

NORMA DE KYT

(KNOW YOUR TRANSACTION)

CONTROLE DE VERSÕES DO DOCUMENTO

Versão	Data	Descrição
1.0	25/08/2026	Primeira emissão

APROVAÇÃO DO DOCUMENTO

Documento revisado, aprovado e ratificado pelos responsáveis abaixo identificados.

gov.br
Documento assinado digitalmente
CAROLINE DE SOUZA CALDEIRA
Data: 26/08/2026 17:06:06-0300
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: 2026.08.26 17:07:53-03'00'
Foxit PDF Reader Versão: 2025.2.0

Dr. Eduardo Salathiel da Silva
Chefe de Compliance
OAB/RJ nº 68.618

1. INTRODUÇÃO, ESCOPO E BASE REGULATÓRIA

1.1. Objetivo do Manual de KYT (Know Your Transaction)

O presente Manual de *Know Your Transaction* (KYT) estabelece as diretrizes normativas e os procedimentos operacionais inegociáveis para o monitoramento contínuo de todas as operações realizadas na infraestrutura da CALDEIRA NEGÓCIOS E INTERMEDIAÇÕES LTDA. O objetivo primordial deste manual é fornecer as ferramentas e regras sistêmicas necessárias para monitorar fluxos fiduciários e rastrear operações com ativos virtuais, visando à identificação tempestiva de atipicidades comportamentais, fracionamento de valores e indícios de Lavagem de Dinheiro e Financiamento ao Terrorismo (PLD/FTP).

Atuando como o principal mecanismo de vigilância contínua da instituição, as rotinas de KYT garantem que o tráfego financeiro transcorra de forma lícita, protegendo ativamente o patrimônio próprio, o dos clientes e a integridade do Sistema Financeiro Nacional (SFN).

1.2. A Integração Estrutural: KYC x KYT

A eficácia da prevenção à lavagem de dinheiro não se esgota na esteira de aceitação e qualificação cadastral do cliente. A integração entre os processos de Conheça Seu Cliente (KYC) e Conheça Sua Transação (KYT) é estrutural e indissociável.

Enquanto o fluxo de KYC possui foco estático, responsável por identificar o indivíduo, verificar sua documentação legal e definir sua capacidade financeira (linha de base de risco) no momento do onboarding, o fluxo de KYT representa a vigilância dinâmica. O monitoramento transacional tem o propósito de garantir a estrita consistência entre o perfil econômico-cadastral declarado pelo cliente e o seu comportamento financeiro efetivo (fiduciário e cripto) no dia a dia da plataforma. Qualquer transação que apresente desvio injustificado em relação a essa linha de base acionará automaticamente os gatilhos sistêmicos de alerta previstos neste manual.

1.3. Base Regulatória Setorial

A arquitetura de monitoramento, os bloqueios sistêmicos e o processo de reporte de suspeitas descritos neste Manual de KYT estão estritamente fundamentados no arcabouço jurídico brasileiro aplicável ao Sistema Financeiro Nacional (SFN) e ao mercado de ativos virtuais. A execução ininterrupta destas diretrizes garante a conformidade da instituição perante os seguintes instrumentos:

- **Lei nº 9.613/1998 (Lei de Lavagem de Dinheiro):** Impõe à instituição a obrigação inegociável de manter os registros de históricos transacionais atualizados. Esta lei fundamenta a obrigatoriedade de elaborar análises internas de inteligência financeira e viabilizar o envio sigiloso de Comunicações de Atividades Suspeitas (CAS) ao COAF.
- **Lei nº 14.478/2022 (Marco Legal dos Criptoativos) e Decreto nº 11.563/2023:** Exigem da instituição a adoção de boas práticas de governança e controles robustos no monitoramento contínuo de clientes e operações. O Decreto consolida a competência do Banco Central do Brasil para regular e supervisionar o setor, visando mitigar de forma ativa os riscos operacionais, sistêmicos e criminais inerentes à negociação descentralizada de criptoativos.
- **Regulação do Banco Central do Brasil:** A Resolução BCB nº 520/2025, especialmente seus arts. 44 a 47, disciplina o controle e o monitoramento de operações com ativos virtuais

e a identificação de operações suspeitas ou irregulares. A Circular BCB nº 3.978/2020 e a Resolução BCB nº 260/2022 serão observadas conforme o perímetro de aplicação, inclusive as alterações promovidas pela Resolução BCB nº 552/2026 às SPSAVs autorizadas.

- **Instrução Normativa RFB nº 2.291/2025 (DeCripto):** Disciplina a prestação de informações sobre operações com criptoativos a partir da competência julho de 2026. Os registros de competências anteriores permanecem sujeitos ao regime então aplicável e às respectivas obrigações de guarda.
- **Regra de Viagem (Travel Rule):** A coleta e a transmissão de dados do originador e do beneficiário fundamentam-se no art. 44 da Resolução BCB nº 520/2025 e observarão o regime de transição previsto na própria norma. A Recomendação 16 do GAFI/FATF será utilizada como referência internacional complementar, sem substituir a regulamentação brasileira.

- **Prevenção a Fraudes:** A Resolução BCB nº 142/2021, com as alterações da Resolução BCB nº 584/2026, passará a abranger serviços de ativos virtuais em 1º de janeiro de 2027, inclusive com retenções cautelares e registros nos casos previstos. A implementação deverá ser preparada sem antecipar como vigente obrigação cujo termo inicial ainda não ocorreu.

