



POLÍTICA DE GESTÃO DE FRAUDES



SUMÁRIO

CONTROLE DE VERSÃO	3
1. OBJETIVO.....	4
2. REFERÊNCIAS NORMATIVAS E REGULATÓRIAS	4
3. DEFINIÇÕES.....	5
4. TIPOS DE FRAUDE	5
5. IDENTIFICAÇÃO E AVALIAÇÃO DOS RISCOS RELACIONADOS A FRAUDE.....	7
6. RESPONSABILIDADES.....	8
6.1. GESTORES DAS ÁREAS OPERACIONAIS.....	8
6.2. ESTRUTURA DE FISCALIZAÇÃO E SUPERVISÃO	8
6.3. DIRETORIA DE GOVERNANÇA, RISCO E CONTROLES INTERNOS	9
6.4. COMITÊ DE ÉTICA	9
6.5. AUDITORIA INTERNA	10
6.6. DEPARTAMENTO DE PRODUÇÃO E SEGURANÇA DA INFORMAÇÃO	10
6.7. <i>CUSTOMER EXPERIENCE</i>	10
6.8. DEPARTAMENTO DE RECURSOS HUMANOS E PESSOAL	11
7. TREINAMENTOS E CONSCIENTIZAÇÃO.....	11
8. INVESTIGAÇÃO E SANÇÕES.....	12
9. CONTROLE DO DOCUMENTO	12
9.1. VIGÊNCIA E DIVULGAÇÃO.....	12
9.2. REVISÃO	12
9.3. DIREITOS AUTORAIS E DISTRIBUIÇÃO	12



CONTROLE DE VERSÃO

Data da Versão	Autores	Número da Versão	Descrição
30/04/2025	Diretoria de Fiscalização e Supervisão; e Diretoria de Governança, Riscos e Controles Internos	1.0	Elaboração inicial do documento; Documento aprovado pelo Conselho de Administração em 30/04/2025



1. OBJETIVO

Esta Política de Gestão de Fraudes (“Política”) tem por objetivo estabelecer princípios e diretrizes da CSD CENTRAL DE SERVIÇOS DE REGISTRO E DEPÓSITO AOS MERCADOS FINANCEIRO E DE CAPITAIS S.A. (“CSD BR” ou “Companhia”) na prevenção, identificação e gestão de fraudes e complementar a Política de Gestão de Riscos e Controles Internos.

Esta Política se aplica e deve ser observada pela alta administração, colaboradores, parceiros, prestadores de serviços, fornecedores e demais terceiros com quem a Companhia mantenha relacionamento.

Por meio desta Política a CSD BR visa: (a) identificar e compreender os riscos e as possibilidades de fraude em produtos, serviços e processos; (b) apresentar as responsabilidades de cada departamento ou função dentro da Companhia em relação à prevenção à fraude; (c) demonstrar o compromisso da Companhia para a prevenção à fraude, que é fundamental para manter a integridade dos serviços prestados.

Os termos e expressões iniciados em maiúsculas, tanto no singular quanto no plural, têm o significado a eles atribuídos no Glossário da CSD BR, disponível em www.csdbbr.com.

2. REFERÊNCIAS NORMATIVAS E REGULATÓRIAS

Essa Política adota como referências:

- Lei nº 8.137, de 27 de dezembro de 1990 (“Lei de Crimes Contra a Ordem Tributária”);
- Lei nº 9.613, de 3 de março de 1998 (“Lei 9.613/98” ou “Lei para prevenção e combate à lavagem de dinheiro”);
- Lei nº 12.846, de 1º de agosto de 2013 (“Lei 12.846/2013” ou “Lei Anticorrupção”);
- Lei nº 13.709, de 14 de agosto de 2018 (“Lei 13.709/2018” ou “LGPD”);
- Resolução BCB nº 304, de 20 de março de 2023 (“RBCB 304/2023”); e
- Resolução CVM nº 135, de 13 de junho de 2022 (“RCVM 135/2022”).

Qualquer referência a qualquer lei ou normativo aplicável será considerado também como uma referência a todas as suas atualizações e regulamentações promulgadas ao abrigo dele, salvo disposição em contrário.



3. DEFINIÇÕES

Para fins desta Política, são considerados os seguintes conceitos:

Fraude – qualquer ato desonesto ou malicioso intencional que envolva falsificação, manipulação ou distorção de produtos, documentos, registros ou resultados com o objetivo de obter vantagem indevida para si, para a Companhia ou para terceiros, ou prejudicar a Companhia ou terceiros. No contexto dos serviços prestados pela Companhia, fraudes podem comprometer a integridade do mercado, a segurança das operações e a confiança nos processos de negociação e custódia. Fraudes podem incluir, mas não se limitam a:

- (i) Furto ou apropriação indevida de ativos;
- (ii) Manipulação ou ocultação de dados e informações;
- (iii) Falsificação de assinaturas, contratos, registros e outros documentos;
- (iv) Evasão ou burla de controles internos, com o objetivo de ocultar operações irregulares ou não autorizadas; e
- (v) Adulteração de resultados, registros contábeis ou relatórios enviados a reguladores e participantes do mercado.

