

CÓDIGO DE CONDUTA E CONFORMIDADE

CONTROLE DE VERSÕES DO DOCUMENTO

Versão	Data	Descrição
1.0	20/08/2026	Primeira emissão

APROVAÇÃO DO DOCUMENTO

Documento revisado, aprovado e ratificado pelos responsáveis abaixo identificados.

gov.br
Documento assinado digitalmente
CAROLINE DE SOUZA CALDEIRA
Data: 20/08/2026 19:03:34-0300
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: 2026.08.20 13:26:00-03'00'
Foxit PDF Reader Versão: 2025.2.0

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

MENSAGEM DA DIRETORIA EXECUTIVA

Caros colaboradores, parceiros e prestadores de serviços,

Atuar como uma Sociedade Prestadora de Serviços de Ativos Virtuais (SPSAV) exige de nós não apenas excelência tecnológica, mas um compromisso inabalável com a ética, a transparência e a segurança. Estamos inseridos em um ecossistema financeiro dinâmico, global e em constante evolução, o que atrai grandes oportunidades, mas também riscos substanciais.

A Caldeira Negócios e Intermediações Ltda. (doravante, "Caldeira OTC" ou "Companhia") construiu sua reputação com base na confiança. Nossos clientes, parceiros institucionais e os órgãos reguladores confiam em nossa capacidade de proteger o Sistema Financeiro Nacional (SFN) contra ilícitos e de resguardar os dados que nos são confiados.

Este Código de Conduta e Conformidade não é apenas um manual de regras; ele reflete o DNA da nossa organização. Ele traduz nossa postura de Tolerância Zero para com crimes financeiros, fraudes e quebras de sigilo. A leitura e a aplicação rigorosa das diretrizes aqui contidas são obrigações de todos nós, independentemente do cargo ou função.

Contamos com o seu compromisso diário para mantermos um ambiente seguro, ético e em plena conformidade. Quando tiver dúvidas, pergunte. Quando suspeitar de algo errado, reporte. A integridade da nossa companhia está nas mãos de cada um de vocês.

Atenciosamente,

A Diretoria Executiva

GLOSSÁRIO DE TERMOS

Para o pleno entendimento das diretrizes deste Código, aplicam-se as seguintes definições:

- **SPSAV:** Sociedade Prestadora de Serviços de Ativos Virtuais. Sociedade sujeita à regulação, autorização e supervisão do Banco Central do Brasil, conforme a modalidade e o estágio regulatório aplicáveis, que presta serviços com ativos virtuais em nome de terceiros.
- **KYC (Know Your Customer):** "Conheça seu Cliente". Processo de identificação e validação de identidade e risco do cliente no momento da abertura da conta.
- **PLD/FTP:** Prevenção à Lavagem de Dinheiro, ao Financiamento do Terrorismo e ao Financiamento da Proliferação de Armas de Destruição em Massa. Conjunto de políticas, procedimentos e controles destinados a identificar, avaliar, monitorar e mitigar esses riscos.
- **COAF:** Conselho de Controle de Atividades Financeiras. Órgão brasileiro de inteligência financeira que recebe os reportes de atividades suspeitas da companhia.
- **Tipping-Off (Sinalização):** Divulgação indevida a cliente ou terceiro de informação sobre comunicação realizada ao COAF ou de elemento cuja revelação possa comprometer análise ou investigação. A Lei nº 9.613/1998 veda dar ciência da comunicação ao COAF a qualquer pessoa, inclusive à pessoa a quem a informação se refira.
- **MFA (Multi-Factor Authentication):** Autenticação de Múltiplos Fatores. Exigência de dois ou mais métodos (como senha + token físico/aplicativo) para acessar os sistemas da empresa.
- **Shadow IT:** Uso de sistemas, dispositivos, softwares, aplicativos de mensageria (ex: Telegram pessoal) e serviços de nuvem sem aprovação explícita do departamento de TI.
- **OTC (Over-The-Counter):** Mercado de Balcão. Negociações institucionais de grandes volumes de criptoativos realizadas de forma direta, fora do livro de ofertas público (Order Book).
- **UBO (Ultimate Beneficial Owner):** Beneficiário Final. A pessoa física que, em última instância, detém o controle de uma empresa (Pessoa Jurídica) cliente.

1. CULTURA DE CONFORMIDADE E TOLERÂNCIA ZERO

O presente Código de Conduta introduz os princípios éticos da organização e estabelece alinhamento com a legislação e a regulamentação aplicáveis ao Sistema Financeiro Nacional (SFN) e ao ecossistema de ativos virtuais, em especial com a Lei nº 14.478/2022, o Decreto nº 11.563/2023 e, conforme aplicável ao estágio regulatório e à modalidade de atuação da instituição, com as Resoluções BCB nº 519/2025, nº 520/2025 e nº 552/2026. Essas normas estabelecem requisitos de autorização, governança, conduta, controles internos, segurança e transparência para as prestadoras de serviços de ativos virtuais.

Considerando a natureza tecnológica e inovadora da companhia como uma Sociedade Prestadora de Serviços de Ativos Virtuais (SPSAV), essas diretrizes visam mitigar os riscos inerentes à velocidade, à globalização e ao pseudoanonimato das redes blockchain, garantindo a proteção do patrimônio próprio e de terceiros que trafega por nossa infraestrutura.

1.1. Tolerância Zero a Ilícitos

A atuação da organização exige o mais alto padrão de integridade para proteger o Sistema Financeiro Nacional (SFN) contra a ocultação de bens, direitos e valores oriundos de atividades ilícitas. Portanto, aplicam-se as seguintes regras fundamentais:

- A instituição adota uma postura de tolerância zero para qualquer tipo de ilícito financeiro, fraude ou tentativa de burla aos limites operacionais estabelecidos pela governança interna.
- A conivência ou a participação intencional de qualquer colaborador em atividades que facilitem crimes financeiros, bem como condutas negligentes de gravidade relevante, estarão sujeitas à apuração e às medidas disciplinares cabíveis, que poderão incluir demissão por justa causa quando presentes os requisitos legais e observada a proporcionalidade da medida.
- Para parceiros e prestadores de serviços, a participação nesses atos ilícitos resultará na rescisão contratual sumária.
- Indícios de atos de natureza criminosa deverão ser imediatamente escalonados ao Compliance e ao Jurídico para preservação de evidências, avaliação das obrigações de comunicação e, quando cabível, acionamento das autoridades competentes, sem prejuízo das medidas civis, trabalhistas e contratuais aplicáveis.

