POLÍTICA CONTRA LAVAGEM DE DINHEIRO E FINANCIAMENTO AO TERRORISMO

“POLÍTICA DE PLD/FT”

TRKBIT TECNOLOGIA E INFORMAÇÃO LTDA

Data: 20 de janeiro de 2024

Versão 2.0

APRESENTAÇÃO

Esta **Política de Prevenção à Lavagem de Dinheiro e Financiamento ao Terrorismo ("PLD/FT")** consolida os princípios e as diretrizes de como a **TRKBIT TECNOLOGIA E INFORMAÇÃO LTDA** gerencia os riscos de lavagem de dinheiro e demais crimes financeiros para a prevenção e combate à lavagem de dinheiro e ao financiamento do terrorismo, em consonância com a legislação e regulamentação vigentes e com as melhores práticas de mercado nacionais e internacionais. Esta Política se aplica aos serviços oferecidos pela **TRKBIT TECNOLOGIA E INFORMAÇÃO LTDA,** pessoa jurídica de direito privado, inscrita no CNPJ nº 41.586.874/0001-50, com sede na Av. das Nações Unidas, nº 14.401, Edifício CJ 3010, Torre C2, Vila Gertrudes, São Paulo – SP, CEP: 04.794-000, e-mail: fale@trkbit.co , telefone: (11) 7703-0597, doravante denominada simplesmente **"TRKBIT";**

A **TRKBIT TECNOLOGIA E INFORMAÇÃO LTDA** opera como prestadora de serviços de tecnologia financeira, especializada em ativos digitais, oferecendo uma ampla gama de soluções aos seus clientes por meio de sua Plataforma.

A **TRKBIT TECNOLOGIA E INFORMAÇÃO LTDA** presta serviços relacionados à blockchain e criptomoedas, especialmente ligados à intermediação de compra e venda de criptoativos, garantindo segurança e sigilo nas transações realizadas pelos clientes. Vale destacar a diferença entre esse tipo de operação, que se assemelha às operações de OTC do mercado financeiro tradicional, com as empresas denominadas "Exchange" de criptoativos.

A presente Política de Prevenção e Combate à Lavagem de Dinheiro e ao Financiamento do Terrorismo ("Política") da **TRKBIT** visa promover a adequação das atividades operacionais da Empresa com as normas pertinentes aos crimes de lavagem de dinheiro e financiamento ao terrorismo ("LDFT").

Esta política se aplica a todos os estagiários, funcionários, prestadores de serviços, exchanges e sócios da **TRKBI**. Todos os envolvidos devem adotar as melhores práticas no cadastramento de clientes, dedicando especial atenção aos conceitos e atividades que auxiliam na prevenção e combate à lavagem de dinheiro e financiamento ao terrorismo.

A Política identificará o conceito de lavagem de dinheiro, bem como as etapas que configuram o delito e as características de pessoas e produtos suscetíveis a envolvimento com este crime.

Além disso, serão tipificadas as operações de lavagem de dinheiro, identificados os controles utilizadospela **TRKBIT** e definidas as regras para aplicação dos formulários "Conheça seu cliente" (KYC).

O conhecimento de algum indício de lavagem de dinheiro deverá ser comunicado ao departamento de Controles Internos e Compliance ("Compliance"), sendo este responsável por averiguar as informações reportadas e, caso aplicável, comunicar aos órgãos reguladores.

O Compliance será igualmente responsável por disponibilizar aos colaboradores da **TRKBIT** treinamentos e palestras que promovam a conscientização sobre o crime de lavagem de dinheiro e desenvolver campanhas/atividades que auxiliem na detecção de operações que caracterizem indícios deste crime.

Esta Política, junto às Políticas de Know Your Customer ("Conheça Seu Cliente") e Política de Compliance, faz parte do Programa de Compliance da **TRKBIT**, que visa nortear e demonstrar o controle do comportamento organizacional da **TRKBIT** e alinhamentos de conformidade, por meio de um complexo de controles internos e procedimentos, os quais consagram os pilares das narrativas de Governança Corporativa: transparência, equidade, prestação de contas e responsabilidade corporativa.

A **TRKBIT** se compromete a desenvolver um conjunto de controles internos no intuito de assegurar: **(i)** o correto cumprimento da legislação; **(ii)** a utilização eficiente e eficaz de todos os recursos; **(iii)** a redução dos níveis de incerteza e minimização da ocorrência de riscos financeiros, operacionais, regulatórios, de imagem ou legais.

Esta política também é parte integrante da Política de Segurança da Informação, também referida como "PSI", documento que orienta e estabelece as diretrizes corporativas de colaboradores envolvidos na operação para a proteção dos ativos de informação e a prevenção de eventual responsabilidade legal.

A **TRKBIT** em atendimento a legislação vigente e em defesa de seus próprios interesses comerciais, determina aos seus colaboradores e parceiros a não divulgação de dados inerentes ao ambiente de trabalho e de seus clientes.

Os colaboradores da **TRKBIT** são diretamente responsáveis pelo devido armazenamento e manipulação dos documentos enviados, devendo garantir o sigilo e a confidencialidade dos mesmos, impedindo a exposição a terceiros ou a outros colaboradores da empresa que não tenham autorização de acesso a essas informações.

A **TRKBIT** também opera em conformidade com a Lei do Marco Civil na Internet (Lei nº 12.965/2014), bem como a Lei nº 13.709/2018 (LGPD - Lei Geral de Proteção de Dados), tendo como premissa a manutenção do sigilo e da segurança das informações de seus clientes. Além disso, está em consonância com a Lei Nº 14.478, de 21 de dezembro de 2022, que estabelece diretrizes para a prestação de serviços de ativos virtuais e a regulamentação das prestadoras de serviços de ativos virtuais.

A **TRKBIT** também observa o Decreto nº 11.563 de 2023, que atribui ao Banco Central

do Brasil a competência como órgão regulador do mercado de criptoativos.

A **TRKBIT** observa as seguintes diretrizes, conforme a Lei 14.478/2022:

I - Livre iniciativa e livre concorrência;

II – Boas práticas de governaça, transparência nas operações e abordagem baseada em riscos;

III - Segurança da informação e proteção de dados pessoais;

IV - Proteção e defesa de consumidores e usuários;
V - Proteção à poupança popular;

VI - Solidez e eficiência das operações; e

VII - Prevenção à lavagem de dinheiro e ao financiamento do terrorismo e da proliferação de armas de destruição em massa, em alinhamento com os padrões internacionais.

A expressão "lavagem de dinheiro" consiste na realização de operações comerciais ou financeiras com a finalidade de incorporar recursos, bens e serviços obtidos ilicitamente.

Etapas do crime e lavagem de dinheiro:

O processo de lavagem de dinheiro envolve 03 (três) etapas, são elas: colocação, ocultação e integração.

A colocação é a etapa na qual o criminoso introduz o dinheiro obtido ilicitamente no sistema econômico mediante depósitos, compra de instrumentos negociáveis ou compra de bens. Isso implica na remoção do dinheiro do local que foi ilegalmente adquirido e sua inclusão, por exemplo, no mercado financeiro.

A ocultação ocorre quando o agente realiza transações suspeitas que caracterizam o crime de lavagem de dinheiro. Nesta fase, diversas transações complexas são realizadas para desvincular a fonte ilegal do dinheiro.

Na etapa de integração, o recurso ilegal é definitivamente incorporado ao sistema econômico e financeiro. A partir destemomento, o dinheiro recebe aparência lícita.

A **TRKBIT** reforça seu compromisso com a conformidade legal, ética e a prevenção de práticas ilícitas, assegurando transparência, segurança e integridade em suas operações relacionadas a blockchain, criptomoedas e tecnologia financeira.

SUMÁRIO

1. OBJETIVO

1.1. Esta Política tem como objetivo orientar as atividades da **TRKBIT TECNOLOGIA E INFORMAÇÃO LTDA**, em conformidade com a legislação vigente, no que se refere à prevenção e combate à lavagem de dinheiro e ao financiamento do terrorismo. Ela estabelece uma estrutura de controles específicos para dificultar, impedir e comunicar a ocorrência de crimes dessa natureza, definindo parâmetros para a aplicação efetiva da abordagem baseada em risco.

1.2. A **TRKBIT** atua como prestadora de serviços de tecnologia financeira, especializada em ativos digitais, oferecendo aos seus clientes uma ampla variedade de soluções por meio de sua Plataforma.

1.3. A **TRKBIT TECNOLOGIA E INFORMAÇÃO LTDA** presta serviços relacionados à blockchain e criptomoedas, com foco especial na intermediação de compra e venda de criptoativos, assegurando segurança e confidencialidade nas transações efetuadas pelos clientes. É importante destacar a distinção entre esse tipo de operação, similar às operações de balcão (OTC) do mercado financeiro convencional, e as empresas conhecidas como "Exchanges" de criptoativos.

1.4. As diretrizes e procedimentos desta Política estão alinhados com a Circular do Banco Central do Brasil nº 3.978/2020. A presente Política foi elaborada considerando o porte, natureza,complexidade, estrutura e modelo de negócio da **TRKBIT.**

1.5. A **TRKBIT** estabelece a presente Política com o intuito de evitar a sua participação em atividades ilícitas, zelando e protegendo seu nome, sua reputação e imagem perante os colaboradores, clientes, prestadores de serviços, reguladores, fiscalizadores e a sociedade. A governança é orientada para a transparência, cumprimento rigoroso de normas e cooperação com as autoridades policiais e judiciárias.

1.6. A **TRKBIT** busca constantemente alinhar-se às melhores práticas de mercado para a prevenção e combate a atos ilícitos, inclusive lavagem de dinheiro e financiamento ao terrorismo,por meio de investimentos e contínua capacitação de seus colaboradores.

1.7. Esta Política deve ser observada por todos os clientes, colaboradores e prestadores de serviços da **TRKBIT**, independentemente do cargo ou área de atuação.

1.8. O presente Programa de Prevenção à Lavagem de Dinheiro e ao Financiamento do Terrorismo (PLD/FT) tem por objetivo estabelecer os princípios éticos, conceitos, regras, procedimentos e controles internos aplicáveis às atividades da **TRKBIT**, relacionadas ao tema.

1.9. O Compliance corporativo consiste na adoção de procedimentos pela **TRKBIT**

com o objetivo de garantir a conformidade e o cumprimento da legislação vigente e dos regulamentos internos e externos, por meio da prevenção e punição de desvios de conduta ou práticas ilegais.

1.10. As diretrizes e procedimentos desta Política foram elaborados conforme a Resolução do Banco Central do Brasil nº 65, de 26 de janeiro de 2021, que trata da regulamentação da política de Compliance aplicável às instituições de pagamento, e também adotam os procedimentos adequados para o combate à corrupção.

1.11. Esta Política define, minimamente: **(i)** o objetivo e o escopo da função de Compliance; **(ii)** a divisão clara das responsabilidades das pessoas envolvidas na função de conformidade, de modo a evitar eventuais conflitos de interesses, principalmente com as áreas de negócios da **TRKBIT**; **(iii)** a alocação de pessoal em quantidade suficiente, adequadamente treinado e com experiência necessária para o exercício das atividades relacionadas com a função de Compliance; **(iv)** a posição na estrutura organizacional da **TRKBIT** da Área de Compliance; **(v)** as medidas necessárias para garantir independência e adequada autoridade aos responsáveis pelas atividades relacionadas com a função de conformidade e do combate à corrupção da Área de Compliance na instituição; **(vi)** o livre acesso dos responsáveis da Área de Compliance às informações necessárias para o exercício de suas atividades; **(vii)** os canais de comunicação direto com os Administradores da **TRKBIT**, para orelato dos resultados decorrentes das atividades relacionadas com a função de conformidade e combate à corrupção, de possíveis irregularidades ou falhas identificadas; e **(viii)** os procedimentospara a coordenação das atividades relativas à função de Compliance com funções de gerenciamento de risco e com a auditoria interna.

1.12. A despeito das normas em vigor não contemplarem especificamente atividades relacionadas aos criptoativos, no intuito de proteger a reputação e a integridade da **TRKBIT**, bem como de todo segmento empresarial relacionado à blockchain e criptoativos, essa Política tem por objetivo estabelecer controles e procedimentos que possam identificar clientes, contrapartes e operações suspeitas, de forma a inibir a entrada ou manutenção de clientes e contrapartes envolvidos em atividades ilegais.

1.13. Neste sentido, formam os pilares do programa de Compliance: **(i)** o suporte da alta administração; **(ii)** a avaliação de riscos, ou Compliance Risk Assessment (CRA); **(iii)** o alinhamento desta Política com o Código de Conduta e os procedimentos e controles internos; **(iv)** a realização de comunicação e treinamentos visando à disseminação da cultura de Compliance dentro da **TRKBIT**; **(v)** os canais de denúncia e ouvidoria; **(vi)** as investigações internas e os reportes; **(viii)** a realização due diligence interna e de terceiros, Clientes, Fornecedores e Parceiros de Negócios; e **(ix)** a realização de auditoria e monitoramento dos programas de Compliance.

