

caldeira
otc



POLÍTICA DE PRIVACIDADE

CONTROLE DE VERSÕES DO DOCUMENTO

Versão	Data	Descrição
1.0	21/08/2026	Primeira emissão

APROVAÇÃO DO DOCUMENTO

Documento revisado, aprovado e ratificado pelos responsáveis abaixo identificados.



Documento assinado digitalmente
CAROLINE DE SOUZA CALDEIRA
Data: 21/08/2026 17:42:24-0300
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: 2026.08.21 17:33:05-03'00'
Foxit PDF Reader Versão: 2025.2.0

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

1. INTRODUÇÃO E IDENTIFICAÇÃO DO CONTROLADOR

A presente Política de Privacidade tem como objetivo demonstrar o compromisso e a transparência da CALDEIRA NEGÓCIOS E INTERMEDIações LTDA. (nome comercial CALDEIRA OTC), pessoa jurídica de direito privado, inscrita no CNPJ sob o nº 32.877.756/0001-00, com sede em Rua Visconde de Sepetiba, 935 - Sala 1025, parte 2 - Centro, Niterói - RJ, 24020-206, doravante denominada simplesmente "Instituição" ou "Controladora", com a privacidade e a proteção dos seus dados pessoais.

No contexto de sua atuação como Sociedade Prestadora de Serviços de Ativos Virtuais (SPSAV), a Instituição trata informações cadastrais, financeiras e transacionais de acordo com as finalidades e bases legais descritas nesta Política, adotando medidas técnicas e administrativas compatíveis com os riscos e com a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018 - LGPD).

1.1. Escopo de Aplicação

Este documento detalha as regras sobre o tratamento de dados pessoais em toda a nossa infraestrutura tecnológica e aplica-se a:

- **Clientes Titulares:** Pessoas físicas (maiores de 18 anos e civilmente capazes) ou representantes legais de pessoas jurídicas cujos dados identificadores foram submetidos, validados e aprovados no processo de qualificação (*Know Your Customer* - KYC).
- **Usuários dos Serviços:** Titulares que utilizam ativamente os serviços de intermediação, corretagem, operações de balcão (OTC) e liquidação fiduciária por meio de nossas plataformas web, aplicativos móveis ou conexões via API.
- **Visitantes e Potenciais Clientes (Leads):** Indivíduos que navegam em nossos ambientes digitais, acessam nossos canais oficiais, ou interagem com nossas campanhas de comunicação e ferramentas de atendimento.
- **Crianças e Adolescentes:** Os serviços de abertura e movimentação de conta não são destinados a menores de dezoito anos. A Instituição não buscará coletar intencionalmente seus dados; caso identifique coleta indevida, adotará medidas para bloquear ou eliminar os dados, ressalvadas as hipóteses legais de conservação, e poderá solicitar comprovação de responsabilidade parental quando necessário.

1.2. Integração Contratual

Esta Política integra os Termos de Uso como aviso de transparência sobre o tratamento de dados pessoais. A criação de credenciais, a navegação ou a utilização dos serviços demonstra ciência de seu conteúdo, mas não constitui consentimento genérico nem substitui consentimento específico, livre, informado e revogável quando essa for a base legal aplicável.

1.3. Base Legal e Regulatória

Esta Política considera, conforme a natureza de cada tratamento e o perímetro efetivamente aplicável à Instituição:

- **Proteção de Dados:** Lei nº 13.709/2018 (LGPD), Resolução CD/ANPD nº 15/2024, sobre comunicação de incidentes de segurança, e Resolução CD/ANPD nº 19/2024, sobre transferências internacionais de dados.

- **Ambiente Digital e Relações de Consumo:** Lei nº 12.965/2014 (Marco Civil da Internet), Decreto nº 8.771/2016 e Lei nº 8.078/1990 (Código de Defesa do Consumidor), quando aplicáveis aos serviços e aos registros tratados.
- **Ativos Virtuais e Obrigações Setoriais:** Lei nº 9.613/1998, Lei nº 14.478/2022, Decreto nº 11.563/2023, Resolução BCB nº 520/2025 e Instrução Normativa RFB nº 2.291/2025, observados o enquadramento da Instituição, os regimes de transição e a finalidade específica do tratamento.

2. QUAIS DADOS PESSOAIS COLETAMOS E COMO AS COLETAMOS

Para prestarmos os nossos serviços com segurança, transparência e em estrita conformidade com as normas do Sistema Financeiro Nacional, coletamos diferentes categorias de dados pessoais durante a sua jornada em nossa plataforma.