Integridade – compromisso com a ética, transparência e conformidade regulatória, assegurando que todas as atividades sejam conduzidas de forma responsável e em alinhamento com os mais altos padrões de governança.

Prevenção – implementação de controles internos robustos, *due diligence* e medidas de mitigação de riscos, visando reduzir a exposição da Companhia a fraudes e irregularidades.

Monitoramento – adoção de mecanismos contínuos de supervisão, auditoria e análise de operações, permitindo a identificação precoce de comportamentos atípicos e o aprimoramento das defesas contra fraudes.

4. TIPOS DE FRAUDE

Para os fins desta Política, consideram-se as seguintes classificações e formas de fraude:

Conflito de interesses e corrupção – situações em que interesses pessoais, profissionais ou financeiros possam influenciar indevidamente no desempenho e/ou em decisões em nome da Companhia, resultando em favorecimento indevido, suborno,



desvio de recursos ou concessão de benefícios em desacordo com as normas internas e externas. Exemplos incluem:

- (i) Pagamento ou recebimento de recursos para fechamento de contratos ou facilitação de processos;
- (ii) Favorecimento de fornecedores, parceiros ou clientes em troca de vantagens pessoais;
- (iii) Uso indevido de cargo ou influência para ganhos privados;
- (iv) Participação oculta em empresas concorrentes ou conflitantes com os interesses da Companhia.

Fraude cibernética – qualquer acesso, ataque, vazamento ou manipulação de dados e sistemas tecnológicos, tanto por colaboradores quanto por agentes externos, visando obter vantagens ilícitas, comprometer a integridade das informações ou prejudicar a Companhia, clientes, investidores ou outros relacionados. Pode incluir:

- (i) Ataques de *hackers* para roubo de informações confidenciais;
- (ii) Uso de *malware*, *phishing*, *ransomware* ou engenharia social para obter credenciais e/ou fraudar sistemas e operações;
- (iii) Violação de segurança da informação para benefício próprio ou de terceiros;
- (iv) Manipulação de sistemas automatizados para desviar recursos ou adulterar dados financeiros.

Fraude documental – qualquer forma de falsificação, adulteração, destruição ou omissão de informações em contratos, registros, assinaturas ou documentos oficiais, com o objetivo de enganar, fraudar processos ou ocultar irregularidades. Inclui, mas não se limita a:

- (i) Fabricação de documentos falsos;
- (ii) Alteração indevida de cláusulas em contratos ou relatórios;
- (iii) Assinaturas forjadas ou utilização de identidades falsas para fraudar operações;
- (iv) Omissão de registros obrigatórios em relatórios contábeis ou regulatórios.

Fraude envolvendo os serviços prestados pela CSD BR – ações fraudulentas no contexto dos serviços prestados pela CSD BR como, dentre outros, entidade registradora, depositário central e câmara de compensação e liquidação de Ativos Financeiros e Valores Mobiliários. Exemplos incluem:



- (i) Fornecimento de informações intencionalmente erradas de operações para ocultar movimentações ilícitas;
- (ii) Manipulação de preços e valores de Ativos para simular rentabilidade;
- (iii) Omissão de informações obrigatórias em sistemas regulatórios;
- (iv) Inclusão de ativos fictícios ou inexistentes para mascarar irregularidades financeiras.

Fraude financeira – qualquer ato de manipulação de registros contábeis, demonstrações financeiras ou informações econômico-financeiras com o objetivo de distorcer a realidade patrimonial da Companhia, ocultar prejuízos, inflar lucros, facilitar acesso indevido a crédito, captar recursos de forma fraudulenta ou induzir terceiros a erro. Exemplos incluem:

- (i) Ocultação ou adulteração de passivos, provisões e despesas;
- (ii) Reconhecimento indevido de receitas ou antecipação de lucros;
- (iii) Manipulação de *valuations* para enganar investidores e stakeholders;
- (iv) Uso de artifícios contábeis para fraudar auditorias ou prestação de informações aos órgãos reguladores.

Fraude operacional – uso indevido ou não autorizado de sistemas, processos, registros e controles internos com o objetivo de mascarar erros, ocultar transações ilícitas ou burlar normas internas e externas. Exemplos incluem:

- (i) Alteração indevida de cadastros, sistemas de controle ou registros de clientes;
- (ii) Movimentação irregular de Ativos sem respaldo documental e/ou em desacordo às normas internas e externas;
- (iii) Uso de informações privilegiadas para obter vantagens indevidas;
- (iv) Violação de segregação de funções para cometer irregularidades.

