. Esse livro-razão é acessível a qualquer pessoa e permite a verificação e rastreamento das operações realizadas.

- Escassez e Mineração: A maioria das criptomoedas possui uma quantidade limitada de unidades que podem ser criadas, o que confere a elas um caráter de escassez. A criação de novas unidades, em muitos casos, é realizada por meio do processo de mineração, que envolve a resolução de problemas computacionais complexos.

1.5.2 Importância do Entendimento

Para o efetivo cumprimento das obrigações de PLD e AML na intermediação de criptoativos, é fundamental que todos os colaboradores da empresa compreendam a natureza e funcionamento dos criptoativos, bem como suas particularidades em relação às moedas fiduciárias tradicionais. Essa compreensão permitirá que a empresa adote procedimentos adequados para mitigar riscos de lavagem de dinheiro e financiamento ao terrorismo associados ao uso de criptoativos.

1.5.3 Tipos de Criptoativos

A empresa trabalha com diversos tipos de criptoativos em suas operações de intermediação. Abaixo estão os principais tipos de criptoativos suportados pela empresa:

- Criptomoedas (ex: Bitcoin, Ethereum, Ripple, Algorand, Cardano, etc)
- Tokens de Utilidade (ex: Chainlink, BAT, CRO, etc)
- Tokens de Segurança (Representam algum valor imobiliário)
- Stablecoins (por exemplo: USDT - Tether, USDC - USD Coin, DAI, etc)
- Tokens Não Fungíveis (ex: NFTs)
- Tokens de Governança (ex: Maker, Compound, Uniswap, etc)
- Tokens de Plataformas Específicas (ex: EOS, Tezos, Tron, etc)

1.5.4 Funcionamento das Criptomoedas e Blockchain

- Blockchain: A blockchain é uma tecnologia de registro distribuído que consiste em uma cadeia de blocos contendo informações de transações. Cada bloco é conectado ao anterior por meio de criptografia, formando uma cadeia imutável e transparente de dados. A

blockchain é a base de funcionamento de muitas criptomoedas e oferece várias vantagens, como segurança, descentralização e transparência.

- Transações de Criptomoedas: As transações de criptomoedas são registradas na blockchain e são públicas, permitindo que qualquer pessoa verifique a validade e o histórico de uma transação. Cada transação é assinada digitalmente para garantir a autenticidade e a segurança das operações.

- Chaves Públicas e Privadas: Para realizar transações com criptomoedas, os usuários utilizam um par de chaves criptográficas: uma chave pública e uma chave privada. A chave pública, também conhecida como endereço da carteira (wallet), é compartilhada com outras pessoas para que possam enviar criptomoedas para o usuário. A chave privada, por outro lado, é mantida em segredo e é usada para assinar digitalmente as transações e autorizar o envio de criptomoedas.

- Mineração: Em muitas criptomoedas, como o Bitcoin, o processo de validação de transações e criação de novos blocos é realizado por mineradores. Os mineradores são participantes da rede que utilizam poder computacional para resolver problemas matemáticos complexos. Quando um minerador resolve um problema, ele pode criar um novo bloco e receber recompensas em criptomoedas por seu trabalho.

- Consenso: A tecnologia blockchain utiliza mecanismos de consenso para garantir que todos os participantes da rede concordem com a versão correta do livro-razão. Diferentes criptomoedas utilizam diferentes algoritmos de consenso, como o Proof of Work (PoW) utilizado pelo Bitcoin, o Proof of Stake (PoS) utilizado pelo Ethereum, entre outros.

- Smart Contracts (Contratos Inteligentes): Os contratos inteligentes são programas autoexecutáveis que são armazenados na blockchain e executados automaticamente quando certas condições são atendidas. Eles permitem a criação de acordos e contratos digitais, sem a necessidade de intermediários, tornando as transações mais rápidas e eficientes.

1.6 Princípios e Padrões Internacionais

1.6.1 Grupo de Ação Financeira (GAFI/FATF)

O Grupo de Ação Financeira (GAFI), também conhecido como Financial Action Task Force (FATF), é uma organização intergovernamental estabelecida em 1989 pelos países do G7 com o objetivo de combater a lavagem de dinheiro e o financiamento ao terrorismo. O GAFI desenvolve e promove políticas e padrões internacionais para fortalecer a integridade do sistema financeiro global e protegê-lo contra a exploração por criminosos e terroristas.

As recomendações do GAFI são amplamente reconhecidas como o padrão internacional para a implementação de medidas eficazes de PLD/AML. Essas recomendações são baseadas em três pilares fundamentais:

- Identificação e avaliação dos riscos: Os países e as instituições financeiras devem identificar e avaliar os riscos de lavagem de dinheiro e financiamento ao terrorismo em suas respectivas jurisdições e setores, a fim de desenvolver estratégias eficazes para mitigar esses riscos.

