POLÍTICA DE GESTÃO DE RISCOS E CONTROLES INTERNOS

[PUBLICO | PUBLIC]

SUMÁRIO

CONTROLE DE VERSÃO 3
1. OBJETIVO 5
2. REFERÊNCIAS REGULATÓRIAS E NORMATIVAS 5
3. DEFINIÇÕES 6
3.1. TAXONOMIA DE RISCOS 8
4. PRINCÍPIOS DE GESTÃO DE RISCOS E CONTROLES INTERNOS 8
5. ESTRUTURA DA GESTÃO DE RISCOS E CONTROLES INTERNOS NA CSD BR 9
5.1. PAPÉIS E RESPONSABILIDADES 10
5.2. GOVERNANÇA E ALÇADAS DE APROVAÇÃO 15
5.3. PARTICIPAÇÃO EM FÓRUNS E INICIATIVAS COLABORATIVAS 16
6. GESTÃO INTEGRADA E TRANSVERSAL DE RISCOS 16
7. METODOLOGIA DE GESTÃO DE RISCOS E CONTROLES INTERNOS 17
7.1. AVALIAÇÃO DE RISCOS 18
7.2. APETITE E TOLERÂNCIA POR RISCO 19
7.3. ASSUNÇÃO DE RISCOS 19
7.4. RELATÓRIOS PERIÓDICOS 20
8. TREINAMENTO E ACULTURAMENTO 21
9. CONTROLE DO DOCUMENTO 22
9.1. VIGÊNCIA E DIVULGAÇÃO 22
9.2. REVISÃO 22
9.3. DIREITOS AUTORAIS E DISTRIBUIÇÃO 22

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
03/12/2025	Diretor Presidente; Diretoria de Governança, Riscos e Controles Internos	13.0	Atualização para refletir a criação do Comitê de Auditoria como órgão estatutário; Padronização do uso do termo departamento, ao invés de área; Documento aprovado pelo Conselho de Administração em 03/12/2025
13/02/2026	Diretor Presidente; Diretoria de Governança, Riscos e Controles Internos	14.0	Atualização em Referências Regulatórias e Normativas e Dicionário de Riscos; Reestruturação do documento; Revisão geral; Criação do Capítulo: 6 Gestão Integrada e Transversal de Riscos; Documento aprovado pelo Conselho de Administração 12/02/2026
17/11/2026	Diretor Presidente; Diretoria de Governança, Riscos e Controles Internos	15.0	Atualização da estrutura de governança e dos papéis e responsabilidades; evolução da taxonomia corporativa de riscos, contemplando os Riscos Corporativos, Riscos Departamentais e Fatores de Risco; aprimoramento da integração entre Política, Metodologia de Gestão de Riscos e Controles Internos e Declaração de Apetite por Riscos; atualização dos conceitos de avaliação, assunção, monitoramento e reporte de riscos; e revisão geral do documento; Documento aprovado pelo Conselho de Administração 06/11/2026

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.

A operacionalização das diretrizes estabelecidas nesta Política é disciplinada pela Metodologia de Gestão de Riscos e Controles Internos, enquanto os parâmetros de apetite, tolerância e limites de exposição aos riscos são estabelecidos na Declaração de Apetite por Riscos da Companhia.

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

Esta Política e a respectiva Metodologia de Gestão de Riscos e Controles Internos observam a regulamentação aplicável à CSD BR, considerando sua atuação como Instituição Operadora de Sistemas do Mercado Financeiro ("IOSMF"), bem como referências regulatórias, normativas e boas práticas nacionais e internacionais aplicáveis à gestão de riscos, controles internos, governança e resiliência operacional.

Constituem referências, conforme aplicáveis:

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

Adicionalmente, são consideradas, conforme aplicáveis, as políticas, normas e demais documentos internos da Companhia relacionados à gestão de riscos e controles internos.

- Política de Gestão de Fraudes;
- Política de Segurança da Informação e Segurança Cibernética;
- Política de Gestão de Continuidade de Negócios ("PGCN");

- Política de Gestão de Serviço de Tecnologia da Informação;
- Política de Gestão de Terceirização de Serviços.

Como referências de boas práticas e frameworks de mercado, são considerados, entre outros:

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

As referências regulatórias, normativas e de boas práticas devem ser consideradas em suas versões vigentes e conforme sua aplicabilidade às atividades, processos e serviços da Companhia.

