POLÍTICA DE GESTÃO DE RISCOS E CONTROLES INTERNOS

SUMÁRIO

CONTROLE DE VERSÃO

Data da Versão	Autores	Número da Versão	Descrição
26/06/2019	Diretor Presidente; Diretoria de Governança, Riscos e Controles	2.0	Elaboração inicial do documento
17/07/2020	Diretor Presidente; Diretoria de Governança, Riscos e Controles	2.1	Revalidação da Política
30/11/2020	Diretor Presidente; Diretoria de Governança, Riscos e Controles Internos	3.0	Ampliação para Política de Riscos, não apenas Operacional; Inclusão do comitê de riscos; Revisão geral
30/03/2021	Diretor Presidente; Diretoria de Governança, Riscos e Controles Internos	4.0	Revisão geral do documento
24/01/2022	Diretor Presidente; Diretoria de Governança, Riscos e Controles Internos	5.0	Revisão geral do documento
18/07/2023	Diretor Presidente; Diretoria de Governança, Riscos e Controles Internos	6.0	Atualização e revisão geral do documento
18/07/2024	Diretor Presidente; Diretoria de Governança, Riscos e Controles Internos	7.0	Padronização de um capítulo com as referências regulatórias normativas em substituição ao Anexo 1
30/12/2024	Diretor Presidente; Diretoria de Governança, Riscos e Controles Internos	8.0	Inclusão do capítulo de Referências Regulatórias e Normativas e do capítulo de Princípios de Gestão de Riscos e Controles Internos; Atualizações considerando a inclusão das atividades de Depósito Centralizado e de Compensação e Liquidação de Ativos; Reestruturação do documento; Revisão geral; Documento aprovado pelo Conselho de Administração em 30/12/2024
13/03/2025	Diretor Presidente; Diretoria de Governança, Riscos e Controles Internos	9.0	Inclusão da referência à Declaração de Apetite por Riscos e à Assunção de Riscos Documento aprovado pelo Conselho de Administração em 13/03/2025

Data da Versão	Autores	Número da Versão	Descrição
05/06/2025	Diretor Presidente; Diretoria de Governança, Riscos e Controles Internos	10.0	Atualização para novo leiaute de documentos. Atualização do Dicionário de Risco; Atualização do desenho de Linhas disposto no capítulo de Papéis e Responsabilidades; Documento aprovado pelo Conselho de Administração em 05/06/2025
01/08/2025	Diretor Presidente; Diretoria de Governança, Riscos e Controles Internos	11.0	Reestruturação do documento; Revisão geral; Documento aprovado pelo Conselho de Administração em 01/08/2025
07/10/2025	Diretor Presidente; Diretoria de Governança, Riscos e Controles Internos	12.0	Atualização do Dicionário de Risco; Atualização no tópico 6.1 Avaliação de Riscos; Documento aprovado pelo Conselho de Administração em 07/10/2025

1. OBJETIVO

Esta Política de Gestão de Riscos e Controles Internos ("Política") visa estabelecer os objetivos, diretrizes, princípios, conceitos e responsabilidades relacionadas a gestão de riscos e controles internos da CSD CENTRAL DE SERVIÇOS DE REGISTRO E DEPÓSITO AOS MERCADOS FINANCEIRO E DE CAPITAIS S.A. ("CSD BR" ou "Companhia"), observadas as melhores práticas de governança e de mercado.

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

2. REFERÊNCIAS REGULATÓRIAS E NORMATIVAS

Este documento utiliza como referências regulatórias e normativas, incluindo, sem se limitar a(s)/o(s):

(i) Resolução CMN n° 4.968, de 25 de novembro de 2021 ("RCMN 4.968/2021");
(ii) Resolução CVM nº 135, de 10 de junho de 2022 ("RCVM 135/2022");
(iii) Resolução BCB nº 304, de 20 de março de 2023 ("RBCB 304/2023");
(iv) Resolução CNSP nº 416, de 20 de julho de 2021 ("RCNSP 416/2021");
(v) Circular Susep nº 638, de 27 de julho de 2021 ("Circular Susep 638/2021");
(vi) Circular Susep nº 619, de 04 de dezembro de 2020 ("Circular Susep 619/2020").

