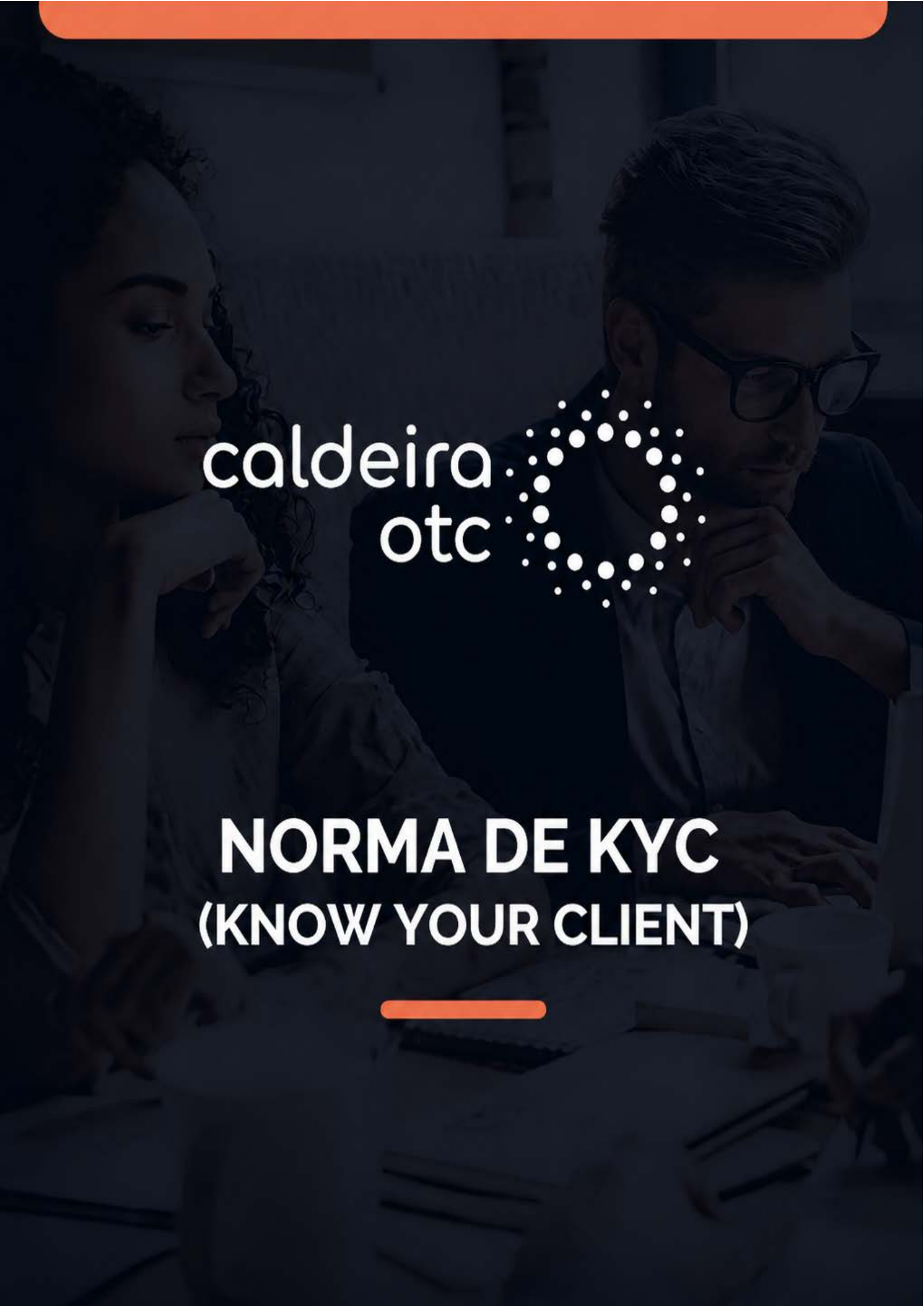




caldeira
otc



NORMA DE KYC (KNOW YOUR CLIENT)

CONTROLE DE VERSÕES DO DOCUMENTO

Versão	Data	Descrição
1.0	06/08/2026	Primeira emissão
1.1	19/08/2026	- Correção da data de emissão da versão 1.0, originalmente registrada como 06/08/2016, sendo o correto 06/08/2026. - Padronização da nomenclatura regulatória, com substituição das referências a SPAV, PSAV e termos correlatos pela sigla SPSAV.

APROVAÇÃO DO DOCUMENTO

Documento revisado, aprovado e ratificado pelos responsáveis abaixo identificados.



Documento assinado digitalmente
CAROLINE DE SOUZA CALDEIRA
Data: 19/08/2026 18:08:47-0300
Verifique em <https://validar.iti.gov.br>

Caroline de Souza Caldeira
Sócia Administradora
Caldeira Negócios e Intermediações Ltda.

**EDUARDO
SALATHIEL
DA SILVA**

Assinado digitalmente por EDUARDO
SALATHIEL DA SILVA
ND: C=BR, O=ICP-Brasil, OU=AC OAB, OU=
11871388002247, OU=VideoConferencia,
OU=Assinatura Tipo A3, OU=ADVOGADO,
CN=EDUARDO SALATHIEL DA SILVA
Razão: Eu sou o autor deste documento
Localização:
Data: 2026.08.19 18:24:20-03'00'
Foxit PDF Reader Versão: 2025.2.0

Dr. Eduardo Salathiel da Silva
Diretor de Conformidade
OAB/RJ nº 68.618

1. OBJETIVOS, ESCOPO E ALINHAMENTO ESTRATÉGICO

1.1. Objetivo Geral

O presente manual estabelece as diretrizes fundamentais e os procedimentos operacionais para o processo de **Conheça Seu Cliente (Know Your Customer - KYC)** da instituição. O objetivo central deste documento é normatizar a identificação, a qualificação, a validação cadastral e os critérios de aceitação de **clientes**, compreendendo pessoas físicas, jurídicas e seus respectivos procuradores ou representantes legais, que busquem estabelecer relacionamento contratual ou transacionar na plataforma.

Essas práticas visam, de maneira coordenada e focada no cliente:

- Assegurar a conformidade regulatória nas etapas de Onboarding e manutenção de contas perante o Sistema Financeiro Nacional (SFN).
- Servir como o braço operacional e procedimental da Política Corporativa de Prevenção à Lavagem de Dinheiro e Financiamento ao Terrorismo (PLD/FTP), identificando os clientes e mitigando o risco de ocultação de bens ou direitos.
- Prevenir fraudes de identidade, falsificação de dados cadastrais, uso indevido de contas por terceiros (contas "laranja") ou tentativas de burla aos limites operacionais estabelecidos pela governança interna.

1.2. Escopo e Abrangência (Foco no Cliente)

Este manual possui aplicação obrigatória e irrestrita a todos os canais de atendimento, plataformas tecnológicas e regimes de relacionamento voltados exclusivamente para a gestão de **clientes** da companhia.

A. Tipos de Clientes Abrangidos

Os ritos de identificação e qualificação descritos neste documento aplicam-se compulsoriamente a:

- Clientes de varejo (pessoas físicas e jurídicas) que utilizem as plataformas digitais ou aplicações conectadas via API para a negociação de ativos virtuais.
- Contrapartes de mercado que operem de forma direta em canais de balcão através da Mesa de Operação OTC corporativas.

B. Abrangência Interna (Pessoal)

As diretrizes aqui dispostas devem ser cumpridas de forma estrita por todos os colaboradores cujas funções possuam interface com a jornada ou a tomada de decisão sobre o cliente, incluindo:

- Analistas das equipes de *Onboarding*, Cadastro, Atendimento e Suporte ao Cliente.
- Operadores de mercado (Traders) e gestores de contas institucionais.
- Equipes de Compliance, Monitoramento de PLD/FTP e o Encarregado de Proteção de Dados (DPO).

1.3. Alinhamento ao Modelo de Negócios (SPSAV)

Considerando que a instituição atua como uma Sociedade Prestadora de Serviços de Ativos Virtuais (SPSAV), este manual foi desenhado de forma a harmonizar a alta disponibilidade e a baixa latência exigidas pelo mercado de criptoativos com a rigidez dos controles cadastrais necessários:

- **Eficiência no Onboarding:** Estabelecer uma estrutura de validação baseada em risco para garantir que clientes de baixo risco acessem a plataforma de forma cênica e ágil, mitigando fricções cadastrais injustificadas.
- **Segurança Operacional:** Garantir que as credenciais e chaves de API emitidas para os clientes transacionarem não exponham os motores de negociação (*trading engines*) a fraudes de liquidação ou acessos não autorizados.
- **Integridade do Capital:** Certificar que os recursos fiduciários ou virtuais movimentados pelos clientes possuam origem identificável, protegendo o patrimônio próprio e de terceiros que trafegam pelo ecossistema de custódia da instituição.