1.14. Os dispositivos contidos nesta Política também observam as diretrizes da

TRKBIT para prevenir e combater situações propensas a atos de corrupção, suborno e fraudes, tanto em relaçãoàs instituições públicas como às empresas privadas, para prevenção, detecção e remediação dos atos lesivos previstos na lei 12.846/2013 (Lei Anticorrupção), e dos requisitos do Compliance Regulatório do Programa de Integridade e Diretrizes para Empresas Privadas publicado pela Controladoria-Geral da União – CGU, Portaria Nº 909/2015.

2. CONCEITOS

2.1. Os conceitos e siglas abaixo referem-se aos termos presentes ao longo desta Política:

2.2. **"ANBIMA"**: Associação Brasileira das Entidades dos Mercados Financeiros e de Capitais.

2.3. **"BACEN"**: Banco Central do Brasil e órgão regulador do mercado conforme Decreto nº11.563/2023.

2.4. **"OTC (Over The Counter)"**: Mercado de balcão, onde há negociar direta de ativos.

2.5. **"Exchange de criptoativos"**: Empresa que possui uma plataforma onde compradorese vendedores podem ofertar criptoativo em um livro de ofertas aberto.

2.6. **"CEIS":** Cadastro de Empresas Inidôneas e Suspensas.

2.7. **"Cadastro":** repositório de dados e documentos fornecidos pelos clientes e validados pelo Compliance da **TRKBIT**.

2.8. **"CEPIM":** Cadastro de Entidades Privadas Sem Fins Lucrativos Impedidas.

2.9. **"Cliente":** pessoa física ou jurídica, que utiliza os Serviços oferecidos pela **TRKBIT**.

2.10. **"CNEP":** Cadastro Nacional de Empresas Punidas.

2.11. **"Conselho de Controle de Atividades Financeiras ("COAF")":** órgão (Unidade de Inteligência Financeira Brasileira) responsável pela aplicação de sanções administrativas, a partir do recebimento, exame e identificação de ocorrências suspeitas de atividades ilícitas de lavagem de dinheiro e financiamento do terrorismo, além de proceder com a comunicação as autoridades competentes para a instauração dos procedimentos cabíveis, quando da conclusão pela existência de fundados indícios de crimes de lavagem de dinheiro e financiamento ao terrorismo;

2.12. **"Criptoativos":** Ativos digitais criptografados, podendo ser criptomoedas ou

tokens (Ex.: Bitcoin, Ethereum, Lite Coin);

2.13. **"Lavagem de Dinheiro":** consiste na realização de operações comerciais ou financeiras com a finalidade de incorporar recursos, bens e Serviços obtidos ilicitamente;

2.14. **"Etapas do crime de lavagem de dinheiro":** O processo de lavagem de dinheiro envolve três etapas, são elas: colocação, ocultação e integração. A colocação é a etapa em que o criminoso introduz o dinheiro obtido ilicitamente no sistema econômico mediante depósitos, compra de instrumentos negociáveis ou compra de bens. Trata da remoção do dinheiro do local que foi ilegalmente adquirido e sua inclusão, por exemplo, ao mercado financeiro. A ocultação é o momento que o agente realiza transações suspeitas e caracterizadoras do crime de lavagem. Nesta fase, diversas transações complexas se configuram para desassociar a fonte ilegal do dinheiro. Na integração, o recurso ilegal integra definitivamente o sistema econômico e financeiro. A partir deste momento, o dinheiro recebe aparência lícita.

2.15. **"Colocação" (etapa da lavagem de dinheiro)":** ingresso dos valores oriundos da prática de crimes antecedentes no Sistema Financeiro, por meio da realização de depósitos ou da aquisição de instrumentos negociáveis oferecidos por instituições financeiras.

2.16. **"Ocultação" (etapa da lavagem de dinheiro):** movimentação do dinheiro de origem ilícita múltiplas vezes, de forma a dificultar o rastreamento contábil, a realização de investigações sobre a origem do dinheiro e facilitar o anonimato.

2.17. **"Integração" (etapa da lavagem de dinheiro):** disponibilização do dinheiro ilícito novamente para os criminosos, com aparência legítima, por meio da incorporação desse recurso no setor econômico, adquirindo bens de alto luxo ou realizando investimentos financeiros, comerciais e industriais.

2.18. **"Estruturação":** permite que mais de um indivíduo conduza os recursos ilegais em múltiplas transações em uma ou mais instituições financeiras, por meio da divisão dos recursos em montantes inferiores àqueles cuja declaração de origem é exigida pelos órgãos governamentais.

2.19. **"Exchange de criptoativos":** Empresa que possui uma plataforma onde compradores e vendedores podem ofertar criptoativo em um livro de ofertas aberto.

2.20. **"FBI":** Federal Bureau of Investigation.

2.21. **"FEBRABAN":** Federação Brasileira de Bancos.

2.22. **"GAFI/FATF":** Grupo de Ação Financeira contra Lavagem de Dinheiro e Financiamento ao Terrorismo (organização intergovernamental).

2.23. **“INTERPOL”:** International Criminal Police Organization.

2.24. **“Know Your Client” (KYC):** Procedimento de “Conheça seu Cliente” que visa identificar, verificar, validar e qualificar os clientes, de modo que seja possível apreciar, avaliar e classificar o cliente com a finalidade de conhecer o seu perfil de risco e sua capacidade econômico-financeira.

2.25. **“Know Your Partner” (KYP):** Procedimento de due diligence para parceiros.

2.26. **“Know Your Employee” (KYE):** Procedimento de due diligence na admissão e contrataçãode colaboradores.

2.27. “**Know Your Transactions” (KYT):** Procedimento de due diligence para identificar, monitorar e relatar transações que possam estar associadas a atividades criminosas, incluindo a lavagem de dinheiro e o financiamento do terrorismo;

2.28. **“OFAC”:** Office of Foreign Assets Control.

2.29. **“Over The Counter” (OTC):** Mercado de balcão, onde há negociar direta de ativos.

2.30. **“Pessoa Exposta Politicamente” (PEP):** Conforme a Circular do Bacen n° 3.978/20, consideram-se PEP os agentes públicos que desempenham ou tenham desempenhado, nos últimos 05 (cinco) anos, no Brasil ou em países, territórios e dependências estrangeiras, cargos, empregos ou funções públicas relevantes, assim como seus representantes, familiares e outras pessoas de seu relacionamento próximo.

2.31. “**UNSC”:** United Nations Security Council.

3. NORMAS DE REFERÊNCIA

3.1. As normas abaixo foram utilizadas pela **TRKBIT TECNOLOGIA E INFORMAÇÃO LTDA** a fim de equacionar esta Política de PLD/FT:

a) Circular 3.680/13 do Banco Central do Brasil;

b) Circular 3.461/09 do Banco Central do Brasil;

c) Circular 3.978/20 do Banco Central do Brasil;

d) Carta Circular 4.001/20 do Banco Central do Brasil;

e) Resolução 4.753/19 do Banco Central do Brasil;

f) Resolução 4.474/16 do Banco Central do Brasil;

g) Instrução CVM 301/99;

h) Instrução CVM 534/13;

i) Instrução CVM 617/19;

j) Lei n° 12.846/2013 – Lei Anticorrupção (Lei do Brasil contrária a práticas, dentre outras, decorrupção ativa empresarial de agentes públicos ou pessoas relacionadas);

k) Lei n° 9.613/98;

l) Lei n° 12.850/13;

m) Lei n° 13.506/17;

n) Lei n° 13.810/19;

o) MP 893/19;

p) Autorregulação ANBIMA;

q) Autorregulação FEBRABAN;

r) Autorregulação ABCRIPTO;

s) Recomendações GAFI/FATF;

4. SERVIÇOS PRESTADOS

4.1. A **TRKBIT TECNOLOGIA E INFORMAÇÃO LTDA** opera como prestadora de serviços de tecnologia financeira, especializada em ativos digitais, oferecendo uma ampla gama de soluções aos seus clientes por meio de sua Plataforma.

4.2. A **TRKBIT TECNOLOGIA E INFORMAÇÃO LTDA** presta serviços relacionados à blockchain e criptomoedas, especialmente ligados à intermediação de compra e venda de criptoativos, garantindo segurança e sigilo nas transações realizadas pelos clientes. Vale destacar a diferença entre esse tipo de operação, que se assemelha às operações de OTC do mercado financeiro tradicional, com as empresas denominadas "Exchange" de criptoativos.

5. RESPONSABILIDADES

5.1. É responsabilidade da **TRKBIT** manter políticas, procedimentos e controles adequados para mitigar e tratar os riscos de compliance e riscos legais, especialmente no que diz respeito à prevenção à lavagem de dinheiro ("PLD") e ao combate ao financiamento do terrorismo ("FT").

5.2. A **TRKBIT** destaca que possui a responsabilidade de combater a entrada de capital originário de atividades ilícitas, espúrias e criminosas, adotando as diligências necessárias para a prevenção de crimes financeiros e condutas contrárias aos valores de probidade que são parte integrante de sua filosofia de negócio. Portanto, para a aplicação das diretrizes da presente política, o Programa de Compliance da **TRKBIT** inclui:

a) Sistema de controles internos para verificar e estabelecer a conformidade de cada área da **TRKBIT**;

b) Treinamento da Administração e seus colaboradores para alinhamento com uma cultura íntegra de conformidade com as regras, boas práticas, valores éticos e procedimentos de Compliance;

c) Estruturação de Departamento de Compliance;

d) Existência de políticas e procedimentos claros;

e) Procedimentos de Client Due Diligence, realizados no âmbito do programa de Know Your Customer (KYC);

f) Due Diligence de Terceiros para compreensão dos riscos inerentes ao relacionamento (riscos à imagem, de suborno e corrupção) através de programas de Know Your Partner (KYP) e KnowYour Employee (KYE).

5.3. A **TRKBIT** opera com ferramentas de monitoramento (operações e cadastro), classificação de risco, alertas, análise e comunicação ao COAF, para detecção de operações e situações suspeitas de PLD/FT. Utiliza ferramentas para a execução de Análise de Due Diligence, utilizando bases reputacionais como listas de sanções nacionais, PEP, listas restritivas internacionais, entre outras.

5.4. A **TRKBIT** não realiza parcerias nem possui relações com países ou clientes presentes em listas de sanções nacionais e internacionais;

5.5. É responsável pelo Programa de Prevenção à Lavagem de Dinheiro e ao Financiamento do Terrorismo (PLD/FT) o Diretor da **TRKBIT**, Sr. **THIAGO GABRIEL BRAZ,** o qual deverá cumprir e fazer cumprir as regras e procedimentos estabelecidos.

5.6. A responsabilidade pela elaboração e redação da presente política é da Dra.

Jessyca Arieira, OAB/RJ 201.582, contratada pela **TRKBIT**. Esta política deve ser revisada sempre que necessário ou, no mínimo, anualmente.

5.7. O STR/SAR (Suspicious Transaction Report / Suspicious Activity Report) está em conformidade com as normativas elencadas neste documento, enviando mensalmente todas as transações realizadas à Receita Federal do Brasil, conforme a Instrução Normativa 1888/2019. A **TRKBIT** reporta mensalmente todas as operações negociadas, identificando as transações e as titularidades de carteiras para as declarações de obrigações acessórias. Em caso de movimentações suspeitas ou incompatíveis, os usuários são automaticamente bloqueados e os valores retidos para disposição da justiça brasileira.

5.8. O reporte externo relacionado a AML/CFT/Regulamentos/Controles é enviado mensalmente, reportando todas as transações realizadas à Receita Federal do Brasil, conforme a Instrução Normativa 1888/2019. A TRKBIT reporta mensalmente todas as operações negociadas, identificando as transações e as titularidades de carteiras para as declarações de obrigações acessórias. Em caso de movimentações suspeitas ou incompatíveis, os usuários são automaticamente bloqueados e os valores retidos para disposição da justiça brasileira.

5.9. O monitoramento do cadastro de clientes é atualizado a cada 90 (noventa) dias, incluindo a obtenção de novas certidões e a atualização da lista de sanções internacionais e nacionais, validadas para garantir o monitoramento e a auditoria dos entes públicos nas transações realizadas pelos usuários. Além disso, os usuários são aprovados após a verificação da compatibilidade financeira, extraída de dados públicos da Receita Federal do Brasil.

5.10. Para o cadastro de clientes, a **TRKBIT** verifica a identidade e a veracidade das informações junto ao Cadastro Nacional de Pessoa Física na Receita Federal do Brasil, garantindo que os dados fornecidos correspondam à pessoa que está realizando o cadastro na plataforma.