A coleta ocorre de forma ativa (quando você nos fornece os dados), automática (durante a utilização e navegação) e indireta (através do enriquecimento via *bureaus* especializados).

Abaixo detalhamos as categorias de dados tratados:

2.1. Dados de Cadastro e Qualificação de Risco (KYC e EDD)

Coletados no momento do *onboarding*, durante solicitações de aumento de limites operacionais (*Tiers*) ou procedimentos de Diligência Avançada (EDD). Incluem:

- Nome completo ou Razão social.
- CPF ou CNPJ.
- Data de nascimento.
- E-mail e Telefone celular.
- Endereço residencial ou fiscal.
- Imagens de documentos civis, como RG e CNH.
- Informações fiscais e comprovantes de renda ou faturamento.
- Informações sobre o modelo de negócio, histórico jurídico e reputacional dos titulares.

2.2. Dados Pessoais Sensíveis (Biometria Facial)

Para garantir a sua segurança e prevenir fraudes de falsidade ideológica na abertura e recuperação de contas, coletamos dados classificados como sensíveis:

- Geometria e biometria facial, capturadas ativamente durante a prova de vida em vídeo (*Liveness Check*).

2.3. Dados Transacionais e Financeiros (KYT e Operações)

Dados gerados e monitorados continuamente a partir da sua interação com as nossas plataformas de *trading* e liquidação fiduciária. Incluem:

- Endereços públicos de carteiras virtuais (*Wallets*).
- *Hashes* de transação em redes *blockchain*.
- Histórico de PIX e TED, incluindo chaves utilizadas, contas de origem e destino, e ID da transação (*End-to-End ID*).
- Volumes transacionados em moeda fiduciária e em criptoativos, além das cotações aceitas.
- Histórico de entradas e saídas de ativos virtuais e valores retidos ou congelados em contas.
- Pontuação de Risco (*Risk Scoring*) atribuída aos endereços de carteiras virtuais.

2.4. Dados de Dispositivos, Navegação e Marketing

Coletados para prover segurança tecnológica aos acessos, além de direcionar campanhas de comunicação (CRM):

- Endereços de IP de acesso transacional.
- Histórico de navegação na plataforma por meio de *cookies* e *pixels*.
- Histórico de interação com nossas campanhas publicitárias, como taxas de abertura e clique em e-mails.
- Faixa de patrimônio ou volume operado, utilizado para a segmentação de campanhas específicas (*VIP*).

2.5. Dados de Atendimento e Suporte (SAC e Ouvidoria)

Informações registradas quando você entra em contato com a Instituição em busca de suporte técnico, operacional ou para o envio de documentação adicional:

- Número de protocolo gerado no atendimento.
- Logs textuais de *chat* e gravações de chamadas de voz, caso aplicável.
- Eventuais documentos anexados voluntariamente por você nos chamados operacionais, tais como declarações de imposto de renda e balanços patrimoniais.

2.6. Uso de Cookies e Tecnologias de Rastreamento

Para otimizar a sua experiência de navegação, compreender o seu comportamento em nossas plataformas e direcionar campanhas de comunicação, a Instituição utiliza *cookies*, *pixels* e tecnologias de rastreamento semelhantes.

2.6.1. O que são *cookies*?

Cookies são pequenos arquivos de texto armazenados temporariamente no seu navegador ou dispositivo (computador, *smartphone* ou *tablet*) quando você acessa os nossos ambientes digitais. Eles permitem que a plataforma reconheça o seu dispositivo e memorize as suas ações e preferências ao longo do tempo.

2.6.2. Categorias de *Cookies* Utilizados:

- **Estritamente Necessários:** São essenciais para o funcionamento básico e seguro da plataforma. Eles viabilizam o tráfego de dados, a manutenção de sessões ativas logadas e o funcionamento de barreiras de segurança cibernética. Por serem vitais para a operação dos serviços prestados, esses *cookies* não podem ser desativados nos nossos sistemas.
- **Analíticos e de Desempenho:** Coletam informações agregadas sobre como você interage com a plataforma (ex: páginas mais visitadas, tempo de permanência, links clicados e eventuais mensagens de erro). Esses dados geram métricas estatísticas que nos ajudam a melhorar continuamente a usabilidade, a estabilidade e a performance da nossa infraestrutura.
- **Marketing e Publicidade:** Utilizados para mapear o seu histórico de navegação, permitindo a criação de perfis comportamentais para a entrega de anúncios, *newsletters* e ofertas de novos produtos que sejam relevantes para você. A coleta de dados por meio desta categoria depende exclusivamente do seu consentimento prévio.