5. IDENTIFICAÇÃO E AVALIAÇÃO DOS RISCOS RELACIONADOS A FRAUDE

A CSD BR busca identificar e compreender os riscos e as possibilidades de fraude associados aos seus serviços, produtos e processos, conforme disposto na Política de Gestão de Riscos e Controles Internos. Com base nisso, desenvolve mecanismos de monitoramento e a adequação de controles preventivos e detectivos para a adequada mitigação desses riscos.



Caso haja mudanças nos serviços, produtos, processos, estrutura organizacional e/ou em normas externas, a Companhia deverá reavaliar se tais mudanças requerem ajustes nos monitoramentos e controles existentes.

6. RESPONSABILIDADES

A gestão de fraudes é um compromisso de toda a Companhia, sendo essencial a definição clara de papéis e responsabilidades para a prevenção, detecção e mitigação de riscos. Todos da Companhia devem:

- (i) Atuar conforme os papéis e responsabilidades descritos nas normas internas e externas aplicáveis à Companhia, incluindo, sem se limitar ao Código de Conduta Ética, Política de Compliance, Política de Gestão de Riscos e Controles Internos, Política de PLD/FTP, Política de Segurança da Informação e Segurança Cibernética;
- (ii) Desempenhar função e manter conduta pautada na integridade, ética e moral, incluindo reportar aos canais de comunicação de denúncias situações suspeitas de fraude, conforme estabelecido no Código de Conduta e Ética da Companhia; e
- (iii) Participar dos treinamentos propostos pela Companhia que abordam, dentre outros assuntos, a gestão de fraude.

A CSD BR não admite ou compactua com a prática ou a facilitação de qualquer forma de fraude, em seu nome, ou cometida por qualquer das pessoas com quem se relacione.

6.1. GESTORES DAS ÁREAS OPERACIONAIS

Os gestores das áreas operacionais, como 1ª linha na estrutura de gestão de riscos, são responsáveis pela gestão diária de processos e riscos, assegurando a aplicação de controles internos eficazes para mitigar fraudes em suas respectivas áreas.

6.2. ESTRUTURA DE FISCALIZAÇÃO E SUPERVISÃO

É responsabilidade da Diretoria de Fiscalização e Supervisão (“DFS”):

- (i) Monitorar, identificar e instituir, na Plataforma, processos e procedimentos para identificação, monitoramento e análise de atividades e/ou operações suspeitas de fraude;



- (ii) Avaliar e monitorar as documentações fornecidas pelos Participantes, seja pela Plataforma ou via correio eletrônico, para justificativa de operações ou no processo de inspeção periódica;
- (iii) Cumprir com os ritos descritos nos regulamentos relativos ao processo disciplinar, em casos de identificação de fraudes na Plataforma; e
- (iv) Cumprir os deveres em relação as responsabilidades atribuídas na Política de Prevenção a Lavagem de Dinheiro, ao Financiamento do Terrorismo e ao Financiamento da Proliferação das Armas de Destruição em Massa (PLD/FTP).

É responsabilidade do Comitê de Fiscalização e Supervisão (“CFS”) fiscalizar a eficiência e eficácia da implementação da Política de Gestão de Fraudes e a estrutura de gestão de riscos da Companhia.

6.3. DIRETORIA DE GOVERNANÇA, RISCO E CONTROLES INTERNOS

É responsabilidade da Diretoria de Governança, Risco e Controles Internos (“GRC”):

- (i) Atuar na gestão e revisão das normas internas que disciplinem a gestão de fraudes de modo que estejam em conformidade com a legislação e normativos vigentes;
- (ii) Assegurar que todos os colaboradores tenham ciência das políticas internas relacionadas à ética e integridade, incluindo esta Política de Gestão de Fraude; e
- (iii) Promover a disseminação da cultura de prevenção e combate à fraude, bem como a divulgação do Canal de Ética da Companhia como meio seguro e confidencial para o reporte de condutas indevidas.

6.4. COMITÊ DE ÉTICA

É responsabilidade do Comitê de Ética em relação às fraudes reportadas:

- (i) Avaliar todas as fraudes reportadas, garantindo tratamento adequado, confidencialidade e imparcialidade na investigação;
- (ii) Reportar à alta administração da Companhia sobre fraudes identificadas, riscos e providências adotadas;



- (iii) Assegurar que denúncias sejam tratadas sem impactos para o denunciante, preservando a identidade e a segurança dos envolvidos.

6.5. AUDITORIA INTERNA

Cabe à Auditoria Interna avaliar a conformidade dos processos de gestão de fraudes, apontando deficiências e recomendações para aprimoramento, bem como monitorar a efetividade dos controles internos implementados para prevenção e mitigação de fraudes, conforme as diretrizes e responsabilidades estabelecidas no Regimento Interno da Auditoria Interna.