- Implementação de medidas preventivas: As instituições financeiras e outras entidades sujeitas às leis de PLD/CFT devem implementar políticas e procedimentos adequados para identificar, verificar e monitorar seus clientes, bem como detectar e reportar atividades suspeitas às autoridades competentes.

- Estabelecimento de um arcabouço legal e regulatório robusto: Os países devem adotar leis, regulamentações e outras medidas para criminalizar a lavagem de dinheiro e o financiamento ao terrorismo, estabelecer sanções eficazes para esses crimes e garantir a cooperação entre as autoridades nacionais e internacionais.

Em junho de 2019, o GAFI emitiu orientações específicas para a regulamentação e supervisão de atividades relacionadas a criptoativos, incluindo a intermediação desses ativos. Essas orientações estabelecem que as empresas envolvidas na intermediação de criptoativos devem estar sujeitas às mesmas obrigações de PLD/AML aplicáveis a outras instituições financeiras, como bancos e corretoras.

1.6.2 Padrões do Financial Action Task Force (FATF) para criptoativos

Em resposta ao crescimento e desenvolvimento do mercado de criptoativos e ao reconhecimento dos riscos associados à lavagem de dinheiro e ao financiamento ao terrorismo, o Financial Action Task Force (FATF) emitiu diretrizes específicas para regulamentar e

supervisionar atividades envolvendo criptoativos. Essas diretrizes têm como objetivo garantir a integridade do sistema financeiro global e proteger os mercados de criptoativos da exploração por criminosos e terroristas.

As principais recomendações do FATF para criptoativos incluem:

- Definição de criptoativos e prestadores de serviços relacionados a criptoativos (VASPs - Virtual Asset Service Providers): O FATF define criptoativos como ativos digitais ou virtuais que utilizam criptografia e tecnologia de registro distribuído (blockchain) para garantir a segurança das transações e a integridade dos dados. Prestadores de serviços relacionados a criptoativos (VASPs) são empresas ou indivíduos que realizam atividades de intermediação, como a compra, venda, troca, transferência e armazenamento de criptoativos.

- Regulamentação e supervisão de VASPs: Os países devem implementar um arcabouço legal e regulatório para licenciar, registrar e supervisionar VASPs, garantindo que essas entidades estejam em conformidade com os requisitos de PLD/AML. Isso inclui a aplicação das mesmas medidas preventivas exigidas para instituições financeiras tradicionais, como procedimentos de Conheça seu Cliente (KYC), monitoramento de transações e reporte de atividades suspeitas.

- Implementação de medidas de PLD/AML para VASPs: Os VASPs devem adotar políticas e procedimentos eficazes de PLD/AML, incluindo a identificação e verificação de clientes, a avaliação e gerenciamento de riscos, o monitoramento contínuo de transações e o reporte de atividades suspeitas às autoridades competentes.

- Cooperação internacional e intercâmbio de informações: Os países devem garantir a cooperação entre as autoridades nacionais e internacionais para combater a lavagem de dinheiro e o financiamento ao terrorismo no setor de criptoativos. Isso inclui o intercâmbio de informações sobre VASPs e seus clientes, bem como a assistência mútua em investigações e processos judiciais.

- Sanções e medidas punitivas: Os países devem estabelecer sanções eficazes e proporcionais para VASPs que não cumpram os requisitos de PLD/AML, incluindo multas, suspensão ou revogação de licenças e, em casos graves, ações criminais.

1.6.3 Cooperação internacional

A cooperação internacional é um elemento-chave na luta contra a lavagem de dinheiro e o financiamento ao terrorismo, especialmente no contexto dos criptoativos, que podem ser transacionados rapidamente e atravessar fronteiras com facilidade. A colaboração entre países, autoridades regulatórias, agências de aplicação da lei e instituições financeiras é essencial para compartilhar informações, identificar tendências emergentes e desenvolver estratégias eficazes para combater esses crimes.

Os principais aspectos da cooperação internacional no âmbito da PLD/AML incluem:

- Troca de informações entre autoridades: As autoridades nacionais devem estabelecer mecanismos eficazes para compartilhar informações relevantes sobre lavagem de dinheiro, financiamento ao terrorismo e outras atividades ilícitas relacionadas a criptoativos. Isso pode incluir a criação de pontos focais, redes de contato e plataformas de compartilhamento de informações para facilitar a cooperação e a coordenação entre as autoridades.

- Assistência mútua jurídica e extradição: Os países devem implementar tratados e acordos bilaterais ou multilaterais que permitam a assistência mútua jurídica e a extradição de criminosos envolvidos em lavagem de dinheiro e financiamento ao terrorismo. Isso pode incluir a cooperação na investigação, coleta de provas, confisco de bens e processamento de casos relacionados a criptoativos.

- Capacitação e treinamento: A cooperação internacional também deve envolver o compartilhamento de conhecimentos, experiências e melhores práticas na área de PLD/AML. Isso pode incluir a realização de programas de capacitação, workshops e seminários para fortalecer as habilidades e competências das autoridades, instituições financeiras e outros atores relevantes no combate à lavagem de dinheiro e ao financiamento ao terrorismo.