- **Compartilhamento de Indícios de Fraude:** A Resolução BCB nº 343/2023, alterada pela Resolução BCB nº 569/2026, alcançará a prestação de serviços de ativos virtuais a partir de 30 de outubro de 2026, conforme seu âmbito de aplicação.

2. GOVERNANÇA E PAPÉIS NO MONITORAMENTO TRANSACIONAL

A eficácia técnica do monitoramento transacional (*Know Your Transaction* - KYT) exige uma estrutura de governança independente, pautada em controles rigorosos de sistemas e na ausência de conflitos de interesse comerciais. Para assegurar a aderência irrestrita às resoluções do Banco Central do Brasil (BCB) e do COAF, ficam definidos os seguintes papéis e alçadas de responsabilidade na gestão do KYT:

2.1. Área de Inteligência Financeira e Compliance

A Gerência de Compliance atua como a proprietária operacional exclusiva dos processos de prevenção e monitoramento transacional. Compete a esta área:

- Monitorar ativamente e de forma contínua os logs de movimentação financeira (fiduciária e em ativos virtuais) dos clientes, visando identificar atipicidades em relação ao perfil econômico-patrimonial declarado no *onboarding*.
- Analisar os alertas disparados pelos motores automatizados e pelo rastreamento *on-chain* (blockchain), instaurando e investigando dossiês internos de análise de risco.
- Possuir autoridade suprema e independente para elaborar e realizar o envio estritamente sigiloso das Comunicações de Atividades Suspeitas (CAS) ao COAF, atuando de forma alheia a pressões ou metas de rentabilidade corporativa.

2.2. Tecnologia e Segurança da Informação (InfoSec)

A equipe de Tecnologia e Segurança Cibernética atua como o braço tecnológico habilitador, sendo a responsável direta por impor e blindar as diretrizes de PLD/FTP dentro da arquitetura de sistemas da CALDEIRA OTC. É de competência estrita da TI/InfoSec:

- Parametrizar e sustentar os motores de liquidação e de risco para aplicar as travas sistêmicas (*circuit breakers*), de forma que operações que excedam os limites de alçada, as janelas temporais ou que acionem listas restritivas sejam bloqueadas imediatamente, de maneira autônoma.
- Garantir tecnologicamente que toda transação, geração de alerta ou acesso a dossiês investigativos por parte dos analistas gere um rastro digital ininterrupto (logs de auditoria).
- Assegurar que estes logs sejam armazenados sob políticas de imutabilidade e criptografados, protegendo-os contra exclusão acidental ou adulteração maliciosa.

2.3. Segregação de Funções (Segregation of Duties - SoD)

Para anular o risco de fraude interna, manipulação indevida do monitoramento ou facilitação dolosa para a lavagem de dinheiro, a instituição adota a Segregação de Funções (SoD) como barreira lógica processual e sistêmica absolutamente inegociável. Ficam estabelecidas as seguintes vedações e segregações:

- **Isolamento Comercial e Operacional:** As equipes comerciais, gerentes de conta (B2B), operadores de mercado (*Traders*) e demais membros responsáveis pela originação de negócios não possuem nenhum privilégio de acesso lógico ou capacidade sistêmica para aprovar, suspender, liberar ou influenciar a tomada de decisão sobre os alertas de transações atípicas gerados pelo KYT. Tampouco possuem autoridade sistêmica para elevar limites ou dispensar o envio de documentações comprobatórias de origem de fundos.
- **Blindagem Investigativa:** O acesso aos painéis de alertas sistêmicos, ferramentas de *Blockchain Analytics* e aos dossiês de investigação do COAF é configurado como classificação Restrita, sendo limitado técnica e nominalmente a um número reduzido de analistas de Inteligência Financeira e Compliance. Este acesso é intransponível e sistemicamente vedado a qualquer outro colaborador não autorizado.

2.4. Alta Administração e Comitê de Risco

Embora a execução técnica e investigativa do monitoramento transacional seja delegada às áreas de Compliance e Tecnologia, a Alta Administração (Diretoria Executiva e Sócios) e o Comitê de Risco detêm o patrocínio estratégico e a responsabilidade institucional final sobre a efetividade do programa de Know Your Transaction (KYT).

Para assegurar a governança de alto nível e o cumprimento dos deveres fiduciários e regulatórios, compete a estas instâncias:

- **Aprovação Formal de Limites e Diretrizes:** É competência exclusiva da Diretoria Executiva aprovar formalmente este Manual de KYT, bem como ratificar os parâmetros sistêmicos de risco, as matrizes de limites temporais e as alçadas financeiras, garantindo que o monitoramento esteja estritamente alinhado ao apetite de risco da CALDEIRA OTC.
- **Revisão Periódica de Eficácia:** Avaliar, com periodicidade mínima anual, os relatórios gerenciais de desempenho emitidos pela área de Compliance. A Alta Administração tem o dever de revisar a eficácia, a precisão e o índice de falsos positivos dos motores de monitoramento automatizado e das ferramentas de *Blockchain Analytics*.
- **Provisão Contínua de Recursos:** Garantir e aprovar o provisionamento de orçamento e recursos tecnológicos necessários para a sustentação das ferramentas de KYT, assegurando que as equipes de Inteligência Financeira e InfoSec operem com sistemas

atualizados e capazes de detectar novas tipologias criminais no ecossistema de ativos virtuais.