Além das referências regulatórias, a metodologia de Gestão de Riscos e Controles Internos da CSD BR utiliza como referência os melhores frameworks de mercado, como:

(i) *Committee of Sponsoring Organizations of the Tradeway Commission* ("COSO");
(ii) *Principles for Financial Market Infrastructures ("PFMI");*
(iii) *Guidance on Cyber Resilience for Financial Market Infrastructures;*
(iv) *Control Objectives for Information and Related Technologies* ("*COBIT*");
(v) *National Institute of Standards and Technology ("NIST");*
(vi) *Information Technology Infrastructure Library ("ITIL");*
(vii) ISO/IEC 27.001:2022;
(viii) ISO/IEC 27.005:2022.

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

(i) **Apetite por risco:** nível de risco que a Companhia está disposta a aceitar em busca de seus objetivos estratégicos;

(ii) **Atividade:** ações específicas realizadas para a composição de um processo ou conjunto de processos executados pela Companhia (ou em seu nome) que produzam ou suportam um ou mais serviços;

(iii) **Compliance ou conformidade:** é o conjunto de práticas, políticas, processos e controles adotados pela Companhia para assegurar a conformidade com normas internas e externas, princípios éticos e boas práticas de governança. Compreende atividades desenvolvidas com o objetivo de prevenir, detectar e/ou remediar condutas que não estejam em conformidade com tais normas, identificando riscos e/ou causas e agindo preventiva e/ou corretivamente.

(iv) **Controles internos:** mecanismos, regras e procedimentos implementados para proporcionar eficiência operacional, mitigar riscos, assegurar a conformidade com leis e regulamentos, bem como promover a confiabilidade das informações geradas;

(v) **Matriz de riscos:** ferramenta que combina a probabilidade de ocorrência de um risco com a gravidade de seu impacto, classificando-o em níveis de criticidade;

(vi) **Processo:** um conjunto estruturado de atividades interligadas que, quando executadas em sequência, garantem a entrega de um produto ou serviço;

(vii) **Risco:** possível evento ou condição incerta que pode impactar negativamente os objetivos da Companhia ou de sua(s) atividade(s), de seu(s) processo(s) e/ou serviço(s);

(viii) **Risco certificado:** avaliação de risco residual realizada após certificação dos controles;

(ix) **Risco inerente e/ou Risco original:** o nível de risco antes de qualquer ação de controle ou mitigação;

(x) **Risco residual:** o risco que permanece após a implementação de controles e medidas de mitigação;

(xi) **Serviço:** é o conjunto de processos estruturados e organizados, destinados a cumprir uma função específica e gerar valor para os Participantes e usuários finais. No caso da Companhia alguns exemplos de serviços incluem o registro de ativos financeiros, depósito centralizado, compensação e liquidação;

(xii) **Sistema de controles internos:** é o conjunto de políticas, normas, procedimentos, processos e/ou e atividades de controle estabelecidas pela Companhia com o propósito de identificar e gerenciar riscos, visando o alcance dos objetivos e metas organizacionais;

(xiii) **Tolerância ao risco:** resiliência da Companhia e sua capacidade de suportar os efeitos adversos decorrentes de um evento de risco.

3.1. DICIONÁRIO DE RISCOS

O objetivo deste dicionário é proporcionar a uniformização de conceitos e entendimentos que serão utilizados na gestão de riscos e controles internos da Companhia, considerando os serviços prestados, não sendo necessariamente todos os riscos aqui elencados aplicáveis à CSD BR.

Este dicionário é utilizado para a construção e atualizações da matriz de risco operacional e da matriz de risco geral do negócio da Companhia, sendo a primeira a matriz de riscos operacionais de cada área da CSD BR que possua processos relevantes, e a segunda, a matriz de riscos estratégicos da Companhia, como uma visão macro.

(i) **Risco de Estratégia:** perdas decorrentes da definição incorreta da estratégia, da má-execução ou da incapacidade de implementá-la.

(ii) **Risco de Conformidade dos Serviços Autorizados da Plataforma:** perda ocasionada pelo descumprimento ou falhas na observância de regras definidas pelos órgãos reguladores, dentre estas o não envio de informações obrigatórias da Plataforma e/ou produzidas pela Diretoria de Fiscalização e Supervisão (DFS) ao regulador.