- Adesão e implementação de padrões internacionais: Os países devem aderir e implementar os padrões internacionais estabelecidos pelo Grupo de Ação Financeira (GAFI/FATF) e outras organizações relevantes, como o Banco Mundial e o Fundo Monetário Internacional (FMI), para garantir a consistência e a eficácia das medidas de PLD/AML em nível global.

- Participação em fóruns e iniciativas internacionais: Os países devem participar ativamente de fóruns e iniciativas internacionais relacionadas à PLD/AML, como a Conferência Internacional sobre Lavagem de Dinheiro e Recuperação de Ativos, a Iniciativa Global para a Transparência Financeira e a Parceria Global contra a Lavagem de Dinheiro. Essa participação permite o intercâmbio de ideias, a identificação de desafios comuns e o desenvolvimento de soluções

cooperativas para enfrentar as ameaças globais da lavagem de dinheiro e do financiamento ao terrorismo.

Referências

- Grupo de Ação Financeira contra a Lavagem de Dinheiro e o Financiamento do Terrorismo (GAFI/FATF) - www.fatf-gafi.org
- Banco Central do Brasil (BCB) - Departamento de Estabilidade Financeira - www.bcb.gov.br/estabilidadefinanceira
- Conselho de Controle de Atividades Financeiras (COAF) - www.gov.br/coaf
- Federação Brasileira de Bancos (Febraban) - www.febraban.org.br
- International Compliance Association (ICA) - www.int-comp.org
- A Associação Brasileira de Criptoeconomia - (ABCripto) www.abcripto.com.br
- Portal da Legislação - http://www4.planalto.gov.br/legislacao/
- Regulação Instrução Normativa RFB Nº 1888/2019
- GOMES, R. C.; SAADI, R. A. Crime Organizado – Lavagem de Dinheiro. Brasília: Academia Nacional de Polícia, 2008.
- ROMANTINI, G. L. O Desenvolvimento Institucional do Combate à Lavagem de Dinheiro no Brasil desde a Lei 9613/98.
- UNODC – UNITED NATIONS OFFICE ON DRUGS AND CRIME. Money Laundering Globalization
- BIO, S. R.; CORNACHIONE JUNIOR, E. B. Sistemas de Informação – Um Enfoque Gerencial. 2. ed. São Paulo: Atlas, 2008

2. Marco Regulatório

2.1 Legislação Brasileira Aplicável

A atividade de intermediação de criptoativos no Brasil está sujeita a um conjunto específico de regulamentações, que tem como objetivo proteger o sistema financeiro e combater crimes como lavagem de dinheiro e financiamento do terrorismo. As principais leis e normas brasileiras aplicáveis incluem:

2.1.1 Lei nº 9.613/1998 - Lei de Lavagem de Dinheiro

Estabelece os crimes de lavagem de dinheiro e determina a obrigatoriedade de comunicação às autoridades competentes sobre operações suspeitas.

2.1.2 Lei nº 12.683/2012

Altera dispositivos da Lei de Lavagem de Dinheiro e estabelece medidas adicionais de prevenção e combate ao financiamento do terrorismo.

2.1.3 Instrução CVM nº 617/2019

Regulamenta as ofertas públicas de distribuição de valores mobiliários, incluindo criptoativos, e estabelece requisitos de transparência e conformidade para as atividades relacionadas a eles.

2.1.4 Instrução CVM nº 497/2011

Dispõe sobre a constituição, a administração, o funcionamento e a divulgação de informações dos fundos de investimento, abrangendo fundos que investem em criptoativos.

2.1.5 Instrução CVM nº 555/2014

Regulamenta os fundos de investimento em participações (FIP), que podem investir em ativos como criptoativos.

2.1.6 Instrução Normativa RFB Nº 1888/2019

Institui e disciplina a obrigatoriedade de prestação de informações relativas às operações realizadas com criptoativos à Secretaria Especial da Receita Federal do Brasil (RFB)

2.2 Normas Internacionais Relevantes

Além da legislação nacional, é importante observar as normas internacionais relevantes, que estabelecem padrões e diretrizes globais para a prevenção à lavagem de dinheiro e combate ao financiamento do terrorismo. Algumas das principais normas incluem:

2.2.1 Recomendações do GAFI (Grupo de Ação Financeira Internacional)

O GAFI é uma organização internacional que define as Recomendações para o combate à lavagem de dinheiro, ao financiamento do terrorismo e à proliferação de armas de destruição em massa. As recomendações do GAFI são amplamente adotadas por diversos países.

2.2.2 Diretivas da União Europeia (UE)

Para empresas que realizam negócios com a UE ou cidadãos da UE, é relevante observar as diretivas europeias de prevenção à lavagem de dinheiro, que também seguem as recomendações do GAFI.