- **Instância de Escalonamento Crítico:** Atuar como órgão colegiado de decisão suprema em cenários de incidentes de extrema gravidade, tais como o congelamento em massa de carteiras decorrente de novas sanções internacionais imprevistas (ex: determinações do CSNU ou OFAC) ou crises de liquidez induzidas pelo acionamento severo de travas de conformidade sistêmica.

3. MONITORAMENTO DO FLUXO FIDUCIÁRIO (OPERAÇÕES EM REAIS - BRL)

O monitoramento do fluxo fiduciário atua na vigilância contínua das movimentações em moeda nacional (BRL) realizadas através das contas e integrações bancárias da instituição. Este pilar do monitoramento assegura que os volumes de entradas (depósitos) e saídas (saques) estejam estritamente alinhados ao perfil de risco e à capacidade econômica comprovada do titular.

3.1. Incompatibilidade Financeira e Patrimonial

O sistema automatizado de monitoramento gerará alertas investigativos imediatos ao identificar transações fiduciárias cujos valores consolidados se apresentem desproporcionais à capacidade financeira, à renda ou ao faturamento informados pelo cliente no momento do cadastro (*onboarding*) ou em sua última atualização documental. Qualquer desvio injustificado em relação a essa linha de base de risco configura atipicidade comportamental e será submetido à análise da equipe de Inteligência Financeira.

3.2. Identificação de Fracionamento de Operações (*Smurfing*)

O motor de risco da instituição é parametrizado com gatilhos específicos para detectar a tipologia de fracionamento, comumente conhecida como *smurfing*. O sistema identificará e alertará a área de Compliance sobre a realização de transações fiduciárias consecutivas com valores imediatamente inferiores aos limites sistêmicos de alçada ou aos tetos estabelecidos para reporte compulsório. Esse padrão comportamental indica uma tentativa dolosa do usuário de burlar os mecanismos automatizados de controle e acionará a abertura de uma investigação imediata.

3.3. Monitoramento de Contas de Passagem (Alta Velocidade Transacional)

O monitoramento avaliará a velocidade e a lógica econômica da movimentação financeira para mitigar a utilização da plataforma como "conta de passagem". Os motores de risco analisarão o comportamento transacional efetivo, gerando alertas para ciclos rápidos de capital — tais como depósitos fiduciários que são imediatamente seguidos por saques do mesmo montante ou convertidos rapidamente em ativos virtuais para remessa externa —, sempre que não houver justificativa ou fundamentação econômica aparente para a operação.

3.4. Mecânica de Limites Temporais (*Rolling Window*) e Consolidação

Para impedir a evasão de controles no fluxo fiduciário e evitar que agentes ilícitos manipulem calendários, a governança dos limites quantitativos máximos de transação obedece a regras sistêmicas baseadas em janelas temporais contínuas:

- **Mecânica de Contagem de Prazo (*Rolling Window*):** O cômputo do limite transacional "Diário" compreende o ciclo ininterrupto de 24 horas a partir da primeira transação executada

pelo cliente. O limite "Mensal" compreende o ciclo contínuo dos últimos 30 dias corridos retroativos. O sistema é expressamente vedado de utilizar meses-calendário estáticos (ex: limite zerado automaticamente a cada dia 1º), mitigando de forma definitiva o risco de os clientes executarem o dobro do limite financeiro permitido na transição entre o último e o primeiro dia do mês.

- **Consolidação de Rotas (Fiduciário + Cripto):** O cômputo sistêmico do consumo dos limites temporais do cliente não é fragmentado. Ele engloba a somatória absoluta do volume transacionado em todas as vias da plataforma: são somados os depósitos e saques fiduciários liquidados ao valor nocional (equivalente convertido em reais) das entradas e saídas *on-chain* de ativos virtuais processadas no mesmo período. O atingimento do teto em qualquer uma destas janelas bloqueia automaticamente o envio de novas ordens sistêmicas no período.

3.5. Monitoramento Específico de Transações via PIX e Integração com o MED

Dada a liquidez instantânea e o funcionamento ininterrupto do arranjo de pagamentos PIX, o monitoramento do fluxo fiduciário exige controles sistêmicos dedicados para mitigar o risco de a plataforma ser utilizada como destino para fraudes, golpes ou lavagem em alta velocidade.

Para a proteção da instituição e do Sistema Financeiro Nacional, aplicam-se as seguintes regras de monitoramento específico:

- **Detecção de Microdepósitos e Contas Mulas:** O motor de risco da instituição deve parametrizar gatilhos para identificar e alertar sobre o recebimento atípico de um alto volume de microdepósitos via PIX em curtas janelas temporais. Atenção especial deve ser dada quando estes depósitos forem originados de múltiplas contas distintas, CPFs diversos ou chaves PIX aleatórias. Este padrão comportamental atua como um forte indicativo de uso da plataforma como "conta laranja" ou fase de testes para escoamento de golpes fracionados, devendo o saldo ser bloqueado preventivamente para a análise de Inteligência Financeira.
- **Integração com o Mecanismo Especial de Devolução (MED):** Quando a Instituição atuar como participante responsável no Pix, deverá manter integração e acompanhamento das notificações do MED. Quando a competência for do PSP ou banco parceiro, o procedimento será executado por esse participante, cabendo à Instituição encaminhar tempestivamente as informações e reconciliar o resultado.
- **Ação de Bloqueio Cautelar (Gatilho MED):** Diante do recebimento de uma notificação formal via MED (por suspeita de fraude, golpe ou falha operacional na instituição de origem), a plataforma acionará um bloqueio cautelar imediato do valor correspondente na conta do cliente.
- **Análise e Devolução:** A equipe de Compliance e Inteligência Financeira conduzirá a análise do alerta e do dossiê do cliente. Caso a suspeita de fraude seja confirmada e não haja justificativa lícita para a transação, a instituição promoverá a devolução técnica dos fundos à conta de origem, respeitando estritamente os prazos legais e os ritos de contestação regulamentados pelo Banco Central para a devolução do PIX.