(iii) **Risco Operacional da Companhia:** perda ocasionada por falhas ou ineficiências nos processos de acompanhamento e supervisão das atividades e/ou processos operacionais da Companhia. Essas falhas podem levar a problemas como a identificação tardia de erros, descumprimento de procedimentos, baixa qualidade na entrega de produtos e serviços, ou até mesmo a incapacidade de detectar e responder adequadamente a eventos adversos;

(iv) **Risco Operacional da Plataforma:** perdas ocasionadas pelo funcionamento incorreto da Plataforma, exceto processos de Compensação e Liquidação, que transponham o NOC - Network Operations Center;

(v) **Risco de Resiliência Cibernética na Plataforma**: perdas decorrentes de ataques cibernéticos, oriundos de *malware*, técnicas de engenharia social, invasões, ataques de rede (*DDoS e Botnets*) etc. que transponham o SOC - *Security Operations Center*;

(vi) **Risco de Vazamento da Informação da Plataforma:** perdas ocasionadas por exposição de dados sigilosos a terceiros, sejam pessoais ou corporativos, podendo acarretar prejuízos à imagem e às ações estratégicas da Companhia;

(vii) **Risco de Eventos Externos e Catástrofes:** perda relacionada a desastres naturais, atentados, vandalismo, greves, paralisações, epidemias e outros eventos independentes da vontade ou das condições da Companhia;

(viii) **Risco de Terceirização:** perda decorrente de que um fornecedor ou parceiro de negócios não tenha capacidade de atender às demandas de produtos, serviços ou materiais necessários para a operação da Companhia ou perda decorrente de situações em que os serviços prestados ou os processos executados por meio de terceirização não atinjam os padrões contratados e esperados;

(ix) **Risco de Mercado:** perdas ocasionadas por oscilações nos preços de mercado, como mudanças no comportamento das taxas de juros, do câmbio, em índices, preços de commodities, derivativos, preço de ações etc;

(x) **Risco de Crédito:** perdas decorrentes de falhas das contrapartes no cumprimento de obrigações contratuais, por não honrar, total ou parcialmente, seus compromissos financeiros;

(xi) **Risco de Liquidez:** perda decorrente da incapacidade (temporal ou não) de cumprir os compromissos assumidos nas datas previstas em função do descasamento entre os ativos disponíveis e os passivos vencidos;

(xii) **Risco de Interconexão:** perdas decorrentes de falhas operacionais ou tecnológicas na interconexão entre Instituições Operadoras de Sistemas do Mercado Financeiro (IOSMF), dentre elas o Sistema de Transferência de Reservas (STR), núcleo do Sistema de Pagamentos Brasileiro (SPB), podendo afetar o sistema financeiro ou a própria Companhia;

(xiii) **Risco de Investimento:** perda financeira enfrentado por IOSMF quando investe seus próprios recursos ou os de seus participantes;

(xiv) **Risco de Monitoramento das Operações da Plataforma:** perdas ocasionadas por falha no monitoramento das operações na plataforma, incluindo a incapacidade de detectar e prevenir atividades fraudulentas e relativas à lavagem

de dinheiro, financiamento do terrorismo e proliferação de armas de destruição em massa;

(xv) **Risco de Indisponibilidade da Plataforma:** perda ocasionada por indisponibilidade da Plataforma;

(xvi) **Risco de Controle de Titularidade:** perdas ocasionadas por falha no controle de titularidade fiduciária e/ou efetiva de Ativos;

(xvii) **Risco de Compensação e Liquidação:** perdas decorrentes de falhas, erros operacionais e de sistemas, erros de parametrização e falhas de cálculos no Módulo de Compensação e Liquidação de Ativos;

(xviii) **Risco de Vazamento de Informações da Companhia:** perda ocasionada pelo vazamento de informações da Companhia.;

(xix) **Risco na Infraestrutura da Companhia:** perda ocasionada por falhas na infraestrutura lógica ou física da Companhia;

(xx) **Risco de Sucessão:** perda ocasionada devido à saída inesperada de funcionários chave, especialmente aqueles em posições de liderança ou com habilidades críticas. Esse risco pode impactar a continuidade dos negócios, a execução de estratégias e a manutenção do conhecimento institucional;

(xxi) **Risco de Imagem:** perda decorrente de quebra da confiança ou credibilidade de que a Companhia desfruta no seu ambiente de negócios. Esta adversidade resulta da interpretação de notícias veiculadas na imprensa, atitudes e declarações dos representantes da Companhia, bem como de eventos externos que possam afetar sua reputação;

(xxii) **Risco Resiliência Financeira:** perdas ocasionadas pelo não cumprimento do orçamento e política de investimentos da Companhia;

(xxiii) **Risco Legal:** perdas decorrentes de penalidades ou decisões desfavoráveis em aspectos legais e regulamentares que envolvam os contratos firmados e as obrigações fiscais, trabalhistas, societárias e específicas do negócio da Companhia emitidas por órgãos reguladores, assim como cancelamento de licenças expedidas previamente pelos reguladores.

