POLÍTICA KYC

“KNOW YOUR CUSTOMER”

Conheça Seu Cliente

TRKBIT TECNOLOGIA E INFORMAÇÃO LTDA

ELABORADO EM 20.01.2023
REVISADO EM 20.01.2024

APRESENTAÇÃO

Este Procedimento de Conheça Seu Cliente, o KYC (“Know Your Customer”), está dentro do escopo do Programa de PLD/CFT e aplica-se aos serviços oferecidos pela **TRKBIT TECNOLOGIA E INFORMAÇÃO LTDA,** pessoa jurídica de direito privado, 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”**;

Esta Política, junto ao Código de Ética e Conduta, faz parte do Programa de Compliance da **TRKBIT**, o qual 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 TECNOLOGIA E INFORMAÇÃO LTDA**, 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 TECNOLOGIA E INFORMAÇÃO LTDA** são diretamente responsáveis pelo devido armazenamento e manipulação dos documentos enviados, devendo garantir o sigilo e a confidencialidade dos dados garantindo a exposição a terceiros ou outros colaboradores da empresa que não tenham alçada de acesso a essas informações.

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

Todos os estagiários, funcionários, prestadores de serviços, Exchange e sócios devem adotar as melhores práticas no momento do cadastro dos clientes e dedicar especial atenção aos conceitos eatividades que auxiliam na prevenção e combate à LD/FT. As leis e regulamentos atrelados a este delito, bem como as regras desta Política devem ser obrigatoriamente cumpridas.

A Política identificará o conceito de lavagem de dinheiro, 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 utilizados pela **TRKBIT** e definidas as regras para aplicação dos formulários "Conheça seu cliente".

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 edesenvolver campanhas/atividades que auxiliem na detecção de operações que caracterizem indícios deste crime.

A **TRKBIT** se compromete a cumprir integralmente as disposições legais pertinentes, incluindo o Marco Civil na Internet Lei nº 12.965/2014 e a Lei nº 13.709/2018 (LGPD - Lei Geral de Proteção de Dados), tendo como premissa a manutenção do sigilo e segurança das informações de seus clientes, 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, bemcomo observando o Decreto nº 11.563 de 2023 que fixou a competência do Banco Central do Brasilcomo 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 governança, 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;
V – Solidez e eficiência das operações; e
VI – Prevenção à lavagem de dinheiro e ao financiamento do terrorismo e da proliferação dearmas 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 3 (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, compras de instrumentos negociáveis ou compras de bens.Trata da remoção do dinheiro do local que foi ilegalmente adquirido e sua inclusão, por exemplo, no mercado financeiro.

A ocultação é o momento que o agente realiza transações suspeitas e caracterizadoras do crime delavagem. 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.

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. O objetivo central do Compliance é capacitar os colaboradores, prestadores de serviços,parceiros e administradores, através de treinamentos, disponibilização de conteúdo e determinação de diretrizes relativas a assuntos relacionados à conformidade legal dos negócios **TRKBIT TECNOLOGIA E INFORMAÇÃO LTDA**, acompanhando e revisando os relatórios do departamento quanto a eventuais descumprimentos regulamentares e legais.

1.2. Além do monitoramento das operações é realizado o processo de Due Dilligence na avaliação de clientes, parceiros, prestadores de serviços e negócios em processo de aquisição, como processo complementar na validação dos dados cadastrais fornecidos.

1.3. O Procedimento KYC tem como escopo principal proteger a **TRKBIT TECNOLOGIA E INFORMAÇÃO LTDA** do envolvimento com atividades ilícitas, bem como indivíduos, jurisdições ou entidades sancionadas, além de garantir que a **TRKBIT** cumpra integralmente todas as respectivas leis, regulamentos ou normas pertinentes ao escopo de PLD/CFT**.**

1.4. O procedimento visa, precipuamente, identificar os reais detentores dos ativos e recursos que circulam na **TRKBIT**, 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 pretendamutilizar os produtos e serviços da **TRKBIT**.

1.5. No procedimento se consigna a estratégia de verificação prévia, em que todos os clientes quedesejam transacionar com a **TRKBIT** têm suas informações meticulosamente analisadas, como forma de evitar a realização de negócios com agentes suspeitos ou potencialmente criminosos. Assim sendo, a **TRKBIT** se resguarda no direito de recusar a realizar transações com clientes cujos registros e fichas criminais contenham marcações ou apontamentos de ocorrências ou fatos negativos e desabonadores.