5.11. Os registros de CDD e documentos, incluindo transações, são mantidos por, no mínimo, 05 (cinco) anos após o término do da relação contratual ou da utilização dos serviços, como forma de resguardo e apoio aos órgãos públicos, caso necessário, para colaborar com eventuais investigações daquele usuário.

6. PROCEDIMENTOS INTERNOS ADOTADOS PELA EMPRESA

6.1. A **TRKBIT TECNOLOGIA E INFORMAÇÃO LTDA** utiliza como referência e analogia os procedimentos internos com o objetivo de previnir a lavagem de dinheiro ou ocultação de bens, direitos e valores, a Circular nº 3.978, DE 23 DE JANEIRO DE 2020 do Banco Central do Brasil.

6.2. Essa política de prevenção será adotada em todos os setores da empresa,

começando pela avaliação dos seus funcionários, parceiros e prestadores de serviços terceirizados, estendendo- se às operações, transações, produtos, serviços e clientes da **TRKBIT.**

6.3. Os presentes procedimentos, bem como a presente política, deverão ser divulgados aos funcionários da instituição, parceiros e prestadores de serviços terceirizados, mediante linguagem clara e acessível, em nível de detalhamento compatível com as funções desempenhadas e com a sensibilidade das informações.

6.4. A **TRKBIT** mantém um departamento interno de Compliance responsável por implementar e garantir o cumprimento dos procedimentos estabelecidos, em cumprimento dos procedimentos alinhados e dispostos por analogia a Circular nº 3.978, de 23 de Janeiro de 2020 do Banco Central do Brasil, previsto na presente política.

6.5. Em conformidade com as diretrizes da circular mencionada, a **TRKBIT** deve estabelecer uma estrutura de gestão de riscos operacionais, incluindo a identificação e avaliação do risco associado ao uso de seus produtos e serviços para fins de lavagem de dinheiro e financiamento do terrorismo.

6.6. A avaliação interna de risco deverá ser totalmente documentada e aprovada pelo Diretor da **TRKBIT**, Sr. **THIAGO GABRIEL BRAZ** e encaminhada aos setores responsáveis pelas tomadas de decisão que possam envolver riscos regulatórios e de prevenção à lavagem de dinheiro. Cabe a ele a responsabilidade de identificar potenciais riscos, definir métricas e tratar os eventuais incidentes identificados.

6.7. Conforme os procedimentos instituídos pela Circular nº 3.978, de 23 de Janeiro de 2020 do Banco Central do Brasil, adotados pela **TRKBIT** por analogia, é determinado que devem ser seguidos procedimentos de identificação que permitam verificar e validar a identidade do cliente, incluindo a obtenção, verificação e validação da autenticidade das informações e identificação do cliente. Isso pode envolver, se necessário, confrontação dessas informações com as disponíveis em bancos de dados de caráter público e privado.

6.8. O Departamento de Compliance da **TRKBIT TECNOLOGIA E INFORMAÇÃO LTDA** é exercido por meio de canal direto da própria empresa, através do Diretor da **TRKBIT**, o Sr. **THIAGO GABRIEL BRAZ**, que contrata um escritório de advocacia para elaboração de pareceres OPINATIVOS sobre aprovação e reprovação. O Departamento de Compliance interno da empresa **TRKBIT TECNOLOGIA E INFORMAÇÃO** utilização do seguinte fornecedor homologado:

- **FORNECEDOR:** IDWALL TECNOLOGIA LTDA, CNPJ: 24.934.106/0001-20- endereço AV PAULISTA NÚMERO 2537 COMPLEMENTO ANDAR 12 CONJ 121 E 122- CEP 01.311-300-BAIRRO/DISTRITO- BELA VISTA MUNICÍPIO- SAO PAULO- UF- SP.

6.9. Da mesma forma, em conformidade com os procedimentos estabelecidos pela Circular nº 3.978, de 23 de janeiro de 2020, emitida pelo Banco Central do Brasil e adotados pela **TRKBIT** por analogia, a empresa deve adotar procedimentos de qualificação de risco através da coleta, verificação e validação de informações, adequados ao perfil de risco do cliente e à natureza da relação de negócio.

6.10. Os procedimentos definidos pela **TRKBIT TECNOLOGIA E INFORMAÇÃO LTDA** para a identificação do cliente e sua qualificação de risco serão detalhados a seguir nesta Política.

7. MONITORAMENTO E TRATAMENTO DE INDÍCIOS DE LAVAGEM DE DINHEIRO

7.1. O monitoramento na **TRKBIT** envolve o acompanhamento do comportamento das movimentações financeiras dos clientes, com o auxílio de ferramentas capazes de gerar alertas baseados nos seguintes fatores:

a) Os serviços financeiros utilizados;

b) O perfil de risco do cliente (“Abordagem Baseada em Risco”);

c) Categoria do criptoativo;

d) Movimentações de recursos incompatíveis com o patrimônio, a atividade econômicaou a ocupação profissional (capacidade econômico-financeira);

e) Depósitos que não demonstram ser resultado de atividades ou negócios normais;

f) Saque de quantia significativa de conta até então pouco movimentada ou de contaque acolheu depósito inusitado;

g) Ocultação dos beneficiários finais ou de terceiros envolvidos;

h) Oscilação significativa de volume ou frequência de transações;

i) Fracionamento de pagamentos;

j) Compatibilidade da movimentação com a conjuntura do mercado;

k) Indicativos de uso de métodos de ofuscação (mixing);

l) Carteiras (wallets) suspeitas.

7.2. A **TRKBIT** adota uma abordagem preventiva ao não atender ou realizar serviços para Pessoas Politicamente Expostas (PEPs).

7.3. As rotinas de monitoramento da **TRKBIT** estruturam-se da seguinte forma:

a) Utilização de tecnologia de inteligência artificial, data analytics e algoritmos para monitorar fluxo de pagamentos, transações, identificar oscilação comportamental em relação à volume, frequência e modalidade, análise de fatores diversos como por exemplo transações em horários suspeitos;

b) Alerta de movimentações financeiras que indiquem forte suspeita de lavagem de dinheiro;

c) Monitoramento mais diligente e especial dos clientes que se enquadrarem como PEPs (Pessoas Expostas Politicamente) e demais perfis de alto risco, com checagens habituais e pesquisas através de bases de dados que confirmem a validade dos dados apresentados, além da aplicação de pesquisas que identifiquem circunstâncias que demonstrem níveis diferentes de risco associado inicialmente;

d) Pesquisa de apontamentos negativos na mídia e checagem periódica nas listas restritivas disponíveis, de maneira a determinar se o relacionamento com o cliente pode ensejar eventuais riscos de imagem para a empresa e seus parceiros estratégicos, além de identificar a existência de envolvimento do cliente em casos de lavagem de dinheiro ou financiamento ao terrorismo;

e) Requisição de documentação adicional que demonstre capacidade econômico-financeira e origem de patrimônio para **(i)** que haja aumento de limites operacionais (aplicáveis de forma compatível com cada perfil de cliente); e **(ii)** nas hipóteses de identificação de suspeita de ilícitos financeiros, de forma a mitigar riscos e permitir maior controle por parte da **TRKBIT**;

f) Análises de compliance das informações e documentos fornecidos pelo cliente **TRKBIT** mediante pesquisa em diversos tipos de cadastros disponíveis.

7.4. O monitoramento se inicia com a coleta de documentos do cliente, seguindo as diretrizes da Circular nº 3.978/2020 do BACEN, que dispõe:

"Art. 16. As instituições referidas no art. 1º devem adotar procedimentos de identificação quepermitam verificar e validar a identidade do cliente:

§ 1º Os procedimentos referidos no caput devem incluir a obtenção, a verificação e a validação da autenticidade de informações de identificação do cliente, inclusive, se necessário, mediante confrontação dessas informações

com as disponíveis em bancos de dados de caráter público e privado.

§ 2º No processo de identificação do cliente devem ser coletados, no mínimo:

I - o nome completo e o número de registro no Cadastro de Pessoas Físicas (CPF), nocaso de pessoa natural; e

II - a firma ou denominação social e o número de registro no Cadastro Nacional daPessoa Jurídica (CNPJ), no caso de pessoa jurídica.

§ 3º No caso de cliente pessoa natural residente no exterior desobrigada de inscrição noCPF, na forma definida pela Secretaria da Receita Federal do Brasil, admite-se a utilizaçãode documento de viagem na forma da Lei, devendo ser coletados, no mínimo, o país emissor, o número e o tipo do documento.

§ 4º No caso de cliente pessoa jurídica com domicílio ou sede no exterior desobrigada deinscrição no CNPJ, na forma definida pela Secretaria da Receita Federal do Brasil, as instituições devem coletar, no mínimo, o nome da empresa, o endereço da sede e o número de identificação ou de registro da empresa no respectivo país de origem."

"**Art. 18**. As instituições mencionadas no art. 1º devem adotar procedimentos que permitam qualificar seus clientes por meio da coleta, verificação e validação de informações, compatíveis com o perfil de risco do cliente e com a natureza da relação de negócio.

§ 1º Os procedimentos de qualificação referidos no caput devem incluir a coleta de informações que permitam:

I - identificar o local de residência, no caso de pessoa natural;
II - identificar o local da sede ou filial, no caso de pessoa jurídica; e
III - avaliar a capacidade financeira do cliente, incluindo a renda, no caso de pessoanatural, ou o faturamento, no caso de pessoa jurídica.

§ 2º A necessidade de verificação e de validação das informações referidas no §1º deve ser avaliada pelas instituições de acordo com o perfil de risco do cliente e com a naturezada relação de negócio.

§ 3º Nos procedimentos de que trata o caput, devem ser coletadas informações adicionais do cliente compatíveis com o risco de utilização de produtos e serviços na prática da lavagem de dinheiro e do financiamento do terrorismo.

§ 4º A qualificação do cliente deve ser reavaliada de forma permanente, de acordo com aevolução da relação de negócio e do perfil de risco.

§ 5º As informações coletadas na qualificação do cliente devem ser mantidas atualizadas.

§ 6º O Banco Central do Brasil poderá divulgar rol de informações a serem coletadas, verificadas e validadas em procedimentos específicos de qualificação de clientes."

7.5. O monitoramento das informações e documentos coletados dos clientes da **TRKBIT** para a análise de Compliance é realizado a cada 90 (noventa) dias, exigindo o reenvio obrigatório da documentação.

7.6. De forma a auxiliar no monitoramento dos clientes, a **TRKBIT** segue o rol indicativo apresentado pela Carta Circular BCB nº 4.001, de 29 de janeiro de 2020, incluindo, mas não se limitando os exemplos abaixo indicados:

a) Situações relacionadas com operações em espécie em moeda nacional, como a realização de depósitos, aportes, saques, pedidos de provisionamento para saque ou qualquer outro instrumento de transferência de recursos em espécie, que apresentem atipicidade em relação à atividade econômica do cliente ou incompatibilidade com a suacapacidade financeira;

b) Situações relacionadas com a identificação e qualificação de clientes, como resistência ao fornecimento de informações necessárias para o início de relacionamento ou para a atualização cadastral, oferecimento de informação falsa ou prestação de informação de difícil ou onerosa verificação, apresentação de irregularidades relacionadas aos procedimentos de identificação e registro das operações exigidos pela regulamentação vigente, seguidas ou não do encerramento do relacionamento comercial;

c) Situações relacionadas com Colaboradores, parceiros e prestadores de serviços terceirizados, como alteração inusitada nos padrões de vida e de comportamento do empregado ou do representante, sem causa aparente.

7.7. De acordo com o disposto na regulamentação aplicável, a seleção de operações e situações que possam configurar indícios dos crimes de lavagem de dinheiro ou financiamento ao terrorismo é realizada pela **TRKBIT** no prazo máximo de 45 (quarenta e cinco) dias contados a partir da data da ocorrência da operação ou da situação, onde a decisão de reporte ao COAF deve ser tomada até o último dia deste prazo.

8. LEGISLAÇÃO BRASILEIRA SOBRE CRIPTOATIVOS E AUTORIDADE REGULADORA

8.1. De acordo com a Lei Nº 14.478, de 21 de dezembro de 2022 que dispõe sobre diretrizes a serem observadas na prestação de serviços de ativos virtuais e na

regulamentação das prestadoras de serviços de ativos virtuais; altera o Decreto-Lei nº 2.848, de 07 de dezembro de 1940 (Código Penal), para prever o crime de fraude com a utilização de ativos virtuais, valores mobiliários ou ativos financeiros; e altera a Lei nº 7.492, de 16 de junho de 1986, que define crimes contra o sistema financeiro nacional, e a Lei nº 9.613, de 03 de março de 1998, que dispõe sobre lavagem de dinheiro, para incluir as prestadoras de serviços de ativos virtuais no rol de suas disposições, caberá um ato do Banco Central do Brasil efetivar a regulação.