(xxiv) **Risco de Fraude:** perda decorrente de atos intencionais, falsificação ou outras práticas desonestas, cometidas por funcionários, fornecedores ou terceiros para obtenção de vantagem indevida para si ou para outrem;

(xxv) **Risco de Gerenciamento de Ativos de TI:** perda decorrentes de falhas no gerenciamento de TI, tais como, na gestão e atualização de certificados digitais,

chaves de segurança, backups, controle de vulnerabilidades, bem como no controle de acessos e ciclo de vida total e obsolescência dos ativos de TI;

(xxvi) **Risco no Desenvolvimento de Sistemas:** perda decorrente em função do software não atenda aos padrões desejados de desenvolvimento, testes, funcionalidade, performance e controles de vulnerabilidades;

(xxvii) **Risco de Mudanças no Sistema:** perda ocasionada por erros no planejamento e/ou execução de mudanças na plataforma ou em demais Ativos de TI;

(xxviii) **Risco de Conflito de Interesse:** perdas ocasionadas pela falha em identificar e gerenciar conflitos de interesses na Companhia, onde interesses pessoais ou externos possam interferir nas responsabilidades profissionais de colaboradores e/ou administradores, comprometendo a integridade e a ética nas operações da Companhia;

(xxix) **Risco de Custódia:** perda financeira derivada de ativos mantidos em custódia nos casos de insolvência, negligência, fraude, administração inadequada ou manutenção de registros inadequada de um custodiante;

(xxx) **Risco de Emissor:** perda financeira de não ser honrado compromisso relacionado à emissão ou ao resgate do principal e dos acessórios do ativo financeiro ou do valor mobiliário e

(xxxi) **Risco Sistêmico:** perda decorrente pela incapacidade de um ou mais participante de honrar suas obrigações pode desencadear um efeito cascata, afetando outros participantes do mercado;

(xxxii) **Risco de concorrência**: perdas decorrentes da incapacidade de competir com os demais players do mercado ou de novos entrantes, seja por diferenças de preços, tecnologia, ou mesmo atitudes anticoncorrenciais, assim como não ser possível implementar a interoperabilidade em termos que viabilizem a competição.

(xxxiii) **Risco de perda pela contaminação em outras linhas de negócio**: risco de contaminação em outras linhas de negócios não típicas de IOSMF que possam impactar nos serviços autorizados

(xxxiv) **Risco de mudança de legislação**: perdas decorrentes de mudanças na legislação que acarretem redução de receita, impactem na estratégia da Companhia, ou seus produtos operados.

(xxxv) **Risco de limite mínimo de patrimônio líquido:** perda de licenças por alteração normativa ou redução de patrimônio que levem a companhia a não mais cumprir

com a garantia dos limites mínimos de patrimônio líquido impostos pela legislação para os sistemas de mercado financeiro que esta opere.

4. PRINCÍPIOS DE GESTÃO DE RISCOS E CONTROLES INTERNOS

A gestão de riscos e controles internos da Companhia é fundamentada em princípios que visam assegurar a identificação, avaliação, monitoramento e mitigação dos riscos associados a Companhia e aos serviços prestados, garantindo a conformidade com as melhores práticas de governança e de mercado, bem como com as normas legais e regulamentares aplicáveis. A seguir, referenciamos alguns dos princípios que norteiam a gestão de riscos e controles internos da Companhia.

(i) ***Accountability*:** todos os colaboradores são co-responsáveis pela gestão adequada dos riscos e pela utilização correta dos controles internos. Cada um é responsável por suas ações e decisões, promovendo uma cultura de responsabilização e confiança.

(ii) **Melhoria contínua:** a Companhia adota o princípio da melhoria contínua, comprometendo-se com a revisão e aprimoramento constante dos processos e/ou das atividades. Isso inclui a incorporação de lições aprendidas, análise de testes, treinamentos periódicos e adaptação a mudanças no ambiente de negócios.

(iii) **Prevenção:** a prevenção é um princípio fundamental na gestão de riscos, visando evitar ou reduzir a possibilidade de ocorrência e os impactos de eventos adversos. A Companhia implementa medidas preventivas e mecanismos de recuperação, realizando testes regulares para assegurar a eficácia dos controles internos.

(iv) **Transparência:** a gestão de riscos e controles internos da Companhia é conduzida com transparência, de modo que as etapas dos processos são documentadas e comunicadas às partes interessadas, conforme aplicável.

(v) **Conformidade:** a Companhia adota um sistema de controles internos robusto, alinhado às regulamentações aplicáveis e às melhores práticas de mercado.