3. DEFINIÇÕES

(i) **Apetite por risco:** nível e natureza dos riscos que a Companhia está disposta a assumir em busca de seus objetivos estratégicos, observados os parâmetros estabelecidos pela Declaração de Apetite por Riscos;

(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, procedimentos e demais atividades de controles estabelecidos para apoiar o alcance dos objetivos da Companhia, contribuir para a gestão dos riscos, promover a eficiência e a confiabilidade dos

processos e informações e assegurar a conformidade com requisitos internos, legais e regulatórios;

(v) **Fator de Risco:** condição, circunstância ou elemento interno ou externo que pode influenciar a probabilidade de ocorrência ou o impacto de um risco, sendo utilizado para compreender e estruturar as principais fontes de exposição associadas aos riscos da Companhia;

(vi) **Matriz de riscos e controles ("MRC"):** instrumento utilizado para estruturar e documentar a identificação e avaliação dos riscos, seus fatores de risco, controles associados e demais elementos necessários ao acompanhamento da exposição aos riscos e do ambiente de controles internos, conforme critérios estabelecidos na Metodologia de Gestão de Riscos e Controles Internos;

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

(viii) **Risco:** efeito da incerteza sobre os objetivos da Companhia, relacionado a eventos ou condições que possam afetar o alcance de seus objetivos estratégicos, operacionais, financeiros, regulatórios ou de continuidade;

(ix) **Risco Corporativo:** risco de natureza estratégica ou transversal, relevante para a Companhia, que representa exposição capaz de afetar seus objetivos, operações, sustentabilidade, resiliência ou cumprimento de obrigações. Sua consolidação permite a visão corporativa de riscos da Companhia;

(x) **Risco Departamental:** risco associado aos processos, atividades e responsabilidades dos departamentos da Companhia, constituindo objeto corporativo de gestão de riscos que contribui para a identificação, avaliação e consolidação das exposições da organização;

(xi) **Risco inerente:** nível de exposição ao risco existente antes de considerados os efeitos dos controles e demais medidas de tratamento aplicáveis;

(xii) **Risco residual:** nível de exposição ao risco remanescente após considerados os efeitos dos controles e demais medidas de tratamento aplicáveis;

(xiii) **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;

(xiv) **Sistema de controles internos:** conjunto integrado de políticas, normas, procedimentos, processos e atividades de controle estabelecidos pela Companhia

para apoiar o alcance de seus objetivos, a gestão dos riscos, a confiabilidade das informações, a eficiência das operações e a conformidade com requisitos internos, legais e regulatórios;

(xv) **Tolerância ao risco:** nível de variação ou exposição ao risco que a Companhia admite em relação ao apetite estabelecido, observados os parâmetros e critérios definidos na Declaração de Apetite por Riscos.

(xvi) **Limite de Risco:** nível máximo de exposição estabelecido pela Companhia para cada Risco Corporativo, correspondente, para fins de enquadramento na Declaração de Apetite por Riscos, à respectiva tolerância máxima. Sua ultrapassagem requer tratamento prioritário, avaliação formal e escalonamento às instâncias competentes, observadas as restrições legais e regulatórias aplicáveis.

3.1. TAXONOMIA DE RISCOS

A CSD BR adota taxonomia corporativa de riscos com o objetivo de estabelecer linguagem comum e proporcionar consistência à identificação, avaliação, consolidação, monitoramento e reporte das exposições da Companhia.

A taxonomia contempla os Riscos Corporativos, os Riscos Departamentais e os Fatores de Risco, permitindo relacionar as exposições identificadas nos processos e atividades à visão consolidada de riscos da Companhia.

A classificação, estrutura, critérios de associação e detalhamento da taxonomia são estabelecidos na Metodologia de Gestão de Riscos e Controles Internos, podendo ser atualizados de acordo com a evolução do ambiente de negócios, regulatório, tecnológico e operacional, observadas as alçadas de governança aplicáveis.

4. PRINCÍPIOS DE GESTÃO DE RISCOS E CONTROLES INTERNOS

A gestão de riscos e controles internos da Companhia é fundamentada em princípios que orientam a identificação, avaliação, tratamento, monitoramento e reporte dos riscos associados à Companhia e aos serviços prestados, e contribui para a conformidade com as normas legais e regulamentares aplicáveis e para adoção de boas práticas de governança e de mercado.

A seguir, referenciamos alguns dos princípios que norteiam a gestão de riscos e controles internos da Companhia.