1.6. Além disso, a **TRKBIT** realiza ainda a chamada “Avaliação Baseada em Riscos”, criada para mitigar os riscos de lavagem de dinheiro e financiamento ao terrorismo. A **TRKBIT** utiliza direcionadores de risco e distribuí um 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 apetitede risco. A partir do risco associado ao cliente, a **TRKBIT** aprova o início e o prosseguimento do relacionamento. Neste documento estão definidos, também, os papéis e responsabilidades no que tange à decisão das medidas a serem empregadas.

1.7. 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.

1.8. A "Exchange" possui um livro de ofertas aberto, onde é possível lançar ordens de compra ou de venda de criptoativos, além de custodiar moeda corrente nacional e criptoativos dos clientes. Já a operação de intermediação, realizada pela **TRKBIT**, consiste exclusivamente na compra ou venda de criptoativos por conta e ordem de terceiro, de modo que não há custódia de moeda corrente nacional ou de criptoativos de terceiros.

1.9. As diretrizes e procedimentos desta Política foram criados conforme a Circular do Banco Centraldo Brasil nº 3.681/2013 e Resolução do Banco Central do Brasil nº 25/2020, e suas respectivas alterações. A presente Política foi elaborada de forma compatível com o porte, a natureza, a complexidade, a estrutura e o modelo de negócio da **TRKBIT**

1.10. A presente Política estabelece as diretrizes e padrões de controles e monitoramento que garantam a conformidade, funcionamento e visam mitigar os riscos da **TRKBIT.**

1.11. As regras aqui definidas devem ser atualizadas pela Área de Compliance da **TRKBIT**, através da análise de eventuais atualizações, revogações ou publicações de novas normas aplicáveis, bem como devem ser revisadas pela diretoria de acordo com periodicidade prevista na regulamentação em vigor.

1.12. Esta Política dispõe sobre as diretrizes referentes ao gerenciamento de risco de crédito, de liquidez e operacional, visando a conformidade da **TRKBIT** com as regulamentações e legislações vigentes, a proteção dos negócios e situação económico-financeira da **TRKBIT**

2. RESPONSABILIDADES

2.1. É responsabilidade da **TRKBIT** manter 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").

2.2. A **TRKBIT** enfatiza que tem como responsabilidade o combate à entrada de capital originário de atividades ilícitas, espúrias e criminosas, e adota as diligências necessárias para prevenir crimes financeiros e condutas contrárias aos valores de probidade interiorizados em sua filosofia de negócios.

2.3. Desta forma, a fim de que sejam aplicadas as 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) Criação de políticas e procedimentos claros;

e) Procedimentos de 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 Know YourEmployee (KYE).

2.4. 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. Além disso, utiliza uma ferramenta para execução da Análise de Due Diligence, baseando-se em bases reputacionais como listas de sanções nacionais, pessoas politicamente expostas (PEP) e listas restritivas internacionais, entre outras fontes pertinentes.

2.5. O monitoramento tem início com a coleta de documentos do cliente, que seguem as indicações dos artigos 16 e 18 da Circular nº 3.978 de 2020 do BACEN, que dispõe:

> **"Art. 16**. As instituições referidas no art. 1º devem adotar procedimentos de identificação que permitamverificar 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 dedados 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), no casode pessoa natural; e
> II - a firma ou denominação social e o número de registro no Cadastro Nacional da PessoaJurídica (CNPJ), no caso de pessoa jurídica.
>
> § 3º No caso de cliente pessoa natural residente no exterior desobrigada de inscrição no CPF, na forma definida pela Secretaria da Receita Federal do Brasil, admite-se a utilização de 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 de inscrição 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 identificaçãoou 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 deinformações 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 a evolução 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."

2.6. A **TRKBIT** reserva-se o direito de não atender ou aceitar Pessoas Expostas Politicamente.

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

2.8. O Diretor de Operações, Sr. **THIAGO GABRIEL BRAZ**, é responsável pelo Programa de Prevenção à Lavagem de Dinheiro e ao Financiamento do Terrorismo (PLDFT), qual deve cumprir e fazer cumprir as regras e procedimentos estabelecidos.

2.9. A responsabilidade pela elaboração e redação da política em comento é da Dra. Jessyca Arieira, OAB/RJ 201.582, contratada pela **TRKBIT**. A presente política deve ser revisada sempre que houver necessidade ou, no mínimo, anualmente.

2.10. Todos os Colaboradores da **TRKBIT** que desempenham quaisquer atividades correlatas aos riscos dispostos nesta Política tem o dever de zelar pela conformidade dos processos de gerenciamento de riscos.