2.6.3. Como Gerenciar as suas Preferências de *Cookies*:

Você tem total controle para aceitar, recusar ou gerenciar a utilização de *cookies* não essenciais. A qualquer momento, você pode exercer as suas escolhas das seguintes formas:

1. **Ajustes no Navegador:** A maioria dos navegadores modernos (como Google Chrome, Safari, Mozilla Firefox e Microsoft Edge) permite que você bloqueie, exclua ou seja avisado antes que um *cookie* seja armazenado. Isso pode ser feito acessando o menu de "Configurações", "Privacidade" ou "Segurança" do seu próprio navegador.
2. **Painel de Preferências e Opt-out:** Para os *cookies* e envios de marketing, você pode gerenciar ou revogar o seu consentimento diretamente no gerenciador de privacidade (*Preference Center*) disponibilizado em nosso site corporativo, ou acionar a opção facilitada de descadastramento (*opt-out*) localizada no rodapé de todas as nossas comunicações comerciais.
3. **Governança do Consentimento de Cookies:** O banner oferecerá opções visíveis e de facilidade equivalente para aceitar, rejeitar ou configurar cookies não necessários, sem caixas pré-marcadas. Cookies analíticos, de personalização ou publicidade que dependam de consentimento permanecerão desativados até a escolha do usuário. O inventário técnico deverá registrar nome, fornecedor, finalidade, categoria e duração de cada tecnologia efetivamente utilizada.

Ressaltamos que o bloqueio de *cookies* Estritamente Necessários diretamente pelo seu navegador poderá comprometer o funcionamento correto da plataforma, impedindo, por exemplo, o seu acesso seguro às áreas de negociação e liquidação financeira.

3. PARA QUAIS FINALIDADES E BASES LEGAIS TRATAMOS SEUS DADOS

Todo e qualquer tratamento de dados pessoais realizado pela Instituição é estritamente vinculado a uma finalidade específica e amparado por uma base legal prevista na Lei Geral de Proteção de Dados (LGPD).

Abaixo, detalhamos os motivos pelos quais utilizamos as suas informações:

3.1. Execução de Contrato (Art. 7º, inciso V, da LGPD)

Tratamos os seus dados para que possamos fornecer a infraestrutura tecnológica necessária para a prestação dos serviços aos quais você aderiu ao aceitar os nossos Termos de Uso. As finalidades incluem:

- Validar a sua identidade para permitir a abertura e a manutenção da sua conta.
- Processar ordens de compra, venda, conversão de ativos virtuais e operações de balcão (OTC).
- Recepcionar depósitos e executar saques em moeda fiduciária (Reais - BRL).
- Prestar suporte técnico, operacional e gerenciar o atendimento ao cliente via SAC.

3.2. Cumprimento de Obrigação Legal ou Regulatória (Art. 7º, inciso II, da LGPD)

Por operarmos no Sistema Financeiro Nacional e no mercado de ativos virtuais, somos rigorosamente regulados e obrigados por lei a reter e tratar certos dados. As finalidades incluem:

- Cumprir as normas de Prevenção à Lavagem de Dinheiro e Financiamento ao Terrorismo (PLD/FTP), estipuladas pela Lei nº 9.613/1998 e pelo COAF.

- Cumprir a obrigação de prestação de informações sobre operações com criptoativos por meio da DeCripto, nos termos da Instrução Normativa RFB nº 2.291/2025, observadas a aplicabilidade, a competência e as regras de transição relativas aos registros anteriores.
- Atender às regras do Arranjo PIX estabelecidas pelo Banco Central do Brasil (BCB), inclusive as relativas ao Mecanismo Especial de Devolução (MED).
- Conservar dossiês cadastrais e registros transacionais pelos prazos e termos iniciais previstos em cada obrigação legal ou regulatória aplicável, de acordo com a matriz de retenção referida no item 6.1.

3.3. Legítimo Interesse e Prevenção à Fraude (Arts. 7º, inciso IX, e 11, inciso II, alínea “g”, da LGPD)

Utilizamos dados para garantir a integridade da plataforma, proteger o seu patrimônio e promover os nossos serviços de forma responsável. As finalidades incluem:

- Realizar o monitoramento transacional contínuo (KYT) e o rastreamento *on-chain* para identificar atipicidades, contas mulas, fraudes ou interação com tipologias ilícitas (ex: *mixers* e *darknet*).
- Aplicar bloqueios cautelares e travas sistêmicas (*Circuit Breakers*) para proteção da conta.
- Realizar a análise comportamental de navegação e o envio de campanhas de marketing, comunicação comercial e ofertas de novos produtos aos clientes ativos, garantindo sempre a opção facilitada de descadastramento (*opt-out*).