- **Definição de Papéis no Pix/MED:** A matriz operacional identificará se a instituição, o banco ou o PSP parceiro atua como participante pagador, recebedor ou provedor de conta. Somente o participante competente executará ações no DICT, bloqueios, devoluções e

mensagens previstos na regulamentação; quando a competência for do parceiro, o caso será encaminhado com informações suficientes, canal de urgência e posterior reconciliação.

4. MONITORAMENTO ON-CHAIN E RASTREAMENTO DE ATIVOS VIRTUAIS (O CORE DO KYT)

Devido à natureza descentralizada e ao pseudoanonimato inerentes aos ativos virtuais, o monitoramento puramente fiduciário é considerado insuficiente para a mitigação plena de riscos. Por esta razão, a instituição aplica o rastreamento técnico da origem e do destino das operações diretamente na *blockchain* como pilar central e indispensável de segurança cibernética e de Prevenção à Lavagem de Dinheiro (PLD/FTP).

4.1. Ferramentas de *Blockchain Analytics*

Para o exercício do monitoramento *on-chain*, é mandatória a utilização contínua de metodologias e ferramentas sistêmicas especializadas de rastreabilidade (tais como Chainalysis, Elliptic ou TRM Labs). A área de Compliance deve utilizar estas soluções de forma ininterrupta para analisar a proveniência dos fundos (depósitos) e a destinação das saídas (saques). A capacidade técnica de identificar as rotas e os vínculos dos ativos virtuais é requisito prévio e inegociável para a listagem ou manutenção do suporte a qualquer ativo na plataforma.

Adicionalmente, a elegibilidade para a manutenção de parcerias com outras SPSAVs ou Exchanges é condicionada à demonstração documental e técnica de capacidade para a transmissão e recepção de dados identificadores de remetentes e destinatários, em estrita conformidade com a *Travel Rule*.

A instituição reserva-se o direito de vedar permanentemente a integração sistêmica com contrapartes que não garantam o compartilhamento seguro desses dados, sendo esta capacidade técnica de conformidade um requisito inegociável para o exercício da atividade de prestação de serviços de ativos virtuais em conjunto com a CALDEIRA OTC.

4.2. Classificação de Risco de Endereços (*Risk Scoring*)

Os sistemas de rastreamento *on-chain* avaliarão o comportamento e o histórico dos endereços de carteiras virtuais interligadas ao cliente, atribuindo-lhes pontuações de risco. O motor transacional emitirá alertas imediatos à equipe de investigação caso as análises apontem que as moedas virtuais depositadas ou sacadas pelo usuário possuam qualquer nível de vínculo com endereços caracterizados como de alto risco.

Exposição Indireta e Falsos Positivos: Vínculo indireto não produzirá bloqueio definitivo automático. A decisão considerará a distância em saltos, direção do fluxo, materialidade, recência, confiabilidade da atribuição, tipo de serviço, endereços compartilhados e possibilidade de falso positivo, com revisão humana nos casos relevantes.

4.3. Tratamento de Sanções e Listas Restritivas

As designações do Conselho de Segurança das Nações Unidas abrangidas pela Lei nº 13.810/2019 serão cumpridas sem demora e no alcance legal aplicável, após validação de identidade. OFAC, União Europeia, Reino Unido e outras listas estrangeiras serão avaliadas conforme nexo jurisdicional, contrato, relacionamento bancário e apetite de risco; salvo obrigação jurídica

específica, constituirão fator de risco e não indisponibilidade legal automática. Homonímias, erros de atribuição e vínculos indiretos exigirão validação e tratamento documentado.

4.4. Tipologias de Alto Risco em Cripto

O monitoramento KYT deflagrará, de maneira automática, investigações internas de alta criticidade sempre que for identificada a interação dos endereços do cliente com tipologias operacionais de ofuscação ou ilicitude. Os gatilhos sistêmicos de alerta englobam, obrigatoriamente, a detecção de carteiras associadas a invasões e ataques cibernéticos (*hacks*), plataformas de ofuscação e mistura de moedas (*mixers*) e mercados ilícitos (como a *Darknet*).

4.5. Proibição de Operações com Criptoativos de Privacidade (*Privacy Coins*)

A instituição proíbe expressamente a operação, a provisão de liquidez ou o suporte a criptoativos desenhados com protocolos de anonimato aprimorado (AECs - *Anonymity-Enhanced Cryptocurrencies*), a exemplo de moedas virtuais como Monero e Zcash. Pelo fato de essas tecnologias ofuscarem intencionalmente a identidade do remetente, do destinatário ou os saldos das transações, elas inviabilizam o rastreamento *on-chain* adequado e dificultam o cumprimento irrestrito das normativas de prevenção à lavagem de dinheiro.