2.11. Cabe aos Administradores/Alta Administração da **TRKBIT**:

- Fazer constar em relatório anual de gerenciamento de riscos de liquidez sua responsabilidade pelas informações divulgadas;
- Assegurar o cumprimento desta Política;
- Revisar e aprovar, anualmente ou na menor periodicidade exigida pela regulamentação, esta Política de Gerenciamento de Riscos;
- Aprovar todos os procedimentos a serem definidos referentes ao disposto nesta Política, como a matriz de riscos, matriz de classificação de Clientes, limites de tolerância ao risco, tratamento de riscos, plano de continuidade de negócios da **TRKBIT**, entre outros;
- Nomear o Diretor de Riscos, que terá as atividades da gestão de risco separadas das atividades da área de auditoria interna da **TRKBIT**

2.12. Cabe ao Diretor de Riscos (CRO) da **TRKBIT**:

- Definir objetivos e elaborar, em conjunto com a Área de Compliance, políticas e procedimentos relacionados ao planejamento estratégicos de risco, matriz de riscos, limites de tolerância ao risco, plano de respostas aos riscos e plano de continuidade de negócios;
- Monitorar o grau de aderência dos processos da estrutura de gerenciamento de riscos às políticas;
- Informar periodicamente à Alta Administração sobre as políticas, procedimentos e eventos objetos desta Política, bem como eventuais atualizações;
- Assegurar o cumprimento desta Política, pelos gestores com funções ou atividades de negócios que geram exposição a riscos, e pelos responsáveis pela definição dos métodos para identificação, avaliação e monitoramento do grau de exposição a riscos operacionais.

2.13. Cabe a área de Compliance, Riscos e Controles Internos:

- Elaborar todos os procedimentos a serem definidos referentes ao disposto nesta Política, como a matriz de riscos, limites de tolerância ao risco, tratamento de riscos, plano de continuidade de negócios da **TRKBIT**, entre outros;

- Monitorar a aderência das áreas e processos da **TRKBIT** a esta Política; o Assegurar o cumprimento desta Política

3. CONCEITOS

3.1. Os conceitos e siglas abaixo são referentes a termos presentes ao longo desta Política:

3.2. **ANBIMA**: Associação Brasileira das Entidades dos Mercados Financeiro e de Capitais.

3.3. **BACEN**: Banco Central do Brasil.

3.4. **OTC (Over The Counter)** – Mercado de balcão, onde há negociar direta de ativos.

3.5. **Exchange de criptoativos** – Empresa que possui uma plataforma onde compradores e vendedorespodem ofertar criptoativo em um livro de ofertas aberto. Há também custódia de moeda correntenacional e criptoativos de terceiros.

3.6. **CEIS**: Cadastro de Empresas Inidôneas e Suspensas.

3.7. **Cadastro:** repositório de dados e documentos fornecidos pelos clientes e validados peloCompliance da TRKBIT.

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

3.9. **Cliente:** pessoa física ou jurídica, que utiliza os serviços oferecidos pela **TRKBIT**.

3.10. **CNEP**: Cadastro Nacional de Empresas Punidas.

3.11. **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 dedinheiro 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.

3.12. **Criptoativos** – Ativos digitais criptografados, podendo ser criptomoedas ou tokens (Ex.:Bitcoin, Ethereum, Lite Coin).

3.13. **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.

3.14. **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 instrumentosnegociáveis 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, orecurso ilegal integra definitivamente o sistema econômico e financeiro. A partir deste momento,o dinheiro recebe aparência lícita.

3.15. **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.

3.16. **Exchange de criptoativos:** Empresa que possui uma plataforma onde compradores e vendedorespodem ofertar criptoativo em um livro de ofertas aberto. Há também custódia de moeda correntenacional e criptoativos de terceiros.

3.17. **FBI**: Federal Bureau of Investigation.

3.18. **FEBRABAN:** Federação Brasileira de Bancos.

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

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

3.21. **INTERPOL**: International Criminal Police Organization.

3.22. **Know Your Customer ("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.

3.23. **Know Your Employee ("KYE")**: Procedimento de due diligence na admissão e contratação de colaboradores.

3.24. **Know Your Partner ("KYP"):** Procedimento de due diligence para parceiros.

3.25. **Lavagem de Dinheiro**: consiste na realização de operações comerciais ou financeiras com a finalidade de incorporar recursos, bens e serviços obtidos ilicitamente.

3.26. **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 origemdo dinheiro e facilitar o anonimato.

3.27. **OFAC**: Office of Foreign Assets Control.

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

3.29. **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 funçõespúblicas relevantes, assim como seus representantes, familiares e outras pessoas de seu relacionamento próximo.

3.30. **UNSC**: United Nations Security Council.

4. COMO SE DÁ O KYC?

4.1. 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**.

4.2. 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.

4.3. 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.

4.4. 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:

I. Primeira Etapa - Envio de documentos

4.5. 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.

4.6. 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.

4.7. 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.

4.8. 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.