3.4. Consentimento do Titular (Art. 11º, inciso I e Art. 7º, inciso I, da LGPD)

Em situações específicas onde a lei exige, solicitamos a sua autorização expressa. As finalidades incluem:

- Tratar biometria facial quando necessária à prevenção à fraude e à segurança do titular nos processos de identificação e autenticação, nos termos do art. 11, inciso II, alínea “g”, da LGPD. O consentimento será utilizado apenas quando constituir base legal válida, específica e livre para a finalidade concreta.
- Enviar *newsletters* e comunicações publicitárias para potenciais clientes (*leads*) que forneceram voluntariamente seus dados em nossas *landing pages* ou aceitaram *cookies* de marketing no site corporativo.

3.5. Exercício Regular de Direitos (Art. 7º, inciso VI, da LGPD)

Os dados podem ser utilizados para resguardar a Instituição ou viabilizar trâmites jurídicos. As finalidades incluem:

- Gerir contestações de transações, atuar na devolução compulsória de fundos via MED e responder a ofícios judiciais ou policiais.
- Conduzir procedimentos legais de sucessão patrimonial, analisando alvarás judiciais ou certidões de óbito para a liberação de saldos aos herdeiros legítimos.

3.6. Perfis e Decisões Automatizadas

A Instituição poderá utilizar regras, indicadores e modelos automatizados para atribuir risco a cadastros, dispositivos, transações e endereços de carteiras. Esses recursos poderão gerar alertas, solicitações de documentos, limites, retenções cautelares ou encaminhamento para análise humana, conforme os Termos de Uso e a legislação aplicável.

O titular poderá solicitar informações claras sobre critérios e procedimentos utilizados e a revisão de decisão tomada unicamente com base em tratamento automatizado que afete seus interesses, resguardados os segredos comercial e industrial. A Instituição realizará revisão por pessoa natural quando previsto em norma, adotado como salvaguarda interna ou necessário diante do risco ao titular.

4. COMPARTILHAMENTO DE DADOS COM TERCEIROS

A Instituição não comercializa, aluga ou vende os seus dados pessoais sob nenhuma hipótese. No entanto, para garantir o funcionamento seguro da plataforma, viabilizar as operações fiduciárias e de criptoativos, e cumprir com nossas rigorosas obrigações regulatórias, o compartilhamento de dados com terceiros (Operadores) e autoridades é indispensável.

O compartilhamento ocorre restritamente com as seguintes categorias de destinatários:

4.1. Parceiros Tecnológicos e Operadores de Infraestrutura

Compartilhamos dados com empresas que fornecem a base tecnológica para a prestação dos nossos serviços, exigindo contratualmente que apliquem as mesmas medidas de segurança e privacidade:

- **Provedores de Computação em Nuvem (Cloud):** Empresas como AWS (Amazon Web Services) e Google Workspace, utilizadas para a hospedagem segura de nossos sistemas, bancos de dados e armazenamento de arquivos.
- **Serviços de Validação de Identidade (KYC):** Fornecedores especializados em tecnologia de OCR e validação de biometria facial (ex: idwall, CAF, Unico) utilizados no processo de *onboarding* para prevenção de fraudes.
- **Plataformas de Atendimento e CRM:** Fornecedores de *software* de Helpdesk (ex: Zendesk, Intercom) para a gestão de tickets de suporte, bem como plataformas de automação de marketing (ex: HubSpot, RD Station, ActiveCampaign) para o envio de comunicações e *newsletters*.

4.2. Ecossistema Financeiro, Prevenção à Lavagem de Dinheiro (PLD) e Fraudes

Para mitigar riscos sistêmicos e processar os fluxos financeiros, integramos nossa plataforma a entidades do mercado tradicional e de ativos virtuais:

- **Instituições Bancárias e de Pagamento (BaaS):** Bancos liquidantes parceiros necessários para o processamento de depósitos, saques e transferências via PIX/TED, bem como para a gestão do Mecanismo Especial de Devolução (MED).
- **Ferramentas de Blockchain Analytics:** Empresas provedoras de *software* de rastreamento *on-chain* (ex: Chainalysis, Elliptic ou TRM Labs), com as quais compartilhamos endereços de carteiras (*wallets*) e *hashes* de transação para a atribuição de *score* de risco e identificação de tipologias ilícitas.
- **Prestadoras de Serviços de Ativos Virtuais (SPSAV) Parceiras (Regra de Viagem / Travel Rule):** Compartilhamento de dados do originador e do beneficiário nas operações e nas fases de implementação em que a regulamentação brasileira o exigir, especialmente conforme a Resolução BCB nº 520/2025. Recomendações do GAFI serão utilizadas como referência, e não como fundamento autônomo de obrigação.