2.3 Órgãos Reguladores e Entidades de Supervisão

No Brasil, a atividade de intermediação de criptoativos é regulamentada e fiscalizada por órgãos específicos. Alguns dos principais são:

2.3.1 Comissão de Valores Mobiliários (CVM)

É responsável por regular, fiscalizar e supervisionar as atividades relacionadas a valores mobiliários, incluindo fundos de investimento que envolvem criptoativos.

2.3.2 Banco Central do Brasil (BCB)

O BCB atua no controle e na fiscalização do sistema financeiro, e suas normas são importantes para as instituições que operam com criptoativos.

2.3.3 Conselho de Controle de Atividades Financeiras (COAF)

O COAF é responsável por receber, examinar e identificar ocorrências suspeitas de atividades ilícitas e comunicá-las às autoridades competentes.

2.3.4 Receita Federal do Brasil (RFB)

A RFB tem um papel importante na fiscalização e tributação das operações com criptoativos.

3. Perfis de Risco

3.1 Identificação dos Perfis de Clientes

A identificação adequada dos perfis de clientes é um elemento essencial na prevenção à lavagem de dinheiro e ao financiamento do terrorismo. Nesse sentido, a empresa estabelece procedimentos para a coleta de informações e a análise de cada cliente, identificando suas características e o propósito das transações. A classificação dos perfis de clientes pode ser realizada com base em critérios como volume de transações, natureza das atividades, origem dos recursos e região de origem ou destino das transações.

3.2 Clientes de Alto Risco

O reconhecimento de clientes de alto risco é um aspecto crucial para um programa de PLD e AML efetivo. Clientes que apresentam características específicas, como pessoas politicamente expostas (PEPs), empresas offshore ou em jurisdições de risco.

3.3 Fatores de Risco para Atividades com Criptoativos

As operações envolvendo criptoativos têm suas particularidades e apresentam riscos específicos para a PLD e o AML. A volatilidade dos preços, a facilidade de transferência de fundos e o anonimato potencial oferecido por algumas criptomoedas podem facilitar a lavagem de dinheiro e o financiamento do terrorismo. Portanto, a empresa deve identificar e avaliar esses fatores de risco para desenvolver estratégias e controles adequados.

3.4 Monitoramento Contínuo de Perfis de Risco

Um programa de PLD e AML eficiente requer o monitoramento contínuo dos perfis de risco dos clientes ao longo do relacionamento comercial. Isso envolve a implementação de sistemas e tecnologias que permitem a detecção de padrões de comportamento incomuns ou transações suspeitas. O monitoramento contínuo é essencial para identificar atividades potencialmente ilícitas, acionar investigações apropriadas e reportar operações suspeitas às autoridades competentes, conforme necessário.

3.5 Definição de Limites Operacionais

Para mitigar o risco de lavagem de dinheiro, a empresa estabelece limites para transações com criptoativos, especialmente aquelas envolvendo clientes de Alto Risco ou operações consideradas atípicas. Esses limites ajudam a evitar movimentações financeiras não justificadas ou desproporcionais.

3.5.1 Pessoa Física abaixo de US$ 10.000,00 mês ou equivalente em reais

Background check, verificação em listas de sanções como OFAC, situação cadastral ativa na receita federal, envio de documentos, self e comprovante de endereço.

3.5.2 Pessoa Física acima de US$ 10.000,00 mês ou equivalente em reais

O mesmo da item 3.5.1 + declaração de imposto de renda ou comprovante de capacidade financeira.

3.5.3 Pessoa Jurídica abaixo de US$ 65.000,00 mês ou equivalente em reais

Background check, verificação em listas de sanções como OFAC, situação cadastral ativa na receita federal, contrato social, envio de documentos dos sócios, self e comprovante de endereço.

3.5.4 Pessoa Jurídica acima de US$ 65.000,00 mês ou equivalente em reais

O mesmo do item 3.5.3 + declaração de faturamento, balanço / declaração de imposto de renda.

3.5.5 Pessoa Jurídica sendo conta digital, instituição/empresa de pagamento que vendam cripto em seu app ou plataforma

O mesmo do item 3.5.4 e limitamos em US$ 10.000,00 mês por CPF (de seus clientes) enviado junto com a solicitação em nosso book de solicitações, contrato de intermediação de ativos digitais onde a mesma se compromete em seguir as mesmas práticas deste manual. Todos os CPF são submetidos ao nosso Background check, verificação em listas de sanções como OFAC, situação cadastral ativa na receita federal e data de nascimento.

4. Conheça seu Cliente (KYC), Colaborador (KYE), Parceiro (KYP), Fornecedor (KYS) e Carteiras (KYW).

4.1 Conheça seu Cliente (KYC)

O Know Your Customer (KYC), ou Conheça Seu Cliente, é um processo essencial no programa de Prevenção à Lavagem de Dinheiro (PLD) e Combate ao Financiamento do Terrorismo (AML).

Ele consiste na coleta, verificação e atualização contínua de informações sobre os clientes da empresa, a fim de conhecer sua identidade, origem dos recursos e propósito das transações. O KYC desempenha um papel crucial na mitigação de riscos e no combate a atividades ilícitas, permitindo a identificação de clientes de alto risco e a detecção de transações suspeitas.