(i) ***Accountability*:** a gestão de riscos e controles internos é responsabilidade de todos, observados os papéis e responsabilidades atribuídos às diferentes instâncias de governança e linhas de atuação. Cada colaborador é responsável por suas ações e decisões, contribuindo para uma cultura de gestão de riscos, controles e responsabilização.

(ii) **Melhoria contínua:** a Companhia adota a gestão de riscos e controles internos como um processo evolutivo, promovendo a revisão e o aprimoramento contínuo de seus processos, práticas e controles, considerando, entre outros aspectos, resultados de avaliações e testes, eventos e perdas, lições aprendidas e mudanças no ambiente de negócios, regulatório, tecnológico e operacional.

(iii) **Prevenção:** a prevenção é um princípio fundamental da gestão de riscos, e busca reduzir a possibilidade de ocorrência e impactos de eventos adversos. A Companhia adota medidas preventivas, mecanismos de resposta e recuperação, e procedimentos de avaliação e monitoramento 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 à estratégia e tomada de decisão da Companhia e promove a colaboração entre os departamentos e as instâncias de governança, observados os respectivos papéis e responsabilidades;

(vii) **Proporcionalidade:** a gestão de riscos e controles internos deve considerar a natureza, relevância, complexidade e exposição aos riscos das atividades, processos e serviços da Companhia, permitindo que os instrumentos e procedimentos de gestão sejam aplicados de forma proporcional ao risco.

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

A estrutura de gestão de riscos e controles internos da Companhia é organizada de acordo com seu modelo de negócio, a natureza de suas operações e a complexidade dos serviços oferecidos, permitindo a adequada gestão, monitoramento e reporte dos riscos

e controles, bem como o acompanhamento das exposições pelas instâncias de governança competentes.

O Departamento de Gestão de Riscos e Controles Internos ("GRCI") da Companhia integra a Diretoria de Governança, Riscos e Controles Internos e estabelece e coordena o modelo corporativo de riscos e controles internos, atuando como 2ª Linha, com independência no exercício de suas atribuições, competência técnica, recursos adequados e acesso às informações, pessoas e demais recursos necessários ao cumprimento de suas responsabilidades.

A estrutura de gestão de riscos e controles internos tem por objetivo contribuir para que os riscos associados às atividades, processos, serviços e interconexões da Companhia sejam identificados, avaliados, tratados, monitorados e reportados de forma adequada, observados os parâmetros estabelecidos na Declaração de Apetite por Riscos.

Para tanto, são utilizados instrumentos que permitem a avaliação contínua dos fatores internos e externos que possam influenciar a exposição da Companhia aos riscos, incluindo aqueles relacionados às interconexões com outras Instituições Operadoras de Sistemas do Mercado Financeiro ("IOSMF"), ao mercado em que atua, ao Sistema de Pagamentos Brasileiro ("SPB") e ao Sistema Financeiro Nacional ("SFN"), proporcionando uma visão abrangente e integrada dos riscos.

A estrutura deve, ainda, contribuir para o adequado tratamento e acompanhamento das recomendações e apontamentos dos órgãos supervisores, da Auditoria Interna e dos Auditores Independentes, conforme aplicável, bem como ser submetida a avaliações e revisões periódicas pelas instâncias de governança competentes.

5.1. PAPÉIS E RESPONSABILIDADES

No contexto da gestão de riscos e controles internos, a Companhia adota modelo de atuação baseado na adequada segregação e coordenação de responsabilidades entre as instâncias de governança, os departamentos responsáveis pela gestão dos riscos e controles, a Diretoria de Governança, Riscos e Controles Internos ("GRC") e a Auditoria Interna.

As responsabilidades são organizadas de forma distinta e complementar, preservando a responsabilidade da gestão sobre os riscos e controles de seus processos, a atuação de

orientação, monitoramento e *challenge* da 2ª Linha, e a independência da avaliação realizada pela 3ª Linha.

As instâncias de governança exercem suas atribuições de direcionamento, supervisão, acompanhamento e decisão, observadas as competências estabelecidas nos respectivos documentos de governança e demais normativos aplicáveis.

Modelo de Atuação - Responsabilidades



Conselho de Administração ("CA") - Responsável por aprovar esta Política e a Declaração de Apetite por Riscos, acompanhar a estrutura de gestão de riscos e controles internos e avaliar periodicamente as exposições relevantes e a adequação dos parâmetros de apetite e tolerância aos riscos, observadas suas competências estatutárias, regulamentares e demais atribuições estabelecidas nos instrumentos de governança da Companhia.