(vi) **Integração e colaboração:** a gestão de riscos e controles internos é integrada aos processos da Companhia, promovendo a colaboração entre as áreas envolvidas.

5. ESTRUTURA DA GESTÃO DE RISCOS E CONTROLES INTERNOS NA CSD BR

A estrutura de Gestão de Riscos e Controles Internos da Companhia foi organizada de acordo com o modelo de negócio, natureza das operações e complexidade dos serviços oferecidos, e permite à alta Administração monitorar os processos de negócio, assim como realizar a gestão adequada de seus riscos.

A área de Gestão de Riscos e Controles Internos ("GRCI") da Companhia é parte integrante da Diretoria de Governança, Riscos e Controles Internos, que atua de forma independente dentro da estrutura organizacional, com competência técnica, recursos adequados e acesso irrestrito a todas as informações, pessoas e locais, para o cumprimento de suas responsabilidades.

O objetivo da gestão de riscos e controles internos da Companhia é gerenciar os riscos à níveis aceitáveis, de forma que os objetivos estratégicos não venham a ser prejudicados.

Para tanto, são utilizadas ferramentas que permitem (i) realizar a avaliação contínua de fatores de risco internos e externos, que impactam a Companhia, bem como de fatores de riscos que a Companhia representa para outras IOSMF nos casos de interconexão com estas, para o mercado em que atua, para o Sistema de Pagamentos Brasileiro ("SPB") e para o Sistema Financeiro Nacional ("SFN") assim como (ii) ter uma visão abrangente dos riscos.

Dessa forma, visa assegurar que os riscos associados às atividades, aos processos e/ou aos serviços sejam reconhecidos e administrados adequadamente, atuando de forma a evitar que possíveis impactos financeiros, de conformidade (legais), de imagem e/ou operacionais atinjam níveis inaceitáveis.

Além disso, a estrutura de Gestão de Riscos e Controles Internos deve:

- Garantir o atendimento das recomendações e dos apontamentos dos órgãos supervisores, bem como dos apontamentos da Auditoria Interna e dos Auditores Independentes;
- Ser submetida a avaliações e revisões periódicas, pelas estruturas de governança cabíveis.

5.1. PAPÉIS E RESPONSABILIDADES

No contexto de gestão de riscos e controles internos, a Companhia atua de acordo com o modelo de linhas, como um meio de esclarecer os papéis e responsabilidades. A interação entre essas linhas ocorre por meio de fóruns, comitês e fluxos formais de reporte, assegurando sua aderência às melhores práticas, conforme descrito a seguir.

1ª Linha – Gestores das Áreas Operacionais - responsáveis pela gestão diária de processos e riscos, bem como pela definição de ações de mitigação, assegurando a conformidade das operações e de seus processos. Devem realizar o reporte proativo das mudanças de processos e de controles internos aos riscos identificados, bem como das deficiências identificadas, a fim de garantir a constante atualização de identificação dos riscos à 2ª Linha. Cada área deve assegurar a conformidade dos processos de forma a apoiar o alcance da estratégia e dos objetivos do negócio.

2ª Linha - Diretoria de Governança, Riscos e Controles Internos ("GRC") - responsável por monitorar a implementação de práticas eficazes pela 1ª Linha e auxiliar no desenvolvimento de seus processos e controles. Revisar e atualizar periodicamente, o sistema de controles internos, a fim de identificar eventuais deficiências para que sejam corrigidas em tempo hábil; auxiliar as áreas de negócio no desenvolvimento de políticas, normas e procedimentos para assegurar que os riscos inerentes às atividades, aos processos e/ou os serviços da Companhia sejam identificados e administrados adequadamente, mantendo-se dentro dos níveis determinados pelo apetite de risco; contribuir para a conformidade e tempestividade dos relatórios contábeis e financeiros; monitorar a apropriada segregação de funções, afim de reduzir e controlar, potenciais

conflitos de interesses existentes nas áreas, e contribuir na tomada de decisão por parte da Alta Administração.

3ª Linha - Diretoria de Fiscalização e Supervisão ("DFS"), Auditoria Interna e Auditoria Independente - responsáveis por fornecer avaliações independentes quanto (i) à eficiência e eficácia dos processos, dos controles e da metodologia de gestão de riscos, conforme aplicável, dos Participantes e da Companhia, respectivamente; e (ii) à aplicação de normas legais e regulamentares a que se sujeita a Companhia, inclusive no que se refere às normas por ela editadas.