1.4. Base Legal, Regulatória e Normativa

A estruturação das diretrizes de KYC atende ao arcabouço jurídico e regulatório aplicável às SPSAVs e instituições reguladas pelo Banco Central do Brasil, mantendo total alinhamento com a Política de Segurança da Informação (PSI) da organização:

- **Lei nº 9.613/1998 (Lei de Lavagem de Dinheiro):** Impõe a obrigação legal de identificar detalhadamente os clientes, manter registros atualizados e estruturar históricos para viabilizar o envio sigiloso de comunicações ao COAF.
- **Lei nº 14.478/2022 (Marco Legal dos Criptoativos):** Exige boas práticas de governança e controle na aceitação e monitoramento de clientes para mitigar riscos operacionais e financeiros no mercado de ativos virtuais.
- **Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais - LGPD):** Fundamenta legalmente a coleta de dados cadastrais sob as bases de cumprimento de obrigação regulatória e execução de contrato, aplicando o princípio da minimização para resguardar a privacidade do cliente.
- **Normativas: Circular 3.978/20, Resoluções 519/25 e 520/25 do Banco Central do Brasil (BCB):** Atendimento às resoluções específicas destinadas a regular a governança, a gestão de riscos e os controles tecnológicos das Sociedades Prestadoras de Serviços de Ativos Virtuais.
- **Instruções Normativas RFB nº 1.888/2019 e nº 2.291/2025:** Obrigam o reporte de todas as transações com criptoativos e o cumprimento de obrigações tributárias e operacionais suplementares. Essas normas exigem a exatidão, a rastreabilidade e a integridade sistêmica dos dados coletados no KYC para garantir a correta vinculação das operações aos respectivos CPFs/CNPJs dos clientes perante a Receita Federal.
- **Padrões Internacionais de Rastreabilidade (Travel Rule - Recomendação 16 do GAFI/FATF):** Estabelece a obrigatoriedade de coleta, processamento e transmissão segura de dados de identificação das partes envolvidas em transferências externas de ativos virtuais. A qualificação cadastral (KYC) realizada nesta instituição possui também a finalidade legal de viabilizar o compartilhamento estrito dessas informações essenciais com outras Sociedades Prestadoras de Serviços de Ativos Virtuais (SPSAVs) e instituições financeiras durante o trânsito de ativos, garantindo a rastreabilidade plena das operações e a prevenção à lavagem de dinheiro, em alinhamento aos reguladores globais.

1.5. Integração Documental e o Manual de Coleta (Anexo II)

Este documento estabelece as premissas, os critérios estratégicos de governança e as diretrizes da Abordagem Baseada em Risco (ABR) para o cliente. Para evitar o engessamento deste manual

corporativo frente a mudanças em formatos de documentos públicos, fica formalizada a integração com o **Anexo II - Manual Operacional de Coleta Documental de KYC**.

O Anexo II atua como o detalhamento tático e complementar deste instrumento, especificando a listagem exata de documentos exigidos, critérios de aceitação de comprovantes, exceções cadastrais e os documentos complementares obrigatórios para processos de Diligência Avançada (EDD).

2. PAPÉIS, RESPONSABILIDADES E GOVERNANÇA INTERNA

A execução das rotinas de KYC (Know Your Customer) e a proteção das informações coletadas dos clientes são responsabilidades de toda a organização. Para assegurar a conformidade regulatória perante as resoluções do Banco Central do Brasil (BCB), o Marco Legal dos Criptoativos e a LGPD, ficam definidos os papéis, alçadas e mecanismos de controle interno focados na gestão cadastral de clientes descritos a seguir:

2.1. Diretoria Executiva e Alta Administração

A Alta Administração detém o patrocínio institucional máximo do programa de KYC, sendo responsável por conferir suporte estratégico e financeiro à sua execução.

- **Aprovação e Governança do Cliente:** Aprovar formalmente este Manual de KYC e as regras de Abordagem Baseada em Risco (ABR) para clientes, revisando-o anualmente.
- **Provisão de Recursos de Onboarding:** Garantir o direcionamento de orçamento e ferramentas de tecnologia (como birôs de validação e APIs cadastrais) necessários para a operação eficiente da esteira de aceitação de clientes.
- **Designação do Diretor de Compliance:** Indicar formalmente perante o Banco Central do Brasil o Diretor Responsável pelo cumprimento das obrigações de Prevenção à Lavagem de Dinheiro (PLD/FTP), assegurando que este possua autonomia para tomada de decisão sobre aceitação ou veto de clientes.

2.2. Área de Compliance e PLD/FTP

A área de Compliance atua como a proprietária operacional e técnica dos processos de qualificação e monitoramento do cliente.

- **Gestão da Esteira Cadastral:** Coordenar e supervisionar os processos de coleta, qualificação e aceitação de clientes, aplicando as regras da ABR para enquadrar os perfis nas respectivas classes de risco.
- **Propriedade de Dados (Data Owner):** A gerência de Compliance é designada formalmente como a proprietária (*Data Owner*) das bases de dados e dos dossiês de clientes de KYC (ativo catalogado como **BD-002** no Modelo de Inventário Centralizado). Cabe a este papel classificar as informações cadastrais, além de autorizar ou revogar os privilégios de acesso a esses repositórios.
- **Monitoramento Comportamental:** Monitorar continuamente os logs de movimentação financeira dos clientes para identificar atipicidades em relação ao perfil econômico declarado. Compete a esta área a elaboração e o envio sigiloso das comunicações de atividades suspeitas ao COAF.

2.3. Área de TI e Segurança da Informação (InfoSec)

A equipe de tecnologia e segurança cibernética atua como habilitadora das camadas de proteção lógica que resguardam exclusivamente as bases de dados e os sistemas de acesso aos dados de clientes.

- **Proteção dos Dados do Cliente:** Implementar e manter mecanismos de criptografia (padrão AES-256 ou superior) para os dados de clientes em repouso e protocolo TLS 1.2 ou superior para os dados cadastrais em trânsito (como integrações via API com birôs externos).
- **Gestão de Identidades e Acessos ao KYC:** Administrar o ciclo de vida de acessos lógicos dos colaboradores às ferramentas de onboarding de clientes, exigindo o uso de senhas complexas e Autenticação Multifator (MFA) de forma inegociável.
- **Rastreabilidade e Imutabilidade:** Configurar e monitorar os rastros digitais de auditoria (logs) gerados a partir de qualquer consulta, alteração ou exportação de dossiês de KYC de clientes. Os logs devem registrar a identificação do usuário, data, hora e IP, sendo armazenados sob políticas de imutabilidade.

2.4. Encarregado pelo Tratamento de Dados Pessoais (DPO)

O DPO atua de forma independente para assegurar que as obrigações regulatórias de identificação civil ocorram em perfeita harmonia com os direitos de privacidade do cliente.

- **Auditoria de Privacidade do Onboarding:** Garantir que a coleta e o armazenamento de documentos e informações dos proponentes atendam à Lei Geral de Proteção de Dados (LGPD).
- **Minimização do Tratamento:** Fiscalizar o fluxo de KYC para certificar que o recolhimento de informações esteja adstrito estritamente à finalidade legal exigida para o cadastro e a execução dos contratos de ativos virtuais, vetando a captação de dados excessivos ou desproporcionais.
- **Interface com o Cliente (Titular):** Atuar como o ponto exclusivo de recebimento e processamento de requisições de clientes (direitos de acesso, retificação ou anonimização de dados cadastrais).

2.5. Segregação de Funções (SoD) e Barreiras Antifraude

Para anular o risco de fraude interna, manipulação indevida de cadastros ou elevação maliciosa de limites operacionais de trading, a companhia adota o princípio da Segregação de Funções (*Segregation of Duties*) como barreira lógica e processual obrigatória:

- **Isolamento Comercial e Operacional:** A equipe comercial, os operadores de mercado (Traders) e as equipes responsáveis por propor ordens de movimentação fiduciária/cripto não possuem privilégios de acesso ou capacidade técnica de aprovar cadastros de clientes, alterar perfis de risco ou definir limites operacionais na base de KYC.
- **Segregação no Desenvolvimento Tecnológico:** O desenvolvedor ou engenheiro de software que projeta as automações de onboarding não possui permissão para publicar códigos no ambiente de produção, nem possui privilégios para consultar os dados reais de identificação dos clientes armazenados nos servidores produtivos em nuvem.
- **Alçadas para Liberação de Clientes:** A aceitação de clientes enquadrados na categoria de Risco Alto ou identificados como Pessoas Politicamente Expostas (PEP) segue uma matriz restrita de controle compartilhado. O analista de onboarding responsável por revisar o dossiê

não possui autonomia individual para liberar a conta; o quórum de aprovação final é obrigatoriamente deslocado para a chefia de Compliance ou para a Diretoria Executiva.