1.2. Responsabilidade Compartilhada

A manutenção de um ambiente seguro e ético é um dever de todos que compõem o ecossistema da companhia. Sendo assim, estabelece-se que:

- A prevenção à lavagem de dinheiro, o monitoramento e a conformidade não são responsabilidades exclusivas do setor de Compliance ou do Diretor Responsável perante o Banco Central. A observância das políticas, controles e deveres de reporte constitui responsabilidade compartilhada de toda a organização, nos limites das atribuições de cada função.
- As diretrizes e regras de prevenção aplicam-se de forma corporativa, obrigatória e irrestrita a todos os indivíduos, ambientes e operações relacionadas à companhia, sem exceções.
- O cumprimento destas regras é obrigatório para os membros da Alta Administração (Diretoria Executiva e Sócios), bem como para colaboradores de todos os níveis hierárquicos, estagiários e menores aprendizes.

- As mesmas obrigações se estendem a prestadores de serviço, consultores independentes e auditores externos, além de fornecedores de infraestrutura tecnológica e provedores de liquidez.
- Qualquer colaborador, parceiro, prestador de serviço ou terceiro que identifique, presencie ou suspeite de um comportamento atípico, fraude ou violação sistêmica que possa facilitar a lavagem de capitais tem o dever inegociável de reportar o fato.

2. PRIVACIDADE E PROTEÇÃO DE DADOS (LGPD)

O tratamento de dados pessoais no ecossistema da instituição exige o mais alto nível de responsabilidade e respeito à privacidade dos titulares. Este tópico foca no manuseio adequado de dados de terceiros e na obrigação de resguardar o sigilo absoluto das informações de clientes e da companhia.

2.1. Minimização e Finalidade

Em estrita conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD), a organização pauta-se pelo princípio da minimização. As seguintes regras regem o acesso e a coleta de informações:

- A coleta de dados pessoais, cadastrais, patrimoniais e societários de clientes deve ser restrita ao mínimo necessário e proporcional para cumprir as obrigações regulatórias perante o Sistema Financeiro Nacional e viabilizar a execução dos contratos.
- O acesso lógico a dossiês de clientes e bancos de dados corporativos é concedido estritamente com base no princípio da "Necessidade de Conhecimento" (Need-to-Know).
- O acesso a informações confidenciais será restrito única e exclusivamente àqueles indivíduos cujas funções corporativas e laborais exijam, de forma explícita e justificada, o contato com tais informações.
- Os colaboradores devem ter ciência de que solicitações de titulares para eliminação de dados pessoais não são absolutas. Dados e registros sujeitos a obrigação legal ou regulatória de conservação, necessários ao exercício regular de direitos ou abrangidos por ordem de preservação deverão ser mantidos pelo prazo aplicável. Para reporte fiscal de criptoativos, deve ser observada a Instrução Normativa RFB nº 2.291/2025 e a sistemática da DeCripto, vigente para operações realizadas a partir de julho de 2026, sem prejuízo da guarda dos registros relativos a períodos anteriormente submetidos à IN RFB nº 1.888/2019.

2.2. Sigilo de Dossiês e Informações Restritas

Os dados gerados, processados e armazenados pela instituição possuem classificações de proteção máximas. É dever fundamental do colaborador proteger a Confidencialidade, Integridade e Disponibilidade (Tríade CID) dessas informações:

- **Sigilo Absoluto:** O colaborador compromete-se a manter sigilo absoluto sobre informações classificadas como Confidenciais e Restritas.
- **Dados de Clientes e Dossiês (KYC):** Todas as informações coletadas no onboarding de clientes, incluindo dados pessoais, mídias, imagens de documentos de identidade civil e relatórios de Background Checks, são classificadas como "Confidencial".
- **Inteligência Financeira (PLD/FTP):** O acesso a comunicações de operações suspeitas encaminhadas ao COAF, aos respectivos dossiês de análise e a eventual Relatório de Inteligência Financeira (RIF) legitimamente recebido é classificado como "Restrita", devendo o seu tráfego ocorrer somente pelos meios seguros e autorizados pela instituição.

- **Ativos Estratégicos:** O dever de sigilo se estende imperativamente aos segredos de negócio da companhia, códigos-fonte, algoritmos proprietários de provisão de liquidez e market making, bem como a chaves criptográficas (como *private keys* e *seeds*) e credenciais de acesso.

2.3. Restrições Operacionais Inegociáveis

Para resguardar a integridade das informações cadastrais, evitar a evasão acidental ou intencional de informações (Shadow IT) e assegurar a conformidade irrestrita com a LGPD, os colaboradores, analistas e operadores sujeitam-se às seguintes proibições absolutas:

- **Uso de Contas Pessoais de E-mail:** É expressamente proibido enviar e-mails, arquivos, relatórios de KYC, dossiês cadastrais de clientes, planilhas ou trechos de código-fonte para contas de e-mail pessoais (ex: Gmail, Outlook.com, Yahoo).
- **Armazenamento em Nuvens Não Homologadas:** É terminantemente proibido transferir, sincronizar ou armazenar dados corporativos confidenciais de clientes, ou qualquer outro dado da companhia, em serviços públicos de nuvem de uso pessoal (ex: Dropbox, Google Drive pessoal, iCloud, OneDrive pessoal).
- **Plataformas de Compartilhamento:** É vedado o uso de sites de transferência rápida e temporária de arquivos (ex: WeTransfer, SendSpace, Pastebin) para trafegar dados Confidenciais ou Restritos.

3. SEGURANÇA NO AMBIENTE DE TRABALHO (MESA LIMPA E TELA LIMPA)

As salvaguardas de sigilo da instituição estendem-se de forma obrigatória ao comportamento físico e lógico dos colaboradores em suas estações de trabalho e instalações da companhia. Para mitigar o risco de acesso visual não autorizado, perda ou exposição acidental de informações confidenciais, todos devem aderir rigorosamente às seguintes diretrizes:

3.1. Tela Limpa (Proteção Lógica e Visual)

- **Bloqueio Manual e Compulsório da Sessão:** É obrigatório o bloqueio manual e imediato da tela do computador ou dispositivo móvel sempre que o colaborador se ausentar de sua estação de trabalho, ainda que por um breve período de tempo.
- **Bloqueio Automático:** Os equipamentos corporativos estão configurados com políticas de segurança que forçam o bloqueio automático por inatividade, sendo considerada violação desta política qualquer tentativa de burlar esse mecanismo.
- **Privacidade de Janelas Ativas:** Durante a condução de análises, manipulação de bases de KYC ou acesso a sistemas críticos, as janelas operacionais devem ser minimizadas ou fechadas sempre que não estiverem em uso ativo ou quando terceiros circularem no perímetro.
- **Películas de Privacidade:** É obrigatório o uso de películas de privacidade nas telas caso o colaborador execute suas funções em áreas com circulação de pessoas.