4.9. 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

4.10. 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.

4.11. 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.

4.12. 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.

4.13. 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.

4.14. 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;

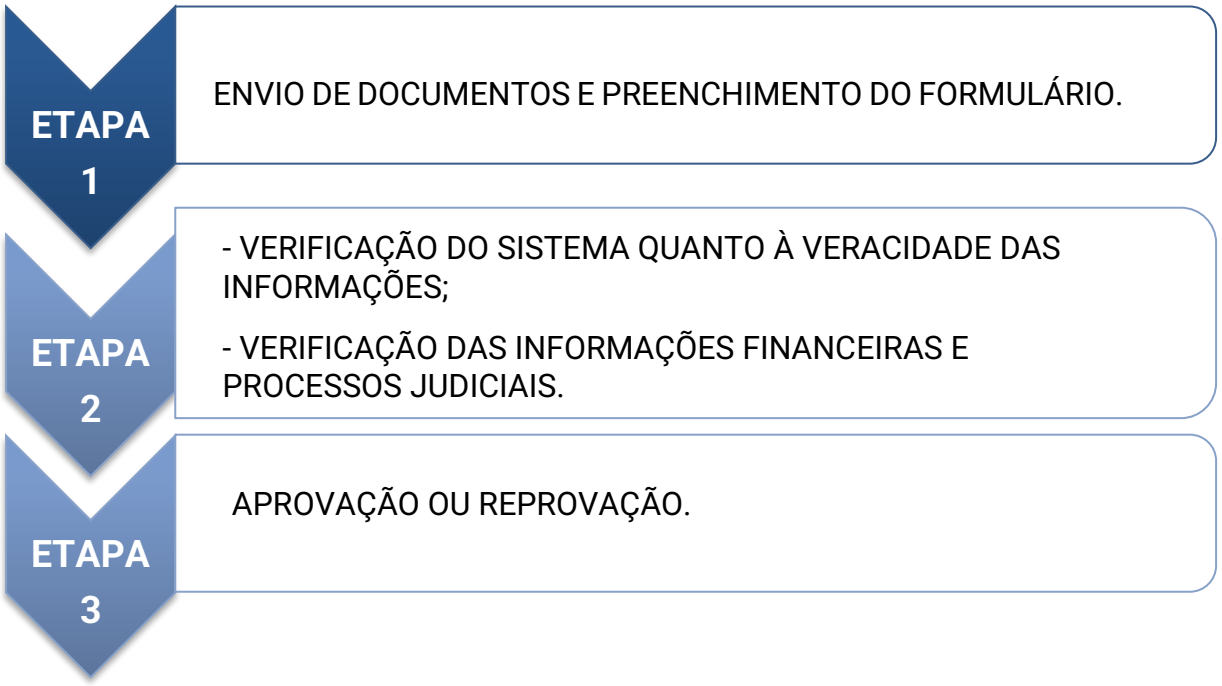
4.15. Os Pareceres Opinativos elaborados pelo excritório de advocacia externo sempre consignarão, em suas conclusões, as ponderações acerca do cliente e das informações consultadas, apontando, assim, por sua aprovação ou reprovação. O referido documento será enviado ao único sócio e administrador da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

4.15.1. 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.

4.16. 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.

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

III – Fluxo Operacional



4.18. 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.

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

4.20. 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.

4.21. 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.

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

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

4.24. 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.

4.25. O formulário KYC, quando preenchido fisicamente, será arquivado na ficha do

cliente, de acordo com os procedimentos estabelecidos pela **TRKBIT**.

5. PROCEDIMENTOS INTERNOS ADOTADOS PELA EMPRESA

5.1 A **TRKBIT** utiliza como referência e analogia aos procedimentos internos, com objetivo deprevenção a lavagem de dinheiro ou ocultação de bens, direitos e valores, a CIRCULAR Nº 3.978, DE 23DE JANEIRO DE 2020 do Banco Central do Brasil.

5.2 Essa política de prevenção será adotada em todos os setores da empresa, começando pela avaliação de seus funcionários, parceiros e prestadores de serviços terceirizados, estendendo-se às operações, transações, produtos, serviços e clientes da **TRKBIT**.

5.3 Os procedimentos mencionados, assim como esta política, devem ser divulgados aos funcionários da instituição, parceiros e prestadores de serviços terceirizados, utilizando uma linguagem clara e acessível, com detalhes compatíveis com as funções desempenhadas e a sensibilidade das informações.

5.4 A **TRKBIT** mantém um departamento interno de Compliance responsável por implementar e garantir o cumprimento dos procedimentos estabelecidos, conforme alinhado e disposto por analogia à Circular nº 3.978, de 23 de Janeiro de 2020, do Banco Central do Brasil, conforme previsto nesta política.