O procedimento de coleta de informações do cliente, também conhecido como Know Your Customer (KYC), envolve a obtenção de dados detalhados sobre a identidade do cliente, incluindo nome, endereço, data de nascimento, número de identificação, entre outros. Além disso, é importante obter informações sobre a natureza das atividades do cliente e a fonte dos recursos utilizados nas transações com criptoativos. Essas informações permitem à empresa avaliar o perfil de risco do cliente e determinar se ele se enquadra em categorias de alto risco que requerem medidas adicionais de due diligence.

Adotamos níveis diferentes de verificação e solicitação de documentos conforme o item 3.5 Definição de Limites Operacionais.

Todo processo de Onboard deve passar pela nossa plataforma.

4.1.1 PEP (Pessoa Politicamente Exposta)

Pessoa que desempenha ou desempenhou funções políticas de alto nível ou tem estreita relação com tais indivíduos, podendo representar riscos adicionais devido ao potencial de influência política. A empresa não trabalha com este perfil de cliente.

4.3 Conheça seu Colaborador (KYE)

O processo de Conheça seu Colaborador (KYE) da empresa tem como objetivo conhecer bem seus colaboradores e avaliar sua integridade e conformidade com as políticas de Prevenção à Lavagem de Dinheiro (PLD) e Combate ao Financiamento ao Terrorismo (AML). Isso é feito através da coleta de informações abrangentes, verificação de referências e verificações de antecedentes criminais. A empresa também mantém uma política de conflito de interesses e fornece treinamento periódico em PLD-AML para conscientizar os colaboradores sobre suas obrigações. O KYE é uma medida importante para mitigar riscos internos e garantir um ambiente de trabalho seguro e confiável.

4.4 Conheça seu Parceiro e Fornecedor (KYP e KYS)

O processo de Conheça seu Parceiro (KYP) da empresa tem como objetivo conhecer bem seus parceiros e fornecedores e avaliar sua integridade e conformidade com as políticas de

Prevenção à Lavagem de Dinheiro (PLD) e Combate ao Financiamento ao Terrorismo (AML). Isso é feito através da coleta de informações detalhadas sobre os parceiros, incluindo sua reputação no mercado, histórico de negócios e conformidade legal. A empresa também verifica se há conexões com pessoas ou entidades envolvidas em atividades ilícitas ou de alto risco. O KYP é uma medida importante para mitigar riscos associados a parcerias comerciais e garantir que a empresa esteja envolvida em transações legítimas e éticas.

4.5 Conheça sua Carteira (KYW)

O processo de Conheça sua Carteira (KYW) da empresa é de extrema importância para garantir que a empresa não receba criptoativos provenientes de carteiras associadas a atividades criminosas, fraudes, hacks ou que estejam em "black lists".

Através do KYW, a empresa coleta informações detalhadas sobre as transações de criptoativos dos clientes, verificando as carteiras utilizadas, os endereços de origem e destino das transações, bem como a análise de histórico de transações. Isso permite identificar padrões suspeitos e transações incomuns, mitigando riscos associados a operações com criptoativos de origem ilícita.

Além disso, o KYW também envolve a utilização de ferramentas de análise de risco e o cumprimento das listas de sanções e black lists internacionais. Isso garante que a empresa não esteja envolvida em transações com carteiras associadas a pessoas ou entidades sancionadas ou envolvidas em atividades ilícitas.

Ao realizar o KYW de forma diligente, a empresa reforça seu compromisso com a conformidade das regulamentações de Prevenção à Lavagem de Dinheiro (PLD) e Combate ao Financiamento ao Terrorismo (AML). Essa prática contribui para proteger a reputação da empresa, evitar riscos de envolvimento em atividades ilegais e fortalecer a integridade e a confiança do mercado de criptoativos.

Além disso, ao identificar transações suspeitas ou ilegítimas durante o processo de KYW, a empresa pode comunicar operações suspeitas às autoridades e órgãos reguladores competentes, contribuindo para a segurança geral do setor de intermediação de criptoativos.

Portanto, o KYW é uma medida fundamental para assegurar a ética e a legalidade das operações da empresa, protegendo-a contra riscos de envolvimento em atividades ilícitas e contribuindo para um ambiente de trabalho seguro e transparente.

4.6 Procedimento de Atualização Cadastral dos Clientes

O procedimento visa manter informações precisas dos clientes. A atualização é feita anualmente e pode ser requisitada pelo compliance a qualquer momento. Utiliza-se a plataforma digital da empresa, além de possíveis informações adicionais por e-mail. A confidencialidade é assegurada, visando proteger os dados contra acesso não autorizado. O processo é vital para a integridade financeira e regulatória, requerendo a colaboração contínua dos clientes.