Comitê de Auditoria ("CoAud") - Atua no assessoramento ao Conselho de Administração, avaliando e acompanhando, no âmbito de suas atribuições, a efetividade e a suficiência da estrutura de gestão de riscos, controles internos e conformidade da Companhia, bem como os reportes e matérias submetidos à sua apreciação. A Auditoria Interna responde diretamente ao CoAud, preservando sua independência em relação às atividades e estruturas avaliadas.

Comitê de Fiscalização e Supervisão ("CFS") - Atua como instância de governança relacionada às atividades de fiscalização e supervisão, acompanhando, no âmbito de suas competências, a atuação da Diretoria de Fiscalização e Supervisão ("DFS") e as

matérias decorrentes das atividades de fiscalização e supervisão, observadas as competências estabelecidas nos respectivos documentos de governança e os deveres de independência e sigilo aplicáveis.

Diretoria Estatutária - Responsável por implementar as diretrizes estabelecidas pelo Conselho de Administração, promover condições e recursos adequados ao funcionamento da estrutura de gestão de riscos e controles internos, acompanhar as exposições relevantes e deliberar sobre matérias e assunções de riscos dentro de suas competências e alçadas.

1ª Linha – Departamentos operacionais - Responsáveis pela gestão dos riscos e controles relacionados aos processos, atividades e serviços sob sua responsabilidade, incluindo a identificação e avaliação dos riscos, a implementação, execução e manutenção dos controles, a definição e execução das medidas de tratamento, a comunicação tempestiva de eventos, mudanças relevantes e deficiências identificadas, bem como o acompanhamento dos respectivos planos de ação.

Os gestores dos departamentos são responsáveis por manter a gestão dos riscos e controles integrada à gestão de seus processos e à tomada de decisão, observadas as diretrizes, a metodologia e os parâmetros de apetite e tolerância estabelecidos pela Companhia.

Os departamentos são também responsáveis por participar dos processos de continuidade de negócios aplicáveis às suas atividades, incluindo a identificação de processos e recursos críticos, o fornecimento e a atualização das informações necessárias às análises de impacto nos negócios e a execução das medidas de continuidade sob sua responsabilidade.

2ª Linha - Diretoria de Governança, Riscos e Controles Internos ("GRC"): Composta pelo Departamento de Gestão de Riscos e Controles Internos ("GRCI") e pelo Departamento de Compliance, atua como 2ª linha, observadas as atribuições específicas de cada uma das estruturas que a integram.

O GRCI é responsável por estabelecer e coordenar o modelo corporativo de gestão de riscos e controles internos da Companhia, incluindo o desenvolvimento, a manutenção e a evolução da metodologia; a coordenação dos processos de identificação, avaliação, tratamento, monitoramento e reporte dos riscos; a coordenação do processo de elaboração, revisão e monitoramento da Declaração de Apetite por Riscos; a orientação

e o *challenge* à 1ª Linha; o monitoramento das exposições aos riscos e do ambiente de controles internos; a realização de avaliações e testes de controles internos, conforme aplicável; o acompanhamento dos planos de ação decorrentes das avaliações realizadas; e a consolidação e o reporte das informações às instâncias de governança competentes.

O Departamento de Compliance é responsável por promover a conformidade com as normas internas e externas aplicáveis à Companhia e fortalecer a cultura ética e de integridade. Atua na orientação à 1ª Linha, no acompanhamento do ambiente regulatório e no monitoramento da aderência às obrigações internas, legais e regulatórias, bem como na realização das atividades de conformidade sob sua responsabilidade. Também promove ações de conscientização e disseminação da cultura de conformidade, acompanha situações de não conformidade e reporta às instâncias de governança competentes os temas relevantes identificados no exercício de suas atividades.

Em conjunto, a GRC promove ações de conscientização e disseminação da cultura de gestão de riscos, controles internos, conformidade, ética e integridade na Companhia, acompanha temas relevantes no âmbito de suas atribuições e reporta às instâncias de governança competentes as informações, exposições e situações relevantes identificadas no exercício de suas atividades.

A atuação da 2ª Linha possui caráter de orientação, monitoramento, avaliação e *challenge* e não substitui as responsabilidades da 1ª Linha pela gestão dos riscos, execução dos controles, conformidade e implementação das medidas de tratamento relacionadas aos processos, atividades sob sua responsabilidade.