Considerando a natureza tecnológica descentralizada da *blockchain*, que impossibilita o bloqueio prévio e absoluto de uma tentativa de depósito externo (transferência *on-chain*) direcionada a um endereço sob custódia da instituição, o motor transacional aplicará rígidas travas de contenção pós-recebimento. Caso a plataforma identifique a entrada de uma moeda de privacidade ou ativo não suportado, os fundos serão imediatamente isolados e colocados em quarentena sistêmica. Ficam sumariamente bloqueadas e proibidas quaisquer transações internas (negociação, conversão) ou solicitações de saque desses ativos pelo usuário na plataforma, cabendo exclusivamente à área de Compliance a condução da investigação e a definição sobre o tratamento dos fundos retidos.

4.6. Regra de Viagem (Travel Rule)

A Instituição implementará a Regra de Viagem de acordo com o art. 44 da Resolução BCB nº 520/2025, o estágio regulatório aplicável e os procedimentos internos aprovados, observando os seguintes controles:

- **Procedimento de Origem (Remetente):** Quando a obrigação for aplicável à operação e à Instituição, coletar, validar e transmitir de forma segura à instituição receptora os dados mínimos do originador e do beneficiário exigidos pela regulamentação brasileira.
- **Procedimento de Destino (Recebedor):** Quando aplicável, verificar a presença, a consistência e a suficiência dos dados recebidos. Ausências ou divergências relevantes serão submetidas a diligência baseada em risco e não produzirão recusa automática sem avaliação do caso e da regra vigente.
- **Gestão de Riscos: Falhas de interoperabilidade, ausência de dados obrigatórios ou recusa injustificada de compartilhamento poderão motivar pausa, diligência adicional, recusa ou devolução da operação, conforme a regulamentação, o contrato e o risco documentado. A classificação definitiva não será automática e exigirá análise proporcional.**

- **Aplicabilidade da Travel Rule:** A coleta, validação, transmissão e retenção de dados do originador e do beneficiário observarão a norma brasileira aplicável, seus limites, prazos,

participantes e dados obrigatórios. Recomendações internacionais serão utilizadas como referência e não como fundamento autônomo de obrigação.

- **Proporcionalidade e Auto Custódia:** Ausência de interoperabilidade ou de dados não implicará classificação definitiva automática como alto risco, e carteiras auto custodiadas não serão presumidas ilícitas apenas por sua natureza. A operação poderá ser pausada, recusada, devolvida ou submetida a diligência adicional conforme a base normativa, o contrato, a capacidade técnica e o risco documentado.

5. GESTÃO DE ALERTAS E INVESTIGAÇÃO INTERNA

A identificação de atipicidades comportamentais nos sistemas de monitoramento fiduciário ou *on-chain* deflagra imediatamente o processo de investigação interna da instituição. A gestão diligente e tempestiva destes alertas é imperativa para separar comportamentos operacionais legítimos de ameaças reais de lavagem de capitais, financiamento ao terrorismo ou fraudes.

5.1. Triagem Inicial, Tratamento de Falsos Positivos e Princípio de Quatro Olhos (Maker-Checker)

Todo alerta gerado pelo motor transacional passará por uma triagem preliminar conduzida pela equipe de Compliance. O analista de Inteligência Financeira confrontará a operação atípica com o dossiê cadastral do cliente (KYC), avaliando se a movimentação é compatível com a capacidade financeira, a origem dos fundos e o modelo de negócio previamente declarados.

Caso a transação seja prontamente justificada pelo histórico consolidado do usuário ou trate-se de um falso positivo decorrente da sensibilidade dos gatilhos sistêmicos, o alerta poderá ser arquivado. Este arquivamento exige, de forma inegociável para todos os níveis de alerta, o registro formal da justificativa analítica que embasou o descarte.

O motor de monitoramento deve integrar, sempre que tecnicamente possível, as informações identificadoras do remetente e do destinatário recebidas via *Travel Rule* aos dossiês de análise transacional.

O cruzamento da identidade declarada pela SPSAV de origem com o comportamento observado na rede blockchain constitui etapa obrigatória para o descarte de alertas de risco ou para a ratificação de comportamentos suspeitos, garantindo a plena rastreabilidade dos ativos e a coerência entre o perfil do cliente e a natureza da movimentação recebida.

Controle de Dupla Validação (Princípio de Quatro Olhos): Para mitigar o risco de oclusão intencional, facilitação dolosa ou erro humano individual, o descarte de alertas não possui alçada autônoma e irrestrita. Caso o alerta gerado envolva tipologias de **Risco Alto** tais como possíveis correspondências em listas de sanções globais (OFAC/ONU), interações com moedas de privacidade, vínculos com *mixers* ou *darknet*, e operações de volumes massivos, o analista primário (*Maker*) não possuirá autonomia sistêmica para arquivá-lo isoladamente. O arquivamento definitivo de falsos positivos nestes cenários exigirá, obrigatoriamente, a revisão independente e a aprovação sistêmica (assinatura digital) de um supervisor de Compliance ou de um segundo analista sênior (*Checker*).

