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

1. OBJETIVO

Estabelecer objetivos, diretrizes, princípios, e responsabilidades relacionada a gestão de riscos e controles internos para promover o fortalecimento e o funcionamento do Sistema de 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. ESTRUTURA DA GESTÃO DE RISCOS E CONTROLES INTERNOS NA CSD BR

A estrutura de Gestão de Riscos e Controles Internos da CSD BR foi organizada de acordo com o modelo de negócio, natureza das operações e complexidade dos produtos, serviços oferecidos, e permite à Administração monitorar os processos de negócio, operacionais e financeiros, assim como os riscos de não conformidade e de descontinuidade.

A Diretoria de Governança, Riscos e Controles Internos ("GRC") atua de forma independente dentro da estrutura organizacional, com competência, recursos suficientes e acesso irrestrito a todas as informações, pessoas e locais, para o cumprimento de suas responsabilidades.

2.1 PAPÉIS E RESPONSABILIDADES

A CSD BR atua de acordo com o modelo de linhas, como um meio de esclarecer os papéis e responsabilidades essenciais para a gestão de riscos e controles, conforme descrito abaixo:

1ª Linha – Gestores das Áreas Operacionais - responsáveis pela gestão diária de processos e riscos, bem como pela definição de ações de mitigação de tais riscos, assegurando a conformidade das operações e estratégias de seus processos.

2ª Linha - Diretoria de Governança, Riscos e Controles Internos ("GRC") - responsável por monitorar a implementação de práticas eficazes pela 1ª Linha e auxiliar a referida linha no desenvolvimento de seus processos e controles.

3ª Linha - Diretoria de Fiscalização e Supervisão ("DFS"), Auditoria Interna e Auditoria Independente - responsáveis por fornecer à alta administração avaliações independentes quanto à eficiência e eficácia dos processos, metodologia de gestão de riscos e eficácia dos controles.

4ª Linha - Comitê de Fiscalização e Supervisão ("CFS") e Conselho de Administração ("CA") - responsáveis por fiscalizar a efetividade e suficiência da estrutura de gestão de riscos inerentes às atividades da Companhia.

Todas as linhas trabalham coletivamente para a criação e proteção de valor com um processo efetivo de comunicação, cooperação e colaboração entre todos os envolvidos.

3. A GESTÃO DE RISCOS E CONTROLES INTERNOS DA CSD BR

O objetivo da Gestão de Riscos e Controles Internos da CSD BR é gerenciar os riscos de forma que os objetivos estratégicos não venham a ser prejudicados. Dessa forma, visa assegurar que os riscos inerentes às atividades sejam reconhecidos e administrados adequadamente, atuando de forma a evitar que os prejuízos financeiros, reputacionais e os impactos negativos à imagem institucional da Companhia atinjam níveis inaceitáveis.

A CSD BR atua de acordo com o princípio da melhoria contínua e determina que o processo de Gestão de Riscos e Controles Internos deve ser sempre revisado e otimizado, com o objetivo de alcançar os melhores resultados.

Os processos que permeiam as etapas da metodologia de Gestão de Riscos e Controles Internos da CSD BR são: identificação, análise, avaliação, tratamento, monitoração, reporte e aculturamento. A metodologia é aplicada por meio das seguintes etapas:

3.1 ENTENDIMENTO, ATUALIZAÇÃO OU ESTRUTURAÇÃO DO PROCESSO

Ao iniciar um trabalho, a equipe de Gestão de Riscos e Controles Internos realiza o entendimento do processo que deve ser apresentado de forma detalhada pelas áreas responsáveis (1ª Linha).

Caso o processo já esteja descrito e desenhado, é realizado o entendimento e se necessário, a sua atualização (fluxograma, se necessário e descritivo em word). Nesta

etapa, é possível identificar e avaliar os controles existentes, definir novos ou melhorar os existentes. As necessidades de melhorias e novas implantações de controles são definidas como planos de ação e são acompanhadas pela equipe de Gestão de Riscos e Controles Internos.

3.2 ACOMPANHAMENTO DA IMPLANTAÇÃO DO PROCESSO

A equipe de Gestão de Riscos e Controles Internos acompanha junto à área responsável (1ª Linha) a implantação do processo para assegurar que a execução seja realizada conforme o definido.