3.2. Mesa Limpa (Proteção Física)

- **Proibição de Documentação Exposta:** Sob nenhuma circunstância documentos impressos contendo dados pessoais de clientes, comprovantes de residência, chaves de API impressas, relatórios financeiros ou *seeds* de recuperação podem ser deixados desacompanhados sobre as mesas de trabalho ou em impressoras compartilhadas.
- **Proteção de Dispositivos de Segurança:** É terminantemente proibido deixar dispositivos físicos de segurança desacompanhados sobre a mesa ou conectados aos computadores.

- **Armazenamento Adequado:** Tokens de Autenticação Multifator (ex: YubiKeys), *Hardware Wallets* (ex: Ledger, Trezor) e cartões de acesso, quando não estiverem em uso, devem ser obrigatoriamente armazenados em gavetas trancadas ou cofres.
- **Salas de Reunião:** Estratégias de mercado ou fluxos lógicos desenhados em quadros brancos devem ser imediatamente apagados ao final das reuniões.

3.3. Descarte Seguro

- **Proibição de Lixo Comum:** Nenhum documento de KYC, papel contendo informações sensíveis ou dados confidenciais de clientes pode ser descartado no lixo comum ao atingir o fim de sua vida útil.
- **Fragmentação Obrigatória:** A destruição e o descarte físico seguro desses papéis devem ocorrer única e obrigatoriamente por meio de fragmentadoras mecânicas (fragmentadoras de papel) disponibilizadas pela instituição.

4. USO ACEITÁVEL DE FERRAMENTAS CORPORATIVAS E COMUNICAÇÃO

A integridade das operações e a proteção da propriedade intelectual da companhia dependem do uso correto e seguro das ferramentas tecnológicas disponibilizadas aos colaboradores. Este tópico estabelece as diretrizes sobre o que é permitido e esperado na utilização de dispositivos, sistemas e canais de comunicação da empresa.

4.1. Comunicação Homologada

Para assegurar a rastreabilidade das informações e a prevenção contra vazamentos de dados (Shadow IT), aplicam-se regras estritas aos canais de comunicação:

- A comunicação interna corporativa, as discussões sobre estratégias de negócios ou trading, a arquitetura de sistemas e o compartilhamento de arquivos devem ocorrer exclusivamente por meio das plataformas de mensageria corporativa oficialmente homologadas e fornecidas pela companhia (ex: Microsoft Teams, Slack corporativo).
- É expressamente proibido o uso de mensageiros pessoais (como contas pessoais de WhatsApp ou Telegram) para a troca de arquivos, documentos ou informações internas da companhia entre colaboradores.
- 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 naquelas ferramentas homologadas internamente pela companhia.
- Para a transferência interna segura de dados e validações necessárias, os colaboradores devem gerar links temporários e protegidos através do sistema de cofre de senhas corporativo (Vault).

4.2. Proteção de Credenciais

O acesso lógico aos sistemas da instituição obedece aos pilares do Princípio do Menor Privilégio e exige a adoção de posturas de segurança inegociáveis por parte de todos os usuários:

- É obrigatório o uso de senhas complexas, contendo exigência de comprimento mínimo e combinação de caracteres (letras, números e símbolos).
- O uso de Autenticação Multifator (MFA) é obrigatório, inegociável e atua como requisito bloqueante para todos os acessos a sistemas corporativos, painéis, VPNs e e-mails.
- Todo usuário deve possuir uma credencial de acesso individualizada e nominal.

- O uso de contas genéricas, compartilhadas ou de suporte técnico coletivo é estritamente proibido para usuários humanos acessarem, consultarem ou manipularem dados.
- O compartilhamento intencional de senhas de sistemas e acessos é considerado violação grave e estará sujeito às medidas disciplinares cabíveis, inclusive demissão por justa causa quando presentes os requisitos legais e observada a proporcionalidade da medida.

4.3. Inexistência de Privacidade no Uso

A empresa fornece os equipamentos e as redes com o objetivo exclusivo de viabilizar a execução das atividades laborais, aplicando-se a premissa de transparência no seu monitoramento:

- Todos os recursos computacionais e tecnológicos fornecidos pela organização (como notebooks, e-mails corporativos, acesso à internet e softwares de mensageria) são ferramentas de trabalho e de propriedade exclusiva da companhia.
- A empresa utiliza ativamente ferramentas de monitoramento em rede e nos dispositivos finais (soluções de EDR e DLP) nas estações de trabalho.
- A companhia pode monitorar, inspecionar e auditar o uso dos recursos corporativos para detectar acessos anômalos, transferências não homologadas, vazamentos de dados ou infrações de segurança, observados os princípios de finalidade, necessidade, proporcionalidade, transparência e segurança aplicáveis ao tratamento de dados pessoais.
- O colaborador deve estar plenamente ciente de que não há qualquer expectativa de privacidade absoluta no uso dos equipamentos e das redes corporativas fornecidas pela empresa.

5. SIGILO INVESTIGATIVO E VEDAÇÃO DE SINALIZAÇÃO (TIPPING-OFF)

Devido à natureza crítica das operações financeiras e das obrigações regulatórias da companhia perante o Sistema Financeiro Nacional, a condução de análises internas de inteligência financeira e o tráfego de relatórios de atividades suspeitas demandam o nível máximo de proteção estrutural e sigilo por parte de todos os colaboradores.

5.1. Proibição Absoluta de Tipping-Off (Sinalização)

Para garantir a efetividade dos controles de Prevenção à Lavagem de Dinheiro (PLD/FTP) e não comprometer investigações em andamento, aplica-se a regra de proibição absoluta de "tipping-off":

- Sob nenhuma hipótese o cliente sob análise, seus representantes legais ou quaisquer terceiros não autorizados poderão ser informados sobre investigações em curso.
- É terminantemente proibido sinalizar ou comunicar, de maneira direta ou indireta, que um alerta transacional foi gerado no monitoramento do cliente.
- É vedado informar a qualquer pessoa não autorizada sobre comunicação de operação suspeita encaminhada ao Conselho de Controle de Atividades Financeiras (COAF) ou revelar elementos de análise interna quando essa divulgação puder comprometer controles, apurações ou obrigações de sigilo. Comunicações ao COAF devem observar a vedação legal de ciência prevista na Lei nº 9.613/1998.