5.5 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.

5.6 A avaliação interna de risco deve ser completamente documentada, aprovada pelo Diretor da **TRKBIT**, Sr. **THIAGO GABRIEL BRAZ**, e encaminhada aos setores responsáveis pelas tomadas de decisão que envolvam 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.

5.7 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, a confrontação dessas informações com as disponíveis em bancos de dados de caráter público e privado.

5.8 O Departamento de Compliance da **TRKBIT TECNOLOGIA E INFORMAÇÃO LTDA** é exercido por meio de um canal direto da própria empresa, através de seu Diretor, Sr. **THIAGO GABRIEL BRAZ**, que contrata um escritório de advocacia para a elaboração de pareceres opinativos sobre aprovação e reprovação. O Departamento de Compliance interno da empresa **TRKBIT** utiliza o 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.

5.9 O escritório de advocacia externo, por sua vez, utiliza o seguinte fornecedor:

- **FORNECEDOR:** COMBATEAFRAUDE S.A., CNPJ: 34.102.645/0001-57, localizado na Rua Tiradentes, 1077 - 5º andar, Centro, Venâncio Aires - RS, CEP 95800-000.

5.10 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.

5.11 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.

6. GERENCIAMENTO DE RISCOS

6.1 Conforme definido na Circular BCB nº 3.681/13, as Instituições de Pagamento devem implementar estrutura de gerenciamento dos riscos operacional, de liquidez e de crédito, entretanto a **TRKBIT** não atua como Instituição da Pagamento, mas observa a presente Circular.

6.2 Esta Política de Gerenciamento de Riscos poderá se desdobrar em: **(i)** outras políticas e estratégias aprovadas e revisadas, anualmente, pela diretoria e/ou pela Alta Administração; **(ii)** a criação de documentação acerca das políticas, estratégias de gerenciamento de riscos e governança da **TRKBIT**, bem como diretrizes sobre a terceirização de serviços e critérios de seleção de prestadores de serviços; **(iii)** manutenção de documentação acerca das políticas, estratégias de gerenciamento de riscos e governança à disposição do Banco Central do Brasil, com diretrizes sobre a terceirização de serviços e de seleção de seus prestadores, incluindo as condições contratuais mínimas necessárias para mitigar o risco operacional, e a continuidade dos serviços de pagamento prestados.

I - <u>Estrutura de gerenciamento de riscos</u>

a) 1ª linha de defesa: Áreas de Negócios e Suporte.

- A primeira linha de defesa é responsável por monitorar e mitigar os riscos associados àsfunções e atividades de negócios.

b) 2ª linha de defesa: Riscos, Controles Internos e Compliance.

- A segunda linha de defesa é responsável pela definição de métodos para identificação, avaliação e monitoramento do grau de exposição aos riscos, alinhadas ao apetite de risco da **TRKBIT**

c) 3ª linha de defesa: Auditoria interna

- A terceira linha de defesa é responsável por verificar e realizar avaliação independente e periódica da efetividade das políticas, métodos e procedimentos para controle e gestão dos riscos, além de verificar a sua efetiva implementação.

II - <u>Risco Operacional</u>

6.3. O risco operacional é a ocorrência de perdas resultantes dos seguintes eventos:

a) Falhas na proteção e na segurança de dados sensíveis relacionados tanto às credenciais dos usuários finais quanto a outras informações trocadas com o objetivo de efetuar transações depagamento;

b) Falhas na identificação e autenticação do usuário final;

c) Falhas na autorização das transações de pagamento;

d) Fraudes internas;

e) Fraudes externas;

f) Demandas trabalhistas e segurança deficiente do local de trabalho;

g) Práticas inadequadas relativas a usuários finais, produtos e serviços de pagamento;

h) Danos a ativos físicos próprios ou em uso pela instituição;

i) Ocorrências que acarretem a interrupção das atividades da instituição de pagamento ou a descontinuidade dos serviços de pagamento prestados;

j) Falhas em sistemas de tecnologia da informação; e

k) Falhas na execução, cumprimento de prazos e gerenciamento das atividades envolvidas em arranjosde pagamento.