5. Monitoramento de Transações

5.1 Detecção de Transações Suspeitas

O monitoramento de transações é uma etapa crucial na prevenção à lavagem de dinheiro e ao combate ao financiamento do terrorismo. A empresa deve implementar sistemas e tecnologias adequadas para monitorar continuamente as operações envolvendo criptoativos. A detecção de transações suspeitas envolve a análise de padrões de comportamento incomuns ou atividades atípicas que possam indicar a lavagem de dinheiro ou o financiamento do terrorismo. Todos os depósitos realizados nas contas da empresa devem ser provenientes exclusivamente das contas de origem dos nossos clientes, com a devida verificação de titularidade correspondente ao cadastro.

5.2 Critérios de Monitoramento

Os critérios de monitoramento de transações são definidos com base em uma análise de risco abrangente e atualizada. A empresa estabelece indicadores e alertas que identificam transações que excedam determinados limites de valor, que ocorram em regiões, países ou jurisdições de alto risco, ou que envolvam clientes classificados como de alto risco. Além disso, transações que apresentem padrões incomuns, como múltiplas transferências pequenas em curtos intervalos de tempo ou grandes volumes de criptoativos movimentados sem justificativa clara, também devem ser objeto de monitoramento especial.

5.3 Ferramentas e Tecnologias Utilizadas

Para o monitoramento efetivo de transações, a empresa usa ferramentas e tecnologias avançadas, como sistemas de análise de dados em tempo real, algoritmos de inteligência artificial e aprendizado de máquina. Essas tecnologias podem ajudar a identificar padrões complexos e comportamentos suspeitos, permitindo uma detecção mais rápida e precisa de transações de alto risco. Além disso, a integração de sistemas de monitoramento com bancos

de dados externos, como listas de sanções e pessoas politicamente expostas, também são fundamentais para aprimorar a eficácia do monitoramento.

5.4 Investigação e Relatórios de Transações Suspeitas

Ao identificar transações suspeitas, a empresa deve conduzir investigações internas aprofundadas para avaliar a veracidade das suspeitas. Caso confirmada a atividade ilícita, a empresa deve elaborar relatórios detalhados sobre as operações suspeitas e reportá-las às autoridades competentes, conforme exigido pela legislação vigente. A comunicação rápida e precisa de transações suspeitas é fundamental para apoiar as autoridades na investigação de atividades criminosas e no combate à lavagem de dinheiro e ao financiamento do terrorismo.

6. Relatórios de Transações Suspeitas

6.1 Procedimentos para Reporte de Operações Suspeitas

Os colaboradores envolvidos no monitoramento de transações são treinados para reconhecer indícios de atividades ilícitas e estar cientes dos procedimentos a serem seguidos caso se deparem com transações suspeitas. A identificação e o reporte preciso e oportuno de operações suspeitas são fundamentais para apoiar as autoridades na investigação e prevenção de crimes financeiros.

6.2 Comunicação com os Órgãos Reguladores

A empresa deve estar preparada para estabelecer uma comunicação eficiente com os órgãos reguladores e entidades de supervisão responsáveis pela prevenção à lavagem de dinheiro e combate ao financiamento do terrorismo. Isso inclui o envio de relatórios de operações suspeitas e a pronta resposta a solicitações de informações por parte das autoridades. Manter uma relação colaborativa e transparente com os órgãos reguladores é essencial para garantir a conformidade com as obrigações legais e demonstrar a eficácia do programa de PLD e AML da empresa.

6.3 Sigilo e Confidencialidade

Os relatórios de operações suspeitas devem ser tratados com o mais alto grau de sigilo e confidencialidade. A divulgação não autorizada dessas informações pode prejudicar as investigações em andamento, colocar em risco a segurança dos clientes e colaboradores da empresa e comprometer a reputação da instituição. Portanto, a empresa estabelece medidas e

controles rigorosos para garantir que os relatórios de transações suspeitas sejam acessados apenas por pessoal autorizado e que a informação seja compartilhada estritamente de acordo com as exigências legais e regulatórias.

O efetivo reporte de operações suspeitas é um pilar fundamental no programa de PLD e AML da empresa. Ao implementar procedimentos claros e treinar adequadamente os colaboradores, a empresa reforça seu compromisso em combater a lavagem de dinheiro e o financiamento do terrorismo, colaborando ativamente com as autoridades competentes para garantir a segurança e a integridade do sistema financeiro e do mercado de criptoativos.

7. Sobre as Responsabilidades

7.1 Responsabilidades da Alta Administração:

A Alta Administração da empresa tem a responsabilidade primária de assegurar a efetiva implementação e adesão às políticas e procedimentos de Prevenção à Lavagem de Dinheiro (PLD) e Combate ao Financiamento ao Terrorismo (AML). Isso inclui o comprometimento com a cultura de conformidade, provendo recursos adequados para o Programa de PLD-AML e garantindo que os objetivos de prevenção e detecção de atividades ilícitas sejam alcançados.