3.3 AVALIAÇÃO DE RISCOS E CONTROLES "MATRIZ DE RISCOS"

A CSD BR utiliza a metodologia RCSA – *Risk and Control Self Assessment*, onde a identificação e avaliação de riscos e controles internos são realizadas por meio de reuniões e entrevistas com os gestores e colaboradores que executam os processos. O resultado dos trabalhos é apresentado à Diretoria e ao CFS que avaliam e aprovam o conteúdo.

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: *Committee of Sponsoring Organizations of the Tradeway Commission ("COSO"), ABNT NBR ISO 31.000:2009, ABNT NBR ISO 31010:2012, Principles for Financial Market Infrastructures – PFMI, Control Objectives for Information and Related Technologies ("COBIT"), National Institute of Standards and Technology ("NIST"), ABNT NBR ISO 27.001: 2005 / ABNT NBR ISO 27.002:2013*.

A CSD BR utiliza ferramenta específica de Gerenciamento de Riscos para documentar o resultado dos trabalhos realizados. As informações são geridas de forma dinâmica, monitoradas e atualizadas continuamente.

3.3.1 Critérios para Avaliação de Riscos e Controles

A avaliação de riscos constitui-se em uma necessidade fundamental para o processo decisório, porque viabiliza condições de se identificar o grau de severidade das perdas inerentes aos riscos aos quais a Companhia se expõe e, então, de estabelecer prioridades na sua gestão.

A avaliação de riscos na CSD BR é realizada de forma qualitativa, onde a experiência e as boas práticas, permitem:

- reduzir a dependência de dados históricos nem sempre disponíveis; e
- atribuir a devida importância à senioridade e à experiência das pessoas na avaliação de riscos.

A avaliação qualitativa é estabelecida por meio dos parâmetros de impacto e frequência e de acordo com o dicionário de riscos da Companhia, que considera os riscos: estratégicos, imagem, financeiros, operacionais, legais e de terceirização.

A avaliação dos controles deve ser definida pela percepção das entrevistas com os gestores das áreas de negócios, quanto a sua descrição, características, maturidade e poder de reduzir o impacto e frequência do risco identificado, medindo grau de efetividade e controle.

O controle interno é uma resposta ao fator de risco. Seu objetivo é reduzir a possibilidade de materialização do evento, trazendo o risco original para o risco residual, alinhado ao apetite a risco da Companhia.

Com a finalização da avaliação de controles identificamos o risco residual. Os pontos de impacto e frequência do risco são reposicionados após avaliação dos controles.

Os planos de ação resultantes da avaliação são acompanhados pela área de Gestão de Riscos e Controles Internos.

Após a identificação do risco residual, com a avaliação do risco e do controle, deve ser definido o tratamento a ser dado ao risco, ou seja, deve ser definida a resposta ao risco, que são medidas para alinhar os riscos com o apetite e a tolerância a eles. A resposta ao risco deve ser classificada de acordo com as seguintes categorias: Evitar, Mitigar, Compartilhar e Aceitar.

O tratamento aos riscos dar-se-á pela aplicação de controles internos, cuja existência ou necessidade deverá ser identificada pela 1ª e 2ª Linhas, e em cada circunstância, devem instituir novos controles internos, a partir da ponderação da relação entre os esforços de implementação e os benefícios estimados. Essas ações devem ser monitoradas e fiscalizadas pela 3ª Linha.

3.4 CERTIFICAÇÃO DE CONTROLES / TESTES DE CONTROLE

A Certificação de Controles é realizada através de procedimento de teste de eficiência e eficácia visando entender se o controle e suas características são suficientes para manter o risco em níveis aceitáveis, dentro do apetite de risco. Os testes objetivam fornecer evidências sobre a efetividade operacional dos controles na prevenção e/ou detecção de irregularidades e/ou distorções relevantes.

3.5 REPORTE DE RESULTADOS

Os resultados dos trabalhos devem ser alinhados com o Diretores responsáveis pelos assuntos avaliados e pela GRC e deve ser levado para conhecimento e aprovação do CFS e CA.