6.4. Para prevenção, identificação, mitigação e tratamento de riscos operacionais, a **TRKBIT** adotará as seguintes medidas e diretrizes:

l) Elaboração e implementação de um plano de contingência e outros mecanismos que garantam a continuidade dos serviços de pagamento prestados;

m) Mecanismos de proteção e segurança dos dados armazenados, processados ou transmitidos;

n) Mecanismos de proteção e segurança de redes, sítios eletrônicos, servidores e canais decomunicação com vistas a reduzir a vulnerabilidade a ataques;

o) Procedimentos para monitorar, rastrear e restringir acesso a dados sensíveis, redes, sistemas,bases de dados e módulos de segurança;
p) Monitoramento das falhas na segurança dos dados e das reclamações dos usuários finais aesse respeito;

q) Revisão das medidas de segurança e de sigilo de dados, especialmente depois da ocorrênciade falhas e previamente a alterações na infraestrutura ou nos procedimentos;

r) Elaboração de relatórios que indiquem procedimentos para correção de falhas identificadas;

s) Realização de testes que assegurem a robustez e a efetividade das medidas de segurança dedados adotadas;

t) Segregação de funções nos ambientes de tecnologia da informação destinados aodesenvolvimento, teste e produção;

u) Identificação adequada do usuário final;

v) Mecanismos de autenticação dos usuários finais e de autorização das transações depagamento;

w) Processos para assegurar que todas as transações de pagamento possam ser adequadamenterastreadas;

x) Avaliações e filtros específicos para identificar transações consideradas de alto risco;

y) Notificação ao usuário final acerca de eventual não execução de uma transação;

z) Mecanismos que permitam ao usuário final verificar se a transação foi executadacorretamente; e

aa) Documentação e armazenamento de informações relacionadas a perdas associadas a riscooperacional.

6.5. Caso a **TRKBIT** terceirize quaisquer funções relacionadas à segurança na prestação dos seus serviços oferecidos aos Usuários, o contrato de prestação de

serviços com estes terceiros deverá prever o disposto nesta Política.

III - Tratamento de Riscos

6.6. Após classificados, os riscos serão analisados para determinar o tratamento adequado. O Tratamento de riscos pela **TRKBIT** será desenvolvido através de procedimento a ser criado pela Área de Compliance, a ser definido conforme cada caso, segundo a seguinte definição:

a) RISCOS SOLUCIONÁVEIS: Os riscos solucionáveis são aqueles que a **TRKBIT** entende serem passíveis de resolução sem impactos relevantes à operação da **TRKBIT**, e assim, consequentemente deixarão de ser riscos na medida em que for implementada a resolução;

b) RISCOS MITIGÁVEIS: Os riscos mitigáveis para a **TRKBIT** são aqueles para os quais, há ações paramitigação e que assim, continuam a existir só que com menor gravidade. c. são aqueles que sefaz a assunção do risco, ou seja, que a **TRKBIT** aceita correr sem estabelecer medidas de mitigação, visto que entende que o risco seria baixo ao seu negócio.

IV - Procedimento de Correção de Falhas

6.7. Os procedimentos de correção de falhas deverão abordar:

a) Identificação de Perdas Operacionais: a apuração da perda decorrente de Incidente constitui fator importante para o cumprimento das exigências dos órgãos reguladores além de prover a **TRKBIT** informações consistentes, padronizadas e atualizadas, decisivas para uma análise quantitativa do gerenciamento do risco na **TRKBIT;**

b) Avaliação da Qualidade dos Controles: a avaliação dos controles tem como objetivo avaliar a efetividade/eficiência dos controles, a fim de verificar se estes estão sendo executados conforme descritos nas matrizes de risco e políticas internas;

c) Plano de Treinamento: o plano de treinamento tem como objetivo, por meio de simulações de incidentes e avaliação de incidentes ocorridos, garantir que os Colaboradores estejam preparados para lidar com incidentes e aptos a identificar situações de riscos e vulnerabilidades.

7. CRITÉRIOS DE APROVAÇÃO

7.1 Após a obtenção dos resultados das buscas feitas pela **TRKBIT** no software provido por seu fornecedor homologado, o escritório externo de advocacia contratado pela **TRKBIT** realiza uma análise pormenorizada a respeito dos resultados, a fim de interpretar as informações obtidas para assim opinar acerca da possibilidade ou não de prestação de serviços para o cliente.

7.2 O escritório de advocacia externo **não** possui, em nenhuma hipótese, condão

decisório.

7.3 Ao longo de sua análise, o responsável pelo compliance da **TRKBIT** irá utilizar-se dos seguintes critérios analíticos:

a) Existência de protestos;

b) Histórico de declarações de imposto de renda;

c) Histórico de vínculos empregatícios contemporâneos e passados;

d) Cadastro em conselhos de profissão;

e) Renda própria estimada;

f) Patrimônio estimado;

g) Usufruto de programas governamentais de assistência social;

h) Inscrição do cliente em listas restritivas de qualquer natureza;

i) Cadastro do cliente em quaisquer autarquias ou associações controladoras;

j) Existência de ficha atribuível ao cliente em qualquer agência nacional ou internacional anticrimes;

k) Existência de processos judiciais de qualquer natureza;

l) Natureza dos processos judiciais eventualmente existentes;

m) Qualidade de Pessoa Exposta Politicamente (“PEP”).