5.2. Vedações de Compartilhamento e Tráfego de Dados Restritos

Os alertas atípicos, dossiês de investigação e comunicações enviadas ao regulador recebem a classificação de segurança máxima da companhia: RESTRITA (ou Estritamente Confidencial). Para blindar a confidencialidade dessas operações, estabelecem-se as seguintes vedações tecnológicas:

- O acesso aos painéis de alertas, ofícios e relatórios do COAF é limitado a um número mínimo e nominal de analistas essenciais da área de Compliance, sendo sistemicamente vedado a equipes comerciais, de atendimento ou a qualquer outro colaborador não autorizado.
- É terminantemente proibido o tráfego ou o compartilhamento de documentos, ofícios ou relatórios do COAF por meio de e-mails convencionais.
- Tais documentos não podem transitar por aplicativos de mensageria instantânea (sejam eles internos corporativos ou externos) ou ser armazenados em dispositivos removíveis (como *pendrives*).

6. GOVERNANÇA E SEGURANÇA FÍSICA

A proteção do ambiente corporativo e dos ativos da instituição requer a aplicação de controles rigorosos tanto nos sistemas lógicos quanto nas instalações físicas. Este tópico estabelece as regras para a prevenção de fraudes internas e para a circulação segura nas dependências da empresa.

6.1. Segregação de Funções (SoD)

Para mitigar o risco de fraude interna, erros críticos, conluio ou manipulação indevida, a empresa adota o princípio da Segregação de Funções (Segregation of Duties - SoD) como barreira lógica e processual relevante:

- **Isolamento Comercial e Operacional:** A equipe comercial, os gerentes de conta e os operadores de mercado (Traders) não possuem qualquer privilégio de acesso ou capacidade sistêmica para aprovar cadastros de clientes, alterar perfis de risco ou definir e elevar limites operacionais na base de KYC.
- **Restrições no Desenvolvimento Tecnológico:** O desenvolvedor ou engenheiro de software que cria ou projeta os códigos não possui permissão para publicá-los no ambiente de produção.
- **Proteção de Fundos e Dados:** Desenvolvedores não podem possuir as chaves de API reais de movimentação de fundos, tampouco privilégios para consultar os dados reais de identificação dos clientes armazenados nos servidores produtivos.
- **Segregação e Reconciliação de Ativos:** Os ativos próprios e os ativos de clientes, bem como as respectivas chaves, registros e posições, deverão permanecer segregados e ser reconciliados com periodicidade e alçadas definidas em política específica e na regulamentação aplicável.
- **Evidências de Existência e Titularidade:** A instituição deverá manter evidências verificáveis da existência, titularidade, movimentação e conciliação dos ativos sob sua responsabilidade, observando as exigências aplicáveis de auditoria independente, prestação de informações e divulgação.

6.2. Acesso Físico e Anti-Carona (Tailgating)

O acesso físico não autorizado representa um risco crítico e pode comprometer a confidencialidade das operações. Dessa forma, as seguintes regras de segurança física devem ser rigorosamente cumpridas:

- **Identificação Obrigatória:** O acesso às dependências da companhia é restrito e controlado. É obrigatório o uso visível de crachá de identificação corporativa ou autenticação biométrica por todos os colaboradores durante todo o período de permanência no escritório.

- **Prevenção contra "Carona" (Tailgating):** É expressamente proibido permitir que pessoas não identificadas ou sem autorização aproveitem a abertura de portas controladas para ingressar nas dependências da empresa. Cada indivíduo tem a obrigação de registrar o seu próprio acesso.
- **Áreas Seguras e de Acesso Restrito:** O ambiente onde operam as equipes de mercado, as Mesas de Operação (Trade Desk), é considerado uma Área Segura e possui acesso restrito apenas aos colaboradores cujas funções exijam a presença no local.
- **Infraestrutura Crítica:** O acesso físico a salas de equipamentos e servidores é rigorosamente restrito, devendo essas áreas permanecer trancadas 24 horas por dia, com controle nominal de entradas e saídas e monitoramento contínuo.

6.3. Governança de Ativos Virtuais, Listagem e Stablecoins

A admissão, o monitoramento, a suspensão e a deslistagem de ativos virtuais deverão observar governança formal, critérios técnicos e medidas de proteção aos clientes.

- **Listagem e Decisão:** A listagem de ativos observará política aprovada, critérios técnicos documentados, instância decisória competente, registro das deliberações, declaração de conflitos de interesses e preservação das evidências utilizadas na decisão.
- **Suspensão e Deslistagem:** A suspensão ou deslistagem deverá considerar o risco do ativo e comunicar aos clientes, quando possível, o motivo, o cronograma, o tratamento de ordens, negociação, retirada, custos e saldos residuais. Medidas imediatas serão admitidas diante de risco relevante, com registro, proporcionalidade, revisão e comunicação tão logo seja possível.
- **Stablecoins:** A admissão e o monitoramento de stablecoins considerarão mecanismo de estabilização, qualidade e transparência das reservas, custódia e segregação, capacidade de resgate, auditoria disponível, paridade, concentração, contraparte, tecnologia, jurisdição e regulação aplicável.
- **Gatilhos de Reavaliação:** Perda de paridade, opacidade ou insuficiência de reservas, falha de resgate, incidente cibernético, ordem de autoridade ou deterioração relevante poderão resultar em monitoramento reforçado, restrição, suspensão ou deslistagem.

7. DEVER DE REPORTE E CANAL DE DENÚNCIAS

O estabelecimento de um ambiente corporativo seguro e transparente depende da colaboração ativa de todos na identificação de anomalias operacionais e éticas. A instituição valoriza a integridade e encoraja o apontamento de irregularidades de forma protegida.

7.1. Dever de Comunicação

A vigilância contra ilícitos é uma responsabilidade compartilhada que exige ação imediata frente a qualquer suspeita:

- Qualquer colaborador, parceiro, prestador de serviço ou terceiro que identifique, presencie ou suspeite de um comportamento atípico, fraude, violação sistêmica ou vulnerabilidade que possa facilitar a lavagem de capitais tem o dever inegociável de reportar o fato.
- Adicionalmente, os colaboradores devem reportar imediatamente à equipe de Segurança da Informação qualquer atividade suspeita, perda de equipamento corporativo, recebimento de e-mails de *phishing* ou comportamento incomum nos sistemas da companhia.

7.2. Utilização do Canal de Denúncias

- Para operacionalizar este dever inegociável de reporte, a instituição disponibiliza e mantém um Canal de Denúncias oficial, o qual é seguro, gerido de forma independente e acessível 24 horas por dia.