6.6. DEPARTAMENTO DE PRODUÇÃO E SEGURANÇA DA INFORMAÇÃO

É responsabilidade do Departamento de Produção e Segurança da Informação (“DPSI”):

- (i) Implementar, monitorar e garantir a efetividade dos controles de segurança cibernética e proteção de dados, incluindo a gestão de acessos e a revogação de permissões a sistemas e informações sensíveis após o desligamento de colaboradores, minimizando riscos de fraudes, vazamento de informações e uso indevido de dados;
- (ii) Atuar na prevenção e resposta a incidentes de segurança que possam comprometer a integridade das operações da Companhia;
- (iii) Assegurar a implementação de medidas técnicas e operacionais para garantir a segurança dos dados e dos sistemas, alinhando-se às diretrizes e regulamentações de segurança da informação e proteção de dados.

6.7. CUSTOMER EXPERIENCE

É responsabilidade da área de *Customer Experience* (“CX”):

- (i) Caso sejam observados ou identificados comportamentos atípicos, inconsistências ou situações que possam indicar riscos operacionais ou de conformidade, CX deve comunicar imediatamente a DFS para a devida análise e adoção de medidas cabíveis;
- (ii) Manter procedimentos, ações e esclarecimentos de dúvidas aos usuários da Plataforma para facilitar a compreensão das regras, funcionalidades e boas práticas da Plataforma;



- (iii) Facilitar o acesso às políticas, regulamento e manuais que possuem as informações essenciais sobre os serviços prestados pela Companhia para as Instituições Elegíveis, os Participantes e eventuais *prospects*.

6.8. DEPARTAMENTO DE RECURSOS HUMANOS E PESSOAL

É responsabilidade do Departamento de Recursos Humanos e Pessoal (“RH e DP”):

- (i) Garantir que os processos de recrutamento e seleção incluam verificações de antecedentes;
- (ii) Implementar processos seguros para desligamentos, garantindo a comunicação tempestiva aos responsáveis pelos controles de acesso, para que sejam adotadas as medidas necessárias de revogação de acessos a sistemas e informações sensíveis.

7. TREINAMENTOS E CONSCIENTIZAÇÃO

A CSD BR promove treinamentos regulares para disseminação de conhecimento e reforço das práticas de prevenção a fraudes. Esses treinamentos são realizados semestralmente e incluem os seguintes temas:

- **Compliance e Código de Conduta e Ética** – discute boas práticas de conformidade regulatória, conduta ética e relacionamento com reguladores e terceiros, incluindo exemplos práticos de como agir em casos de suspeita ou identificação de irregularidades;
- **Gestão de Riscos e Controles Internos** – apresenta a forma de atuação, objetivos e metodologia aplicada pela CSD BR em gestão de riscos e controles internos, demonstrando como os controles internos ajudam na prevenção e mitigação de riscos;
- **PLD/FTP** – aborda temas relacionados à prevenção à lavagem de dinheiro, financiamento do terrorismo e proliferação de armas de destruição em massa, destacando práticas suspeitas e medidas de mitigação;
- **Segurança da Informação** – apresenta temas relacionados à segurança da informação e cibernética, abordando temas como *phishing* e outras práticas enganosas em ambiente online.



8. INVESTIGAÇÃO E SANÇÕES

Os casos de suspeita de fraude reportados deverão ser investigados conforme os ritos estabelecidos para os diferentes tipos de fraude descritos no Regulamento da Plataforma e demais políticas e documentos da Companhia, observando o sigilo dos envolvidos.

A negligência e/ou falha voluntária no descumprimento desta Política, por qualquer das pessoas nela citadas, é passível de punição nos termos da legislação, normativos vigentes e Código de Conduta Ética da Companhia.

9. CONTROLE DO DOCUMENTO

9.1. VIGÊNCIA E DIVULGAÇÃO

Este documento deverá ser divulgado no site da Companhia após a sua aprovação pelo Conselho de Administração, entrando em vigor na data mais recente do quadro no item “CONTROLE DE VERSÃO”, acima, cancelando e substituindo o documento vigente desde a data imediatamente anterior.

9.2. REVISÃO

Este documento deverá ser revisado, no mínimo, anualmente, considerando a data de publicação mais recente (quadro no item “CONTROLE DE VERSÃO”, acima), podendo ser atualizado a qualquer tempo para incorporar melhorias, corrigir erros ou atender normativos.

9.3. DIREITOS AUTORAIS E DISTRIBUIÇÃO

A Companhia possui sobre esse documento todos os direitos de elaboração, alteração, reprodução e distribuição. Este documento substitui todas as versões anteriores. A Companhia não se responsabiliza por versões desatualizadas, modificadas, ou por quaisquer versões provenientes de outras fontes que não a fonte oficial designada para fornecer este material.