2.6. Comitê de Segurança da Informação e Riscos (Gestão de Crises)

O Comitê de Crise atua como o órgão máximo de decisão colegiada em situações excepcionais que afetem as bases cadastrais dos clientes da instituição.

- **Gestão de Incidentes com Dados de Clientes:** Ser imediatamente mobilizado de forma extraordinária na Sala de Crise (*War Room*) caso as ferramentas de segurança identifiquem um vazamento confirmado ou forte suspeita de comprometimento do banco de dados de KYC (Incidente Crítico Nível N4).
- **Voz Única e Alçada de Decisão:** O Comitê detém a autoridade exclusiva para aprovar a redação de comunicados regulatórios e públicos direcionados ao BCB, à ANPD, ao mercado e aos clientes titulares afetados pelo incidente.

2.7. Governança de Exceções Cadastrais (Política de Waiver)

As diretrizes de identificação e coleta documental descritas neste manual e no **Anexo II** possuem caráter compulsório para todos os clientes da instituição. Contudo, reconhecendo a complexidade de determinados arranjos societários e a morosidade na emissão de certidões em algumas jurisdições, a companhia adota uma Política de Exceções Cadastrais (Waiver), aplicável exclusivamente em caráter provisório e justificado.

Nenhum operador, analista de atendimento ou membro da equipe comercial possui autoridade ou capacidade sistêmica para dispensar unilateralmente a entrega de documentos obrigatórios de KYC. O processo de exceção deve obedecer estritamente ao rito de governança estabelecido abaixo:

A. Critérios de Elegibilidade e Risco Compensatório

A solicitação de aprovação por exceção só será admitida se a área de negócios ou relacionamento comercial comprovar formalmente:

- **Impedimento Temporário:** A impossibilidade material do cliente em fornecer a documentação exigida no prazo padrão, atestando que o documento está em fase de emissão.
- **Mitigação de PLD/FTP:** A apresentação de documentos alternativos ou informações públicas secundárias que forneçam à área de Compliance um nível de segurança probatória aceitável e equivalente sobre a identidade ou a origem dos recursos.
- **Vedação Absoluta:** É terminantemente proibida a concessão de waivers para a dispensa de identificação de Beneficiários Finais (UBOs) ou para a omissão de consultas a listas de sanções internacionais (OFAC, ONU) e enquadramento PEP.

B. Alçadas de Aprovação

A liberação operacional de um cliente com pendência documental formalizada por meio de waiver exige aprovação colegiada. O dossiê de exceção deverá tramitar pelo seguinte fluxo hierárquico:

- **Parecer Comercial:** A área de negócios emite um memorando interno justificando o interesse estratégico no cliente e solicitando o waiver.

- **Parecer de Risco (Compliance):** O analista de KYC emite um parecer técnico apontando o risco residual aceito pela falta do documento.
- **Aprovação Final:** A liberação da conta (e a parametrização dos limites temporais) dependerá da assinatura formal e conjunta do Diretor Executivo (CEO) e do Diretor de Compliance.

C. Prazo de Regularização e Congelamento Sistêmico (SLA)

Toda exceção aprovada nasce com um prazo de validade improrrogável para regularização da pendência documental por parte do cliente:

- **Prazos Estipulados:** O waiver terá validade máxima de 30 dias corridos para clientes domiciliados no Brasil e 60 dias corridos para clientes estrangeiros domiciliados no exterior.
- **Ação de Bloqueio Automático:** A equipe de Tecnologia deve parametrizar os motores de liquidação para que, no dia seguinte ao vencimento do prazo do waiver sem o envio do documento faltante, a conta do cliente sofra um bloqueio automático (Freeze) para novas entradas e ordens de trading. Apenas liquidações de saques residuais serão permitidas até o saneamento da pendência.

D. Rastreabilidade e Auditoria

Todas as exceções aprovadas e os pareceres envolvidos devem ser anexados ao dossiê digital do cliente e armazenados com a classificação de confidencialidade aplicável aos dados de KYC. A área de Compliance manterá um registro centralizado (Registro de Waivers) contendo a volumetria de exceções ativas, que deverá ser apresentado em reuniões de prestação de contas à Alta Administração ou requisitado em inspeções do Banco Central do Brasil.

Esta redação protege a plataforma: a equipe comercial consegue trazer o cliente grande que ainda está esperando sair uma certidão específica, mas a Diretoria assina a responsabilidade e o sistema corta o acesso do cliente automaticamente se ele não entregar o documento no prazo.

3. PROCEDIMENTOS OPERACIONAIS DE COLETA E VALIDAÇÃO (ONBOARDING)

O processo de aceitação e entrada de novos clientes na instituição fundamenta-se na **Abordagem Baseada em Risco (ABR)**, combinando a agilidade e a automação necessárias para o ecossistema de uma SPSAV com as camadas de proteção jurídica exigidas pelo Banco Central do Brasil (BCB), pelo COAF e pela LGPD.

3.1. Premissas de Identificação Cadastral e Minimização (Foco no Cliente)

Em estrita conformidade com o princípio da minimização previsto na LGPD, a coleta de dados cadastrais, patrimoniais e societários de clientes é restrita ao mínimo necessário e proporcional para cumprir as obrigações regulatórias de identificação civil e fiscal perante o SFN e viabilizar a execução dos contratos de ativos virtuais, assegurando a capacidade tecnológica de atendimento ao regime informacional exigido pelas INs RFB nº 1.888/2019 e nº 2.291/2025.

Os fluxos de onboarding são estruturados para capturar e validar dados de:

- **Pessoas Físicas (PF):** Dados de identificação civil, regularidade fiscal, histórico jurídico, domicílio, contato, ocupação profissional e declaração de renda/patrimônio estimados.

- **Pessoas Jurídicas (PJ):** Dados de constituição societária, regularidade CNPJ, regularidade fiscal, trabalhista e regulatória, modelo de negócio, histórico jurídico, faturamento e a identificação completa de sócios administradores, procuradores e do quadro de Beneficiários Finais (UBO - *Ultimate Beneficial Owners*).

3.2. Critérios de Validação Tecnológica e Due Diligence do Cliente

Para suportar o volume transacional e mitigar fraudes de identidade, a esteira de onboarding utiliza mecanismos automatizados de validação de dados integrados à plataforma corporativa, orientando-se pelos seguintes critérios de *Due Diligence*:

- **Sincronização com Órgãos Oficiais:** Consulta automática via APIs seguras às bases da Receita Federal do Brasil para checagem da regularidade de CPFs e CNPJ, bloqueando preventivamente proponentes com situação cadastral suspensa, baixada ou cancelada.
- **Background Checks de Risco Cadastral:** Cruzamento automatizado do nome e documento do cliente contra listas globais de sanções (OFAC, ONU, União Europeia), registros de procurados de autoridades policiais (Interpol, Polícia Federal) e cadastros de processos judiciais relevantes para PLD/FTP.
- **Prova de Vida Digital (Liveness Check):** Captura obrigatória de imagem facial biométrica instantânea (*selfie*) com validação de movimento em tempo real, mitigando fraudes de falsificação ideológica ou uso de identidades de terceiros.

3.3. Abordagem Baseada em Risco (ABR), Tiers de Clientes e Política de Limites Temporais

Após o processamento dos dados declarados e das checagens automatizadas, as ferramentas de Compliance realizarão a triagem para enquadrar o cliente em um dos três níveis de risco cadastral. Este enquadramento determina as alçadas de aprovação e os limites quantitativos máximos, controlados de forma sistêmica por janelas de tempo:

Nível de Risco	Critérios Cadastrais de Enquadramento	Alçadas de Aprovação e Revisão	Limites Temporais e Unitários (Fiduciário + Cripto)
Risco Baixo (Verde)	Clientes PF com dados perfeitamente regulares nas bases oficiais, sem apontamentos restritivos e com perfil de renda padrão.	Onboarding automatizado pelo sistema de Compliance. Revisão cadastral programada a cada 24 meses.	Limite Mensal: R\$ 50.000,00 Limite Diário: R\$ 10.000,00 Atingir o teto de qualquer uma das janelas bloqueia automaticamente o envio de novas ordens sistêmicas no período.
Risco Médio (Amarelo)	Clientes PJ padrão (sem estruturas societárias complexas) ou proponentes PF com pequenas inconsistências cadastrais.	Liberação condicionada à revisão e assinatura manual de um analista. Revisão cadastral anual.	Limite Mensal: R\$ 250.000,00 Limite Diário: R\$ 50.000,00 Limite por Operação: Transações unitárias que ultrapassem R\$ 30.000,00 são retidas para validação manual da mesa de operações.
Risco Alto (Vermelho)	Clientes de volumes massivos (Mesas OTC), empresas com cadeias societárias complexas, PEP ou alta volatilidade.	Bloqueados até execução de EDD. Exige aprovação formal assinada pela Diretoria de Compliance. Revisão semestral.	Limites Customizados (Tailor-Made). Tetos diários, mensais e por operação definidos individualmente em Comitê, limitados estritamente à

			capacidade econômico-financeira (faturamento/patrimônio) comprovada na EDD.
--	--	--	---