8.2. Como a regulamentação complementar ainda não foi elaborada pelo Banco Central do Brasil, órgão competente instituído pelo Decreto nº 11.563/23, a **TRKBIT** não é supervisionada por órgão competente, pois não há previsão legal de sua constituição até o momento, ficando sujeita apenas à fiscalização da Receita Federal do Brasil.

8.3. Desde 2019, de acordo com a Instrução Normativa 1.888/2019 emitida pela Receita Federal do Brasil em agosto de 2019, a **TRKBIT** se submete às regras da Receita Federal do Brasil enviando todas as transações realizadas no ambiente **TRKBIT** com todas as identificações de "hashs" e valores de moedas negociados e quem são os titulares, sendo certo que todas essas informações são enviadasà Receita Federal do Brasil até o último dia útil do mês subsequente da transação.

8.4. As normas as quais foram utilizadas pela **TRKBIT** a fim de equacionar esta Política de PLD/FT:

a) Circular 3.680/13 do Banco Central do Brasil;

b) Circular 3.461/09 do Banco Central do Brasil;

c) Circular 3.978/20 do Banco Central do Brasil;

d) Carta Circular 4.001/20 do Banco Central do Brasil;

e) Resolução 4.753/19 do Banco Central do Brasil;

f) Resolução 4.474/16 do Banco Central do Brasil;

g) Instrução CVM 301/99;

h) Instrução CVM 534/13;

i) Instrução CVM 617/19;

j) Lei n° 12.846/2013 – Lei Anticorrupção (Lei do Brasil contrária a práticas, dentre outras,de corrupção ativa empresarial de agentes públicos ou pessoas relacionadas);

k) Lei n° 9.613/98;

l) Lei n° 12.850/13;

m) Lei n° 13.506/17;

n) Lei n° 13.810/19;

p) MP 893/19;

q) Autorregulação ANBIMA;

r) Autorregulação FEBRABAN;

s) Autorregulação ABCRIPTO;

t) Recomendações GAFI/FATF;

8.5. A **TRKBIT** observa as normas do Banco Central do Brasil como parâmetros de mercado, por entender que as instituições autorizadas a funcionar pelo Banco Central do Brasil podem oferecer exclusivamente serviços de ativos virtuais ou integrá-los a outras atividades, conforme a regulamentação a ser editada pelo órgão nacional.

8.6. Além disso, a **TRKBIT** atua em conformidade com o Marco Civil na Internet Lei nº 12.965/2014, bem como a Lei nº 13.709/2018 (LGPD - Lei Geral de Proteção de Dados), tendo como princípio fundamental a preservação do sigilo e da segurança das informações de seus clientes.

9. PROCESSO DE ONBOARDING

9.1. O cadastro de clientes é um elemento essencial na prevenção e combate ao crime de Lavagem de Dinheiro e Financiamento ao Terrorismo (LDFT). O cumprimento rigoroso da Política de Regras e Procedimentos do departamento de Cadastro ("Cadastro") é imperativo para assegurar a integridade e conformidade nas operações da **TRKBIT**.

9.2. A ficha cadastral da **TRKBIT** é clara, objetiva e segregada para pessoas físicas e jurídicas. A análise cuidadosa de toda a documentação é realizada para confirmar a veracidade do cadastro.

9.3. Considerando as principais diretrizes e regras existentes no mercado financeiro e de negociação de criptoativos, bem como a análise dos principais casos de lavagem de dinheiro, é possível relacionar as pessoas mais sensíveis de envolvimento com o crime de lavagem de dinheiro.

9.4. Os formulários de “Conheça seu cliente” (“KYC”) devem ser aplicados aos clientes pessoas físicas e jurídicas. Todos os campos devem ser preenchidos com seriedade e clareza, permitindo a exata definição do perfil do cliente.

9.5. Sempre que necessário, os responsáveis pelo preenchimento dos formulários devem realizar visitas aos clientes e, quando aplicável, aos seus estabelecimentos comerciais. Tais visitaspodem ser periodicamente refeitas, e visitas especiais devem ser efetuadas em qualquer situaçãode anormalidade ou mudança no comportamento operacional do cliente.

9.6. O respectivo formulário é disponibilizado aos clientes no ato do cadastramento dos dados para a abertura de conta, ou seja, antes do início de suas operações. O preenchimento do formulário poderá ser solicitado pelo Compliance quando este entender necessário o preenchimento e/ou atualização dos respectivos dados.

9.7. O formulário “Conheça seu cliente” (KYC) será arquivado eletronicamente, quando assim preenchido, ou fisicamente junto ao dossiê cadastral do cliente.

9.8. A **TRKBIT** supervisiona constantemente as condutas profissionais e pessoais de seus colaboradores, repreendendo severamente qualquer descumprimento dos princípios éticos da instituição.

9.9. A **TRKBIT** recebe a documentação do cliente ou parceiro como 1ª (primeira) etapa no processo de onboarding, seguindo os trâmites dos artigos 16 e 18 da Circular nº 3.978 de 2020 do BACEN:

I. Primeira Etapa - Envio de documentos

9.10. O cliente **Pessoa Jurídica** ou parceiro envia a documentação exigida, sendo:

a) Contrato Social de Constituição da empresa e demais alterações;

b) Comprovante de endereço;

c) Balanço ou declaração de faturamento assinado pelo contador, com detalhamento mensal dos últimos 12 (doze) meses;

d) Último recibo de entrega da declaração sobre operações realizadas com criptoativos, enviadas para Receita Federal referente a Instrução Normativa 1.888/2019;

e) Dos sócios: RG ou CNH, ambos com CPF; Selfie com o documento; Comprovante deresidência;

f) Endereço da Wallet;

g) Dados da empresa e de seu quadro societário;

h) Faturamento declarado dos últimos 12 (doze) meses atualizados;

i) Se em seu quadro societário há Pessoas Expostas Politicamente (PEP);

j) Se houve alteração no quadro societário nos últimos 12 (doze) meses;

k) Se os sócios da empresa possuem histórico criminal relacionado a práticas ilícitas previstas na Lei nº 9.613/98, Lei nº 12.846 e correlatas;

l) Wallets cadastradas de sua titularidade;

m) Se há, em sua empresa, regulamentação ou normas específicas sobre práticas de Anticorrupção, Lavagem de Dinheiro e Financiamento ao Terrorismo;

n) Se a empresa possui Programa de Compliance e como é feito;

o) Como se dá o Processo de "Conheça seu cliente" ("KYC"), "Conheça seu Parceiro" ("KYP") e "Conheça seu Fornecedor" ("KYS"), além de outras informações pertinentes.

9.11. O cliente **Pessoa Física** envia a seguinte documentação exigida:

b) Nome completo;

c) Data de Nascimento;

d) Documento de Identificação Pessoal Oficial com data de emissão não superior a 10 (dez) anos;

e) CPF;

f) E-mail;

g) Telefone;

h) Endereço completo (logradouro, nº, complemento, bairro, cidade, Estado e CEP);

i) Nome da mãe;

j) Estado Civil;

k) Sexo;

l) Profissão;

m) Foto Selfie segurando documento de identificação pessoal oficial;

n) Wallets cadastradas de sua titularidade;

o) Última declaração de Imposto de Renda Pessoa Física ou comprovação de fundos;

p) Recibo da IN 1888/2019 da RFB;

9.12. Após o envio dos documentos e preenchimento do formulário pelo candidato a cliente, o documento é encaminhado ao Diretor da **TRKBIT**, Sr. **THIAGO GABRIEL BRAZ**, para elaborar a etapa ”2” do processo de Onboarding.

9.13. Após o envio da documentação, a equipe interna verifica a veracidade dos documentos apresentados para garantir que pertençam ao cliente que efetuou o envio e se de fato conferem com as informações na base de dados da Receita Federal do Brasil, Banco Central do Brasil e Sistema Público do Brasil, verificando, ainda, se o usuário se encontra em jurisdição proibida.

9.14. Após a conclusão da verificação para garantir a autenticidade e veracidade dos documentos perante a Receita Federal do Brasil, Banco Central do Brasil e Sistema Público do Brasil, bem como a confirmação de que o usuário não está utilizando um endereço de uma jurisdição proibida, será iniciada a 2ª (segunda) etapa do processo de onboarding.

II. Segunda Etapa - Verificação financeira e jurídica do sistema interno

9.15. Verificam-se as seguintes informações financeiras e jurídicas do cliente:

a) Renda Mensal estimada e declarada (em R$);

b) Patrimônio estimado e declarado;

c) Análise do endereço do cliente;

d) Análise do histórico de declarações do Imposto de Renda;

e) Análise de possíveis protestos;

f) Análise do histórico de trabalho do cliente, bem como a sua remuneração estimada;

g) Verificação de recebimento de benefício ou auxílio social governamental;

h) Verificação da existência de processos judicias em nome do cliente que possam ser impeditivosde realização do negócio;

i) Verificação da declaração de que não é Pessoas Expostas Politicamente;

j) Consulta nas listas impeditivas nacionais e internacionais, como: CNJ, COAF, FBI e ONU;

k) Consulta nos Sites: Receita Federal, Portal da Transparência, Órgãos Reguladores, SCPC/Serasa, Tribunais Estaduais, Eleitorais, Trabalhistas, Superiores e Mídias;

l) Análise do relatório de faturamento dos 12 (doze) últimos meses, assinado e datadopelo contador responsável e dos respectivos sócios.

m) Background Check que retorna informações como: **(i)** PEP (Pessoas Expostas Politicamente); **(ii)** Mandado de Prisão Expedido; **(iii)** Consultas às Listas de Sanções Nacionais e Internacionais:

- COAF – Conselho de Controle de Atividades Financeiras
- CEAF – Centro de Estudos e Aperfeiçoamento Funcional
- CNEP – Cadastro Nacional de Empresas Punidas
- MTE- Ministério do Trabalho
- CNJ – Conselho Nacional de Justiça
- TSE – Tribunal Superior Eleitoral
- CEIS – Cadastro de Empresas Inidôneas e Suspensas
- EU – Lista de sanções da União Européia
- FBI – Polícia Federal dos Estados Unidos
- GOV UK – Lista de sanções do Reino Unido
- INTERPOL – Organização Internacional de Polícia Criminal
- OFAC – Agência de Controle de Ativos Estrangeiros dos EUA
- UNSC- Conselho de Segurança das Nações Unidas
- Consulta nos Sites: Receita Federal, Portal da Transparência, Órgãos reguladores, SCPC/Serasa, Tribunais Estaduais, Eleitorais, Trabalhistas, Superiores e Mídias;

n) Verificação de existência de ações judiciais e administrativas.

9.16. Na etapa 2, o sistema revisita as informações elencadas para verificar se há

algum impedimento jurídico, financeiro ou alguma atividade atípica em nome do candidato.

9.17. Cada candidato a cliente será verificado antes da aprovação, com base no preenchimento do Formulário de Identificação e verificação da veracidade das informações através do fornecedor homologado e contratado pela **TRKBIT**:

- **FORNECEDOR:** IDWALL TECNOLOGIA LTDA, CNPJ: 24.934.106/0001-20- endereço AV PAULISTA NÚMERO 2537 COMPLEMENTO ANDAR 12 CONJ 121 E 122 - CEP 01.311-300-BAIRRO/DISTRITO- BELA VISTA MUNICÍPIO- SAO PAULO- UF- SP.

9.18. Uma vez adquiridas tais informações, a área responsável envia os documentos e demais informações coletadas para o escritório externo de advocacia, responsável pelo seu processamento para fins de realização do procedimento de Parecer Opinativo acerca do "Know Your Client" da **TRKBIT**, dispondo acerca de sua aprovação ou reprovação a ser auferida com base em uma pesquisa realizada em plataformas de busca especializadas, destinadas à verificação de integridade dos indivíduos consultados.