4.3. Autoridades Governamentais, Reguladores e Órgãos Judiciais

Como entidade regulada, a Instituição possui o dever legal inegociável de compartilhar dados com o Estado Brasileiro, o que ocorre nas seguintes situações:

- **Receita Federal do Brasil (RFB):** Prestação das informações exigidas pela DeCripto, instituída pela Instrução Normativa RFB nº 2.291/2025, conforme a condição da Instituição como declarante, os dados obrigatórios e a competência aplicável.
- **Conselho de Controle de Atividades Financeiras (COAF):** Envio sigiloso de dossiês e comunicações de atividades financeiras suspeitas, sendo estritamente vedado por lei informar o cliente sobre a existência deste reporte (*vedação de tipping-off*).
- **Banco Central do Brasil (BCB):** Compartilhamento de dados via infraestrutura do Sistema Financeiro Nacional, especialmente na aprovação ou rejeição de contestações de fraude via PIX (MED).
- **Órgãos de Defesa do Consumidor, Policiais e Judiciais:** Envio de dados e logs de acesso a autoridades competentes (ex: Polícia Federal, Procon) mediante requisição formal, ofício civil/criminal ou determinação judicial para a condução de investigações.
- **Validação de Solicitações:** Antes do compartilhamento, a Instituição verificará a autenticidade, a competência da autoridade, o escopo, a base jurídica e a necessidade dos dados solicitados, salvo impedimento legal. O fornecimento será limitado ao necessário e manterá registro da solicitação, da decisão e das informações entregues.

5. TRANSFERÊNCIA INTERNACIONAL DE DADOS

A Instituição possui sua sede e operações no Brasil, porém, para garantir alta disponibilidade, escalabilidade e segurança de nível global, utiliza infraestrutura tecnológica fornecida por empresas multinacionais. Em decorrência disso, os seus dados pessoais podem ser transferidos, armazenados e processados em servidores localizados fora do território nacional.

A transferência internacional de dados ocorre restritamente nos seguintes cenários:

- **Hospedagem e Bancos de Dados (Cloud):** Armazenamento do sistema central, arquivos documentais e *backups* em servidores de provedores de nuvem (como a AWS), tipicamente localizados nos Estados Unidos (ex: região da Virgínia/EUA).
- **Cumprimento da Regra de Viagem (Travel Rule):** Quando exigido pela regulamentação brasileira e conforme o regime de transição aplicável, compartilhamento seguro de dados do originador e do beneficiário com a instituição receptora, inclusive em transferências internacionais de ativos virtuais.
- **Serviços de Análise (Analytics e PLD):** Uso de provedores globais de tecnologia para o rastreamento *on-chain* e combate à lavagem de dinheiro.
- **Ferramentas de Suporte e CRM:** Utilização de plataformas globais de *Helpdesk* (ex: Zendesk), automação de marketing e *Web Analytics*, cujos data centers majoritariamente encontram-se nos Estados Unidos ou Europa.

5.1. Garantias Legais e Salvaguardas

Antes de realizar transferência internacional, a Instituição identificará os agentes, países, categorias de dados, finalidades, riscos e o mecanismo autorizado nos termos da LGPD e da regulamentação da ANPD. Conforme o caso, utilizará decisão de adequação, cláusulas-padrão contratuais aprovadas pela ANPD incorporadas integralmente e sem alteração, cláusulas específicas aprovadas, normas corporativas globais ou outra hipótese legal aplicável. Informações atualizadas

e, quando cabível, cópia das cláusulas poderão ser solicitadas ao Encarregado, preservados os segredos comercial e industrial.

6. PRAZOS DE RETENÇÃO E ARMAZENAMENTO

A Instituição armazena os seus dados pessoais de forma segura e somente pelo tempo estritamente necessário para cumprir com as finalidades para as quais foram coletados, ou para resguardar o cumprimento de exigências legais vigentes.

É fundamental compreender que a solicitação de encerramento da sua conta e o término do nosso contrato não resultam na exclusão imediata de todos os seus dados pessoais.