4ª Linha - Comitê de Fiscalização e Supervisão ("CFS") e Conselho de Administração ("CA") - responsáveis por avaliar o funcionamento e a eficácia do gerenciamento de riscos e controles internos, avaliar e monitorar as exposições de risco e fiscalizar a efetividade e suficiência da estrutura de gestão de riscos inerentes às atividades, aos processos e/ou os serviços da Companhia.

As linhas de atuação operam respeitando suas governanças específicas, mas contribuem coletivamente para a gestão integrada de riscos e controles internos. Cada área desempenha, entre outras, às atividades, aos processos e/ou os serviços descritos abaixo, sem prejuízo de outras atividades e responsabilidades previstas em seus regimentos e/ou outros documentos internos:

(i) **Auditoria Interna e Auditoria Independente:** atuam como 3ª Linha, sendo responsáveis pela realização de auditorias periódicas, conforme disposto nos respectivos planos de trabalho.

(ii) **CFS:** atua como 4ª Linha, sendo responsável por monitorar o cumprimento das normas de autorregulação e a atuação da DFS, bem como por receber e analisar os relatórios emitidos pela segunda e terceira linha para fiscalizar a efetividade e suficiência da estrutura de gestão de riscos, controles internos e *compliance* da Companhia.

(iii) **CA:** atua como 4ª Linha, e é responsável por (i) aprovar esta Política, assegurando que esteja alinhada com as diretrizes estratégicas da Companhia, (ii) avaliar periodicamente se o apetite e a tolerância ao risco definidos pela Companhia continuam adequados, (iii) receber e analisar os relatórios emitidos pela segunda e terceira linha, conforme aplicável, garantindo que os resultados dessas avaliações e as recomendações relativas a eventuais deficiências identificadas

sejam discutidos em nível estratégico e que eventuais ações corretivas e/ou de melhorias sejam implementadas quando necessário.

(iv) **DFS:** atua como a 3ª Linha, sendo responsável pela fiscalização e supervisão, direta ou indiretamente, (i) das operações cursadas e dos atos praticados pelos Participantes nos sistemas e mercados administrados pela Companhia; (ii) das atividades de organização e acompanhamento de mercado desenvolvidas pela Companhia; e (iii) da aplicação de normas legais e regulamentares a que se sujeita a Companhia, inclusive no que se refere às normas por ela editadas.

(v) **Diretoria Estatutária:** é responsável por definir os princípios e diretrizes que norteiam a gestão de riscos e controles internos, bem como por assegurar a alocação de recursos adequados para a implementação das políticas e procedimentos de gestão de riscos e controles internos. A Diretoria Estatutária também é responsável pela tomada de decisões que envolvam a assunção de riscos.

(vi) **Gestores das Áreas Operacionais:** atuam como 1ª Linha.

(vii) **GRC:** é responsável pela elaboração e gestão desta Política, bem como por atuar como 2ª Linha, monitorando a implementação de práticas eficazes pela 1ª Linha, e auxiliando as áreas operacionais no desenvolvimento de seus processos e controles. É responsável também por supervisionar e assegurar a conformidade das atividades e processos com as regulamentações internas e externas, realizar testes nos controles internos da 1ª Linha, bem como por comunicar eventuais falhas ou desvios às instâncias apropriadas.

Na CSD BR, a interação entre as linhas ocorre de forma coordenada, estruturada e orientada à geração de valor. Essa integração é essencial para garantir uma visão sobre os riscos, promover a eficiência dos controles e assegurar a conformidade com os padrões regulatórios e expectativas do mercado.

A interação entre a primeira e a segunda linha é contínua e estratégica. A primeira linha é responsável pelo mapeamento dos processos, pela realização de autoavaliações, pela comunicação de incidentes e falhas, bem como pelo acompanhamento da evolução dos planos de ação. Já a segunda linha atua no estabelecimento de diretrizes de controles internos, no suporte à identificação e avaliação de riscos, na definição de controles mitigatórios e na condução de treinamentos. Essa relação é operacionalizada por meio

de uma ferramenta, que centraliza o acompanhamento das obrigações e planos de ação, promovendo transparência e rastreabilidade.

A segunda e a terceira linha mantêm uma interação robusta que permeia o compartilhamento estruturado de informações críticas, como a Matriz de Riscos Corporativa (MRC) elaborada por GRCI, os relatórios emitidos pela Auditoria Interna, o relatório anual de GRC e o status dos planos de ação. Essa troca contínua fortalece a visão integrada sobre os riscos e contribui para a efetividade das avaliações independentes realizadas pela Auditoria Interna.