7.4 Muito embora a lista de critérios seja extensa, é importante ressaltar que a conclusão final a ser tomada pelo responsável pelo Compliance acerca da aprovação ou não do cliente em muito dependerá da natureza dos apontamentos levantados pelo software de busca, e não por sua quantidade total.

7.5 De todo modo, serão critérios definitivos na reprovação do cliente:

a) A existência de processos judiciais de natureza criminal de qualquer tipo;

b) Envolvimento em escândalos de natureza fiscal, econômica ou pública;

c) Sua inscrição em cadastros protetivos de crédito;

d) Sua inscrição em lista restritiva;

e) Passagem por qualquer autoridade policial, seja ela nacional ou

internacional.

f) A falta de lastro financeiro que comprove o poderio monetário para a realização da operação desejada.

8. LIMITES OPERACIONAIS

8.1 Os limites operacionais foram desenhados de forma a serem condizentes com a capacidade econômico-financeira, combinando com a utilização de Abordagem Baseada em Risco ("ABR"), onde mensura-se a exposição aos riscos a partir dos dados pessoais do cliente.

8.2 A **TRKBIT** possui limites operacionais amparados da seguinte forma:

a) Classificação Nível 1

- **Depósito-Reais:** R$ 10.000,00
- **Stablecoins:** R$ 10.000,00
- **Limite Semanal:** R$ 10.000,00
- **Saque-Reais:** R$ 10.000,00
- **Bitcoin:** Equivalente a R$ 10.000,00

Solicitação Nível 1:

- Submissão de documento de identificação pessoal válido e autêntico;
- Submissão de prova de vida, que consiste em envio de Selfie (foto de si mesmo) segurando o documento de identificação pessoal;
- Submissão de comprovante de residência de até 03 (três) meses anteriores;
- Background Check: retorna informações como i) PEP (Pessoas Expostas Politicamente); ii) Mandado de Prisão Expedido; iii) Listas de Sanções Nacionais e Internacionais (CEPIM, CEIS, CNEP, UNSC, COAF, OFAC, INTERPOL); iv) Ações judiciais e administrativas;
- Declaração de wallets do usuário;
- Recibo das Declarações de IN 1888/2019.

b) Classificação Nível 2

- **Depósito-Reais**: R$ 50.000,00
- **Stablecoins:** R$ 50.000,00
- **Limite Semanal:** R$ 50.000,00
- **Saque-Reais:** R$ 50.000,00
- **Bitcoin:** BTC equivalante a R$ 50.000,00

Solicitação Nível 2:

- Submissão de documento de identificação pessoal válido e autêntico;
- Submissão de prova de vida, que consiste em envio de Selfie (foto de si mesmo) segurando o documento de identificação pessoal;
- Submissão de comprovante de residência de até 3 (três) meses anteriores;
- Background Check: retorna informações como i) PEP (Pessoas Expostas Politicamente); ii) Mandado de Prisão Expedido; iii) Listas de Sanções Nacionais e Internacionais (CEPIM, CEIS, CNEP, UNSC, COAF, OFAC, INTERPOL); iv) Ações judiciais e administrativas;
- Declaração de wallets do usuário;
- Recibo das Declarações de IN 1888/2019.

c) Classificação Nível 3

- **Depósito-Reais:** R$ 100.000,00 ou mais
- **Stablecoins:** R$ 100.000,00 ou mais
- **Limite Semanal:** R$ 100.000,00 ou mais
- **Saque-Reais:** R$ 100.000,00 ou mais
- **Bitcoin:** BTC equivalente a R$ 100.000,00 ou mais

Solicitação Nível 3

- Submissão de documento de identificação pessoal válido e autêntico;
- Submissão de prova de vida, que consiste em envio de Selfie (foto de si mesmo) segurando o documento de identificação pessoal;
- Submissão de comprovante de residência de até 03 (três) meses anteriores;
- Background Check: retorna informações como i) PEP (Pessoas Expostas Politicamente); ii) Mandado de Prisão Expedido; iii) Listas de Sanções Nacionais e Internacionais (CEPIM, CEIS, CNEP, UNSC, COAF, OFAC, INTERPOL); iv) Ações judiciais e administrativas;
- Busca de Mídias Negativas;
- Submissão de formulário de Onboarding para fins de declaração e comprovação de capacidade econômico-financeira, com a devida demonstração da origem dos recursos a serem investidos;

- Submissão de documentos e constitutivos (PJ): i) Cópia do Contrato Social; ii) Cópia do Documento de Identificação do QSA; iii) Comprovante de endereço da empresa;

- Submissão de documentos financeiros: i) extrato bancário; ii) Balanço contábil assinado por contador; iii) Cópia da primeira página da Declaração de Imposto de Renda; iv) Documento comprobatório do faturamento médio mensal dos últimos doze meses; v) Outro documento hábil a demonstrar a situação financeira patrimonial e lastro financeiro para as operações. (vi) Demonstração de lastro financeiro de capital mensal de R$ 500.000,00 (quinhentos mil reais); (vii) Recibo das Declarações de IN 1888/2019.