7.2 Responsabilidades do Departamento de PLD-AML:

O Departamento de PLD-AML tem a responsabilidade de desenvolver, implementar e manter as políticas e procedimentos de PLD-AML da empresa. Além disso, é responsável por conduzir a devida diligência dos clientes, parceiros e fornecedores, monitorar as transações em busca de atividades suspeitas e realizar a comunicação de operações suspeitas quando necessário. O departamento também deve fornecer treinamento e conscientização regular para todos os colaboradores envolvidos nas atividades de intermediação de criptoativos.

7.3 Responsabilidades dos Colaboradores:

Todos os colaboradores da empresa têm a responsabilidade de cumprir as políticas e procedimentos de PLD-AML estabelecidos. Isso inclui a coleta adequada de informações dos clientes, parceiros e fornecedores, a verificação de sua conformidade com as regulamentações aplicáveis e a comunicação de quaisquer atividades suspeitas ou atípicas ao Departamento de PLD-AML. Os colaboradores também devem participar de treinamentos e conscientização periódicos para garantir o entendimento contínuo das políticas e procedimentos de PLD-AML.

7.4 Responsabilidades da Área de Conformidade e Auditoria Interna:

A área de Conformidade e Auditoria Interna tem a responsabilidade de revisar periodicamente a eficácia das políticas e procedimentos de PLD-AML da empresa. Isso inclui a realização de auditorias internas, a verificação da adesão às regulamentações e a identificação de áreas de melhoria. A área de Conformidade também é responsável por manter a empresa atualizada em relação às mudanças nas leis e regulamentações de PLD-AML.

7.5 Responsabilidades da Área Jurídica:

A Área Jurídica tem a responsabilidade de fornecer orientações legais relacionadas às atividades de intermediação de criptoativos da empresa. Isso inclui a revisão de contratos, políticas e procedimentos de PLD-AML para garantir sua conformidade com as leis e regulamentações aplicáveis. A Área Jurídica também deve auxiliar na resposta a quaisquer solicitações de autoridades e órgãos reguladores relacionadas a investigações ou auditorias.

7.6 Responsabilidades do Departamento de Recursos Humanos:

O Departamento de Recursos Humanos tem a responsabilidade de garantir que todos os colaboradores sejam devidamente informados sobre suas obrigações em relação às políticas e procedimentos de PLD-AML. Isso inclui o fornecimento de treinamento adequado e a manutenção de registros de treinamento. O Departamento de Recursos Humanos também é responsável por garantir que processos adequados de seleção, contratação e treinamento sejam implementados para assegurar que os colaboradores tenham as habilidades necessárias para cumprir suas responsabilidades relacionadas ao PLD-AML.

8. Políticas Internas e Procedimentos.

8.1 Política de PLD e AML

A empresa deve desenvolver e implementar uma política interna clara e abrangente de Prevenção à Lavagem de Dinheiro (PLD) e Combate ao Financiamento do Terrorismo (AML). Essa política deve refletir o compromisso da empresa em cumprir as regulamentações nacionais e internacionais aplicáveis e estabelecer diretrizes específicas para as atividades de intermediação de criptoativos. A política de PLD e AML deve abranger todas as etapas do ciclo de vida do cliente e das transações, desde a coleta de informações iniciais até o monitoramento contínuo e reporte de operações suspeitas. Além disso, ela deve definir as responsabilidades e obrigações dos colaboradores em relação à PLD e AML.

8.2 Políticas de Conformidade com Criptoativos

Devido à natureza específica das operações com criptoativos, é importante que a empresa estabeleça políticas de conformidade específicas para esse mercado. Isso inclui diretrizes para a verificação da origem e autenticidade dos criptoativos, a prevenção de atividades fraudulentas relacionadas a criptomoedas, e o estabelecimento de critérios para a inclusão ou exclusão de determinados criptoativos das operações da empresa. As políticas de conformidade com criptoativos devem estar alinhadas com as regulamentações vigentes e serem revisadas e atualizadas regularmente para se adequar às mudanças no cenário regulatório e tecnológico.

8.3 Procedimentos de Controle Interno

A empresa deve implementar procedimentos internos de controle rigorosos para garantir a conformidade com as políticas de PLD e AML. Isso inclui a designação de um responsável pela PLD e AML, que será o ponto focal para questões relacionadas a esses temas, e a realização de revisões periódicas de processos e controles para garantir sua eficácia. Também é importante estabelecer mecanismos de comunicação interna eficazes para disseminar informações sobre novas regulamentações, riscos identificados e melhores práticas no campo da PLD e AML.

8.4 Documentação e Registro

Todos os procedimentos, decisões e medidas relacionadas à PLD e AML devem ser devidamente documentados e registrados. Isso inclui registros de transações, relatórios de operações suspeitas, treinamentos realizados, atualizações de políticas e procedimentos, entre outros. Manter uma documentação completa e organizada é essencial para fins de auditoria, demonstração de conformidade às autoridades reguladoras e para proteção da empresa em caso de investigações ou disputas futuras.