7.3. Garantia de Anonimato e Não-Retaliação

A companhia protege rigorosamente aqueles que atuam em defesa de sua conformidade e ética:

- A instituição assegura a confidencialidade do relato e o anonimato do denunciante, restringindo o acesso às informações ao mínimo necessário. Quando o canal disponibilizar opção de denúncia anônima, a identidade não será exigida, sem prejuízo das hipóteses legais de acesso ou revelação determinadas por autoridade competente.
- A empresa proíbe expressamente e tratará como falta gravíssima qualquer tipo de retaliação, assédio, intimidação, discriminação ou penalização (seja ela profissional ou pessoal) contra o colaborador que realizar a denúncia de irregularidades de boa-fé.
- Para garantir a imparcialidade e a segurança do denunciante, as apurações decorrentes dos relatos serão conduzidas sob estrito sigilo por instâncias imparciais da organização, como o Comitê de Risco e Segurança ou por meio de auditoria externa.

7.4. Atendimento, Reclamações e Ouvidoria

A instituição manterá mecanismos acessíveis, seguros e rastreáveis para atendimento e tratamento de reclamações, observada a regulamentação aplicável ao seu enquadramento.

- **Atendimento:** Os canais de atendimento deverão fornecer protocolo, informações sobre etapas e prazos e acesso a atendimento humano em situações críticas, com registros suficientes para acompanhamento, supervisão e melhoria dos serviços.
- **Ouvidoria:** Quando exigível, a Ouvidoria atuará como instância final interna, com responsável formalmente designado, independência, tratamento documentado, resposta conclusiva e reporte periódico à administração, conforme manual próprio e canais oficialmente divulgados.

8. MEDIDAS DISCIPLINARES E SANÇÕES

O encerramento deste código reforça a seriedade do compromisso de cada indivíduo com a segurança e a ética da companhia. O cumprimento das diretrizes deste Código de Conduta, bem como das normas e procedimentos associados, é obrigatório.

8.1. Proporcionalidade da Sanção

- A inobservância ou violação intencional das regras estabelecidas expõe a instituição, seus clientes e parceiros a riscos sistêmicos e financeiros inaceitáveis.
- Em caso de violações confirmadas, a companhia aplicará as sanções cabíveis, as quais serão estritamente proporcionais à gravidade da infração e ao nível de dolo envolvido.

8.2. Escalada de Penalidades

As medidas disciplinares seguem uma estrutura de escalada, dependendo da criticidade e da intenção do ato infracional:

- **Advertência Verbal ou Escrita:** Aplicada em casos de descuidos operacionais sem dolo e que não resultem em exposição de dados críticos ou perdas financeiras (por exemplo, deixar a tela desbloqueada ao se ausentar da mesa ou falhar repetidamente em simulações de *phishing*).
- **Suspensão de Acessos e Sanções Administrativas:** Suspensão temporária do trabalhador ou rebaixamento imediato de privilégios sistêmicos enquanto o incidente é investigado pela companhia.
- **Demissão por Justa Causa (ou Rescisão Contratual):** Poderá ser aplicada em casos de violação grave, após apuração dos fatos e conforme a natureza do vínculo, os requisitos legais ou contratuais e a proporcionalidade da medida, incluindo situações como envio não autorizado de dados de clientes (KYC) para e-mails ou nuvens pessoais, compartilhamento intencional de credenciais, alteração fraudulenta de limites operacionais, desativação proposital de controles de segurança ou inserção de código malicioso nos sistemas da companhia.
- **Ações Civis e Penais:** Atos que configurem crime (como fraudes, peculato, invasão de dispositivo informático ou lavagem de dinheiro) ou que causem danos financeiros diretos resultarão no acionamento imediato das autoridades policiais e judiciais competentes para a devida responsabilização civil e criminal do infrator.

9. CONFLITO DE INTERESSES E ABUSO DE MERCADO

A integridade das nossas operações exige que as decisões profissionais sejam tomadas de forma independente, no interesse legítimo da companhia e de seus clientes, com observância da legislação, da regulamentação e dos deveres aplicáveis. Conflitos de interesse reais, potenciais ou aparentes devem ser identificados, declarados, avaliados e adequadamente mitigados.

9.1. Abuso de Mercado (Insider Trading e Front-Running)

Considerando que a instituição atua como uma Sociedade Prestadora de Serviços de Ativos Virtuais (SPSAV) provendo liquidez, desenvolvendo algoritmos proprietários de *market making* e gerindo grandes volumes através de Mesas de Operação de Balcão (OTC), os colaboradores possuem acesso a informações sensíveis, estratégicas e não públicas. Neste contexto, é terminantemente proibido:

- **Uso indevido de informação confidencial e, quando aplicável, Insider Trading:** Utilizar informação relevante e não pública obtida em razão do vínculo com a instituição para realizar negociações pessoais, beneficiar terceiros ou obter vantagem indevida. Quando o ativo ou instrumento estiver sujeito ao regime de valores mobiliários, também deverão ser observadas as normas específicas de uso de informação privilegiada e abuso de mercado.
- **Front-Running:** Antecipar-se ao mercado ou a uma grande ordem de um cliente institucional operando em benefício próprio antes que a ordem do cliente seja executada, utilizando-se da assimetria de informações fornecida pela infraestrutura da companhia.
- **Vazamento Estratégico:** Compartilhar dicas financeiras, tendências de fluxo de caixa de OTC ou estratégias de arbitragem proprietárias da empresa com terceiros, amigos ou familiares.

9.2. Negociações Pessoais (Personal Trading)

Embora a companhia respeite a liberdade financeira de seus colaboradores, as negociações privadas no mercado de ativos virtuais não podem colocar em risco a lisura da instituição.

- As negociações pessoais de criptoativos não podem, sob nenhuma hipótese, conflitar com as posições comerciais da empresa ou operar contra os interesses de nossos clientes.
- Colaboradores que ocupam posições sensíveis, tais como Operadores de Mercado (Traders), Desenvolvedores de algoritmos (Quants) e profissionais com acesso à infraestrutura de custódia, podem estar sujeitos a controles específicos de negociação pessoal. Eventuais declarações de carteiras, períodos de restrição ou impedimentos de negociação deverão estar previstos em procedimento interno, possuir finalidade de compliance definida e observar os princípios de necessidade, proporcionalidade e segurança no tratamento dos dados.

9.3. Atividades Paralelas e Relacionamentos Societários

O compromisso com a instituição exige transparência sobre atividades externas que possam gerar divisões de lealdade:

- **Vínculos Externos:** É proibido atuar como consultor, empregado, membro de conselho ou possuir participação societária relevante em empresas concorrentes diretas ou *exchanges* sem a prévia, expressa e formal autorização da Diretoria Executiva.
- **Contratação de Terceiros:** A seleção e a homologação de fornecedores de tecnologia ou provedores de liquidez devem seguir critérios estritamente técnicos e comerciais. É vedado o direcionamento de contratos para beneficiar empresas pertencentes a amigos ou familiares.
- **Dever de Declaração:** Caso o colaborador identifique qualquer situação pessoal que possa ser interpretada como um conflito de interesses, o fato deve ser imediatamente reportado à sua liderança e à gerência de *Compliance* para análise e registro.