9. ABORDAGEM BASEADA EM RISCO

9.1 Em compasso com as recomendações do GAFI/FATF e demais normas de 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.

9.2 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;

9.3 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.

10. MECANISMOS E MÉTRICAS DE AVALIAÇÃO DE RISCO

10.1. 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 empregue 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 atosilícitos 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 Brasilou 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) Mídias negativas;

11. PESSOAS EXPOSTAS POLITICAMENTE (PEP)

11.1. A **TRKBIT** possui atenção especial durante os procedimentos de cadastro, contratação, atualização de informações, prestação de serviços e monitoramento de operações de clientes e colaboradores, uma vez que se resguarda em não operar, atender ou contratar pessoas expostas politicamente.

12. PROTEÇÃO DE DADOS PESSOAIS

12.1. A coleta, acesso e tratamento de dados pessoais dos clientes, colaboradores e fornecedores pessoas físicas da **TRKBIT** é necessária para o cumprimento das obrigações desta Política, estando em conformidade com a Lei Geral de Proteção de

Dados (Lei nº 13.709, de 14 de agosto de 2018).

12.2. Não obstante, é dever da **TRKBIT**, de seus colaboradores e fornecedores, prezar pela segurançae privacidade dos dados pessoais tratados, bem como pela sua utilização dentro dos limites necessários à finalidade aqui proposta, sempre com transparências e em observância à legislação vigente, bem como Política de Privacidade da **TRKBIT**.

13. COMITÊ DE ÉTICA E COMPLIANCE

13.1. Não obstante, é dever da **TRKBIT**, de seus colaboradores e fornecedores, prezar pela segurançae privacidade dos dados pessoais tratados, bem como pela sua utilização dentro dos limites necessários à finalidade aqui proposta, sempre com transparências e em observância à legislação vigente, bem como Política de Privacidade da **TRKBIT**.

13.2. 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.

13.3. 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.

13.4. 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.

15. ATUALIZAÇÃO CADASTRAL

15.1. 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.

15.2. 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.

16. CANAL DE DENÚNCIAS

16.1. A **TRKBIT** 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.

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

16.3. A denúncia será tratada pelo Departamento de Compliance, que possui canal direto através do e-mail: fale@trkbit.co, 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 finalda Diretoria da **TRKBIT**.

16.4. O canal direto da Diretoria Executiva ficará a cargo do Diretor responsável através do e-mail: fale@trkbit.co.

16.5. O canal direto da Ouvidoria ficará a cargo do Diretor responsável através do e-mail: fale@trkbit.co.

16.6. O canal direto em caso de emergência, canal de denúncias ou casos em que todas as áreasdevem ser acionadas pelo email fale@trkbit.co.

17. DISPOSIÇÕES GERAIS

17.1. 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.

17.2. O Comitê de Ética e Compliance deliberará sobre a comunicação à Unidade de Inteligência Financeira (“COAF”) acerca de atividades suspeitas e atípicas.

17.3. Caso o perfil do cliente não esteja de acordo com as normas correlacionadas nas Políticas de Compliance, Prevenção à Lavagem de Dinheiro (“PLD”), Know Your Customer (“KYC”), Privacidade e nos Termos de Uso, serão aplicáveis as regras da Política de Cancelamento e Devolução e/ou o Usuárionão será aceito na plataforma.

18. DIREITO APLICÁVEL E FORO

18.1. 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.

18.2. A presente versão deste instrumento foi elaborada pela Dra. Jessyca Arieira Araújo, OAB/RJ 201.581, responsável apenas pela elaboração das políticas.

18.3. Quaisquer disputas ou controvérsias oriundas de quaisquer atos praticados no âmbito da utilização das Aplicações pelos usuários, 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 da cidade de São Paulo/SP, como sendo o único competente para dirimir qualquer controvérsia oriunda do presente Termo, renunciando expressamente a qualquer outro, por mais privilegiado que seja.

19. APROVAÇÃO/VIGÊNCIA

19.1. 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.

Jessyca arieira

Consultora Externa Jessyca Arieira AraujoOAB/RJ 201.582

COO & Representante Legal THIAGO GABRIEL BRAZ