9.19. A verificação da veracidade das informações prestadas pelo responsável do Compliance ao escritório externo de advocacia, são verificadas a partir do sistema do fornecedor homologado:

- **FORNECEDOR:** COMBATE A FRAUDE S.A. - CNPJ: 34.102.645/0001-57. R. Tiradentes, 1077 - 5º andar – Centro - Venâncio Aires - RS, 95800-000; e ETHQUO ETHICAL QUOTIENT SERVICOS DE COMPLIANCE E TECNOLOGIA LTDA - 39.545.663/0001-27

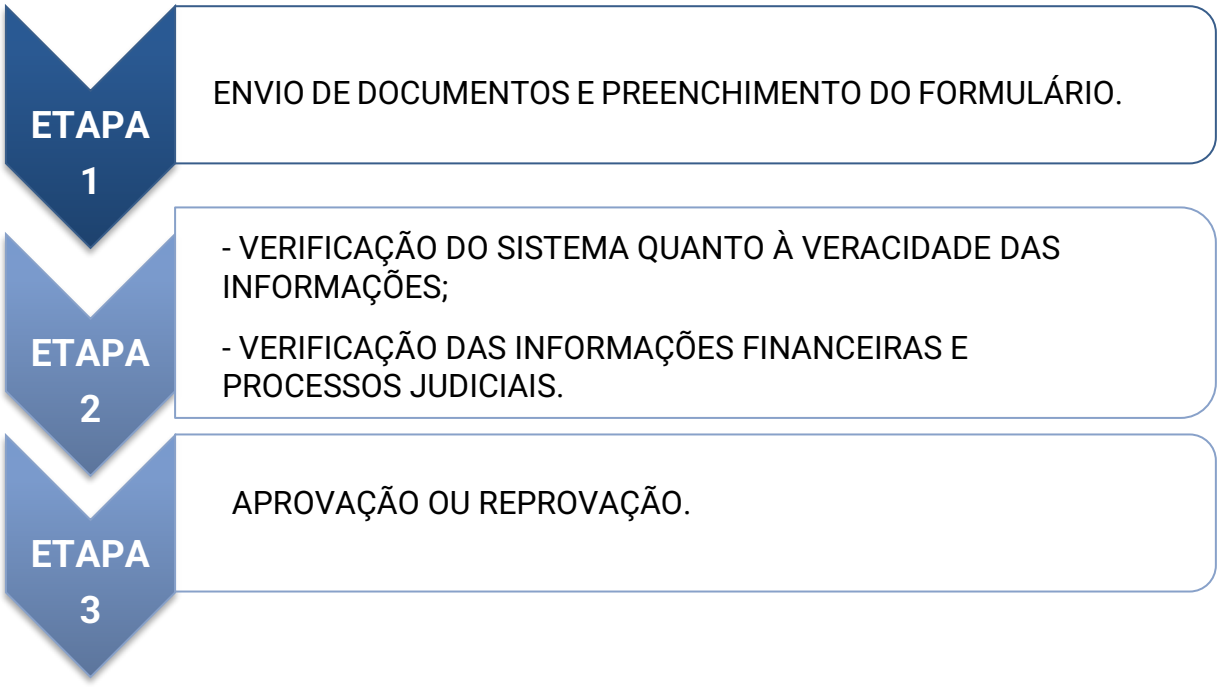
9.20. Os Pareceres Opinativos elaborados pelo excritório de advocacia externo sempre consignarão, em suas conclusões, as ponderações acerca do cliente e das informações consultadas, apontando, assim, por sua aprovação ou reprovação. O referido documento será enviado ao único sócio e administrador da **TRKBIT**, o Sr. **THIAGO GABRIEL BRAZ**, que será o responsável final pela decisão acerca do fornecimento dos serviços pela **TRKBIT**.

9.20.1. O escritório de advocacia externo **apenas** elabora pareceres opinativos, de forma que a responsabilidade de seguir ou não com as recomendações expostas são exclusivas dos sócios. O escritório de advocacia externo e a advogada externa **não** possuem, em nenhuma hipótese, condão decisório.

9.21. O monitoramento das informações e documentos coletados do cliente para a análise de compliance é realizado a cada 90 (noventa) dias, devendo ser reenviada a documentação obrigatória.

9.22. Quanto mais precisas e atualizadas forem as informações coletadas e registradas, maior será a capacidade de identificação de atos ilícitos.

III – Fluxo Operacional



9.21. Após a verificação do sistema, o cliente poderá ser aprovado, estabelecendo limites operacionais e sujeito a monitoramento rigoroso de todas as transações, sempre enviadas à Receita Federal do Brasil mensalmente.

9.22. Se o cliente for reprovado durante o processo de verificação, o cadastro é automaticamente bloqueado na plataforma.

9.23. Não são permitidos cadastros em nome de terceiros e em caso de comprovante de endereço em nome de outrem, será verificado o parentesco ou será exigida a comprovação da residência através de contrato de locação ou outro documento pertinente ao caso.

9.24. Não são permitidas transferências para contas de terceiros e nem envios de ativos digitais paracontas de terceiros. Todas as transações são realizadas com a mesma titularidade do usuário.

9.25. Não são permitidos cadastros de menores de 18 (dezoito anos) ou incapazes.

9.26. A **TRKBIT** se reserva ao direito de não atender ou aceitar Pessoas Expostas Politicamente (“PEP”).

9.27. A **TRKBIT** não realiza parcerias e não possui relações com países que estejam na lista de sanções nacionais, ou com clientes que estejam na lista de sanções nacionais e internacionais.

10. PROCEDIMENTOS DE PREVENÇÃO A ATOS ILÍCITOS DE LAVAGEM DE DINHEIRO E FINANCIAMENTO AO TERRORISMO

10.1. Em razão de a **TRKBIT** ter a responsabilidade da manter as políticas, procedimentos e controles apropriados para mitigar e tratar riscos de compliance e riscos legais, principalmente no que tange à prevenção à lavagem de dinheiro (“PLD”) e combate ao financiamento do terrorismo (“CFT”), a empresa estabeleceu procedimentos de prevenção e combate a atos ilícitos para PLD/CFT, utilizando-se das melhores práticas de mercado, conforme detalhados abaixo:

I – “CONHEÇA SEU CLIENTE” (KYC)

10.2. O objetivo principal do procedimento de KYC (Know Your Customer) é proteger a **TRK** do envolvimento com atividades ilícitas, bem como indivíduos, jurisdições ou entidades sancionadas, além de garantir que a **TRK** cumpra integralmente todas as respectivas leis, regulamentos ou normas pertinentes ao escopo de PLD/CFT.

10.3. O procedimento KYC visa identificar os reais detentores dos ativos e recursos que circulam na **TRK**, sendo o elemento mais importante no processo de prevenção à lavagem de dinheiro e ao financiamento do terrorismo, visando prover direcionamento e padronização para o início, a manutenção e o monitoramento do relacionamento com aqueles que utilizam ou pretendam utilizar os produtos e serviços da **TRK**.

10.4. No procedimento se consigna a estratégia de avaliação baseada em riscos, criada para mitigar os riscos de lavagem de dinheiro e financiamento ao terrorismo. A **TRK** utiliza direcionadores de risco e distribuí determinado peso, de modo a atribuir a cada cliente e operação o grau de suscetibilidade à lavagem de dinheiro e ilícitos financeiros, equacionando com suas métricas de apetite de risco. A partir do risco associado ao cliente, a **TRK** aprova o início e o prosseguimento do relacionamento.

10.5. O processo de KYC tem início durante o "Onboarding" do cliente na **TRKBIT**, ou seja, no momento em que o cliente abre sua conta na **TRKBIT**.

10.6. O formulário correspondente é disponibilizado aos clientes durante o cadastro de dados para a abertura de conta, ou seja, antes do início de suas operações. O

preenchimento do formulário pode ser solicitado pelo Compliance sempre que este julgar necessário para a atualização ou complementação dos dados.

10.7. Os formulários de "Conheça seu cliente" ("KYC") são aplicados tanto a clientes pessoas físicas quanto jurídicas. Todos os campos devem ser preenchidos com seriedade e clareza, permitindo uma definição precisa do perfil do cliente.

10.8. A **TRKBIT** recebe a documentação do cliente como 1ª (primeira) etapa no processo de onboarding, seguindo os trâmites dos artigos 16 e 18 da Circular nº 3.978 de 2020 do BACEN:

→ **Primeira Etapa - Envio de documentos**

10.9. O cliente **Pessoa Jurídica** ou parceiro envia a documentação exigida, sendo:

a) Contrato Social de Constituição da empresa e demais alterações;

b) Comprovante de endereço;

c) Balanço ou declaração de faturamento assinado pelo contador, com detalhamento mensal dos últimos 12 (doze) meses;

d) Último recibo de entrega da declaração sobre operações realizadas com criptoativos,enviadas para Receita Federal referente a Instrução Normativa 1.888/2019;

e) Dos sócios: RG ou CNH, ambos com CPF; Selfie com o documento; Comprovante deresidência;

f) Endereço da Wallet;

g) Dados da empresa e de seu quadro societário;

h) Faturamento declarado dos últimos 12 (doze) meses atualizados;

i) Se em seu quadro societário há Pessoas Expostas Politicamente (PEP);

j) Se houve alteração no quadro societário nos últimos 12 (doze) meses;

k) Se os sócios da empresa possuem histórico criminal relacionado a práticas ilícitas previstas na Lei nº 9.613/98, Lei nº 12.846 e correlatas;

l) Wallets cadastradas de sua titularidade;

m) Se há, em sua empresa, regulamentação ou normas específicas sobre

práticasde Anticorrupção, Lavagem de Dinheiro e Financiamento ao Terrorismo;

n) Se a empresa possui Programa de Compliance e como é feito;

o) Como se dá o Processo de “Conheça seu cliente” (“KYC”), "Conheça seu Parceiro” (“KYP”)e "Conheça seu Fornecedor” (“KYS”), além de outras informações pertinentes.

10.10. O cliente **Pessoa Física** envia a seguinte documentação exigida:

a) Nome completo;

b) Data de Nascimento;

c) Documento de Identificação Pessoal Oficial com data de emissão não superior a 10 (dez) anos;

d) CPF;

e) E-mail;

f) Telefone;

g) Endereço completo (logradouro, nº, complemento, bairro, cidade, Estado e CEP);

h) Nome da mãe;

i) Estado Civil;

j) Sexo;

k) Profissão;

l) Foto Selfie segurando documento de identificação pessoal oficial;

m) Wallets cadastradas de sua titularidade;

n) Última declaração de Imposto de Renda Pessoa Física ou comprovação de fundos;

o) Recibo da IN 1888/2019 da RFB.

10.11. Após o envio dos documentos e preenchimento do formulário pelo candidato a

cliente, o documento é encaminhado ao Diretor da **TRKBIT**, Sr. **THIAGO GABRIEL BRAZ**, para elaborar a etapa ”2” do processo de Onboarding.

10.12. Após o envio da documentação, a equipe interna verifica a veracidade dos documentos apresentados para averiguar se pertencem ao cliente que efetuou o cadastro e se de fato essas informações coincidem com as informações na base de dados da Receita Federal do Brasil, Banco Central do Brasil e Sistema Público do Brasil, verificando, ainda, se o usuário se encontra em jurisdiçãoproibida.

10.13. Após a conclusão da verificação para garantir a autenticidade e veracidade dos documentos perante a Receita Federal do Brasil, Banco Central do Brasil e Sistema Público do Brasil, bem como a confirmação de que o usuário não está utilizando um endereço de uma jurisdição proibida, será iniciada a 2ª (segunda) etapa do processo de onboarding.

→ **Segunda Etapa - Verificação financeira e jurídica do sistema interno**

10.14. Verificam-se as seguintes informações financeiras e jurídicas do cliente:

a) Renda Mensal estimada e declarada (em R$);

b) Patrimônio estimado e declarado;

c) Análise do endereço do cliente;

d) Análise do histórico de declarações do Imposto de Renda;

e) Análise de possíveis protestos;

f) Análise do histórico de trabalho do cliente, bem como a sua remuneração estimada;

g) Verificação de recebimento de benefício ou auxílio social governamental;

h) Verificação da existência de processos judicias em nome do cliente que possam ser impeditivosde realização do negócio;

i) Verificação da declaração de que não é Pessoas Expostas Politicamente;

j) Consulta nas listas impeditivas nacionais e internacionais, como: CNJ, COAF, FBI e ONU;

k) Consulta nos Sites: Receita Federal, Portal da Transparência, Órgãos Reguladores, SCPC/Serasa, Tribunais Estaduais, Eleitorais, Trabalhistas, Superiores e Mídias;

l) Análise do relatório de faturamento dos 12 (doze) últimos meses, assinado e datadopelo contador responsável e dos respectivos sócios.

m) **Background Check**: que retorna informações como **(i)** PEP (Pessoas Expostas Politicamente); **(ii)** Mandado de Prisão Expedido; **(iii)** Consultas às Listas de Sanções Nacionais e Internacionais:

- COAF – Conselho de Controle de Atividades Financeiras
- CEAF – Centro de Estudos e Aperfeiçoamento Funcional
- CNEP – Cadastro Nacional de Empresas Punidas
- MTE- Ministério do Trabalho
- CNJ – Conselho Nacional de Justiça
- TSE – Tribunal Superior Eleitoral
- CEIS – Cadastro de Empresas Inidôneas e Suspensas
- EU – Lista de sanções da União Européia
- FBI – Polícia Federal dos Estados Unidos
- GOV UK – Lista de sanções do Reino Unido
- INTERPOL – Organização Internacional de Polícia Criminal
- OFAC – Agência de Controle de Ativos Estrangeiros dos EUA
- UNSC- Conselho de Segurança das Nações Unidas
- Consulta nos Sites: Receita Federal, Portal da Transparência, Órgãos reguladores, SCPC/Serasa, Tribunais Estaduais, Eleitorais, Trabalhistas, Superiores e Mídias;

n) Verificação de existência de ações judiciais e administrativas.

10.15. Na etapa 2, o sistema revisita as informações elencadas para verificar se há algum impedimento jurídico, financeiro ou alguma atividade atípica em nome do candidato.