3ª Linha - Auditoria Interna - responsável por fornecer avaliação independente sobre a adequação e a efetividade da governança, da gestão de riscos e dos controles internos da Companhia, observados seu mandato, planejamento e normas aplicáveis.

A Auditoria Interna responde diretamente ao Comitê de Auditoria (“CoAud”), preservando sua independência em relação às atividades e estruturas avaliadas e reportando os resultados de seus trabalhos às instâncias competentes.

Asseguração e Supervisão Independente - complementarmente às três linhas e às instâncias de governança interna, a Companhia está sujeita à atuação de agentes externos de asseguração, supervisão, fiscalização e avaliação, que contribuem, de acordo com suas respectivas competências e escopos de atuação, para o fortalecimento

da governança corporativa e para a avaliação da gestão de riscos, dos controles internos e da conformidade.

Essa camada pode compreender, entre outros, a Auditoria Independente, organismos de certificação, órgãos reguladores e supervisores, demais autoridades competentes e outros agentes externos relacionados às atividades e interdependências da Companhia, não constituindo uma linha adicional de responsabilidade e não substituindo as atribuições da Governança, da 1ª, 2ª ou 3ª Linha.

Diretoria de Fiscalização e Supervisão ("DFS") – Exerce, de forma independente, suas atribuições de fiscalização e supervisão, direta ou indiretamente, das operações e dos atos praticados pelos Participantes nos sistemas e mercados administrados pela Companhia, bem como das atividades de organização e acompanhamento de mercado por ela desenvolvidas e da observância das normas legais e regulamentares que lhe são aplicáveis, inclusive daquelas por ela editadas, preservadas suas competências específicas e os deveres de sigilo.

A DFS mantém sua interação com o Comitê de Fiscalização e Supervisão ("CFS"), observadas as respectivas competências, independência e os fluxos de governança aplicáveis.

Integração e interação do modelo – A atuação das instâncias de governança, das três linhas, da DFS e da camada de asseguração e supervisão independente ocorre de forma coordenada, observadas suas respectivas competências, responsabilidades, independência, segregação de funções e, quando aplicável, os deveres de sigilo.

A interação entre essas estruturas ocorre por meio dos mecanismos de governança, fluxos de informação, reportes, fóruns, comitês e processos de escalonamento aplicáveis, contribuindo para uma visão integrada das exposições aos riscos, do ambiente de controles internos e da conformidade, bem como para subsidiar a tomada de decisão pelas instâncias competentes.

A interação e o compartilhamento de informações não implicam transferência de responsabilidades entre as estruturas, permanecendo cada uma responsável pelo exercício das atribuições que lhe são próprias.

5.2. GOVERNANÇA E ALÇADAS DE APROVAÇÃO

Os instrumentos que compõem a estrutura de gestão de riscos e controles internos da Companhia estão sujeitos às alçadas de aprovação estabelecidas nesta Política e nos respectivos instrumentos de governança, observadas a natureza e a materialidade das alterações propostas.

Instrumento / decisão	Proposição / Coordenação	Apreciação	Aprovação
Política de Gestão de Riscos e Controles Internos	GRCI	Diretoria Estatutária e CoAud	CA
Alteração material da Política	GRCI	Diretoria Estatutária e CoAud	CA
Metodologia de Gestão de Riscos e Controles Internos	GRCI	Diretoria Estatutária e CoAud	Diretoria Estatutária
Alteração material da Metodologia	GRCI	Diretoria Estatutária e CoAud	Diretoria Estatutária
Aprimoramentos e ajustes técnico-operacionais da Metodologia	GRCI	—	GRCI
Declaração de Apetite por Riscos – RAS	GRCI	Diretoria Estatutária e CoAud	CA
Alteração material de apetite, tolerância ou limites	GRCI	Diretoria Estatutária e CoAud	CA
Permanência temporária de exposição acima do apetite e dentro da tolerância	1ª Linha	GRCI — avaliação técnica	Diretoria Estatutária
Assunção ou manutenção excepcional de exposição acima do limite	1ª Linha, com avaliação da GRCI	CoAud — apreciação e recomendação	CA

As decisões relativas à assunção ou manutenção de exposições superiores ao apetite deverão observar as condições estabelecidas na Declaração de Apetite por Riscos, incluindo a fundamentação pela 1ª Linha, a avaliação técnica da GRCI, as medidas de tratamento e monitoramento aplicáveis e o escalonamento às instâncias competentes, conforme as respectivas alçadas.