Diretrizes Complementares de Controle de Limites e Janelas Temporais:

- **Mecânica de Contagem de Prazo (Rolling Window):** O limite "Diário" compreende o ciclo de 24 horas a partir da primeira transação, e o "Mensal" compreende o ciclo contínuo de 30 dias corridos retroativos. O sistema não deve utilizar meses-calendário estáticos (ex: limite zerado a cada dia 1º) para evitar o risco de clientes executarem o dobro do limite financeiro na transição entre o último e o primeiro dia do mês.
- **Consolidação de Rotas (Fiduciário + Cripto):** O cômputo do consumo dos limites temporais engloba a somatória absoluta do volume transacionado em todas as vias: depósitos e saques fiduciários liquidados, acrescidos do valor nocional (equivalente em reais) das entradas e saídas on-chain de ativos virtuais no mesmo período.
- **Majoração de Limites (Upgrade de Tier):** Solicitações para elevar os tetos temporais preestabelecidos exigem que o cliente submeta novos comprovantes de renda ou faturamento. Essa solicitação deflagra um novo ciclo obrigatório de requalificação de risco antes de qualquer liberação nos motores de liquidação.

3.4. Identificação de Pessoas Politicamente Expostas (PEP)

O enquadramento de um proponente (ou de seu Beneficiário Final) como Pessoa Politicamente Expostas (PEP) configura obrigatoriamente um gatilho de **Risco Alto**, sujeitando o cliente às seguintes premissas de controle:

- **Identificação Proativa:** Consulta automatizada para monitorar se o proponente exerce ou exerceu, nos últimos 5 (cinco) anos, cargos ou funções públicas relevantes, abrangendo também seus familiares de primeiro grau e estreitos colaboradores.
- **Enhanced Due Diligence (EDD):** Obrigatoriedade de preenchimento de declaração detalhada de origem de fundos fiduciários ou virtuais, acompanhada de comprovação patrimonial robusta (conforme regras dispostas no Anexo II).
- **Alçada Dual de Aprovação:** O analista de onboarding não possui autonomia individual para liberar contas PEP. A aceitação e abertura do relacionamento dependem formalmente da anuência expressa e assinada do Diretor Responsável por PLD/FTP (Compliance) ou da Diretoria Executiva.

3.5. Práticas de Mesa Limpa e Tela Limpa na Operação de Onboarding

Para mitigar o risco de vazamento de informações cadastrais ou acesso visual não autorizado aos dados dos clientes dentro das dependências da companhia, todos os analistas e operadores devem aderir rigorosamente às práticas de proteção física e lógica:

- **Regras de Tela Limpa:** Analistas que operem interfaces de onboarding, bases de dados ou dossiês de clientes devem garantir que essas janelas sejam minimizadas ou fechadas imediatamente quando não estiverem em uso ativo. É obrigatório o uso de películas de privacidade nas telas caso o colaborador execute suas funções em áreas com circulação de pessoas, e o bloqueio manual da sessão é mandatório ao se afastar da estação de trabalho.

- **Regras de Mesa Limpa e Descarte:** É terminantemente proibido manter documentos impressos contendo dados pessoais de clientes, comprovantes residenciais ou fotos de prova de vida expostos sobre as mesas ou em impressoras compartilhadas. Nenhum documento de KYC pode ser descartado em lixo comum; sua eliminação física deve ocorrer obrigatoriamente por meio de fragmentadoras mecânicas disponibilizadas pela companhia.

3.6. Integração com o Manual de Coleta Documental (Anexo II)

Este manual estabelece os critérios e as premissas de elegibilidade, classificação e risco do cliente. O detalhamento prático, as listas de documentos aceitos para cada tipo de cadastro (PF e PJ), as exceções cadastrais aceitáveis e os documentos complementares de riqueza exigidos para o Risco Alto (Diligência Avançada - EDD) não constam deste corpo principal, estando integrados e normatizados diretamente no **Anexo II - Manual Operacional de Coleta Documental de KYC** deste instrumento.

3.7. Acordos de Nível de Serviço (SLA) e Prazos Operacionais de Onboarding

Para harmonizar a necessidade de baixa latência exigida pelo ecossistema de criptoativos com a rigidez dos controles cadastrais do Banco Central do Brasil (BCB), a esteira de aceitação de clientes operará sob Acordos de Nível de Serviço (SLAs) internos rigorosos.

A área de Compliance compromete-se a respeitar os seguintes prazos máximos para a emissão da primeira resposta (aprovação, rejeição ou requisição de documentos adicionais) a contar do momento em que o cliente submete o dossiê completo na plataforma:

A. Matriz de SLAs por Nível de Risco

- **Risco Baixo (Verde):**
 - **SLA de Aprovação:** Imediato / Tempo Real.
 - **Fluxo de Trabalho:** Processo de *onboarding* e liberação 100% automatizados pelos sistemas corporativos, dependendo exclusivamente do tempo de resposta das integrações e APIs de checagem biométrica e bases oficiais.
- **Risco Médio (Amarelo):**
 - **SLA de Análise Manual:** Até 48 horas úteis.
 - **Fluxo de Trabalho:** Tempo máximo alocado para que o analista da equipe de Compliance revise pequenas inconsistências cadastrais, cruze os dados divergentes e realize a assinatura manual atestando a liberação da conta.
- **Risco Alto (Vermelho), PEP e Mesas OTC:**
 - **SLA de Diligência Avançada (EDD):** Até 96 horas úteis (4 dias úteis).
 - **Fluxo de Trabalho:** Período destinado à verificação profunda da documentação de origem da riqueza, análise do organograma societário (UBOs) e tramitação do dossiê para a aprovação formal e assinatura da Diretoria de Compliance.

B. Gestão de Pendências e Congelamento de Prazos (Clock Pause)

Caso a equipe de análise identifique a necessidade de exigir documentos complementares ou correções (ex: comprovante de endereço ilegível, selfie desfocada, ou falta de certidão no Anexo III), as seguintes regras se aplicam:

1. **Pausa do SLA Interno:** O tempo de contagem do SLA da equipe de Compliance é imediatamente paralisado assim que o analista envia a notificação de pendência (*push*, *e-mail* ou interface web) ao cliente.
2. **Prazo de Resolução pelo Cliente:** A partir da notificação, clientes enquadrados no Risco Médio terão um prazo máximo de 30 (trinta) dias para a resolução das pendências. Para clientes de Risco Alto em processo de EDD, o prazo limite para o envio das evidências comprobatórias será de 15 (quinze) dias corridos.
3. **Arquivamento por Decurso de Prazo:** A inércia do proponente em sanar as pendências documentais nos prazos supracitados resultará no cancelamento automático da solicitação de *onboarding*, exigindo que o usuário reinicie o processo de qualificação do zero caso deseje transacionar no futuro.

C. Monitoramento de Desempenho (KPIs)

A gerência de Compliance atuará no monitoramento contínuo desses SLAs. O Tempo Médio de Aprovação (*Time-to-Approve*) e o volume de cadastros paralisados na esteira manual serão acompanhados como Indicadores Chave de Desempenho (KPIs), devendo ser reportados periodicamente à Alta Administração para garantir o dimensionamento adequado da equipe de retaguarda.

3.8. Coleta de Dados para fins de Regra de Viagem (Travel Rule)

Os dados básicos de identificação validados durante o processo de *onboarding* e diligência cadastral — especificamente Nome Completo/Razão Social, CPF/CNPJ e os respectivos endereços públicos de carteira (*wallet*) vinculados ao cliente — possuem a finalidade operacional adicional de compor o pacote de informações obrigatório exigido pelas normativas internacionais de transparência.

Sempre que o cliente solicitar uma transferência externa de ativos virtuais direcionada a outra instituição (SPSAV), a companhia utilizará este repositório cadastral para extrair e transmitir, de forma criptografada e segura, os dados do remetente à instituição de destino. O compartilhamento destas informações é compulsório, inegociável e visa exclusivamente garantir a rastreabilidade da operação em estrito cumprimento à Recomendação 16 do GAFI/FATF e às exigências do Sistema Financeiro Nacional, constituindo requisito essencial para a liquidação de movimentações externas na plataforma.