10.16. Cada candidato a cliente será verificado antes da aprovação, com base no preenchimento do Formulário de Identificação e verificação da veracidade das informações através do fornecedor homologado e contratado pela **TRKBIT**:

- **FORNECEDOR:** IDWALL TECNOLOGIA LTDA, CNPJ: 24.934.106/0001-20- endereço AV PAULISTA NÚMERO 2537 COMPLEMENTO ANDAR 12 CONJ 121 E 122 - CEP 01.311-300-BAIRRO/DISTRITO- BELA VISTA MUNICÍPIO- SAO PAULO- UF- SP.

10.17. Uma vez adquiridas tais informações, a área responsável envia os documentos e demais informações coletadas para o escritório externo de advocacia, responsável pelo seu processamento para fins de realização do procedimento de Parecer Opinativo acerca do "Know Your Client" da **TRKBIT**, dispondo acerca de sua aprovação

ou reprovação a ser auferida com base em uma pesquisa realizada em plataformas de busca especializadas, destinadas à verificação de integridade dos indivíduos consultados.

10.18. A verificação da veracidade das informações prestadas pelo responsável do Compliance ao escritório externo de advocacia, são verificadas a partir do sistema do fornecedor homologado:

- **FORNECEDOR:** COMBATE A FRAUDE S.A. - CNPJ: 34.102.645/0001-57. R. Tiradentes, 1077 - 5º andar – Centro - Venâncio Aires - RS, 95800-000;

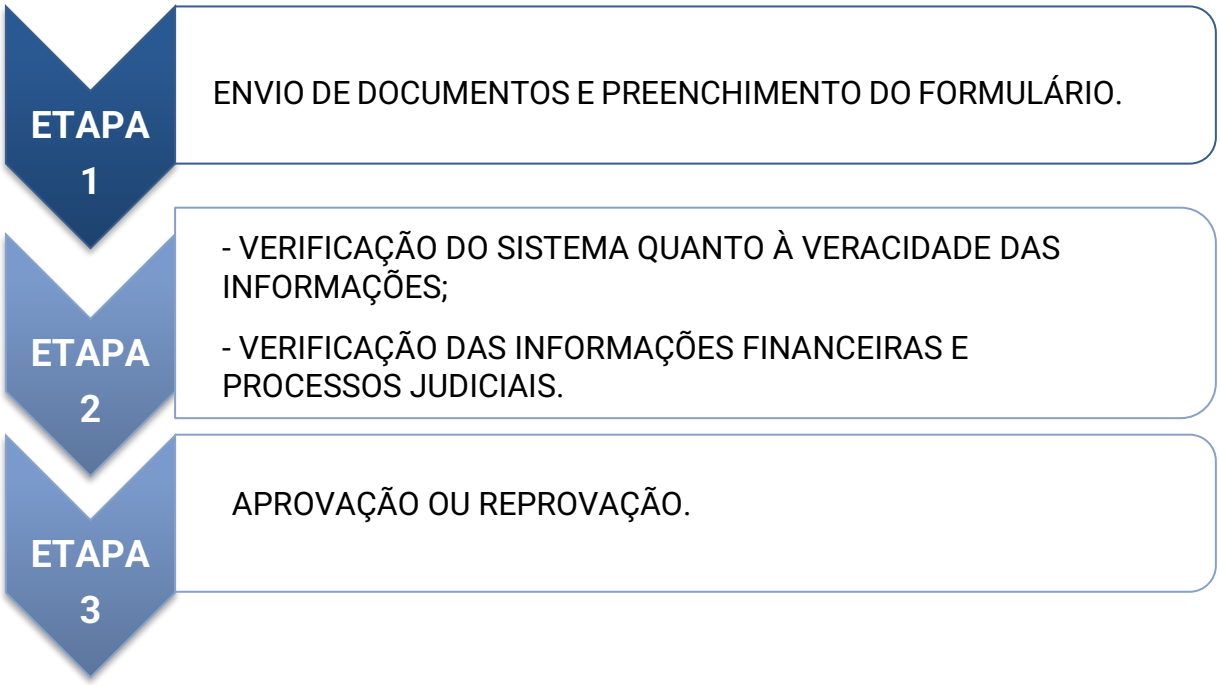
10.19. Os Pareceres Opinativos elaborados pelo excritório de advocacia externo sempre consignarão, em suas conclusões, as ponderações acerca do cliente e das informações consultadas, apontando, assim, por sua aprovação ou reprovação. O referido documento será enviado ao único sócio e administrador da **TRKBIT**, o Sr. **THIAGO GABRIEL BRAZ**, que será o responsável final pela decisão acerca do fornecimento dos serviços pela **TRKBIT**.

10.19.1. O escritório de advocacia externo **apenas** elabora pareceres opinativos, de forma que a responsabilidade de seguir ou não com as recomendações expostas são exclusivas dos sócios. O escritório de advocacia externo e a advogada externa **não** possuem, em nenhuma hipótese, condão decisório.

10.20. O monitoramento das informações e documentos coletados do cliente para a análise de compliance é realizado a cada 90 (noventa) dias, devendo ser reenviada a documentação obrigatória.

10.21. Quanto mais precisas e atualizadas forem as informações coletadas e registradas, maior será a capacidade de identificação de atos ilícitos**.**

→ **Fluxo Operacional**



10.22. Após a verificação do sistema, o cliente poderá ser aprovado, estabelecendo limites operacionais e sujeito a monitoramento rigoroso de todas as transações, sempre enviadas à Receita Federal do Brasil mensalmente.

10.23. Se o cliente for reprovado durante o processo de verificação, o cadastro é automaticamente bloqueado na plataforma.

10.24. Não são permitidos cadastros em nome de terceiros e em caso de comprovante de endereço em nome de outrem, será verificado o parentesco ou será exigida a comprovação da residência através de contrato de locação ou outro documento pertinente ao caso.

10.25. Não são permitidas transferências para contas de terceiros e nem envios de ativos digitais paracontas de terceiros. Todas as transações são realizadas com a mesma titularidade do usuário.

10.26. Não são permitidos cadastros de menores de 18 (dezoito anos) ou incapazes.

10.27. A **TRKBIT** se reserva ao direito de não atender ou aceitar Pessoas Expostas Politicamente (“PEP”).

10.28. A **TRKBIT** não realiza parcerias e não possui relações com países que estejam na lista de sanções nacionais, ou com clientes que estejam na lista de sanções nacionais e internacionais.

10.29. O formulário KYC, quando preenchido fisicamente, será arquivado na ficha do cliente, de acordo com os procedimentos estabelecidos pela **TRKBIT**.

II – “CONHEÇA SEU PARCEIRO” (KYP)

10.30. O KYP (Know Your Partner) tem como finalidade estabelecer critérios para contratação ou manutenção de Parceiros de Negócios, visando combater fraudes, crimes relacionados à Lavagemde Dinheiro e Financiamento ao Terrorismo.

10.31. Um processo de KYP feito de maneira eficiente permite à **TRK** conhecer a identidade do parceiro, compreender a natureza das atividades, garantir a legitimidade da fonte de renda, detectar padrões suspeitos ou potencialmente fraudulentos e interromper a fraude antes que ocorra. Além disso, a diligência prévia e periódica ajuda a assegurar a identificação, qualificação e classificação dos parceiros, prevenindo Lavagem de Dinheiro e Financiamento ao Terrorismo, e evitando o envolvimento com pessoas mencionadas em listas sancionadoras, incluindo as do Conselho de Segurança das Nações Unidas.

10.32. Os procedimentos e diretrizes relacionadas ao KYP pela **TRK** são:

a) Verificar bons antecedentes de integridade dos Parceiros de Negócios;

b) Monitoramento de Parceiros de Negócios relevantes;

c) Monitoramento de contratações e rescisões contratuais de Parceiros de Negócios;

d) Atualização cadastral;

e) Assegurar que os Parceiros de Negócios sejam contratados por exigência legal ou sob ajustificativa de se tratarem profissionais qualificados para os serviços, sendo assim adequados para atender as necessidades legítimas da **TRK**;

f) Assegurar que os Parceiros de Negócios detenham as habilidades, recursos, experiência, credenciais e qualificações apropriadas para cumprir suas obrigações com relação aos serviços a serem prestados a **TRK**;

g) Consultar as informações disponíveis em sites especializados em prevenção à Lavagem de Dinheiro e Financiamento do Terrorismo e lista de sanção imposta por resoluções doConselho de Segurança das Nações Unidas;
h) Realizar a análise da situação de crédito e endividamento;

i) Prevenir a utilização do sistema financeiro por estes indivíduos para crimes de lavagem de dinheiro, financiamento a atividades terroristas, tráficos de drogas e armamentos e demais atividades criminosas; e

j) Prevenir a responsabilização da **TRK** por atos de terceiros, com base na legislação vigente, incluindo a Lei Anticorrupção Lei nº 12.846/2013.

10.33. Os Colaboradores da **TRK** devem agir para prevenir quaisquer situações que possam causar ou sugerir conflito de interesses nas relações entre Colaboradores, Fornecedores, Parceiros de Negócio, Prestadores de Serviços, Órgãos Públicos ou concorrentes e que, se não revelados, podem vir a abalar a confiança e credibilidade dos Colaboradores e da **TRK.**

III – "CONHEÇA SEU EMPREGADO" (KYE)

10.34. O procedimento KYE (Know Your Employee) da **TRKBIT** engloba um conjunto de regras, procedimentos e controles destinados à contratação e acompanhamento de situações que possam caracterizar algum tipo de risco ou desvio. Esse procedimento tem como objetivo principal a prevenção à lavagem de dinheiro, financiamento ao terrorismo e outros atos ilícitos.

10.35. O processo busca minimizar riscos associados a atos ilícitos, como lavagem de dinheiro,fraudes e divulgação do sigilo dos clientes e dos negócios da empresa.

10.36. Para atingir esse objetivo, a contratação de novos colaboradores deve seguir as fases abaixo:

a) Estudo justificativo da necessidade de aquisição de profissionais com quantidades de proficiências necessárias ao atendimento dos objetivos de uma determinada área;

b) O estudo justificativo deve ser desenvolvido pelo responsável da área que deseja realizar a aquisição de novos colaboradores, devendo conter uma análise detalhada do atual estado da equipe sob seu comando levando-se em conta os KPIs adotados para medição dedesempenho e qualidade dos serviços desenvolvidos determinando em sua justificativa o perfil e as proficiências de cada um dos colaboradores que precisam ser contratados.

c) Análise do referido estudo por parte da diretoria responsável e a compatibilização da requisição da área ao planejamento estratégico e ao orçamento econômico-financeiro anual;

d) A análise do estudo dever ser feita de forma a determinar se a requisição feita pelo estudo justificativo é necessário. Se os perfis dos profissionais requisitados atendem a cultura e os objetivos da empresa e se o estudo pode ser compatibilizado ao planejamento estratégico eeconômico-financeiro;

e) É de responsabilidade do diretor da área impactada a validação junto as demais diretorias e áreas que porventura sofram algum impacto direto ou

indireto. Também é de responsabilidade do diretor apontar qualquer modificação ao estudo que se faça necessárioe a aprovação parcial, total ou recusa do mesmo;

f) Elaboração de cronograma de aquisição e onboarding dos novos colaboradores;

g) Uma vez o estudo aprovado será desenvolvido o cronograma de aquisição, estabelecendo o período inicial e final de disponibilização das vagas. Tal cronograma será desenvolvido pelo diretor da área, a diretoria financeira e a diretoria de RH, na ausência do responsável pela diretoria de RH a presença deve ser substituída pelo colaborador que esteja responsabilizado, mesmo que momentaneamente pelas tarefas do cargo.

h) Execução do processo seletivo e efetivação da contratação dos colaboradores;

10.37. O processo seletivo deverá cumprir necessariamente 04 (quatro) fases: **i)** análise de proficiênciatécnica; **ii)** análise curricular; **iii)** análise documental; e a **iv)** análise de soft skills. As fases devem ser realizadas necessariamente nessa ordem e serão realizadas pelo responsável da área com acompanhamento do diretor da área.

10.38. A execução do processo seletivo poderá ser facilitada por uma empresa terceira especializada em recursos humanos na ausência ou na sobrecarga da área ou diretoria interna responsávelpelo assunto. Independente do caso, o poder decisório sobre a contratação de um colaborador será do diretor e do responsável da área.

10.39. Um Comitê voltado a análise de aquisições de colaboradores formado por diretores, o Comitê de Compliance, Comitê de Segurança da informação e o Comitê de Conduta Ética poderão aplicar restrições a contratação de colaboradores.

10.40. A **TRKBIT** valoriza a averiguação comportamental, a repreensão de condutas antiéticas e a gestão de conflitos de interesses que tenham o potencial de comprometer a integridade da cultura organizacional da empresa. Essa abordagem reforça o compromisso da **TRKBIT** em manter uma cultura organizacional sólida e íntegra.