5.2. Abertura de Dossiês Investigativos (Relatórios de Inteligência Interna)

Caso o alerta automatizado ou a denúncia atípica não seja prontamente justificada pela capacidade financeira ou pelo histórico do cliente na triagem inicial, o analista tem o dever de instaurar um dossiê investigativo, formalizado como um Relatório de Inteligência Interna. Este dossiê tem como finalidade aprofundar a investigação e deve consolidar todas as evidências do comportamento suspeito, incluindo os extratos fiduciários, os comprovantes de rastreamento *on-chain* gerados pelas ferramentas de *Blockchain Analytics* e quaisquer informações ou documentos complementares solicitados para atestar a licitude das operações.

5.3. Acordo de Nível de Serviço (SLA) de Investigação

A análise de alertas observará prazo interno aprovado com base no risco, na complexidade e nos prazos legais ou regulamentares aplicáveis. Eventual referência a 45 (quarenta e cinco) dias constitui limite interno de gestão, não prazo regulatório, e não poderá atrasar comunicação, indisponibilidade ou outra providência obrigatória.

Ao término deste prazo regulatório, o dossiê investigativo deve ser formalmente encerrado pelo analista de Compliance. O encerramento exige a emissão de um parecer conclusivo, justificado e assinado, que determine a destinação da análise: o seu arquivamento definitivo (caso a operação tenha sido justificada durante a diligência) ou a sua elevação para reporte formal às autoridades de inteligência financeira.

Natureza do SLA: O prazo de 45 (quarenta e cinco dias) constitui limite interno de gestão e não prorroga prazo legal ou regulamentar. Prevalecerá sempre o menor prazo aplicável à comunicação, ao bloqueio, à indisponibilidade ou a outra providência obrigatória. Caso complexo poderá ter análise interna estendida mediante justificativa e aprovação, sem atrasar medida legal.

6. AÇÕES DE MITIGAÇÃO E CONGELAMENTO DE ATIVOS

A eficácia do monitoramento transacional exige a capacidade de interrupção imediata de fluxos financeiros anômalos. As ações de mitigação e congelamento atuam como a última barreira de defesa da CALDEIRA OTC para impedir a consolidação da lavagem de dinheiro, a evasão de divisas ou o financiamento ao terrorismo por meio de sua infraestrutura.

6.1. *Circuit Breakers* e Travas Sistêmicas Automáticas

A infraestrutura tecnológica poderá aplicar travas preventivas parametrizadas, proporcionais ao evento detectado e sujeitas a registro e revisão. Excesso de limite, alerta de risco ou vínculo indireto com endereço restritivo não produzirá bloqueio definitivo automático; a medida deverá observar fundamento, escopo, duração, revisão humana e condição de liberação, sem prejuízo de indisponibilidade legal obrigatória.

6.2. Congelamento por Ordem de Autoridades (Ordens Judiciais e CSNU)

Ordens judiciais serão cumpridas no exato escopo, valor e prazo determinados. Designações do Conselho de Segurança das Nações Unidas abrangidas pela Lei nº 13.810/2019 serão executadas sem demora, após validação de identidade e conforme o alcance legal aplicável. A indisponibilidade não será ampliada a ativos ou valores não alcançados sem fundamento específico.

6.3. Quarentena de Depósitos Cripto e Estornos de Titularidade Divergente

Depósitos de ativos virtuais associados a indicadores de alto risco, como ataques cibernéticos, serviços de mistura ou mercados ilícitos, poderão ser isolados ou submetidos a restrição cautelar proporcional enquanto houver análise. A classificação da ferramenta não será tratada isoladamente como prova de origem ilícita e exigirá validação de atribuição, materialidade, recência e possibilidade de falso positivo.

De forma análoga no fluxo fiduciário, aportes realizados a partir de contas bancárias cuja titularidade (CPF/CNPJ) seja divergente daquela cadastrada e aprovada pelo cliente na plataforma serão sumariamente retidos. Em ambos os cenários de quarentena, ficam terminantemente proibidas quaisquer operações de negociação ou solicitações de saque desses valores por parte do usuário. Caberá, exclusivamente, à área de Inteligência Financeira e Compliance a condução da investigação interna e a deliberação final sobre o tratamento do ativo, que poderá resultar na devolução técnica dos fundos à sua conta ou endereço de origem (estorno) ou na manutenção do seu bloqueio.

6.4. Governança de Restrições, Bloqueios e Liberações

Classificação e Registro: Cada medida distinguirá alerta, restrição cautelar interna, bloqueio Pix/MED, indisponibilidade decorrente de sanção e cumprimento de ordem. Deverão ser registrados fundamento, escopo, pessoa, ativo ou valor, responsável, início, duração, revisão e condição de liberação. Sempre que possível, a restrição ficará limitada à operação ou ao valor relacionado; bloqueio integral dependerá de ordem, obrigação legal ou necessidade concreta e proporcional devidamente documentada.

Liberação e Devolução: Cumprimentos e liberações exigirão dupla verificação e reconciliação. Ativo de alto risco não será devolvido automaticamente ao endereço de origem quando isso puder reenviar recursos a agente sancionado ou ilícito; Compliance, Operações e Jurídico definirão o tratamento e, quando necessário, solicitarão orientação da autoridade competente.

7. REPORTE REGULATÓRIO E COMUNICAÇÕES OFICIAIS

A instituição atua de forma proativa na proteção do Sistema Financeiro Nacional, cumprindo rigorosamente seu dever de reporte legal para garantir que os resultados do monitoramento transacional sejam convertidos em inteligência financeira acionável pelas autoridades.