3.9. Encerramento de Relacionamento (Offboarding)

O encerramento definitivo de contas, seja por solicitação voluntária do cliente, inatividade ou decisão administrativa, seguirá rigorosamente os fluxos operacionais, prazos e tratamentos de saldos residuais definidos na Norma Operacional de Encerramento de Relacionamento e Desligamento de Clientes.

4. CLASSIFICAÇÃO, SIGILO E PROTEÇÃO DE DADOS DE CLIENTES

A proteção e a salvaguarda dos dados cadastrais, financeiros e transacionais coletados dos clientes durante a jornada de KYC constituem obrigações contratuais e regulatórias fundamentais para a instituição. A gestão e o manuseio dessas informações regem-se rigidamente pelos critérios de classificação de risco e sigilo digital descritos neste capítulo.

4.1. Nível de Classificação dos Dados do Cliente (KYC)

Para assegurar que a proteção aplicada aos dados dos clientes seja proporcional ao risco de sua exposição, todas as informações coletadas no Onboarding e no monitoramento comportamental recebem a classificação de segurança máxima para dados pessoais dentro da organização:

Nível de Classificação: CONFIDENCIAL

Definição Institucional: Informações sensíveis do cliente cujo vazamento, alteração, acesso não autorizado ou perda acidental pode causar impactos financeiros diretos, severos danos à reputação da companhia, exposição de segredos de negócio ou violar exigências legais imperativas, sujeitando a instituição a penalidades severas da LGPD e do Banco Central do Brasil.

Exemplos de Ativos Abrangidos: Dados pessoais cadastrais, mídias e imagens de documentos de identidade civil, comprovantes de residência, biometrias faciais de prova de vida, declarações de faturamento societário, relatórios de *Background Checks* e históricos de enquadramento de risco do cliente.

4.2. Governança e Rastreabilidade do Ativo de Clientes

Todos os repositórios lógicos e servidores que tratam as informações cadastrais dos clientes são mapeados centralizadamente para garantir a transparência em auditorias do Banco Central do Brasil.

- **Identificação do Ativo:** Conforme o Modelo de Inventário Centralizado de Ativos, o banco de dados que armazena os dossiês de clientes (KYC) é catalogado sob o **ID BD-002**.
- **Proprietário do Ativo (Data Owner):** A posição de proprietário formal é exercida pelo **Gestor de Compliance**. Compete exclusivamente a este papel autorizar ou revogar nominalmente os privilégios de acesso técnico ao repositório BD-002.
- **Métricas de Recuperação do Ativo:** O repositório BD-002 possui metas rígidas de resiliência tecnológica associadas à Análise de Impacto no Negócio (BIA), fixando o Objetivo de Tempo de Recuperação (**RTO**) em no máximo **4 horas** e o Objetivo de Ponto de Recuperação (**RPO**) em no máximo **1 hora** em cenários de desastre ou indisponibilidade.

4.3. Princípios de Acesso Lógico aos Dados do Cliente

A concessão de privilégios de acesso às interfaces de consulta, bancos de dados corporativos ou sistemas de suporte que tratam informações de clientes é rigidamente governada por três pilares de segurança:

1. **Princípio do Menor Privilégio (Least Privilege):** Cada analista de onboarding ou sistema integrado receberá estritamente o nível mínimo de permissão técnica necessária para o desempenho exato de suas atribuições na esteira de validação do cliente.
2. **Necessidade de Conhecimento (Need-to-Know):** O acesso lógico aos dossiês de clientes salvaguardados sob o nível Confidencial será restrito única e exclusivamente àqueles indivíduos cujas funções corporativas exijam, de forma explícita e justificada, o contato com tais informações.
3. **Contas Nominais Invioláveis:** É terminantemente proibido o uso de contas genéricas, compartilhadas ou de suporte técnico coletivo para a consulta ou manipulação de dados de clientes. Todo usuário deve possuir uma credencial de acesso individualizada e nominal.

4.4. Autenticação e Rastreabilidade (Logs de Auditoria)

Como barreiras técnicas de proteção cibernética contra acessos indevidos e vazamentos de dados de clientes, aplicam-se obrigatoriamente as seguintes premissas:

- **Autenticação Multifator (MFA):** O uso de MFA é obrigatório, inegociável e atua como requisito tecnológico bloqueante para a autenticação em qualquer sistema corporativo ou painel administrativo de onboarding que armazene dados de clientes. Priorizam-se chaves físicas de hardware (YubiKeys) ou aplicativos autenticadores baseados em tempo (TOTP).
- **Logs de Auditoria do Cliente:** Toda e qualquer interação humana ou sistêmica com o banco de dados de KYC (BD-002) — incluindo logins bem-sucedidos ou falhas, consultas cadastrais, alterações de dados ou comandos de exportação — deve gerar um rastro digital ininterrupto de auditoria (*log*).
- **Conteúdo Mínimo do Log:** Cada registro de auditoria gerado deve conter, obrigatoriamente, a identificação nominal do analista, a data e hora exata do evento (carimbo de tempo), o endereço IP de origem e o comando ou dado do cliente consultado. Os logs são armazenados sob políticas de imutabilidade.

4.5. Restrições de Manuseio e Compartilhamento pelo Operador Interno

Para resguardar a integridade das informações cadastrais e assegurar a conformidade irrestrita com a LGPD, o analista e o operador interno que lidam diretamente com o cliente devem observar as seguintes proibições absolutas:

- **Uso de Contas de Comunicação Corporativa:** Discussões internas sobre a documentação de clientes de KYC devem ocorrer exclusivamente por meio das plataformas oficiais homologadas e fornecidas pela companhia.
- **Proibição Absoluta de Canais e Ambientes Pessoais:** É expressamente vedado ao operador ou analista enviar relatórios de KYC ou dossiês cadastrais de clientes para contas de e-mail pessoais (ex: Gmail, Outlook, Yahoo). É igualmente proibido transferir, sincronizar ou armazenar dados corporativos Confidenciais de clientes em serviços públicos de nuvem de uso pessoal (ex: Dropbox, Google Drive pessoal, iCloud).
- **Restrições em Mensageiros Corporativos:** É terminantemente proibido o compartilhamento ou tráfego de dados pessoais e cadastrais de clientes (KYC), em texto claro ou anexo, por meio de qualquer plataforma de mensageria, mesmo ferramentas homologadas internamente, em estrita conformidade com a LGPD e as normas de sigilo. Para a transferência de dados e validações necessárias, devem ser gerados links temporários protegidos através do sistema de cofre de senhas corporativo (*Vault*).

4.6. Diretrizes de Mesa Limpa e Tela Limpa na Operação de Cadastro

As salvaguardas de sigilo dos dados dos clientes estendem-se de forma obrigatória ao comportamento físico dos analistas de onboarding em suas estações de trabalho, aplicando-se de maneira estrita as regras de Mesa Limpa e Tela Limpa estabelecidas corporativamente:

- **Bloqueio Manual e Compulsório da Sessão:** É obrigatório o bloqueio manual imediato da tela do computador sempre que o analista de onboarding ou colaborador se ausentar de sua estação de trabalho, ainda que por um breve período de tempo.
- **Privacidade de Janelas Ativas:** Durante a condução de análises de dossiês ou manipulação de bases de KYC, as janelas operacionais devem ser minimizadas sempre que

terceiros circularem no perímetro físico. É obrigatório o uso de películas de privacidade nas telas caso o colaborador execute suas funções em áreas com circulação de pessoas.

- **Proibição de Documentação Exposta e Descarte Seguro:** Sob nenhuma circunstância documentos de KYC impressos, comprovantes de clientes ou relatórios financeiros podem ser deixados desacompanhados sobre as mesas de trabalho ou em impressoras compartilhadas. Ao atingirem o fim de sua vida útil, nenhum papel contendo tais dados pode ser descartado no lixo comum; sua destruição e descarte físico seguro devem ocorrer obrigatoriamente por meio de fragmentadoras mecânicas disponibilizadas pela instituição.

5. HARMONIZAÇÃO ENTRE KYC, BLOCKCHAIN E DIREITOS DO TITULAR (LGPD)

O tratamento de dados pessoais no ecossistema de uma SPSAV exige a conciliação entre as obrigações regulatórias de identificação civil do cliente e as características arquitetônicas imutáveis das redes descentralizadas.

5.1. Atendimento aos Direitos dos Clientes Titulares

A instituição garante aos clientes o exercício pleno de seus direitos previstos na LGPD (acesso, correção, portabilidade e revogação de consentimento) por meio de um canal de comunicação direto operado pelo DPO. O tratamento de informações apoia-se legalmente nas bases de Cumprimento de Obrigação Legal ou Regulatória e Execução de Contrato.