10.41. Neste sentido, nosso Departamento de Compliance:

a) Aplica due diligence periódico;

b) Realiza questionários;

c) Realiza backcground checkings;

d) Realiza treinamentos e estabelece um diálogo aberto;

e) Avalia relacionamentos com órgãos públicos;

f) Utiliza cláusulas de anticorrupção em todos os instrumentos que regulam as relaçõesentre as partes.

IV – "CONHEÇA SUAS TRANSAÇÕES" (KYT)

10.42. O KYT (Know Your Transactions), ou Conheça Suas Transações, é um conjunto de procedimentos e práticas utilizados para identificar, verificar e monitorar as transações financeiras realizadas na **TRKBIT**.

10.43. O objetivo principal do KYT é garantir a integridade e conformidade das operações, prevenindo atividades ilícitas como a lavagem de dinheiro e o financiamento ao terrorismo. Isso inclui a análise detalhada das transações, identificação dos participantes envolvidos, verificação da legalidade e origem dos fundos, bem como o monitoramento contínuo para identificar padrões suspeitos ou atividades fora do comum. O KYT é fundamental para mitigar riscos e garantir a segurança e transparência nas operações financeiras.

10.44. Esse procedimento está previsto na Recomendação nº 20 do GAFI e se aplica a todas as operações realizadas pela **TRKBIT**, incluindo, mas não se limitando a:

a) Mercado de Balcão (OTC) para investidores que operam com altos volumes;

b) Serviços de intermediação que concectam usuários para realizar transações operacionais com criptoativos em geral, dentro do ambiente over-the-counter;

c) Custódia de criptoativos no Blockchain.

10.45. O processo de KYT envolve osseguintes procedimentos:

I – <u>Identificação do Cliente</u>

10.46. A **TRKBIT** realizará uma due diligence completa para identificar e verificar a identidade de todos os clientes, conforme exigido pela legislação aplicável e pelas melhores práticas do setor.

10.47. Na primeira fase do processo de KYT, procedemos à solicitação de documentos que atestem o poderio financeiro do cliente, compatível com a transação desejada. Entre esses documentos, incluem-se:

a) Balanço ou Balancete nos últimos 12 meses atualizados;

b) Declaração de IRPJ da Pessoa Jurídica;

c) Documento de identificação dos sócios;

d) Foto selfie do sócio segurando de forma legível o documento de identificação;

e) Comprovante de residência atualizado dos sócios (até os últimos 3 meses);

f) Certidão da IN 1888/2019 dos 3 (três) últimos meses;

g) Carteiras de criptoativos (caso de criptoativos);

h) Endereço do Wallet de sua titularidade (caso de criptoativos);

i) Contrato de prestação de serviço assinado (caso de criptoativos);

j) Formulário KYC Preenchido.

II – Monitoramento de Transações

10.48. A **TRKBIT** implementará sistemas de monitoramento contínuo para identificar padrões incomuns ou suspeitos de atividade em todas as transações realizadas em sua plataforma. Serão estabelecidos critérios para a detecção de transações atípicas, incluindo volume, frequência e natureza das transações.

III – Análise de Investigação

10.49. Todas as transações identificadas como suspeitas serão prontamente investigadas pela equipe de conformidade da **TRKBIT**. Serão realizadas análises aprofundadas para determinar a legitimidade e origem dos fundos envolvidos na transação suspeita.

IV – Relato de Transações Suspeitas

10.50. Caso a **TRKBIT** tenha motivos razoáveis para suspeitar que uma transação esteja relacionada a atividades criminosas ou financiamento ao terrorismo, ela comunicará prontamente suas suspeitas à unidade de inteligência financeira (UIF), conforme exigido por lei.

V - Verificações Adicionais de Segurança

10.51. Realizamos verificações do score do cliente junto ao SERASA, consultamos o CENPROT para identificar eventuais protestos em seu nome e averiguamos se o cliente foi beneficiário de algum tipo de auxílio ou benefício social. Essas verificações são conduzidas por meio do sistema Combate à Fraude, bem como consultas aos sistemas governamentais que disponibilizam informações relacionadas aos dados

dos clientes.

10.52. Após a verificação do lastro financeiro do cliente, será estabelecido um teto para transações e transferências. Caso o cliente ultrapasse esse limite estabelecido, haverá um bloqueio imediato em suas transações.

10.53. Limites seguros de transações desempenham um papel crítico na gestão de riscos financeiros para empresas como a **TRKBIT TECNOLOGIA E INFORMAÇÃO LTDA**. Esses limites são estabelecidos com o objetivo de proteger tanto a empresa quanto seus clientes contra possíveis fraudes, atividades ilícitas e perdas financeiras significativas. Aqui estão alguns pontos importantes a serem considerados ao discorrer sobre limites seguros de transações:

a) Mitigação de Riscos Financeiros: Estabelecer limites de transações é uma estratégia fundamental para mitigar os riscos financeiros associados às operações da empresa. Esses limites ajudam a evitar que transações de alto valor ou incomuns passem despercebidas, reduzindo assim a exposição a atividades fraudulentas ou suspeitas;

b) Proteção contra Lavagem de Dinheiro e Financiamento ao Terrorismo: Limites de transações ajudam a prevenir a lavagem de dinheiro e o financiamento do terrorismo, pois dificultam a realização de grandes transações que possam ser usadas para ocultar a origem ilícita dos fundos. Ao estabelecer limites razoáveis, a empresa pode identificar mais facilmente transações suspeitas e tomar as medidas necessárias para relatar e investigar essas atividades;

c) Proteção dos Clientes: Limites de transações também protegem os clientes da empresa, evitando que se envolvam em transações financeiras de alto risco que possam resultar em perdas significativas. Ao estabelecer limites adequados, a empresa pode garantir que seus clientes não sejam expostos a transações potencialmente prejudiciais ou fraudulentas.

d) Conformidade Regulatória: Estabelecer limites de transações está em conformidade com os requisitos regulatórios e normas internacionais, como as diretrizes do GAFI (Grupo de Ação Financeira contra a Lavagem de Dinheiro e o Financiamento do Terrorismo). Muitas autoridades reguladoras exigem que as empresas implementem medidas para monitorar e controlar as transações financeiras de seus clientes, incluindo a definição de limites apropriados.

e) Gerenciamento de Fluxo de Caixa: Além de mitigar riscos, os limites de transações também ajudam no gerenciamento do fluxo de caixa da empresa, garantindo que ela possa honrar seus compromissos financeiros sem comprometer sua

11. ABORDAGEM DE RISCO

11.1. Em compasso com as recomendações do GAFI/FATF e demais normas referência, a Política se perfaz em especial através do procedimento de Abordagem de Risco (identificação de fatores de determinação do risco), a fim e detectar as suspeitas nas operações e reportá-las.

11.2. Os riscos são subdivididos em:

a) <u>Alto Risco - REPROVADOS:</u> Os riscos são significativos, normalmente reprovados no Onboarding. A **TRKBIT** deve aplicar controles mais restritivos para reduzir o risco, tais como diligência reforçada e o monitoramento mais rigoroso.

Serão considerados de Alto Risco:

I) Clientes domiciliados ou sediados em cidades de fronteira com outros países;
II) Clientes que sejam pessoa politicamente exposta;
III) Clientes que declaram ter, pelo menos, uma das seguintes atividades:

- Sem atividade formal;
- Comercialização de joias, pedras e metais preciosos, objetos de arte e antiguidades;
- Compra e venda de imóveis;
- Revenda de automóveis usados;
- Comércio de armamento;
- Empresas de turismo;
- Importação e Exportação;
- Clubes esportivos;
- Igrejas e congregações religiosas;
- Casas de apostas, cassinos ou jogos de azar.

b) <u>Médio Risco:</u> Os riscos precisam de análise adicional e a decisão deve ser tomada pela **TRKBIT**.

Serão considerados de Médio Risco:

I) Empresas sem comprovação de lastro suficiente para garantir as operações;
II) Empresas com ações judiciais não impeditivas da atividade;
III) Empresas cujos sócios não possuem histórico com movimentação em criptoativos.

c) <u>Baixo Risco ou Padrão:</u> Representa o Risco Base em relação ao qual as regras comerciais normais são aplicáveis.

Serão considerados de Baixo Risco ou Padrão:

I) Clientes que tenham comprovado renda e a origem dos valores;
II) Clientes com o código de atividade econômica correto;
III) Clientes que enviaram os Recibos exigidos pela IN 1888/2019 da RFB.
IV) Clientes que enviaram a documentação de identificação completa e não possuem ações judiciais;

11.3. Cada cliente e parceiro da **TRKBIT** recebe uma designação de risco de acordo com o seu perfil, o que orienta, em grande parte, as diligências a serem aplicadas de maneira específica. O tratamento baseado no equilíbrio de riscos assegura que os casos com maior impacto negativo sejam tratados de forma diferenciada. Essa abordagem personalizada permite ajustar as medidas de due diligence e monitoramento conforme a avaliação de risco associada a cada cliente e parceiro, garantindo uma resposta proporcional às características específicas de cada caso.

12. MECANISMOS E MÉTRICAS DE AVALIAÇÃO DE RISCO

12.1. Os mecanismos e métricas de avaliação de risco foram desenvolvidos em alinhamento com as especificidades do modelo de negócio da **TRKBIT** e seu porte. Essa mensuração ocorre através da criação de matrizes que apresentam ponderações sobre os fatores de risco, conferindo uma estrutura para a análise sistemática dos riscos envolvidos nas operações da empresa, e são projetadas para considerar vários aspectos, como:

a) Persecução penal:
- Terrorismo, inclusive financiamento do terrorismo;
- Tráfico de seres humanos e contrabando de migrantes;
- Exploração sexual, inclusive de crianças;
- Lavagem de dinheiro;
- Participação em grupo criminoso organizado e crime organizado;
- Tráfico de narcóticos e substâncias psicotrópicas;
- Tráfico de armas;
- Corrupção e suborno;
- Fraude;
- Improbidade administrativa;
- Crimes contra o SFN (Lei 7.492/86);
- Falsificação de moeda;
- Falsificação e pirataria de produtos;
- Crimes ambientais;
- Lobismo (atos de pressão sobre pessoas ou poderes públicos);
- Homicídio, lesão corporal grave;

- Sequestro, privação ilegal de liberdade e tomada de reféns;
- Roubo ou furto;
- Contrabando;
- Crimes fiscais (relacionados a impostos diretos e indiretos);
- Extorsão;
- Falsificação;
- Pirataria; e
- Utilização de informação privilegiada e manipulação do mercado;

b) PEP ou PPE (Pessoa Exposta Politicamente): É dada uma especial atenção quanto às operações realizadas pelas pessoas que se enquadrem nesta categoria e àqueles que possuem relacionamento próximo com PEPs, uma vez que são agentes que estão mais expostos à prática de atos ilícitos e oferecem maior risco ao Sistema Financeiro Nacional. A **TRKBIT** se reserva ao direito de não aprovar PEP. São consideradas politicamente expostas aquelas pessoas que desempenham ou tenham desempenhado, nos últimos 05 (cinco) anos, cargos, empregos ou funções públicas relevantes, no Brasil ou em outros países, territórios e dependências estrangeiros, assim como seus representantes, familiares e outras pessoas de seu relacionamento próximo.

c) Domicílio em País não cooperante (Specially Designated Nations);

d) Sanções em listas restritivas;

e) Localização Geográfica;

f) Mídia negativa.

13. CONFLITOS DE INTERESSES

13.1. Os Conflitos de Interesses podem surgir quando interesses particulares ou alheios à **TRKBIT** influenciam concentradamente o julgamento ou a transparência no desempenho dos Administradores, Colaboradores e terceiros em relação aos negócios da empresa. A imparcialidade da pessoa pode ser prejudicada, especialmente nos seguintes casos.

a) Relacionamento de parentesco ou por afinidade;

b) Uso de informação confidencial;

c) Conflito de interesses na indicação e contratação de Colaboradores;

d) Conflito de interesses na indicação e contratação de Fornecedores ou Prestadores de Serviços;

e) Conflitos de interesses com Agentes Públicos.

13.2. A presente Política estabelece regras para identificar, gerenciar e mitigar potenciais ou conflitos de interesses, com o objetivo de preservar e proteger os interesses da **TRKBIT**, garantindo transparência e independência em suas relações.

13.3. Os Colaboradores da **TRKBIT** devem agir proativamente para prevenir situações que possam causar ou sugerir conflitos de interesses nas relações entre Colaboradores, Fornecedores,Parceiros de Negócio, Prestadores de Serviços, Órgãos Públicos ou concorrentes. A não revelação dessas situações pode abalar a confiança e recompensa dos Colaboradores e da **TRKBIT**.