7.1. Comunicação de Atividades Suspeitas (CAS)

Compete à área responsável por PLD/FTP e ao diretor designado decidir, formalizar e transmitir de modo sigiloso as comunicações ao COAF. Havendo decisão fundamentada de comunicar, o envio será realizado até o dia útil seguinte, nos termos da regulamentação aplicável, sem equiparar esse prazo a 24 horas corridas e sem aguardar o encerramento de SLA interno que possa atrasar a obrigação.

7.2. Proibição Absoluta de Sinalização (*Tipping-off*)

A condução de análises internas de inteligência financeira e o tráfego de relatórios de atividades suspeitas demandam o nível máximo de proteção estrutural da instituição. Sob nenhuma hipótese o cliente sob análise, seus representantes legais, ou terceiros não autorizados poderão ser informados, de maneira direta ou indireta, sobre a existência de um alerta transacional no monitoramento, a condução de uma investigação interna ou o envio de um reporte de atividade

suspeita ao COAF. Adicionalmente, para blindar a confidencialidade da operação, é terminantemente proibido o tráfego ou o compartilhamento de documentos e ofícios do COAF por meio de e-mails, aplicativos de mensageria instantânea (internos ou externos) ou dispositivos removíveis.

7.3. Suporte à Conformidade Fiscal (INs RFB nº 1.888/2019 e nº 2.291/2025)

A arquitetura de KYT deverá assegurar a integridade e a rastreabilidade dos dados necessários à DeCripto, instituída pela Instrução Normativa RFB nº 2.291/2025 para as operações realizadas a partir de julho de 2026. Dados de períodos anteriores observarão o regime aplicável à respectiva competência e os prazos de guarda correspondentes.

8. RETENÇÃO DE DADOS, SIGILO E AUDITORIA (LGPD)

A condução das rotinas de monitoramento transacional (KYT) e a salvaguarda dos registros financeiros ocorrem em perfeita harmonia com a Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais - LGPD). O tratamento destas informações fundamenta-se nas bases legais de cumprimento de obrigação legal ou regulatória e na prevenção à fraude.

8.1. Classificação Restrita de Alertas e Dossiês

Os dados resultantes do monitoramento transacional exigem o nível máximo de proteção da instituição. Todos os logs de alertas, os dossiês de investigação e as comunicações encaminhadas ao COAF recebem a classificação corporativa RESTRITA ou equivalente, com acesso limitado a pessoas nominalmente autorizadas. A comunicação realizada pela instituição não será denominada RIF: o Relatório de Inteligência Financeira é produzido pelo COAF a partir das informações recebidas.

8.2. Prazos de Guarda (Matriz de Retenção Regulatória)

Em estrita conformidade com as exigências do Banco Central do Brasil, do COAF e da Receita Federal, os históricos financeiros e os relatórios investigativos não podem ser excluídos imediatamente após o fim do relacionamento com o cliente. A guarda dessas informações obedecerá à seguinte matriz temporal compulsória:

- **Registros Transacionais e Análises:** A matriz de retenção definirá, por categoria, o fundamento, o termo inicial e o prazo aplicável. Os registros abrangidos pelos arts. 44 e 45 da Resolução BCB nº 520/2025 serão mantidos por, no mínimo, cinco anos, sem prejuízo de prazo superior previsto em norma específica.
- **Alertas, Análises e Comunicações ao COAF:** Serão conservados pelo prazo exigido na regulamentação de PLD/FTP aplicável à Instituição, com sigilo, acesso restrito, termo inicial documentado e extensão apenas quando houver fundamento legal, investigação, litígio ou ordem de preservação.

8.3. Exceção ao Direito ao Esquecimento e Dados On-Chain

O pedido de exclusão de dados (direito ao esquecimento) formalizado por um cliente com base na LGPD não possui caráter absoluto frente às obrigações de prevenção a ilícitos financeiros. Dados pessoais atrelados a históricos transacionais e saldos não podem ser excluídos imediatamente, devendo respeitar a retenção obrigatória. Adicionalmente, em virtude da natureza descentralizada

da tecnologia, os dados registrados diretamente nas redes *on-chain* (como endereços públicos de carteiras, *hashes* de transação e saldos transferidos) são tecnologicamente imutáveis e não podem ser alterados ou apagados pela CALDEIRA OTC.

O efetivo cumprimento do descarte, após a expiração dos prazos regulatórios de 5 a 10 anos, dar-se-á exclusivamente de forma *off-chain*. A instituição promoverá a sanitização e destruição criptográfica dos bancos de dados internos, apagando a tabela que correlaciona a identidade civil do cliente à sua chave pública na *blockchain*, promovendo assim a quebra de vínculo e a anonimização irreversível do registro.

Validação do Descarte: A exclusão de uma tabela de correlação, isoladamente, não será presumida anonimização irreversível. A instituição avaliará os meios razoáveis disponíveis para reidentificação e, encerrado o prazo sem fundamento de conservação, eliminará ou anonimizará os dados sob seu controle conforme avaliação técnica e a matriz de retenção aprovada.