6.1. Retenção Regulatória Compulsória

Em estrita conformidade com as determinações e normas do Banco Central do Brasil (BCB), do Conselho de Controle de Atividades Financeiras (COAF) e da Receita Federal do Brasil (RFB), os seus registros cadastrais, dossiês documentais completos (KYC) e todo o histórico transacional devem ser retidos de forma compulsória.

- **Prazo por Categoria:** Não haverá prazo único de cinco a dez anos para todos os dados. A matriz de retenção indicará, para cada categoria, finalidade, fundamento legal ou regulatório, prazo mínimo e máximo, responsável, controle de acesso e destinação após o término.
- **Termo Inicial e Preservação:** O início da contagem será definido por categoria, podendo corresponder à operação, coleta, encerramento da finalidade ou término do relacionamento. Ordem de autoridade, investigação, auditoria, disputa ou legal hold poderá suspender o descarte apenas dos dados relacionados e pelo período necessário.

6.2. Suspensão do Direito de Eliminação

Solicitações de eliminação ou anonimização serão avaliadas caso a caso. Obrigações legais ou regulatórias, exercício regular de direitos, prevenção à fraude, ordem de preservação ou outra hipótese do art. 16 da LGPD poderão justificar a conservação, que ficará restrita aos dados necessários e será explicada ao titular quando cabível.

Encerrado o prazo aplicável e inexistindo fundamento para conservação, os dados serão eliminados, anonimizados ou mantidos em arquivo restrito quando houver base legal remanescente. O descarte deverá ser documentado e considerar cópias, backups, sistemas de terceiros e limitações técnicas aplicáveis.

7. A NATUREZA IMUTÁVEL DA BLOCKCHAIN (AVISO ESPECÍFICO DE SPSAV)

Devido à arquitetura descentralizada que fundamenta as redes de criptoativos operadas pela Instituição, o tratamento de dados *on-chain* (diretamente na rede) possui limitações tecnológicas intrínsecas que diferem dos sistemas de banco de dados tradicionais.

7.1. Imutabilidade Tecnológica

É fundamental que você tenha ciência de que os dados registrados diretamente em redes *blockchain* públicas, tais como os endereços públicos de carteiras (*wallets*), os *hashes* de transação e os saldos atrelados são, por sua própria natureza tecnológica, imutáveis. Isso significa que, uma

vez processada e validada a transação na rede externa, é tecnicamente impossível que a Instituição altere, oculte ou apague essas informações.

7.2. Descarte por Anonimização (*Quebra de Vínculo Off-Chain*)

Diante dessa barreira tecnológica, o cumprimento do direito à exclusão de dados segue um rito específico no mercado de ativos virtuais.

Uma vez expirados os prazos legais de retenção compulsória (descritos no Item 6 desta Política), o procedimento de descarte e eliminação de dados consistirá, de forma exclusiva, na destruição dos registros nas bases de dados internas (*off-chain*) da Instituição.

A Instituição adotará medidas tecnicamente disponíveis sobre os sistemas que controla, como exclusão de identificadores desnecessários, desvinculação, restrição de acesso ou retenção segregada. A eliminação de uma tabela de correlação não garante, por si só, anonimização irreversível dos registros públicos da blockchain; o resultado será avaliado caso a caso, considerando os meios razoáveis disponíveis para reidentificação.

8. DIREITOS DOS TITULARES DOS DADOS

A Instituição assegura a você o pleno exercício de seus direitos previstos na Lei Geral de Proteção de Dados (Lei nº 13.709/2018 - LGPD). A qualquer momento, mediante requisição formal aos nossos canais de atendimento, você poderá solicitar:

- **Confirmação e Acesso:** Obter a confirmação de que tratamos os seus dados e solicitar o acesso a eles.
- **Correção e Atualização:** Requerer a correção de dados incompletos, inexatos ou desatualizados, mantendo o seu dever de veracidade perante o seu cadastro.
- **Portabilidade:** Solicitar a portabilidade dos seus dados cadastrais a outro fornecedor de serviço ou produto.
- **Revogação do Consentimento:** Revogar, a qualquer momento, o consentimento fornecido anteriormente para o tratamento de dados específicos (como envios de campanhas de *marketing*), sem que isso afete a legalidade do tratamento realizado antes da revogação.
- **Informações sobre Compartilhamento:** Solicitar informações sobre as entidades públicas e privadas com as quais compartilhamos os seus dados.
- **Adequação do Tratamento:** Solicitar anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade, observadas as hipóteses legais de conservação.
- **Oposição e Decisões Automatizadas:** Opor-se a tratamento realizado em desconformidade e solicitar informações e revisão de decisão tomada unicamente com base em tratamento automatizado que afete seus interesses.
- **Petição e Reclamação:** Apresentar petição perante a ANPD e reclamação aos órgãos de defesa do consumidor, sem prejuízo dos canais internos de atendimento e do Encarregado.