13.4. A Área de Compliance será a responsável por indicar os parâmetros sobre conflitos de interesses na **TRKBIT**.

13.5. Ao identificar alguma situação que possa configurar um conflito de interesses, o Colaborador deverá relatar a ocorrência por meio do Canal de Denúncias. Isso contribui para a transparência e a integridade das relações na empresa.

14. REGISTRO E MONITORAMENTO DE TRANSAÇÕES

14.1. As transações e operações financeiras realizadas pelos clientes da **TRKBIT** devem ser registradas e continuamente monitoradas para identificar possíveis indicativos de lavagem de dinheiro ou financiamento ao terrorismo. Esse monitoramento considera as situações definidas nas normas do setor, especialmente a condição de pessoas politicamente expostas.

14.2. Para garantir a origem lícita dos criptoativos negociados, a **TRKBIT** utiliza mecanismos de mercado como parte do processo de KYT (Conheça Seu Cliente). Isso garante que os ativos transacionados não possuam ou não tenham sido utilizados em atividades ilícitas.

14.3. A empresa realiza um segundo processo interno que consiste no monitoramento de um banco de dados próprios contendo endereços de carteiras utilizadas em crimes como pirâmide financeira, fraudes e subtração de ativos no Brasil.

14.4. Se positivo em qualquer uma das duas validações mencionadas, o cadastro do cliente é encerrado imediatamente e um aviso a UIF – Unidade de Inteligência Financeira é realizado.

14.5. Como forma de precaução, em consonância com a legislação brasileira e organismosinternacionais, a **TRKBIT** adota as seguintes práticas:

a) Realiza as operações de compra e venda de cripto ativos exclusivamente

através transferências bancárias provenientes de contas em que o titular seja o próprio cliente excluindo a possibilidade de recebimento de transferências de contas conjuntas;

b) Determina alçadas de negociação de acordo com a documentação de capacidade financeira fornecida pelo cliente;

c) Não realiza negociações de volumes acima das alçadas operacionais estipuladas sem comprovação de capacidade financeira prévia por parte do cliente;

d) Realiza extensa análise dos documentos e informações fornecidas pelo cliente e de seu negócio no momento do cadastro;

e) Monitora as operações realizadas pelos clientes a luz das alçadas determinadas durante a análise de compliance;

f) Monitora as movimentações realizadas pelos clientes a luz de análise histórico dos valores médios operados;

g) Na constatação de desvio em valor de operação frente a análise histórica, ainda que dentro das alçadas estabelecidas na análise de compliance requerendo a atualização cadastral com o fornecimento de informações adicionais referentes origem dos valores operados; e

h) Na ausência de justificativas documentais suficientes que subsidiem determinadasoperações ou até mesmo o aumento injustificado da média das operações as mesmas serãointerrompidas.

15. TREINAMENTO

15.1. O treinamento de Prevenção à Lavagem de Dinheiro (PLD) e Combate ao Financiamento ao Terrorismo (CFT) na **TRKBIT** é contínuo e aplicado a todos os colaboradores elegíveis, envolvendo mitigar riscos e evitar desvios na Política.

15.2. Os treinamentos têm por objetivo:

a) Esclarecer as responsabilidades legais de cada um dos envolvidos;

b) Prover suporte e conhecimento sobre os procedimentos e regulamentações aplicáveis;

c) Aprofundar o conhecimento que os colaboradores têm das exigências e responsabilidades legais e regulamentares, bem como das diretrizes da **TRKBIT** referente ao tema de PLD/CFT;

b) Capacitar os colaboradores a identificar, prevenir, tratar e comunicar situações de riscoou com prevenção de ocorrência de lavagem de dinheiro ou financiamento do terrorismo nas atividades realizadas.

15.3. A **TRKBIT** compreende que o treinamento de seus colaboradores é crucial para que esta Política seja eficaz e cumpra com os seus objetivos.

16. PROTEÇÃO DE DADOS PESSOAIS

16.1. A coleta, acesso e tratamento de dados pessoais de clientes, colaboradores e fornecedores de pessoas físicas pela **TRKBIT** são necessários para cumprir as obrigações desta Política, estando em conformidade com a Lei Geral de Proteção de Dados (Lei nº 13.709, de 14 deagosto de 2018).

16.2. Não obstante, a **TRKBIT**, seus colaboradores e fornecedores têm o dever de zelar pela segurança e privacidade dos dados pessoais tratados. A utilização desses dados deve ocorrer dentro dos limites necessários à proposta específica, com transparência e em conformidade com a legislação vigente, incluindo a Política de Privacidade da **TRKBIT**.

17. COMUNICAÇÃO

17.1. As situações com indícios ou evidências de atos ilícitos identificadas durante o relacionamento devem ser comunicadas imediatamente ao Comitê de Ética e Compliance.

17.2. O Comitê de Ética e Compliance deliberará sobre a comunicação à Unidade de Inteligência Financeira Conselho de Controle de Atividades Financeiras (“COAF”) de atividades suspeitas e atípicas, com base em relatório de identificação das atividades mencionadas na seção “MONITORAMENTO E TRATAMENTO DE INDÍCIOS DE LAVAGEM DE DINHEIRO”. O prazo de comunicação é de até 45 (quarenta e cinco) dias contados da identificação da atividade. Independente da comunicação, a **TRKBIT** fará a guarda da documentação relativa às atividades.

17.3. Serão aplicadas sanções disciplinares aos indivíduos que tentarem ou praticarem retaliação contra quem, de boa-fé, denunciar ou manifestar queixa, suspeita, dúvida ou preocupação relativas a possíveis violações às diretrizes desta Política; e fornecer informações ou assistência nas apurações relativas a tais possíveis violações.

17.4. Também deverão ser aplicadas sanções aos indivíduos que, comprovadamente, utilizarem de má-fé ao comunicarem possíveis violações às

diretrizes desta Política ou comunicarem fatos sabidamente falsos.

17.5. Os fornecedores que omitirem informações ou agirem em contrariedade a esta Política, além das sanções legais, poderão ter seu contrato de prestação de serviço rescindido, sujeito a multa, observadas as disposições contratuais.

18. COMUNICAÇÃO AO COAF

18.1. Casos suspeitos identificados no monitoramento realizado pela **TRKBIT** e que apresentarem indícios de Lavagem de Dinheiro ou Financiamento ao Terrorismo serão submetidospara análise de Área de Compliance.

18.2. Após a análise da Área de Compliance e identificação de ilícitos,será realizada comunicação para registro no site do COAF. Caso a situação suspeita envolva Pessoa Exposta Politicamente (PEP), esta informação também deverá ser reportada no acesso ao sistema do COAF.

18.3. A comunicação ao COAF será realizada no prazo legal e sem dar ciência aos envolvidos ou a terceiros. Em caso de inexistência de comunicações em determinado ano, a **TRKBIT** providenciará o envio de declaração negativa, até 10 (dez) dias úteis após o encerramento do referido.

19. DEPARTAMENTO DE COMPLIANCE

19.1. O Departamento de Compliance da **TRKBIT** é exercido por canal direto na própria empresa,tendo como responsável pelo Compliance o Sr. **THIAGO GABRIEL BRAZ**, único sócio administrador da **TRKBIT**. Além disso, a **TRKBIT** contrata um escritório de advocacia externo para a elaboração de pareceres opinativos sobre aprovação e reprovação dos clientes, com a utilização do seguinte fornecedor homologado:

- **FORNECEDOR:** COMBATE A FRAUDE S.A. CNPJ: 34.102.645/0001- 57. R. Tiradentes, 1077 - 5º andar – Centro - Venâncio Aires - RS, 95800-000 e ETHQUO ETHICAL QUOTIENT SERVICOS DE COMPLIANCE E TECNOLOGIA LTDA - 39.545.663/0001-27

19.2. O Departamento de Compliance atua com as seguintes responsabilidades:

a) Executar os controles dos processos de KYC e PLD/CFT;

b) Identificar e avaliar os riscos de Compliance das gerências proprietárias de riscos;

c) Direcionar e treinar os stakeholders, diretoria, gerências e todos os colaboradores em assuntos de Compliance;

d) Monitorar continuamente e relatar novos riscos de Compliance identificados nos negócios;

e) Elaborar junto às gerências responsáveis por cada área de negócio as políticas e procedimentos que devem estar alinhadas ao Código de Conduta e Ética da **TRKBIT**, mitigando os riscos já mapeados;

f) Assessorar a Administração e as áreas de negócio nas tomadas de decisão que envolvem riscos.

19.3. A **TRKBIT** entende que o Compliance dentro da empresa deve ser independente, com funções que incluem:

a) Viabilizar a aderência e cumprimento de leis, regras e normas aplicáveis ao negócio;

b) Avaliar a observância de Princípios éticos e Normas de Conduta;

c) Implementar e atualizar regulamentos e normas internas;

d) Estabelecer Procedimentos e Controles Internos;

e) Aplicar testes periódicos e elaborar planos de contingência;

f) Avaliar a segregação de funções a fim de evitar conflitos de interesses;

g) Avaliar Riscos e Controles Internos, através de relatório (Gestão de Compliance);

h) Desenvolver Políticas Internas que previnam problemas de não conformidade;

i) Fomentar o desenvolvimento da Cultura de: **(i)** prevenção a lavagem de dinheiro através de treinamentos específicos; **(ii)** controle, juntamente com os demais pilares do sistema de controles internos, na busca da conformidade; **(iii)** interlocução com Órgãos Reguladores e Fiscalizadores, Associações de Classe e importantes participantes do mercado; **(iv)** promoção da profissionalização da função e auxílio na criação de mecanismos de revisão de regras de mercado, legislação e regulamentações pertinentes.

20. ATUALIZAÇÃO CADASTRAL

20.1. A **TRKBIT** deve identificar alterações substanciais e relevantes nas informações que possuem a respeito de seus clientes, a fim de alimentar

adequadamente os seus sistemas e mensurar os riscos envolvidos nos seus relacionamentos. As informações deverão ser atualizadas anualmente.

20.2. A acurácia dos dados cadastrais são o substrato para a realização do monitoramento das operações, viabilizando a identificação analítica de situações que configurem indícios de lavagem de dinheiro e financiamento ao terrorismo.

21. CANAL DE DENÚNCIA

21.1. A **TRKBIT TECNOLOGIA E INFORMAÇÃO LTDA** conta com um canal de comunicação que permite o recebimento de denúncias no que tange às irregularidades, admitindo-se inclusive denúncias anônimas, sendo proibida a retaliação de denunciantes. O canal é destinado tanto ao público interno quanto ao público externo: fale@trkbit.co

21.2. A **TRKBIT TECNOLOGIA E INFORMAÇÃO LTDA** garante a confidencialidade e a proteção ao denunciante de boa-fé, valendo- se de um procedimento transparente no que concerne ao acompanhamento da denúncia.

21.3. A denúncia será tratada pelo Departamento de Compliance, que é responsável por tomar os depoimentos das partes envolvidas, examinar a documentação existente, se houver, e realizar o que for necessário para que sejam tomadas providências e penalidades cabíveis a depender da decisão final da Diretoria da **TRKBIT TECNOLOGIA E INFORMAÇÃO LTDA**.

22. DIREITO APLICÁVEL E FORO

22.1. Esta Política é regida de acordo com a legislação brasileira. Dúvidas e situações não previstas nesta Política poderão ser encaminhadas para o e-mail: fale@trkbit.co , onde serão primeiramente resolvidas pela **TRKBIT** e, caso persistam, deverão ser solucionadas pelos Órgãos do sistema brasileiro de defesa do consumidor.

22.2. A presente versão deste instrumento foi elaborada pela Dra. Jessyca Arieira Araújo - OAB/RJ 201.582, responsável apenas pela elaboração das políticas.

22.3. Quaisquer disputas ou controvérsias oriundas de quaisquer atos praticados no âmbito da utilização das Aplicações pelos clientes e usuários da **TRKBIT**, inclusive com relação ao descumprimento desta Política ou à violação dos direitos da **TRKBIT**, de seus empreendimentos, de outros usuários e/ou de terceiros, de direitos de propriedade intelectual, de sigilo e de personalidade, serão processadas no foro da Comarca de São Paulo - SP, como sendo o único competente para dirimir qualquer controvérsia oriunda do presente instrumntto, renunciando expressamente a qualquer outro, por mais privilegiado que seja.

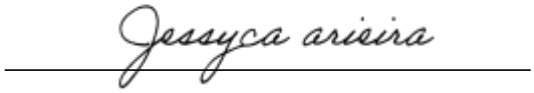
23. APROVAÇÃO E VIGÊNCIA

23.1. O presente documento possui aprovação da Diretoria Executiva e vigência indeterminada e deverá ser revisado anualmente ou sempre quando necessário.

São Paulo, 20 de janeiro de 2024.

_____

COO & Representante Legal
THIAGO GABRIEL BRAZ



Responsável pela elaboração das Políticas
JESSYCA ARIEIRA
OAB/RJ 201.582