8.4. Tuning, Testes de Efetividade dos Controles Internos e Periodicidade

A integridade e a precisão dos sistemas automatizados de monitoramento (KYT) são essenciais para a robustez do programa de PLD/FTP. A área de Compliance, em conjunto com a área de Tecnologia, realizará avaliações e calibragens (*tuning*) para validar a eficácia dos gatilhos sistêmicos de alerta. Estes testes garantem que as travas operacionais e os cruzamentos de rastreabilidade *on-chain* operem de forma ininterrupta e precisa, ajustando-se a novas tipologias criminais e evitando um volume excessivo de falsos positivos.

Periodicidade e Gatilhos de Calibragem:

Para garantir a aderência regulatória e a efetividade do monitoramento, o procedimento de *tuning* dos motores de risco não poderá ser genérico, devendo obedecer aos seguintes prazos e gatilhos:

- **Calibragem Ordinária:** As avaliações e os ajustes paramétricos (*tuning*) devem ser executados e documentados com **frequência mínima semestral**.
- **Calibragem Extraordinária:** O processo de *tuning* deverá ser acionado de forma imediata e extraordinária sempre que:
    1. Houver a detecção ou notificação (via COAF, BCB ou inteligência de mercado) de uma nova tipologia de fraude ou lavagem de dinheiro não mapeada anteriormente pelas regras sistêmicas.
    2. Ocorrer o lançamento de novos produtos financeiros, integração com novas *exchanges* ou suporte a novas *blockchains* na plataforma da instituição.
    3. Os relatórios gerenciais apontarem uma taxa anormal e excessiva de falsos positivos que esteja comprometendo o Acordo de Nível de Serviço (SLA) de investigação da equipe.

Qualquer falha ou vulnerabilidade identificada nos motores de risco durante estes testes será classificada com criticidade máxima, obedecendo a Acordos de Nível de Serviço (SLAs) estritos de correção pela equipe de Segurança da Informação.

9. TREINAMENTO, CAPACITAÇÃO TÉCNICA E CONSCIENTIZAÇÃO EM KYT

A efetividade do monitoramento transacional (*Know Your Transaction* - KYT) e a proteção da instituição dependem intrinsecamente do nível de especialização técnica e da atualização contínua dos analistas que operam os motores de risco. Para garantir a correta interpretação dos alertas e a aderência às normativas de PLD/FTP, a CALDEIRA OTC estabelece um programa obrigatório e contínuo de capacitação.

9.1. Obrigatoriedade de Capacitação Inicial e Contínua

Todo colaborador alocado na área de Inteligência Financeira e Compliance com acesso aos painéis de alertas sistêmicos e aos dossiês de investigação deve, obrigatoriamente, passar por um treinamento específico sobre este Manual de KYT e sobre a Política Corporativa de PLD/FTP. A concessão de acessos lógicos e privilégios sistêmicos para operar na triagem de falsos positivos e na elaboração de comunicações ao COAF é estritamente condicionada à conclusão com êxito deste módulo inicial. A área deverá promover, no mínimo semestralmente, reciclagens do conteúdo para toda a equipe.

9.2. Certificação em Ferramentas de *Blockchain Analytics* Considerando que a instituição obriga a utilização contínua de metodologias e ferramentas sistêmicas especializadas de rastreabilidade *on-chain* (conforme a Seção 4.1), o conhecimento prático nestes *softwares* é inegociável.

- **Treinamento Oficial:** Os analistas de Compliance deverão ser submetidos a treinamentos oficiais fornecidos pelas próprias desenvolvedoras das soluções contratadas pela CALDEIRA OTC (ex: programas de certificação da Chainalysis, Elliptic ou TRM Labs).
- **Atualização de Módulos:** Os colaboradores responsáveis pela investigação *on-chain* devem manter suas certificações ativas e atualizadas, garantindo a capacidade técnica de identificar ofuscações avançadas, rotas de *mixers*, saltos entre *blockchains* diferentes (*chain-hopping*) e o uso de pontes descentralizadas (*bridges*).

9.3. Atualização sobre Tipologias Criminais do Ecossistema Cripto

Devido à rápida e constante evolução das fraudes no ecossistema de ativos virtuais, o programa de capacitação deve prever módulos focados nas novas tipologias criminais. As campanhas de treinamento atualizarão os analistas sobre:

- Novas formas de fracionamento de valores e *smurfing* no ambiente cripto.
- Padrões transacionais vinculados a ataques cibernéticos (*hacks*), *ransomware* e esquemas de pirâmide (*scams*).
- Riscos associados a inovações tecnológicas, como carteiras não custodiais complexas, contratos inteligentes (DeFi) e novas gerações de moedas de privacidade (*Privacy Coins*).

9.4. Registro e Comprovação de Conformidade (Auditoria)

Todos os treinamentos, certificações externas e workshops aplicados à equipe de Inteligência Financeira e Compliance deverão ser rigorosamente documentados. As listas de presença, trilhas sistêmicas de conclusão de módulos de e-learning e os certificados oficiais de *Blockchain Analytics* emitidos devem ser arquivados pelo setor de Recursos Humanos e pelo Diretor Responsável.

A documentação servirá como evidência da capacitação e da efetividade dos controles. Quando aplicável ao processo de autorização, será disponibilizada para o relatório de asseguração razoável previsto na Instrução Normativa BCB nº 704/2026, com as alterações da Instrução Normativa BCB

nº 739/2026, sem transformar essa exigência específica em obrigação geral de certificação contínua.