Anualmente a GRC emite relatório de avaliação sobre o funcionamento e a eficácia do gerenciamento de riscos e de controles internos, contendo as recomendações quanto às eventuais deficiências identificadas.

O relatório visa atender, como melhor prática, o disposto na Resolução CMN nº 4.968/2021, que dispõe sobre os sistemas de controles internos das instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil, respectivamente, bem como o disposto na Resolução CVM nº 135/2022, que dispõe sobre o funcionamento dos mercados regulamentados de valores mobiliários; a constituição, organização, funcionamento e extinção das entidades administradoras de mercado organizado.

Toda documentação relacionada à Gestão de Riscos e Controles Internos, é arquivada em diretório e ferramenta específica, utilizada como repositório de informações. Estas informações são mantidas por, no mínimo, 5 (cinco) anos, e ficam à disposição dos órgãos reguladores.

3.6 MONITORAMENTO, INFORMAÇÃO E ACULTURAMENTO

3.6.1 Monitoramento

O processo de gestão de riscos e controles internos deve ser continuamente aprimorado e alinhado ao planejamento estratégico e à identidade da Companhia.

O planejamento de trabalho da equipe de Gestão de Riscos e Controles Internos é definido anualmente. Já, a avaliação de riscos e controles da Matriz de Riscos Geral da CSD BR é realizada no mínimo anualmente.

Os planos de ação definidos ao longo do trabalho de gestão de riscos e controles internos, bem como os planos de ação definidos para o trabalho executado pela Auditoria Interna, são monitorados e avaliados pela equipe de Gestão de Riscos e Controles Internos.

3.6.2 Informação

As atividades e resultados da gestão de riscos devem ser alinhados e reportados às partes interessadas, incluindo aquelas com responsabilidade e com responsabilização pelos planos de ação identificados e avaliação contínua de seus riscos como 1ª Linha.

Todo o processo de gestão de riscos e seus resultados devem ser formalizados através de mecanismos apropriados, alinhados e reportados, com o objetivo de fornecer informações para a tomada de decisão, e também proporcionar a melhoria contínua da gestão de riscos e controles internos.

3.6.3 Aculturamento

A GRC, em parceria com as demais áreas, é responsável por disseminar, a toda a Companhia, a cultura, realizar treinamentos e participar da comunicação sobre os eventuais riscos que terceiros possam representar no âmbito de seus negócios.

Também são realizadas ações de conscientização sobre temas relevantes para a Companhia, por meio de participação no Conversando (evento mensal promovido pelo Departamento de Recursos Humanos) e por meio do GRC em Pauta (newsletter).

4. CONTROLE DO DOCUMENTO

4.1 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.

4.2 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.

4.3 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.

5. ANEXO 1

5.1 REFERÊNCIAS – FRAMEWORKS DE MERCADO

- *Committee of Sponsoring Organizations of the Tradeway Commission* (“COSO”)
- *Principles for Financial Market Infrastructures - PFMI*
- *Guidance on Cyber Resilience for Financial Market Infrastructures (CPMI-IOSCO)*
- *Control Objectives for Information and Related Technologies* (“*COBIT*”)
- *National Institute of Standards and Technology (“NIST”)*
- *Information Technology Infrastructure Library (“ITIL”)*
- ABNT NBR ISO 27.001: 2005 / ABNT NBR ISO 27.002:2013
- ABNT NBR ISO 31.000:2009
- ABNT NBR ISO 31010:2012

5.2 REFERÊNCIA REGULATÓRIA - BCB

- Resolução BCB nº 304, de 20 de março de 2023

5.3 REFERÊNCIA REGULATÓRIA - CVM

- Resolução CVM nº 135, de 10 de junho de 2022

5.4 REFERÊNCIAS REGULATÓRIAS – SUSEP

- Circular Susep nº 249/2004
- Resolução CNSP nº 416, de 20 de julho de 2021
- Circular Susep nº 521, de 24 de novembro de 2015
- Circular Susep nº 638, de 27 de julho de 2021
- Circular SUSEP nº 619, de 04 de dezembro de 2020