A alçada aplicável será determinada pela natureza e pelo impacto da alteração, e não exclusivamente pelo instrumento em que ela seja formalizada. Alterações que afetem princípios, responsabilidades ou a estrutura de governança estabelecidos nesta Política,

bem como alterações materiais nos parâmetros de apetite, tolerância ou limites de riscos, deverão observar as respectivas alçadas de aprovação.

5.3. PARTICIPAÇÃO EM FÓRUNS E INICIATIVAS COLABORATIVAS

A Companhia participa, conforme aplicável, de fóruns, grupos de trabalho e iniciativas colaborativas promovidas por órgãos reguladores e supervisores, IOSMF e demais agentes do mercado, destinados à discussão e ao desenvolvimento de temas relacionados às suas atividades, incluindo gestão de riscos, continuidade de negócios, resiliência operacional e cibernética, bem como outros assuntos relevantes para a segurança, eficiência e estabilidade dos sistemas e mercados em que atua.

A participação nessas iniciativas contribui para o acompanhamento da evolução do ambiente de riscos, para a identificação de interdependências e potenciais exposições decorrentes das relações com outras instituições e agentes do mercado e para o aprimoramento contínuo das práticas de gestão de riscos e controles internos da Companhia.

6. GESTÃO INTEGRADA E TRANSVERSAL DE RISCOS

A gestão de riscos é realizada de forma integrada e consistente, considerando os principais riscos associados às atividades, processos, serviços e relacionamentos com terceiros, bem como a complexidade, a criticidade e as interdependências existentes. Essa abordagem contribui para que os riscos relevantes sejam identificados, avaliados, tratados, monitorados e reportados de forma coordenada, observada a adequada segregação de responsabilidades e a estrutura de governança estabelecida nesta Política.

Os riscos e controles internos são tratados de forma transversal, considerando as relações entre departamentos, processos, serviços, sistemas, prestadores de serviços e demais agentes relevantes, de modo a permitir uma visão abrangente das exposições da Companhia e a identificação de interdependências, concentrações e potenciais efeitos decorrentes da materialização dos riscos. As informações resultantes da identificação, avaliação, tratamento e monitoramento dos riscos são consolidadas e reportadas às instâncias competentes, contribuindo para a tomada de decisão e para o acompanhamento das exposições em relação aos parâmetros estabelecidos na Declaração de Apetite por Riscos.

No âmbito dessa abordagem são considerados, entre outros, os riscos relacionados à fraude, terceiros e dependências externas, tecnologia, segurança da informação e segurança cibernética, continuidade de negócios e demais fatores internos ou externos que possam afetar processos, serviços ou objetivos da Companhia. Esses riscos são considerados de forma integrada e transversal, observadas suas características, interdependências e os normativos específicos aplicáveis.

A estrutura, os critérios e os instrumentos utilizados para identificação, classificação, avaliação, consolidação e monitoramento dos riscos e controles internos são estabelecidos na Metodologia de Gestão de Riscos e Controles Internos, observadas as diretrizes desta Política.

7. METODOLOGIA DE GESTÃO DE RISCOS E CONTROLES INTERNOS

A Metodologia de Gestão de Riscos e Controles Internos estabelece os critérios, procedimentos, instrumentos e parâmetros para a identificação, avaliação, tratamento, monitoramento e reporte dos riscos e controles internos da Companhia, observadas as diretrizes e responsabilidades estabelecidas nesta Política e os parâmetros definidos na Declaração de Apetite por Riscos.

A Metodologia deve proporcionar abordagem estruturada, integrada e proporcional à natureza, relevância, complexidade e exposição aos riscos das atividades, processos e serviços da Companhia, e permitir a avaliação dos riscos inerentes, dos controles associados e dos riscos residuais, bem como sua consolidação e monitoramento.

A Metodologia disciplina, entre outros aspectos, a identificação e avaliação dos riscos, a identificação e classificação dos controles internos, a avaliação do risco inerente e residual, a realização de avaliações e testes de controles, o tratamento e acompanhamento das exposições identificadas, o monitoramento dos riscos e controles e o respectivo reporte às instâncias competentes.

Considerando o caráter dinâmico da gestão de riscos e o processo evolutivo do ambiente de negócios, regulatório, tecnológico e operacional, a Metodologia poderá ser revisada e aprimorada pelo GRCI, mediante fundamentação técnica e de forma proporcional à natureza, relevância, complexidade e exposição aos riscos dos processos avaliados.