Além disso, a atuação conjunta das três linhas é viabilizada por fóruns executivos, comitês temáticos, ciclos de reporte estruturados e mecanismos formais de escalonamento. Esses canais asseguram o fluxo contínuo de informações relevantes, seja por meio de reuniões ordinárias e extraordinárias ou envio de relatórios, fortalecendo a tomada de decisão baseada em riscos e promovendo o alinhamento entre estratégia, operação e conformidade.

Mais do que uma divisão de responsabilidades, o modelo das linhas representa um ecossistema colaborativo, no qual cada instância contribui para a integridade, a resiliência e a sustentabilidade da Companhia. Essa sinergia amplia a capacidade organizacional de antecipar ameaças, capturar oportunidades e responder com agilidade às transformações do ambiente regulatório e operacional.

5.2. PARTICIPAÇÃO EM FÓRUNS E INICIATIVAS COLABORATIVAS

A Companhia participa de grupo de trabalho permanente (“Fórum-IOSMF”) do BCB, envolvendo demais IOSMFs e representantes do BCB e da CVM, que discute os temas correlatos às atividades de IOSMFs, incluindo, sem se limitar a, gestão de riscos, continuidade de negócios, e resiliência cibernética, considerando as interdependências existentes e aquelas que potencialmente venham a ser estabelecidas.

Tanto no âmbito desse quanto de outros fóruns, a Companhia, com apoio da área de Gestão de Riscos e Controles Internos, realiza avaliações abrangentes sobre o mapeamento de riscos, monitoramento contínuo e estabelecimento de mitigadores a serem estabelecidos para garantir a segurança e eficiência das interconexões.

6. METODOLOGIA DE GESTÃO DE RISCOS E CONTROLES INTERNOS

A Metodologia de Gestão de Riscos e Controles Internos da Companhia é um conjunto estruturado de processos e práticas que visam identificar, avaliar, tratar, monitorar e reportar os riscos associados às suas atividades e/ou aos seus processos. Essa metodologia promove uma abordagem preventiva e eficaz, integrando a gestão de riscos à estratégia organizacional e fomentando uma cultura de controle e governança sólida.

O processo de construção e elaboração da Matriz de Riscos e Controles (MRC) está descrito na Metodologia de Gestão de Riscos e Controles Internos, documento integrante dos normativos da Companhia e alinhado às melhores práticas de mercado e de governança. e inclui:

(i) **Entendimento, atualização ou estruturação de processos:** esta etapa envolve a compreensão detalhada das atividades e procedimentos que compõem os processos da Companhia, identificando os riscos inerentes e os processos que necessitam de controles internos mais robustos. Com base nesse entendimento, os processos são atualizados ou estruturados para incorporar práticas de gestão de riscos e controles internos, garantindo que estejam alinhados com as melhores práticas e regulamentações aplicáveis.

(ii) **Acompanhamento da implantação do processo:** nesta fase, é realizado o acompanhamento da implementação dos processos estruturados, assegurando que todas as etapas sejam executadas conforme planejado e que os controles internos estejam operacionais.

(iii) **Avaliação de riscos e identificação de controles:** a avaliação contínua dos riscos é realizada para identificar possíveis falhas e áreas de melhorias, bem como eventuais riscos novos em decorrência da introdução de novos produtos e serviços ou de modificação relevante em produtos e serviços existentes, mudanças significativas em processos, sistemas, operações, modelo de negócio e normas legais e regulamentares, permitindo que seja realizada a identificação ou aprimoramento dos controles internos associados, garantindo que os riscos sejam gerenciados de forma eficaz.

(iv) **Execução de testes e Certificação de Controles:** testes são executados para verificar a eficácia dos controles internos. A certificação dos controles assegura

que os controles internos estejam funcionando conforme o esperado e que os riscos estejam sendo mitigados adequadamente.

(v) **Reporte de resultados:** os resultados das avaliações e testes são documentados e reportados às partes interessadas e aos organismos de governança, conforme aplicável, proporcionando transparência e *accountability* no processo de gestão de riscos.

(vi) **Monitoramento e aculturamento contínuo:** a última etapa envolve o monitoramento contínuo dos riscos e controles, bem como a promoção de uma cultura de gestão de riscos dentro da Companhia. Treinamentos e atualizações regulares são realizados para manter todos os colaboradores alinhados com as práticas de gestão de riscos.