10. PREVENÇÃO À CORRUPÇÃO, SUBORNO E RELACIONAMENTO COM O SETOR PÚBLICO

A organização atua em um ecossistema financeiro regulado e preza pela integridade em todas as suas interações. Em consonância com a Lei nº 12.846/2013, no relacionamento com a Administração Pública, e com suas regras internas de integridade aplicáveis também às relações privadas, a companhia proíbe práticas de corrupção, suborno, fraude e tráfico de influência.

10.1. Tolerância Zero a Suborno e Vantagens Indevidas

Estendendo a postura institucional de tolerância zero para ilícitos financeiros, aplicam-se as seguintes regras de integridade comercial:

- **Proibição Absoluta:** É estritamente proibido oferecer, prometer, autorizar ou entregar, de forma direta ou indireta, qualquer tipo de vantagem indevida, pagamento, propina ou "taxa de facilitação" a agentes públicos ou parceiros privados. Essa regra aplica-se a tentativas de obter favorecimento, agilizar processos burocráticos ou influenciar decisões de negócios.
- **Recebimento de Vantagens:** Nenhum colaborador pode solicitar ou aceitar favores, pagamentos ou benefícios pessoais em troca de aprovar cadastros, favorecer fornecedores, ou ignorar limites sistêmicos da companhia.

10.2. Brindes, Presentes e Hospitalidade

O oferecimento ou recebimento de presentes pode criar percepções de conflito de interesses ou disfarçar tentativas de suborno. Para blindar a operação:

- **Brindes Institucionais:** A aceitação ou oferta de presentes deve se restringir a itens institucionais de baixo valor comercial (como canetas, cadernos e itens com o logotipo da empresa emissora), distribuídos como prática comum de cortesia.
- **Proibição de Valores:** É terminantemente proibido o recebimento ou a oferta de presentes em dinheiro (espécie), cartões-presente, transferências bancárias ou criptoativos, independentemente da quantia.
- **Hospitalidade:** Convites para eventos, jantares de negócios ou viagens patrocinadas por terceiros devem possuir um propósito comercial legítimo, razoabilidade e devem ser previamente comunicados e aprovados pela liderança direta e pela área de *Compliance*.

10.3. Relacionamento com Reguladores e Agentes Públicos

Dado o papel da instituição de reportar e atuar junto a órgãos como o Banco Central do Brasil (BCB), COAF e a Receita Federal, o relacionamento com o setor público exige o mais alto grau de retidão institucional e cumprimento de obrigações acessórias:

- **Transparência e Cooperação:** Durante inspeções, auditorias independentes ou requisições de informações por parte dos órgãos reguladores, os colaboradores devem agir com total transparência e espírito de cooperação institucional.
- **Proteção e Integridade de Registros:** É proibido ocultar, destruir, falsificar ou alterar documentos, registros transacionais, relatórios de KYC ou dossiês de análise sujeitos a obrigação de guarda ou solicitados por autoridade competente. Os colaboradores devem preservar a veracidade, integridade e rastreabilidade das informações utilizadas nas prestações regulatórias e fiscais, incluindo a Declaração de Criptoativos (DeCripto), instituída pela Instrução Normativa RFB nº 2.291/2025 para operações realizadas a partir de julho de 2026.
- **Pessoas Expostas Politicamente (PEP):** O relacionamento com PEPs, familiares, estreitos colaboradores e pessoas jurídicas a eles relacionadas deverá observar a regulamentação e a abordagem baseada em risco, com diligência reforçada, monitoramento compatível e alçadas de aprovação definidas na política interna. É proibida qualquer tentativa de burlar ou reduzir controles para favorecer o ingresso ou a permanência de clientes por influência política ou pessoal.

11. RESPEITO NO AMBIENTE DE TRABALHO E RELAÇÕES HUMANAS

A instituição reconhece que o seu maior ativo são as pessoas. A manutenção de um ambiente de trabalho seguro, ético, colaborativo e pautado pelo respeito mútuo é fundamental para a sustentabilidade de nossas operações e para o bem-estar físico e psicológico de todos os colaboradores e parceiros.

11.1. Diversidade, Inclusão e Não Discriminação

A companhia valoriza a pluralidade de ideias e perfis, promovendo ativamente um ecossistema de igualdade de oportunidades.

- É terminantemente proibida qualquer forma de discriminação, marginalização ou preconceito com base em raça, cor, etnia, religião, gênero, identidade de gênero, orientação sexual, idade, estado civil, nacionalidade, deficiência ou qualquer outra característica pessoal.

- As decisões corporativas de recrutamento, promoção, remuneração e desligamento devem ser pautadas única e exclusivamente no mérito, nas competências técnicas, no desempenho e no alinhamento aos valores éticos institucionais.

11.2. Combate ao Assédio Moral e Sexual

A organização adota uma postura de tolerância zero contra qualquer conduta que configure assédio ou que crie um ambiente de trabalho hostil, intimidador ou ofensivo.

- **Assédio Moral:** Repudiamos condutas abusivas repetitivas, humilhações, perseguições, constrangimentos públicos, exposição ao ridículo ou cobranças desproporcionais que atentem contra a dignidade e a saúde mental do colaborador.
- **Assédio Sexual:** É estritamente proibida qualquer insinuação, conduta, comentário verbal ou contato físico de cunho sexual não consensual, bem como o uso de posição hierárquica para tentar obter favores de natureza íntima ou sexual.
- **Utilização do Canal de Denúncias:** Qualquer colaborador que seja vítima ou que presencie atos de assédio e discriminação tem o direito e o dever de reportar o fato utilizando o Canal de Denúncias da instituição, o qual é operado de forma segura e independente 24 horas por dia.
- **Garantia de Não-Retaliação:** A empresa assegura a confidencialidade e o anonimato do denunciante, inclusive mediante opção de anonimato quando disponibilizada pelo canal, e proíbe expressamente qualquer retaliação, intimidação ou penalização profissional contra quem, de boa-fé, denunciar abusos no ambiente de trabalho.

11.3. Saúde, Segurança e Prevenção ao Uso de Substâncias

Considerando a extrema criticidade das operações financeiras e os riscos sistêmicos inerentes à atuação e gestão de infraestrutura de uma Sociedade Prestadora de Serviços de Ativos Virtuais (SPSAV), o pleno estado de consciência e o discernimento técnico dos colaboradores são inegociáveis.