9. Auditoria e Revisão do Programa de PLD e AML

9.1 Auditorias Internas

A empresa deve realizar auditorias internas periódicas para avaliar a eficácia e a conformidade de seu programa de Prevenção à Lavagem de Dinheiro (PLD) e Combate ao Financiamento do Terrorismo (AML). As auditorias são realizadas por profissionais independentes e objetivos, que

revisam os procedimentos, controles e políticas da empresa em relação à PLD e AML. Essa análise detalhada permite identificar eventuais falhas e áreas de melhoria no programa e, assim, promover aperfeiçoamentos contínuos.

9.2 Revisão de Políticas e Procedimentos

A legislação e as regulamentações relacionadas à PLD e AML estão em constante evolução, assim como o cenário do mercado de criptoativos. Por essa razão, é crucial que a empresa revise regularmente suas políticas e procedimentos de PLD e AML para garantir que eles estejam em conformidade com as últimas exigências legais e sejam efetivos na mitigação dos riscos. A revisão deve ser conduzida por especialistas e levar em consideração a evolução das melhores práticas e as recomendações das autoridades reguladoras.

9.3 Testes de Simulação (Simulação de Crises)

Além das auditorias e revisões, a empresa também pode realizar testes de simulação de crises para avaliar a capacidade de resposta do programa de PLD e AML em situações de emergência. Esses testes simulam cenários de lavagem de dinheiro ou financiamento do terrorismo, permitindo que a empresa avalie como suas equipes reagem e respondem a essas situações. Os resultados dos testes são usados para identificar possíveis vulnerabilidades no programa e para aprimorar os procedimentos de resposta a crises.

9.4 Melhorias Contínuas

Com base nos resultados das auditorias, revisões e testes de simulação, a empresa deve implementar melhorias contínuas em seu programa de PLD e AML. Essas melhorias podem incluir a atualização de políticas e procedimentos, o aprimoramento dos sistemas de monitoramento de transações, a realização de treinamentos adicionais para a equipe, entre outras medidas. O objetivo é aperfeiçoar constantemente o programa e garantir que ele permaneça eficaz e em conformidade com as regulamentações aplicáveis.

10. Conclusão e Compromisso com a PLD e AML

10.1 Compromisso da Empresa

A Prevenção à Lavagem de Dinheiro (PLD) e o Combate ao Financiamento do Terrorismo (AML) são questões de extrema importância para a empresa, seus clientes e o sistema financeiro

como um todo. Neste manual, foram apresentadas as melhores práticas brasileiras e internacionais relacionadas à PLD e AML, especialmente voltadas para atividades de intermediação de criptoativos. Ao seguir essas diretrizes, a empresa reforça seu compromisso com a integridade, a transparência e a segurança das operações no mercado de criptoativos.

10.2 Responsabilidade de Todos

A eficácia do programa de PLD e AML depende do comprometimento de todos os colaboradores da empresa. Cada membro da equipe desempenha um papel fundamental na identificação e prevenção de atividades ilícitas. É responsabilidade de todos estar cientes das políticas e procedimentos estabelecidos, além de cumprir rigorosamente suas obrigações em relação à PLD e AML.

10.3 Aperfeiçoamentos Contínuos

A PLD e o AML são áreas dinâmicas que estão sempre evoluindo para se adaptar às mudanças nos mercados financeiros e às ameaças emergentes. Por essa razão, a empresa está comprometida em realizar revisões periódicas e aperfeiçoamentos contínuos em seu programa de PLD e AML. Isso garantirá que as práticas e controles estejam atualizados e sejam capazes de mitigar os riscos mais recentes.

10.4 Colaboração com as Autoridades

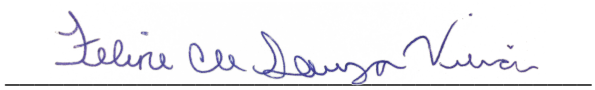
A empresa também reafirma seu compromisso em colaborar plenamente com as autoridades reguladoras e entidades de supervisão, sempre que necessário. O reporte de operações suspeitas e a comunicação transparente com os órgãos competentes são fundamentais para fortalecer a segurança do mercado de criptoativos e contribuir com a prevenção e o combate a atividades ilícitas.

10.5 Proteção dos Clientes e da Empresa

Ao implementar um programa robusto de PLD e AML, a empresa busca proteger não apenas seus próprios interesses, mas também os de seus clientes. A prevenção à lavagem de dinheiro e o combate ao financiamento do terrorismo são pilares essenciais para garantir a confiança e a segurança dos clientes em suas operações com criptoativos.

10.6 Agradecimento

Por fim, a empresa agradece a todos os colaboradores que contribuíram para a elaboração deste manual e reconhece a importância do esforço coletivo na construção de um ambiente financeiro mais seguro e transparente. O compromisso contínuo com a PLD e o AML é um reflexo do comprometimento da empresa com a ética, a conformidade e a responsabilidade nos negócios.



Felipe de Souza Vieira

São Paulo, 08 de Agosto de 2023