8.1. Restrição ao Direito de Eliminação (*Direito ao Esquecimento*)

É fundamental alertar que o direito à eliminação de dados pessoais não é absoluto, especialmente quando contraposto às normativas financeiras nacionais.

Conforme detalhado no item 6, a conservação observará uma matriz por categoria de dado, finalidade, fundamento, termo inicial e prazo aplicável; não se presume um prazo único de cinco a dez anos para todo o conjunto de dados pessoais.

Pedidos de eliminação, anonimização ou bloqueio serão avaliados individualmente. A Instituição conservará somente os dados necessários enquanto subsistir obrigação legal ou regulatória, exercício regular de direitos, prevenção à fraude, ordem de preservação ou outra hipótese do art. 16 da LGPD, informando a justificativa quando cabível.

8.2. Prazos e Procedimentos de Atendimento (SLA)

Para resguardar o seu patrimônio, garantir a segurança da informação e evitar incidentes de engenharia social ou fraudes, todas as solicitações para o exercício de direitos previstos na LGPD estarão sujeitas a um processo prévio de validação de identidade do solicitante.

Uma vez confirmada a identidade do solicitante, a Instituição analisará e responderá às requisições com transparência e nos prazos previstos na LGPD, na regulamentação da ANPD e nas demais normas aplicáveis a cada direito.

- **Confirmação Simplificada:** A confirmação da existência de tratamento será fornecida imediatamente, em formato simplificado, quando solicitada nessa modalidade, nos termos do art. 19 da LGPD.
- **Declaração Completa:** A declaração clara e completa sobre origem dos dados, inexistência de registro, critérios utilizados e finalidade do tratamento será fornecida em até 15 (quinze) dias, nos termos do art. 19 da LGPD. Os demais direitos observarão os prazos específicos aplicáveis e a complexidade da solicitação, sem extensão indevida.

8.2.1. Justificativa de Não Atendimento

Na hipótese de a solicitação não poder ser atendida, a Instituição fornecerá resposta fundamentada no prazo aplicável, indicando as razões de fato ou de direito e, quando cabível, a possibilidade de petição à ANPD ou de utilização de outros canais competentes.

9. SEGURANÇA DA INFORMAÇÃO

A Instituição emprega os melhores esforços e adota medidas técnicas, administrativas e organizacionais robustas para proteger os seus dados pessoais contra acessos não autorizados, perdas, alterações, destruição ou vazamentos.

A nossa infraestrutura de segurança contempla os seguintes controles e barreiras tecnológicas:

- **Criptografia:** Garantimos a proteção das informações utilizando padrões rigorosos de criptografia, tanto para dados em trânsito pela rede (*protocolo TLS 1.3*) quanto para dados armazenados em repouso nos nossos bancos de dados e *backups* (*padrão AES-256*).
- **Controle de Acessos Rigoroso:** Aplicamos o Controle de Acesso Baseado em Funções (RBAC), assegurando que nossos colaboradores tenham visibilidade apenas das informações estritamente necessárias para a execução de suas tarefas diárias (*Need-to-Know*). Além disso, mantemos trilhas de auditoria e *logs* imutáveis para monitorar e registrar qualquer acesso aos dossiês de clientes.
- **Autenticação Multifator (MFA):** A utilização da Autenticação Multifator (MFA) atua como uma barreira de proteção cibernética inegociável. Ela é um requisito tecnológico bloqueante

tanto para o acesso dos nossos colaboradores aos sistemas internos, quanto para a sua autenticação e aprovação de transações nas interfaces da nossa plataforma.

- **Isolamento e Travas Sistêmicas:** Mantemos uma rigorosa segregação entre os nossos ambientes operacionais e de teste. Também operamos travas sistêmicas de segurança que impedem automaticamente a realização de depósitos fiduciários ou transferências envolvendo contas bancárias de titularidade divergente, exigindo sempre a correlação de mesma titularidade (Mesmo CPF/CNPJ).

9.1. Resposta a Incidentes de Segurança e Comunicação

A Instituição adota diretrizes estritas de governança e matrizes de risco estruturadas para atuar de forma rápida e eficaz na contenção de eventuais ameaças cibernéticas.