Ressalta-se que o compartilhamento estruturado de dados pessoais e cadastrais (tais como nome, CPF/CNPJ e endereços de carteiras virtuais) com outras Sociedades Prestadoras de Serviços de Ativos Virtuais (SPSAVs) ou instituições financeiras, quando realizado no âmbito de transferências externas de ativos virtuais, não constitui violação de privacidade ou quebra de sigilo bancário.

Este fluxo de informações é uma exigência imperativa para o atendimento da *Travel Rule* (Regra de Viagem) e encontra-se estritamente amparado na base legal do Cumprimento de Obrigação Legal ou Regulatória (Art. 7º, II, da LGPD), visando a rastreabilidade financeira e a prevenção à lavagem de dinheiro.

5.2. O Limite do Direito de Eliminação frente à Retenção Regulatória

O pedido de exclusão de dados ou "esquecimento" feito por um cliente **não é absoluto**. Dados pessoais atrelados a históricos transacionais, saldos e os dossiês documentais completos de KYC não podem ser excluídos imediatamente a pedido do usuário. Em conformidade com as exigências do Banco Central do Brasil, do COAF e da Receita Federal, esses registros cadastrais devem ser retidos e mantidos armazenados de forma segura por um período compulsório de 5 a 10 anos após o encerramento definitivo do relacionamento contratual com o cliente.

Os procedimentos técnicos para o bloqueio de acesso do usuário e a comunicação jurídica de encerramento estão dispostos na Norma Operacional de Encerramento de Relacionamento e Desligamento de Clientes.

5.3. Segregação On-Chain vs. Off-Chain e Anonimização por Quebra de Vínculo

Em virtude da natureza descentralizada e imutável da tecnologia blockchain, os dados registrados diretamente nas redes *on-chain* (como endereços públicos de carteiras/*public keys*, hashes de transação e saldos) não podem ser alterados ou apagados pela companhia.

Para atender à LGPD sem violar a limitação técnica da tecnologia, o procedimento de exclusão do cliente (após expirados os prazos de retenção regulatória) consistirá em atuar exclusivamente sobre as bases internas (*off-chain*), apagando os dados cadastrais (Nome, CPF, documentos) do banco de dados de KYC (BD-002). Ao destruir a tabela que correlaciona a identidade civil do cliente ao seu endereço público de carteira, a companhia promove a efetiva anonimização do registro, desidentificando o rastro na blockchain perante a instituição.

6. MONITORAMENTO TRANSACIONAL E PERFIL DO CLIENTE

O processo de KYC exige o monitoramento contínuo focado na consistência entre o perfil econômico-cadastral declarado pelo cliente no onboarding e seu comportamento transacional efetivo fiduciário e cripto.

6.1. Identificação de Atipicidades Comportamentais

A área de Compliance parametrizará os sistemas automatizados para disparar alertas sempre que uma movimentação do cliente apresentar desvios em relação à sua linha de base de risco. Os gatilhos de monitoramento incluem:

- **Incompatibilidade Patrimonial:** Transações fiduciárias ou virtuais cujos valores consolidados sejam desproporcionais à capacidade financeira, renda ou faturamento informados pelo cliente.
- **Fracionamento de Operações (*Smurfing*):** Realização de transações consecutivas com valores imediatamente inferiores aos limites estabelecidos para reporte compulsório, indicando tentativa de burlar os mecanismos automatizados de controle.
- **Rastreamento de Origem na Blockchain:** Alertas imediatos se as análises apontarem que as moedas virtuais enviadas ou sacadas pelo cliente possuem vínculos com endereços listados em sanções internacionais, carteiras associadas a hacks, plataformas de mistura (*mixers*) ou mercados ilícitos.

6.2. Sigilo Absoluto dos Alertas e Reportes de Inteligência

A condução de análises internas de inteligência financeira e o tráfego de relatórios de atividades suspeitas demandam o nível máximo de proteção da instituição, em estrita observância à Lei nº 9.613/1998 e às normas do COAF.

Nível de Classificação: RESTRITA (ou Estritamente Confidencial)

Definição Institucional: O nível mais alto de criticidade corporativa. O acesso a esses arquivos e logs de alertas é limitado a um número mínimo e nominal de analistas essenciais da área de Compliance, sendo vedado a qualquer outro colaborador.

Vedações de Tráfego e Sinalização (*Tipping-off*): É terminantemente proibido o tráfego ou compartilhamento de documentos do COAF por meio de e-mails, aplicativos de mensageria instantânea ou dispositivos removíveis. Sob nenhuma hipótese o cliente sob análise ou terceiros poderão ser informados, direta ou indiretamente, sobre a existência de um alerta ou o envio de um reporte de atividade suspeita ao COAF.

7. GESTÃO DE INCIDENTES COM DADOS CADASTRAIS DE CLIENTES

Este capítulo estabelece os procedimentos táticos focados exclusivamente na proteção do cliente e no cumprimento de obrigações de comunicação regulatória caso ocorra um comprometimento do

banco de dados de KYC (BD-002). As ações técnicas de infraestrutura cibernética e failover de nuvem secundária seguem o **Plano de Resposta a Incidentes - PRI.pdf** corporativo.

7.1. Tipificação do Incidente de KYC como Crítico (Nível N4)

A confirmação ou forte suspeita de vazamento de bases de dados cadastrais, exposição de documentos de identidade de clientes, ou alteração fraudulenta de travas de conformidade regulatória enquadram o evento automaticamente como **Incidente Crítico (Nível N4)**. O evento dispara a mobilização imediata e compulsória do Comitê de Crise na Sala de Crise dedicada (*War Room*) no prazo máximo de 30 minutos.

7.2. Procedimento de Proteção ao Cliente Titular

- **Preservação Forense:** Qualquer colaborador que detectar um comportamento sistêmico anômalo na visualização ou exportação de dados de clientes tem a obrigação de reportar imediatamente ao CISO, abstando-se de tentar investigar por conta própria para não contaminar as evidências forenses necessárias para a ANPD e autoridades policiais.
- **Contenção de Acessos:** A equipe técnica executará a invalidação compulsória de todos os tokens de sessão ativos e o bloqueio imediato de credenciais de analistas ou robôs de onboarding identificados como comprometidos, interrompendo o fluxo ilícito de extração de dados de clientes.

7.3. Fluxo de Notificação Regulatória

- **Notificação à ANPD e Clientes Titulares (LGPD):** Nos cenários onde o incidente de segurança possa acarretar risco ou dano relevante aos direitos dos clientes (como o vazamento de cópias de documentos civis do onboarding), o Comitê de Crise coordenará a notificação formal à ANPD e aos clientes afetados, detalhando a natureza do evento e as medidas de proteção adotadas, em estrita conformidade com os ritos e prazos da LGPD.
- **Notificação ao Banco Central do Brasil (BCB):** O Diretor Responsável garantirá o reporte formal ao órgão regulador sobre incidentes considerados relevantes que afetem de forma substancial a integridade operacional cadastral da SPSAV, cumprindo os prazos determinados pelas normativas vigentes.

8. CONSCIENTIZAÇÃO E CULTURA EM KYC

A segurança dos dados dos clientes coletados no Onboarding depende intrinsecamente do comportamento e da cultura de conformidade dos colaboradores que operam a esteira cadastral.

8.1. Treinamento de Onboarding Funcional e Capacitação Continuada

- **Treinamento Obrigatório:** Todo novo colaborador, estagiário ou prestador com acesso à esteira cadastral deve, obrigatoriamente, passar por treinamento focado neste Manual de KYC, práticas de PLD/FTP e conformidade com a LGPD durante sua primeira semana. A liberação de acessos lógicos para visualização de dados de clientes é condicionada à conclusão deste módulo.
- **Engenharia Social voltada ao Cliente:** As campanhas periódicas (no mínimo semestrais) devem focar no treinamento contra técnicas de engenharia social voltadas ao roubo de dados de clientes, incluindo ataques de *phishing* direcionados aos analistas de cadastro, fadiga de MFA e tentativas de fraude de identidade em canais de atendimento.

8.2. Monitoramento de Endpoints e Inexistência de Privacidade no Uso

Os analistas e operadores de KYC declaram estar cientes de que todos os recursos computacionais fornecidos são ferramentas de trabalho e de propriedade exclusiva da companhia. A empresa utiliza soluções ativas de monitoramento (EDR/DLP) nas estações de trabalho para detectar acessos anômalos à base de dados de clientes (BD-002) ou transferências não homologadas de relatórios cadastrais (*Shadow IT*), não havendo expectativa de privacidade absoluta no uso dos equipamentos corporativos.