- **Drogas Ilícitas:** É expressamente proibido o consumo, a comercialização, a distribuição ou o porte de drogas ilícitas nas dependências físicas da companhia, em eventos corporativos ou durante o exercício das atividades laborais operadas em regime de trabalho remoto (*home office*).
- **Álcool:** É vedado o consumo de bebidas alcoólicas durante o horário de expediente ou o comparecimento ao trabalho em estado de embriaguez, garantindo que as atividades de alta sensibilidade — como a liberação de limites, a custódia de ativos e o monitoramento investigativo — operem livres de qualquer comprometimento de juízo.

12. COMUNICAÇÃO EXTERNA, IMPRENSA E REDES SOCIAIS

No mercado financeiro e no ecossistema de criptoativos, a reputação, a credibilidade e a confiança são ativos críticos. Informações divulgadas de forma inadequada, precipitada ou por canais não oficiais podem gerar impactos de mercado, danos à marca e expor a companhia a riscos regulatórios.

12.1. Porta-Vozes Oficiais e Relacionamento com a Imprensa

A comunicação institucional com veículos de mídia, jornalistas, formadores de opinião e a comunidade de investidores deve ser unificada e estratégica.

- **Comunicação Autorizada:** Apenas membros da Diretoria Executiva ou colaboradores formalmente designados pela equipe de Relações Públicas (PR) ou *Marketing* estão autorizados a conceder entrevistas, emitir comunicados de imprensa institucionais ou falar em nome da companhia.
- **Abordagens Externas:** Caso qualquer colaborador seja abordado por jornalistas, blogueiros, influenciadores digitais ou pesquisadores buscando informações sobre a instituição, suas operações ou seus clientes, ele deve abster-se de fazer comentários e direcionar a solicitação imediatamente ao setor de comunicação competente.
- **Transparência Regulatória:** Ao comunicar-se em nome da companhia, seja em entrevistas, press releases ou materiais publicitários, é estritamente vedada a divulgação de mensagens, selos ou afirmações que sugiram que a instituição já possui autorização definitiva do Banco Central do Brasil enquanto perdurar o período de licenciamento transitório, assegurando conformidade com as regras de transparência da Resolução BCB nº 520/2025.

12.2. Postura em Redes Sociais Pessoais

A companhia respeita a liberdade de expressão de seus colaboradores em suas redes sociais pessoais (como LinkedIn, X/Twitter, Instagram, Discord ou Reddit). Contudo, o limite dessa liberdade encontra-se na preservação do sigilo corporativo e na proteção da imagem da instituição.

- **Proteção de Informações:** É estritamente proibido expor, comentar ou publicar qualquer tipo de informação classificada como Confidencial ou Restrita em redes sociais ou fóruns públicos. Isso abrange, inegociavelmente, os segredos de negócio, a arquitetura de redes, estratégias de *trading* algorítmico, códigos-fonte proprietários, informações de incidentes operacionais e dados cadastrais de clientes.
- **Opiniões Pessoais vs. Institucionais:** Ao participar de debates ou publicar conteúdos relacionados ao mercado financeiro, regulação ou criptoativos, o colaborador não deve usar seu vínculo com a empresa para dar "peso oficial" à sua opinião. Se houver risco de confusão, deve-se deixar claro que a opinião expressa é estritamente pessoal e não reflete o posicionamento da instituição.
- **Bom Senso e Reputação:** Espera-se que os profissionais ajam com bom senso e civilidade no ambiente digital. O envolvimento em discussões públicas agressivas (*flame wars*), discursos de ódio ou comportamentos antiéticos reflete negativamente na reputação do indivíduo e pode, por associação, comprometer a imagem de integridade e profissionalismo exigida de quem opera infraestruturas financeiras críticas.

13. CONCORRÊNCIA LEAL E RELAÇÃO COM FORNECEDORES

A instituição valoriza o livre mercado e pauta o seu crescimento na excelência técnica, na inovação e na qualidade dos serviços prestados. A nossa atuação deve ser sempre ética e fundamentada no estrito cumprimento das leis antitruste, não admitindo atalhos ou práticas anticompetitivas para a obtenção de resultados comerciais.

13.1. Defesa da Concorrência (Antitruste)

A companhia compete de forma vigorosa, mas sempre com integridade e respeito às regras do mercado financeiro e de ativos virtuais.

- **Proibição de Acordos Anticompetitivos:** É terminantemente proibido interagir com concorrentes diretos (tais como outras *exchanges*, corretoras ou mesas de OTC) com o

objetivo de firmar acordos, formais ou informais, para fixação de preços, padronização de taxas (*fees*), manipulação de *spreads* ou divisão de mercados e carteiras de clientes.

- **Inteligência Competitiva:** A coleta de informações sobre a concorrência e sobre o ecossistema de criptoativos deve ser realizada única e exclusivamente por meios legais e públicos. É estritamente proibido o uso de espionagem, suborno, quebra de sigilo ou qualquer outro meio ilícito para obter vantagens comerciais ou descobrir segredos de negócio de terceiros.

13.2. Contratação Ética e Gestão de Terceiros

A resiliência operacional da companhia depende diretamente da qualidade, segurança e integridade de sua cadeia de suprimentos tecnológica. O processo de seleção de prestadores de serviços e parceiros deve ser transparente e imparcial.

- **Critérios de Homologação:** A contratação de fornecedores — especialmente aqueles que proveem serviços de alta criticidade, como processamento em nuvem, custódia e sistemas de *Blockchain Analytics* — deve ser baseada estritamente em critérios técnicos, comerciais e de maturidade em segurança cibernética.
- **Proibição de Favorecimento:** A seleção não pode ser influenciada por conflitos de interesses. É absolutamente vedado o direcionamento de contratos corporativos ou escolhas de fornecimento para beneficiar empresas pertencentes a amigos, familiares ou entidades nas quais o colaborador possua interesse pessoal ou societário.
- **Avaliação de Risco (Due Diligence):** A contratação de qualquer fornecedor que tenha acesso a dados confidenciais, dados pessoais de clientes ou infraestrutura crítica para a operação da companhia será sempre precedida de uma rigorosa análise de risco de terceiros.

- **Exigência de Conformidade:** Todos os parceiros de negócios e fornecedores de tecnologia homologados devem, obrigatoriamente, assinar Acordos de Confidencialidade (NDA) e firmar o compromisso de aderência à Lei Geral de Proteção de Dados Pessoais (LGPD) antes de qualquer acesso lógico ou compartilhamento de informações ser concedido pela organização.