Ajustes técnico-operacionais poderão contemplar procedimentos, instrumentos de avaliação, níveis de detalhamento, técnicas de análise, modelos de testes e demais parâmetros de aplicação, desde que preservados os princípios, objetivos, responsabilidades e diretrizes estabelecidos nesta Política e os parâmetros definidos na Declaração de Apetite por Riscos.

As alterações deverão possuir justificativa e rastreabilidade e observar as respectivas alçadas de aprovação quando implicarem mudanças materiais na estrutura da Metodologia, nos princípios ou responsabilidades estabelecidas nesta Política ou nos parâmetros de apetite, tolerância e limites de riscos.

7.1. AVALIAÇÃO DE RISCOS

A avaliação de riscos na Companhia é um processo contínuo e sistemático destinado a identificar, analisar e avaliar os riscos aos quais a Companhia está ou possa vir a estar exposta, considerando suas atividades, processos, serviços, objetivos, interdependências e o ambiente interno e externo em que atua.

A avaliação deve considerar tanto os riscos que possam afetar a Companhia quanto, conforme aplicável, os potenciais impactos decorrentes de suas atividades, serviços e interconexões sobre Participantes, outras IOSMF, prestadores de serviços relevantes, o mercado e as infraestruturas e sistemas com os quais a Companhia se relaciona.

A avaliação dos riscos deve considerar a taxonomia adotada pela Companhia e permitir sua análise sob diferentes níveis e perspectivas, incluindo os riscos corporativos, os riscos departamentais e os fatores de risco associados, de forma a possibilitar a identificação das causas e exposições relevantes e sua adequada consolidação.

A avaliação deve considerar o risco inerente, previamente aos efeitos dos controles e demais medidas de tratamento, e o risco residual, considerando os controles e medidas aplicáveis, de modo a permitir avaliar a exposição remanescente e subsidiar sua comparação com os parâmetros estabelecidos na Declaração de Apetite por Riscos.

A avaliação deve considerar critérios de impacto e probabilidade, bem como outros critérios e perspectivas de análise definidos na Metodologia, conforme a natureza, relevância, complexidade e exposição ao risco, de modo a permitir sua classificação, priorização, tratamento e monitoramento.

7.2. APETITE E TOLERÂNCIA POR RISCO

A Companhia estabelece parâmetros de apetite, tolerância e limites de exposição aos riscos, considerando seus objetivos estratégicos, modelo de negócio, natureza e complexidade de suas operações e serviços, adotando abordagem compatível com seu perfil de atuação e com a relevância de suas atividades como IOSMF, bem como com a necessidade de preservar a segurança, a conformidade, a continuidade e a resiliência de suas atividades.

Os parâmetros de apetite, tolerância e limite de exposição são estabelecidos para cada Risco Corporativo na Declaração de Apetite por Riscos da Companhia, observadas as respectivas alçadas de aprovação. A avaliação do enquadramento considera o risco residual consolidado de cada Risco Corporativo, apurado conforme os critérios definidos na Metodologia de Gestão de Riscos e Controles Internos, preservada a rastreabilidade das exposições associadas aos Riscos Departamentais.

As exposições aos riscos devem ser monitoradas em relação aos parâmetros de apetite, tolerância e limite estabelecidos, de modo a permitir a identificação tempestiva de desvios, a avaliação de sua evolução e a adoção das medidas de tratamento, acompanhamento e escalonamento aplicáveis, conforme a Declaração de Apetite por Riscos.

7.3. ASSUNÇÃO DE RISCOS

O processo de assunção de riscos pela Companhia deve ocorrer de forma criteriosa, fundamentada e documentada, em conformidade com os parâmetros estabelecidos na Declaração de Apetite por Riscos, observadas as respectivas competências e alçadas de decisão.

A permanência temporária de exposições acima do apetite e dentro da tolerância máxima dependerá de justificativa formal da 1ª Linha, avaliação técnica da GRCI, definição de plano de tratamento, prazo determinado e medidas de monitoramento reforçado, bem como aprovação pela Diretoria Estatutária, conforme as condições previstas na Declaração de Apetite por Riscos.

As exposições que ultrapassarem o limite estabelecido deverão ser objeto de tratamento prioritário e escalonamento às instâncias competentes. A eventual assunção ou manutenção excepcional dessas exposições dependerá de apreciação e recomendação

do Comitê de Auditoria e deliberação do Conselho de Administração, observadas as restrições legais e regulatórias aplicáveis.