8.3. Sanções Disciplinares por Violação de Sigilo do Cliente

A inobservância ou violação intencional das regras de sigilo do cliente expõe a companhia a riscos financeiros e sistêmicos inaceitáveis. Em casos de infrações confirmadas na manipulação de dados de KYC, o setor de Recursos Humanos e Compliance aplicará sanções proporcionais:

- **Advertência:** Aplicada em casos de descuidos operacionais sem dolo (ex: deixar a tela desbloqueada ao se ausentar da mesa ou falhar em simulações de *phishing*).
- **Demissão por Justa Causa (ou Rescisão Contratual):** Aplicada de forma sumária em casos de violação grave, como o compartilhamento intencional de senhas de onboarding, envio não autorizado de dados de clientes para e-mails ou nuvens pessoais, ou alteração fraudulenta e intencional de limites operacionais e perfis de risco de clientes. Ações criminosas serão alvo de acionamento imediato das autoridades policiais para responsabilização civil e criminal.



ANEXO I - MATRIZ DE RETENÇÃO DE DOCUMENTOS DE KYC

Esta matriz padroniza os prazos de guarda e os ritos de eliminação de mídias de clientes e históricos transacionais após o encerramento das contas, em conformidade com as regras do SFN e da LGPD. Trata-se de um documento controlado classificado como **Confidencial / Restrito**, revisado a cada 6 meses.

ID do Ativo	Categoria / Tipo de Documento de Clientes	Proprietário (Data Owner)	Justificativa Base Legal Regulamentar	Prazo de Retenção (Pós-Encerramento da Conta)	Método de Descarte Final (Ambiente Off-Chain)
BD-002A	Dados Cadastrais Básicos do Cliente (Nome, CPF/CNPJ, Endereço, E-mail, Telefone)	Gestor de Compliance	- Lei nº 9.613/1998 - Marco Legal dos Criptoativos - Obrigações Regulatórias do BCB	5 a 10 anos (Conforme normativas do Banco Central)	Destruição Criptográfica / Quebra de Vínculo: Exclusão irreversível das tabelas off-chain que associam a identidade civil do cliente à sua chave pública na blockchain.
BD-002B	Mídias e Evidências Probatórias (RG/CNH digitalizados, Contratos Sociais e Selfies de Prova de Vida)	Gestor de Compliance	- Regras de Onboarding de SPSAVs (BCB) - LGPD (Execução de Contrato)	5 a 10 anos (Alinhado ao prazo de retenção do relacionamento)	Sanitização de Dados: Execução de wipe lógico nos servidores de arquivos em nuvem e fragmentação mecânica imediata de cópias residuais físicas.
BD-002C	Dossiês de Análise de Risco (Relatórios de Background Checks, buscas em Listas e Pareceres PEP)	Gestor de Compliance	- Abordagem Baseada em Risco (BCB) - Diretrizes de Governança de PLD/FTP (COAF)	5 anos (Prazo prescricional para auditoria de triagem)	Wipe Criptográfico: Destruição permanente das chaves lógicas de criptografia que dão acesso aos arquivos de pareceres em nuvem.
BD-001	Logs Transacionais do Cliente (Registros de depósitos, saques, fiduciários e ordens de trading)	Diretor de Tecnologia	- Instruções Normativas RFB nº 1.888/2019 e nº 2.291/2025 - Marco Civil da Internet	5 anos (Prazo mínimo para fiscalização e reportes tributários)	Anonimização Estrutural: Eliminação dos dados cadastrais identificáveis off-chain atrelados ao log, mantendo o registro numérico e anonimizado.
RIF-COAF	Relatórios de Inteligência e Suspeitas (Alertas analisados e comunicações enviadas ao COAF)	Diretoria de Compliance	- Lei nº 9.613/1998 (Sigilo de Reportes) - Resoluções do COAF (Vedação de Tipping-off)	10 anos (Prazo máximo de segurança para salvaguarda de investigações)	Destruição Lógica Inviolável: Exclusão definitiva do cofre digital de senhas (Vault) e sanitização completa, com termo de destruição assinado pelo Diretor de Compliance.

ANEXO II - MANUAL OPERACIONAL DE COLETA DOCUMENTAL DE KYC

Este anexo operacional integra e complementa o corpo principal do Manual de KYC, estabelecendo a listagem exaustiva de documentos aceitos, critérios de validação e regras para a Diligência Avançada (EDD).

1. LISTAGEM DE DOCUMENTOS DE IDENTIFICAÇÃO ACEITOS (CLIENTES PF, PJ E PROCURADORES)

- **Documentos Oficiais com Foto:** Carteira Nacional de Habilitação (CNH) digitalizada ou física, Cédula de Identidade Civil (RG) ou Registro Nacional de Estrangeiros (RNE).
- **Crítérios de Aceitação:** Os documentos não podem apresentar rasuras, indícios de manipulação digital ou estarem replastificados. A data de emissão deve ser inferior a 10 (dez) anos a contar da data de solicitação do onboarding.

2. CRITÉRIOS DE ACEITAÇÃO PARA COMPROVANTES DE ENDEREÇO (CLIENTES PF E PJ)

- **Mídias Aceitas:** Contas de consumo público (água, energia elétrica, gás ou telefone fixo) e extratos bancários de instituições reguladas pelo BCB, emitidos com prazo máximo de 90 (noventa) dias.
- **Exceções e Casos Especiais:** Caso o proponente não possua comprovante em seu nome próprio:
 - **Cônjuges:** Aceitação de comprovante em nome do cônjuge mediante apresentação obrigatória de Certidão de Casamento ou Declaração de União Estável digitalizada.
 - **Parentes de Primeiro Grau (Pais/Filhos):** Aceitação mediante cruzamento dos dados de filiação contidos no documento de identidade oficial apresentado acompanhado de declaração de residência em favor do cadastrado, emitido pelo titular da conta de consumo público ou da conta bancária.
 - **Locatários:** Apresentação do contrato de locação de imóvel residencial vigente acompanhado de conta de consumo em nome do locador. O endereço informado deverá corresponder às instalações físicas de uso efetivo e exclusivo da empresa, não sendo aceitos endereços de coworking, escritórios virtuais ou outros espaços compartilhados.

3. DOCUMENTAÇÃO SOCIETÁRIA E OPERACIONAL OBRIGATÓRIA (CLIENTES PJ)

- **Atos Constitutivos:** Contrato Social consolidado (com todas as alterações vigentes) registrado na Junta Comercial, ou Estatuto Social acompanhado da Ata de Eleição da Diretoria atual publicada em diário oficial (para Sociedades Anônimas).
- **Regularidade Fiscal:** Cartão CNPJ emitido no site da Receita Federal com situação cadastral "Ativa" na data de processamento do onboarding.
- **Mapeamento de Sócios e UBO:** Organograma societário (se aplicável) assinado pelo representante legal detalhando a cadeia de controle até a identificação das Pessoas Físicas consideradas Beneficiárias Finais (UBO) com mais de 25% de participação.
- **Descrição Formal do Modelo de Negócio:** Apresentação de documento descritivo oficial (*Executive Summary*, Pitch Deck, ou Memorial Descritivo de Atividades assinado pelo Diretor/Administrador), detalhando:
 - A natureza das atividades operacionais e principais fontes de receita.

- Público-alvo (B2B, B2C, Governo) e os principais canais de distribuição/comercialização.
- Fluxo financeiro estimado (nacional e internacional) e a justificativa para a utilização da infraestrutura de ativos virtuais da instituição.
- **Dossiê de Histórico Jurídico e Regulatório:**
 - Certidões Cíveis, Criminais e de Falência/Recuperação Judicial emitidas pelas Justiças Federal e Estadual da sede da PJ (abrangendo os últimos 5 anos).
 - Certidão de Regularidade do FGTS (CRF) e Certidão Negativa de Débitos Trabalhistas (CNDT).
 - Comprovação de registro, autorização ou dispensa de balcão regulatório perante órgãos competentes, se a atividade fim exigir (ex: CVM, BACEN, SUSEP).

4. LISTAGEM DOCUMENTAL PARA DILIGÊNCIA AVANÇADA (EDD - RISCO ALTO, PEP E CRIPTOATIVOS/OTC)

Clientes enquadrados na categoria de Risco Alto, Pessoas Politicamente Expostas (PEP) ou que operem em modelos de alta complexidade (como Mesas OTC e outras estruturas baseadas em criptoativos) devem fornecer, obrigatoriamente, comprovações robustas de sua integridade financeira e regulatória:

A. Para Pessoas Físicas (PF)

- Cópia integral do recibo de entrega e da Declaração de Imposto de Renda de Pessoa Física (DIRPF) do último exercício fiscal.
- Extratos bancários consolidados de outras contas de sua titularidade em instituições do SFN abrangendo os últimos 3 (três) meses de movimentação.
- Escrituras públicas de compra e venda de imóveis ou contratos de alienação de ativos que justifiquem aportes patrimoniais massivos extraordinários.