Embora utilizemos infraestrutura de ponta e protocolos rigorosos para a proteção do nosso ecossistema, reconhecemos que a segurança da informação é um processo de melhoria contínua. Na hipótese excepcional de ocorrência de um incidente de segurança que possa acarretar risco ou dano relevante aos seus dados pessoais ou patrimônio, a Instituição compromete-se a atuar com total transparência e presteza, adotando as seguintes medidas:

- **Mitigação e Contenção Imediata:** Acionamento automático dos nossos protocolos internos de resposta a incidentes para isolar a infraestrutura afetada, neutralizar a ameaça e cessar a vulnerabilidade sistêmica.
- **Comunicação Transparente ao Titular:** Quando o incidente puder acarretar risco ou dano relevante, os titulares afetados serão comunicados no prazo regulamentar aplicável, por canais adequados. A comunicação indicará natureza e categorias de dados, riscos, medidas adotadas, contato do Encarregado e recomendações, sem divulgar informação que amplie o risco de segurança.
- **Reporte Regulatório:** A Controladora notificará a ANPD e, quando aplicável, o Banco Central do Brasil ou outra autoridade competente no prazo, formato e conteúdo previstos na regulamentação vigente. Caso todas as informações não estejam disponíveis de imediato, serão fornecidas complementações no prazo regulamentar, mantendo-se evidências da avaliação e das comunicações realizadas.

10. CONTATO DO ENCARREGADO DE DADOS (DPO)

Para atuar como o canal de comunicação oficial entre a Instituição, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD), nomeamos um Encarregado pelo Tratamento de Dados Pessoais (DPO).

Caso você tenha qualquer dúvida sobre esta Política de Privacidade, deseje exercer os seus direitos previstos na LGPD ou precise realizar requisições relacionadas ao tratamento dos seus dados pessoais, por favor, entre em contato com o nosso Encarregado através dos canais abaixo:

- **Nome do Encarregado (DPO):** [Nome do profissional ou da consultoria terceirizada]
- **E-mail Oficial (Canal de Atendimento):** [ex: dpo@suaempresa.com.br ou privacidade@suaempresa.com.br]
- **Telefone de Contato:** [Opcional, inserir se aplicável]

A Instituição compromete-se a receber, analisar e responder a todas as suas solicitações de forma transparente e tempestiva, respeitando os prazos estipulados pela legislação vigente.

11. ATUALIZAÇÕES E ALTERAÇÕES DESTA POLÍTICA

O mercado de ativos virtuais, a infraestrutura tecnológica e a legislação de proteção de dados estão em constante evolução. Por essa razão, a Instituição reserva-se o direito de revisar, modificar e atualizar esta Política de Privacidade a qualquer momento.

Essas alterações têm como objetivo refletir o aprimoramento contínuo dos nossos processos de segurança, a introdução de novas funcionalidades na plataforma ou a estrita adequação a novas diretrizes regulatórias emitidas pela Autoridade Nacional de Proteção de Dados (ANPD), Banco Central do Brasil (BCB) ou Receita Federal.

11.1. Como você será notificado

Sempre que realizarmos alterações materiais ou significativas nas condições de tratamento dos seus dados pessoais, comprometermo-nos a comunicá-lo com antecedência razoável à entrada em vigor das novas regras. Essa notificação ocorrerá das seguintes formas:

- Envio de um comunicado direto para o e-mail principal cadastrado e validado em sua conta.
- Exibição de um aviso em destaque (*pop-up*, *banner* ou notificação *push*) durante o seu primeiro acesso à plataforma *web* ou aplicativo móvel após a atualização.

11.2. Ciência e Novas Finalidades

A versão mais recente deste documento estará sempre disponível em nossos canais oficiais, indicando claramente a "Data da Última Atualização" no cabeçalho ou rodapé do texto.

A continuidade do uso dos serviços após a publicação da nova versão demonstrará ciência das informações atualizadas, mas não será tratada como consentimento para nova finalidade que dependa dessa base legal. Quando necessário, a Instituição solicitará consentimento específico e permitirá sua recusa ou revogação, informando as consequências e preservando os tratamentos amparados por outras bases legais.

11.3. Governança e Controle de Versões

A versão, a data de vigência e a síntese das alterações serão publicadas. Mudanças materiais serão submetidas à validação de Jurídico, Compliance, Segurança da Informação e do Encarregado, com aprovação institucional e preservação do histórico de versões e das evidências de comunicação.