- **Cláusulas Contratuais de Controle:** Terceiros com acesso a dados pessoais, informações confidenciais ou infraestrutura crítica deverão assumir obrigações compatíveis com o risco contratado, incluindo confidencialidade, proteção de dados, segurança da informação, comunicação de incidentes, continuidade, direito de auditoria e regras para subcontratação.
- **Extensão das Obrigações:** Os contratos deverão exigir, quando aplicável, que empregados, representantes e subcontratados autorizados do terceiro observem obrigações equivalentes, permanecendo o contratado responsável por sua gestão e supervisão nos termos do instrumento.

13.3. Governança do Código, Treinamento e Evidências

A efetividade deste Código dependerá de responsabilidades definidas, capacitação periódica e evidências verificáveis de sua implementação.

- **Responsabilidades e Aprovação:** Compliance será responsável pela manutenção deste Código; o Jurídico validará alterações relevantes; a Diretoria competente aprovará as

versões e exceções materiais; e a Auditoria avaliará sua efetividade conforme planejamento baseado em riscos.

- **Treinamento e Evidências:** Os públicos abrangidos receberão treinamento inicial e periódico, com registro de participação, conteúdo, avaliação e ações de reforço quando necessárias. As evidências deverão permanecer disponíveis no repositório oficial pelo prazo aplicável.
- **Exceções e Revisão:** Exceções deverão ser temporárias, justificadas, aprovadas pela alçada competente, acompanhadas de controle compensatório e data de revisão. O Código terá controle de versões e será revisto periodicamente e sempre que houver alteração legal, regulatória, operacional ou de risco relevante.

14. BASE LEGAL E REGULATÓRIA

Este Código deve ser interpretado em conjunto com a legislação e a regulamentação aplicáveis à instituição, considerando sua modalidade de atuação, seu status perante o Banco Central do Brasil e os períodos de transição ou adequação previstos nas normas.

14.1. Regulação de Ativos Virtuais, Governança e Conduta

- **Lei nº 14.478/2022 e Decreto nº 11.563/2023:** estabelecem o marco legal dos ativos virtuais e atribuem ao Banco Central do Brasil competência para regular, autorizar e supervisionar as prestadoras de serviços de ativos virtuais, preservadas as competências legais de outros órgãos, inclusive da Comissão de Valores Mobiliários.

- **Resolução BCB nº 519/2025:** disciplina os processos de autorização relacionados ao funcionamento das sociedades prestadoras de serviços de ativos virtuais e os requisitos aplicáveis à administração, governança, estrutura, capital e controles da instituição.

- **Resolução BCB nº 520/2025:** disciplina a constituição e o funcionamento das sociedades prestadoras de serviços de ativos virtuais e a prestação desses serviços por outras instituições autorizadas pelo Banco Central do Brasil.

- **Resolução BCB nº 552/2026:** inclui as SPSAVs autorizadas no escopo de normas do Banco Central sobre política de conformidade, segurança cibernética, relacionamento com clientes, controles internos, ouvidoria e outras obrigações correlatas. Entre as normas diretamente relacionadas a este Código destacam-se as Resoluções BCB nº 65/2021, nº 85/2021, nº 155/2021 e nº 260/2022.

- **Resolução CMN nº 5.280/2026 e Lei Complementar nº 105/2001:** submetem as SPSAVs ao regime legal de sigilo das operações, devendo o acesso e o compartilhamento de informações observar competência, finalidade, necessidade e segurança.

14.2. PLD/FTP, Sanções e Sigilo de Comunicações

- **Lei nº 9.613/1998:** estabelece deveres de identificação, manutenção de registros, monitoramento e comunicação de operações suspeitas ao COAF, incluindo a vedação de dar ciência da comunicação a qualquer pessoa.

- **Lei nº 13.810/2019 e Resolução BCB nº 44/2020, quando aplicável:** disciplinam o cumprimento de medidas de indisponibilidade de ativos relacionadas a sanções do Conselho de Segurança das Nações Unidas e os procedimentos de comunicação às autoridades competentes.

14.3. Privacidade, Integridade e Obrigações Fiscais

- **Lei nº 13.709/2018 (LGPD):** rege o tratamento de dados pessoais e exige observância aos princípios de finalidade, adequação, necessidade, segurança, prevenção e prestação de contas, sem prejuízo das hipóteses legais de conservação de dados e cumprimento de obrigações legais e regulatórias.

- **Instrução Normativa RFB nº 2.291/2025:** institui a Declaração de Criptoativos (DeCripto) e substitui a sistemática da IN RFB nº 1.888/2019 para operações realizadas a partir de julho de 2026.

- **Lei nº 12.846/2013 e Lei nº 12.529/2011:** fundamentam, respectivamente, as diretrizes de integridade no relacionamento com a Administração Pública e as regras de defesa da concorrência previstas neste Código.

- **Lei nº 14.457/2022, quando aplicável:** estabelece medidas de prevenção e combate ao assédio sexual e a outras formas de violência no ambiente de trabalho, inclusive obrigações relacionadas a regras internas e canais de denúncia para organizações abrangidas pela norma.

TERMO DE CIÊNCIA E ACEITE DO CÓDIGO DE CONDUTA E CONFORMIDADE

Por meio deste instrumento, e em conformidade com as diretrizes da Caldeira Negócios e Intermediações Ltda., declaro formalmente que:

1. Recebi, li e compreendi integralmente as diretrizes estabelecidas no Código de Conduta e Conformidade da instituição.
2. Estou ciente de minhas responsabilidades e concordo em cumprir rigorosamente as normas de Tolerância Zero, Proteção de Dados (LGPD), Prevenção à Lavagem de Dinheiro e ao Financiamento do Terrorismo e da Proliferação (PLD/FTP), Integridade e Reporte Fiscal aplicável, inclusive a DeCripto nos termos da IN RFB nº 2.291/2025, além das regras de Mesa e Tela Limpa, Sigilo e uso de ferramentas corporativas.
3. Entendo o meu dever inegociável de utilizar o Canal de Denúncias caso identifique suspeitas de fraudes ou desvios éticos.
4. Estou ciente de que a inobservância destas regras poderá resultar em medidas disciplinares proporcionais à gravidade da conduta e à natureza do vínculo, inclusive rescisão contratual ou demissão por justa causa quando legalmente cabível, sem prejuízo de eventual responsabilização civil, administrativa e criminal.

Compreendo que a assinatura deste termo é condição indispensável para o meu vínculo empregatício ou prestação de serviços à companhia.

Nome Completo: _____

CPF: _____

Cargo / Função: _____

Empresa / Terceiro (se aplicável): _____

[Cidade - Estado], _____ de _____ de 20____.

Assinatura (Física ou Digital)