A 1ª Linha é responsável pela gestão dos riscos sob sua responsabilidade, incluindo a proposição da assunção de riscos, quando aplicável, sua fundamentação e o acompanhamento das respectivas exposições. A aprovação da assunção de risco pela instância competente não transfere a responsabilidade da 1ª Linha por sua gestão, devendo o risco assumido permanecer monitorado e ser reavaliado quando ocorrerem alterações relevantes nas condições que fundamentaram sua assunção.

O GRCI, no exercício das atribuições da 2ª Linha, acompanha as exposições decorrentes das assunções de riscos, realizando o acompanhamento independente da gestão realizada pela 1ª Linha e o reporte às instâncias competentes, observados os parâmetros estabelecidos na Declaração de Apetite por Riscos.

Quando identificar exposição que requeira decisão formal de assunção e esta não tenha sido tempestivamente submetida pela 1ª Linha, o GRCI poderá promover seu escalonamento às instâncias competentes, independentemente de provocação da área gestora, sem prejuízo da responsabilidade da 1ª Linha pela gestão do risco.

7.4. RELATÓRIOS PERIÓDICOS

A Companhia mantém um processo estruturado de reporte periódico às instâncias de governança, com o objetivo de contribuir para o acompanhamento da gestão de riscos e controles internos. Esses relatórios fornecem uma visão consolidada e estratégica do perfil de riscos corporativos, permitindo que as instâncias de governança competentes, quais sejam, a Diretoria Estatutária, o Comitê de Auditoria e o Conselho de Administração, acompanhem a evolução dos principais temas, as exposições relevantes e a efetividade das medidas de tratamento, subsidiando a tomada de decisão com informações qualificadas e tempestivas.

O conteúdo dos relatórios contempla uma visão abrangente das atividades e processos de gestão de riscos, incluindo a identificação e avaliação dos riscos inerentes e residuais, o acompanhamento dos planos de ação e demais medidas de tratamento, a avaliação de efetividade dos controles internos, os indicadores de risco e, conforme aplicável, o enquadramento das exposições residuais consolidadas dos Riscos Corporativos em relação aos parâmetros de apetite, tolerância e limite estabelecidos na Declaração de

Apetite por Riscos, preservada a visibilidade das exposições departamentais relevantes e das respectivas medidas de tratamento.

As informações reportadas pelo GRCI consideram, conforme aplicável, as informações fornecidas pelas áreas responsáveis e os resultados das atividades de monitoramento e avaliação realizadas pela 2ª Linha.

Além disso, os relatórios periódicos podem contemplar, conforme aplicável, informações relevantes relacionadas a mudanças regulatórias, eventos, tendências, situações de mercado, estudos ou análises específicas que possam impactar ou contribuir para a avaliação do perfil de riscos da Companhia. Os reportes podem contemplar, ainda, outros temas relevantes para o perfil de riscos da Companhia, incluindo segurança da informação, continuidade de negócios, recuperação de desastres e saída ordenada, conforme aplicável.

8. TREINAMENTO E ACULTURAMENTO

O GRCI, em parceria com os demais departamentos e com o Departamento de Recursos Humanos, promove e participa de ações de treinamento e aculturamento relacionados à gestão de riscos e controles internos, observando as responsabilidades de cada área. Essas ações têm como objetivo disseminar boas práticas, ampliar o conhecimento sobre gestão de riscos e controles internos e fortalecer a cultura de riscos, controles e conformidade entre os colaboradores.

Também podem ser realizadas ações de conscientização sobre temas relevantes para a Companhia, por meio de treinamentos, eventos, comunicações e outros instrumentos de disseminação de conhecimento e fortalecimento da cultura de riscos, controles internos e conformidade.

A 1ª Linha contribui para o processo de aculturamento, promovendo a aplicação das diretrizes de gestão de riscos e controles internos nos processos e atividades sob sua responsabilidade, bem como participando e promovendo a participação de suas equipes nas ações de treinamento e conscientização aplicáveis, especialmente naquelas de caráter obrigatório.

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 CONTROLE DE VERSÃO, revogando e substituindo o documento de data imediatamente anterior.

O presente documento permanecerá vigente até sua revogação ou substituição.

9.2. REVISÃO

Este documento deverá ser revisado, no mínimo, anualmente, considerando a data mais recente do quadro CONTROLE DE VERSÃO, 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.