6.1. AVALIAÇÃO DE RISCOS

A avaliação de riscos na Companhia é um processo contínuo e sistemático que visa identificar, avaliar e mitigar os riscos associados às suas atividades e/ou aos seus processos, descritos na Metodologia de Gestão de Riscos e Controles Internos da CSD BR, assim como os eventuais riscos constantes no Dicionário de Riscos da Companhia a qual está possa estar sujeita.

Nesse processo também são avaliados os fatores de risco que a Companhia representa para as outras IOSMF, para seus Participantes, para Prestadores de Serviço Crítico, para o mercado em que atua, para o Sistema de Pagamentos Brasileiro (SPB), para o Sistema Financeiro Nacional (SFN) e para a STR (Sistema de Transferência de Reservas).

A avaliação de riscos é realizada com base nos critérios de impacto e probabilidade, permitindo identificar a severidade das possíveis perdas e estabelecer prioridades na gestão dos riscos, sendo formalizados na ferramenta de gestão de riscos.

A Companhia possui procedimentos específicos de contratação e gestão de serviços de terceiros, orientando quanto aos procedimentos, rotinas e condutas a serem observados para mitigar riscos e reduzir custos. Realiza-se a definição da criticidade dos serviços e, com base nisso, avaliações reputacionais e *due diligence* específicas, adotando processos robustos para avaliar e monitorar os riscos, especialmente para prestadores de serviços de risco alto ou crítico.

6.2. APETITE E TOLERÂNCIA POR RISCO

Os parâmetros para apetite por riscos são definidos qualitativamente e avaliados no contexto da estratégia de negócio e adoção de risco da Companhia, que seguem uma abordagem conservadora. De forma geral, a Companhia adota um apetite ao risco muito baixo e/ou baixo, priorizando a segurança, a conformidade e a estabilidade operacional na gestão de suas atividades e processos, conforme discriminado em sua Declaração por Apetite por Riscos.

6.3. ASSUNÇÃO DE RISCOS

O processo de assunção de riscos pela Companhia é realizado de forma criteriosa e alinhada com a Declaração de Apetite por Riscos da Companhia. A assunção de riscos deve ser documentada pela área de Gestão de Riscos e Controles Internos, e aprovada pelos órgãos de governança de acordo com a Declaração de Apetite por Riscos.

Os riscos assumidos devem ser monitorados continuamente pela área de Riscos e Controles Internos para garantir que permaneçam dentro dos níveis aceitáveis.

6.4. RELATÓRIOS PERIÓDICOS

A Companhia mantém um processo estruturado de reporte periódico às instâncias de governança, com o objetivo de assegurar a eficácia da gestão de riscos e controles internos. Esses relatórios fornecem uma visão consolidada e estratégica do perfil de riscos corporativos, permitindo que os órgãos de governança, quais sejam, a Diretoria Estatutária, o Conselho de Administração e os Comitês de Assessoramento do Conselho de Administração, acompanhem a evolução dos principais temas por meio de recebimento das informações da área de GRCI, com avaliação da efetividade das ações mitigatórias e tomem decisões com base em informações qualificadas e tempestivas.

O conteúdo dos relatórios contempla uma visão abrangente das atividades e processos de gestão de riscos, incluindo à identificação e avaliação dos riscos, acompanhamento das ações de mitigação implementadas, monitoramento contínuo da efetividade dos controles internos e indicadores de risco.

Além disso, os relatórios periódicos asseguram que a Companhia esteja em conformidade com todas as regulamentações aplicáveis, analisando as mudanças regulatórias e seu impacto nos processos da Companhia. Eles também avaliam a eficácia dos controles de segurança e dos planos de continuidade de negócios e recuperação de

desastres e de saída ordenada, sendo fundamentais para a tomada de decisões estratégicas, garantindo que a Companhia esteja preparada para enfrentar os desafios e riscos associados às suas atividades.

7. TREINAMENTO E ACULTURAMENTO

A GRCI, em parceria com as demais áreas, participa ativamente da execução de treinamentos obrigatórios, os quais são gerenciados pelo Departamento de Recursos Humanos ("RH"). Esses treinamentos têm como objetivo disseminar boas práticas, aumentar o conhecimento sobre a gestão eficaz de riscos e promover a cultura de conformidade entre os colaboradores.

Também são realizadas ações de conscientização sobre temas relevantes para a Companhia, por meio de eventos e agendas promovidos pelo RH, assim como por meio da publicação de *newsletters* e informativos emitidos pela GRC.

8. CONTROLE DO DOCUMENTO

8.1. VIGÊNCIA E DIVULGAÇÃO

Este documento deverá ser divulgado no site da Companhia após 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.

8.2. 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.

8.3. 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.