B. Para Pessoas Jurídicas (PJ Tradicional)

- Balanço Patrimonial assinado por contador habilitado contendo o respectivo número de registro no CRC.
- Declaração de Faturamento Bruto Anual assinada conjuntamente pelo representante legal da empresa e pelo contador responsável.
- Demonstração do Resultado do Exercício (DRE) recente atestando a capacidade operacional e financeira da empresa para suportar os volumes de negociação pretendidos nas Mesas OTC.

C. Para Mesas OTC, Exchanges e Modelos Baseados em Criptoativos (SPSAV)

Além dos documentos dispostos nos itens A e B anteriores, as empresas que operam com ativos virtuais devem comprovar a aderência à Lei nº 14.478/2022 (Marco Legal dos Criptoativos) e normativas correlatas, mediante entrega de:

- **Evidência de Autorização Regulatória:** Cópia da licença, autorização provisória ou protocolo de pedido de autorização de funcionamento perante o Banco Central do Brasil (ou regulador equivalente no país de origem, caso seja estrangeira).
- **Comprovante de Regularidade Fiscal Específica:** Relatórios comprobatórios de envio, demonstrativos de conformidade ou recibos de entrega referentes à Instrução Normativa RFB nº 1.888/2019 e Instrução Normativa RFB nº 2.291/2025, demonstrando o estrito

cumprimento das obrigações de prestação de informações sobre operações com criptoativos à Receita Federal.

- **Parecer de Auditoria Externa Independente:** Cópia do último relatório de auditoria (focado em demonstrações financeiras e/ou avaliação de controles de custódia e *Proof of Reserves* - PoR), se aplicável.
- **Dossiê de Prevenção à Lavagem de Dinheiro (PLD/FTP):** Manual ou Política Corporativa de PLD/FTP formalmente aprovada pela diretoria da empresa cliente, acompanhada do organograma ou nomeação do Diretor de Compliance responsável perante o COAF/BCB.
- **Comprovação de Capacidade Técnica para Travel Rule (Regra de Viagem):** Apresentação de evidências documentais, políticas internas ou certificações técnicas que atestem que a instituição parceira ou cliente (Mesa OTC, Exchange, SPSAV) possui protocolos sistêmicos seguros e ativamente implementados para o envio, recepção e validação de dados de identificação de remetentes e destinatários em transferências de ativos virtuais, atestando sua plena capacidade tecnológica de cumprir a Recomendação 16 do GAFI/FATF.



ANEXO III - QUESTIONÁRIO DE DILIGÊNCIA AVANÇADA (EDD) PARA CLIENTES PJ DE ALTO RISCO

Objetivo: Reunir dados e evidências técnicas sobre a estrutura de governança, políticas internas, segurança cibernética e mitigação de riscos de fraude e lavagem de dinheiro das empresas classificadas como Risco Alto (Mesas OTC, SPSAVs e institucionais).

Este formulário deve ser preenchido, assinado eletronicamente pelo Diretor de Compliance, CISO ou Representante Legal do proponente, e acompanhado das evidências documentais exigidas.

Bloco 1: Estrutura Organizacional e Governança

1. Quem é o Diretor/Gestor formalmente responsável pelas políticas de PLD/FTP e Compliance da instituição? *(Favor informar Nome, Cargo, E-mail e CPF/Identificação).*
2. A empresa possui Comitê de Auditoria, Riscos ou Compliance ativo? Se sim, com qual periodicidade as regras e limites internos são revistos?
3. A estrutura societária da empresa envolve subsidiárias, holdings ou filiais localizadas em jurisdições consideradas de alta opacidade fiscal (Paraísos Fiscais) ou sob monitoramento do GAFI/FATF? Se sim, justifique a necessidade comercial dessa arquitetura.

Bloco 2: Políticas de PLD/FTP e Integridade da Operação

4. A instituição possui uma Política de Prevenção à Lavagem de Dinheiro e Financiamento ao Terrorismo (PLD/FTP) formalizada, documentada e aprovada pela Alta Administração? *(Fornecer o documento como evidência).*
5. A empresa adota uma Abordagem Baseada em Risco (ABR) para a aceitação e monitoramento de seus próprios clientes (KYC/KYB)? Descreva sucintamente como os níveis de risco são classificados na sua esteira de onboarding.
6. Como é realizado o monitoramento e a identificação de Pessoas Politicamente Expostas (PEP) e de indivíduos/entidades listados em sanções internacionais (OFAC, ONU, UE) na sua operação?
7. Qual ferramenta ou metodologia a sua empresa utiliza para realizar a análise de origem e rastreabilidade de ativos virtuais (*Blockchain Analytics* - ex: Chainalysis, Elliptic, TRM Labs)? Como procedem em caso de identificação de moedas com vínculos ilícitos (mixers, darknet)?

Bloco 3: Governança Regulatória e Reportes Compulsórios

8. (Exclusivo para SPSAVs) Descreva os procedimentos internos e tecnológicos implementados na sua organização para assegurar o cumprimento integral das exigências de prestação de informações da Instrução Normativa RFB nº 1.888/2019 e da Instrução Normativa RFB nº 2.291/2025. Como é garantida a exatidão e a rastreabilidade dos dados transacionais vinculados aos CPFs/CNPJs enviados à Receita Federal?
9. A empresa possui canal direto ou integração sistêmica estruturada para o envio de Comunicações de Atividades Suspeitas (CAS) ao COAF ou órgão de inteligência financeira equivalente? Quantos reportes ou alertas atípicos foram gerados/analísados nos últimos 12 meses?

10. A sua instituição já foi alvo de auditorias, fiscalizações ou processos sancionatórios por parte de reguladores financeiros (BCB, CVM, RFB ou estrangeiros) nos últimos 5 anos? Se sim, quais planos de remediação foram aplicados?
11. A sua instituição possui capacidade sistêmica e operacional para cumprir os requisitos da *Travel Rule* (Regra de Viagem - Recomendação 16 do GAFI/FATF), garantindo o envio, a recepção e a validação segura de dados de identificação de remetentes e destinatários em transferências externas de ativos virtuais? Caso positivo, especifique brevemente o protocolo ou a solução tecnológica utilizada para a troca destas mensagens de conformidade.

Bloco 4: Segurança Cibernética e Proteção de Dados

12. A empresa possui uma Política de Segurança da Informação (PSI) institucionalizada? Os dados cadastrais de seus clientes são armazenados sob quais critérios de criptografia e restrição de acesso?
13. Como a sua operação mitiga o risco de fraude de identidade (fraude ideológica) em sua própria plataforma? É utilizada validação biométrica e prova de vida (*Liveness Check*)?
14. Quem é o Encarregado pelo Tratamento de Dados Pessoais (DPO) da sua organização? Como a sua infraestrutura assegura os princípios de minimização e conformidade com a LGPD (ou regulamento de privacidade equivalente)?

Bloco 5: Estrutura Operacional, Custódia e Risco de Produto

15. A instituição opera com subcontas, contas "Omnibus" ou atua como intermediária provendo liquidez/infraestrutura para outras *exchanges* não reguladas (*Nested Services*)? Se sim, como é garantida a transparência do Beneficiário Final (UBO) nas transações?
16. A sua empresa negocia, provê liquidez ou oferece custódia para criptoativos com protocolos de anonimato aprimorado (*AECs / Privacy Coins*, ex: *Monero*, *Zcash*)?
17. Como é gerida a custódia dos ativos virtuais da operação? As chaves privadas são geridas integralmente por infraestrutura própria (descreva brevemente) ou há utilização de provedores de custódia terceirizados (*Custody-as-a-Service*, ex: *Fireblocks*, *BitGo*)?
18. Quais são as três principais jurisdições (países) de origem e destino dos recursos fiduciários movimentados pela sua empresa nos últimos 12 meses?

Checklist Consolidado de Anexos Obrigatórios (EDD)

Para agilizar a análise da sua solicitação, assinale os documentos que estão sendo enviados em anexo a este questionário:

- ☐ Cópia da Política Corporativa de PLD/FTP vigente.
- ☐ Balanço Patrimonial (Assinado por contador) e DRE recente.
- ☐ Declaração de Faturamento Bruto Anual.
- ☐ Organograma Societário detalhando UBOs (>25%).
- ☐ Evidência de Licença/Autorização de Funcionamento (BCB ou equivalente).
- ☐ Comprovantes de Reporte e Adequação Fiscal (INs RFB nº 1.888/2019 e nº 2.291/2025) (Se aplicável).

Declaração de Responsabilidade:

Declaro, na qualidade de representante legal/diretor de conformidade, que as informações prestadas neste questionário são expressão fiel da verdade e que os manuais e políticas anexados refletem os controles operacionais vigentes na instituição.

Data: __/__/____

Assinatura: _____

(Assinatura digital ICP-Brasil ou certificado corporativo válido)

