POLÍTICA DE GERENCIAMENTO DE RISCOS E CONTROLES INTERNOS DA SANEPAR

Ano - 2024

1. DISPOSIÇÕES GERAIS

Revisada na 12ª Reunião Extraordinária do Conselho de Administração - CA, realizada no dia 19 de dezembro de 2024 (Versão 6).

2. INTRODUÇÃO

A Sanepar reforça seu compromisso com uma cultura de integridade por meio da implementação de diretrizes claras de governança e de um processo integrado de gerenciamento de riscos e controles internos. O objetivo é garantir que os riscos sejam avaliados de maneira eficaz e utilizados como instrumentos para a tomada de decisões pelos órgãos de governança. Isso permite que a Sanepar compreenda os cenários nos quais opera e o impacto gerado para as partes interessadas, buscando sempre atingir suas metas estratégicas. A empresa continua a se aprimorar e a adotar práticas de boa governança, focando na sustentabilidade social, financeira e ambiental, com o propósito de gerar e preservar valor ao longo do tempo.

3. OBJETIVOS

Incorporar a visão e a prática de gerenciamento de riscos e controles internos à tomada de decisões da Sanepar. Estabelecendo princípios, diretrizes, regras, responsabilidades e conceitos, de forma a possibilitar a identificação, avaliação, tratamento, monitoramento e comunicação dos riscos e dos controles internos nos processos da Companhia.

4. ABRANGÊNCIA

Esta Política é fomentada e orientada pela Administração da Companhia e aplica-se a todos os empregados, gestores, agentes de governança, terceiros, instituições parceiras e a todas as partes relacionadas à Sanepar.

5. REFERÊNCIAS

BRASIL. Presidência da República. Lei nº 13.303, de 30 de junho de 2016, dispõe sobre o estatuto jurídico da empresa pública, da sociedade de economia mista e de suas subsidiárias, no âmbito da União, dos Estados, do Distrito Federal e dos Municípios. Brasília DOU de 1º.7.2016.

BRASIL. CVM. Resolução Comissão de Valores Mobiliários 80 de 02 de maio de 2022.

COSO. Committee of Sponsoring Organizations of the Treadway Commission. Internal Control – Integrated Framework. New York: AICPA, 1992.

COSO. Committee of Sponsoring Organizations of the Treadway Commission – Internal Control - Integrated Framework. 2013.

Guide to the CICS Common Body of Knowledge (CBOK). Internal Control Institute, Edition III, v.1. 2017.

IIA. The IIA Research Foundation. IIA DOCUMENTO DE EXPOSIÇÃO Três Linhas de Defesa, 2019. Disponível no site > https: //global.theiia.org/translations/PublicDocuments /3LOD-IIA-Exposure-Document-Portuguese.pdf> Acesso em 23 de julho de 2020.

6. DEFINIÇÕES

Os principais termos citados nesta política corporativa incluem:

i. **1ª linha**: nível de atuação que lidera e dirige ações (incluindo gerenciamento de riscos) e a aplicação de recursos para atingir os objetivos da organização;

ii. **2ª linha:** são as diversas funções corporativas que buscam fornecer expertise, apoio, monitoramento e questionamento quanto ao gerenciamento de riscos;

iii. **3ª linha:** presta avaliação e assessoria independentes e objetivas à gestão e ao órgão de governança sobre a adequação e eficácia da governança e do gerenciamento de riscos para apoiar o atingimento dos objetivos organizacionais e promover e facilitar a melhoria contínua;

iv. **Ação mitigatória**: medida adotada pela Companhia que proporciona uma redução da sua exposição ao risco e que busca atenuar a possibilidade de materialização do risco;

v. **Apetite a Risco:** nível máximo de exposição de impacto dos riscos para o acionamento da governança de riscos;

vi. **Avaliação dos sistemas de controles internos**: avaliação do processo de negócio que permite identificar os riscos e os controles internos necessários para mitigá-los;

vii. **Controle Interno**: é um processo conduzido pela estrutura de governança, administração e outros profissionais da organização, e desenvolvido para proporcionar segurança razoável com respeito à realização dos objetivos relacionados às operações, divulgação e conformidade;

viii. **COSO:** (Committee of Sponsoring Organizations of the Treadway Commission / Comitê das Organizações Patrocinadoras): instituição privada, sem fins lucrativos, que visa prover documentos e/ou relatórios financeiros com o maior nível de veracidade possível, utilizando, para isto, princípios como ética organizacional, transparência, controles internos, gerenciamento de riscos e governança corporativa. Este Comitê estabeleceu as metodologias denominadas COSO ERM (Enterprise Risk Management/ Gestão de Riscos Corporativos), referência de mercado no tema e COSO IF (Controles Internos/Integrated Framework);

ix. **Custo-Benefício:** Consiste na redução do risco de falhas quanto ao cumprimento dos objetivos e metas de uma atividade, porém dentro do conceito de que o custo não deve exceder os benefícios proporcionados;

x. **Dono do Risco**: diretor executivo da Companhia, o qual terá o papel de monitorar e tratar os riscos corporativos que lhe forem designados;

xi. **Facilitador de Riscos:** profissionais nomeados pelos Donos dos Riscos para assessorá-los em suas atribuições e atividades referente aos riscos corporativos;

xii. **Fator de Risco:** qualquer condição que, combinada ou individualmente, possa potencializar a probabilidade de materialização do risco;

xiii. **Focal da diretoria:** profissionais designados pelos seus diretores, para atuar na execução da avaliação dos sistemas de controles internos dos processos de sua diretoria;

xiv. **Focal do processo:** empregados designados pelos seus gerentes para dar suporte as atividades de controles internos dos processos;

xv. **Impacto do risco:** avaliação qualitativa e/ou quantitativa do efeito da materialização do risco na Companhia;

xvi. **Indicador de risco:** métrica utilizada para monitorar e analisar a variação dos riscos corporativos mapeados a partir de dados obtidos no ambiente interno e externo à Companhia;

xvii. **Materialização do risco:** ocorre quando o risco, objeto ou não de controle e tratamento, se materializa em um evento ou fato, impactando os objetivos, a sequência, viabilidade, perenidade ou sustentabilidade dos negócios da Companhia.

xviii. **Matriz de riscos:** representação gráfica da exposição dos riscos corporativos identificados pela Sanepar de acordo com a criticidade de cada risco, que é estabelecida pela avaliação de seu impacto versus sua probabilidade;

xix. **Perfil de risco:** disposição da Companhia para incorrer em riscos. Exemplos de perfis de risco: conservador, moderado e agressivo;

xx. **Plano de trabalho integrado de gerenciamento de riscos**: documento elaborado pela área de gerenciamento de riscos e controles internos contendo o planejamento periódico das atividades a serem executadas, reportadas e apresentadas, prazos, recursos necessários e responsáveis;

xxi. **Portfólio de riscos:** catálogo de apresentação das características e informações de cada risco, sendo elas: descrição do risco e de seu (s) fatore (s), criticidade do risco bruto e do residual, ações mitigatórias existentes, resposta (s) ao risco e planos de ação e de contingências, se aplicável;

xxii. **PPI:** Plano Plurianual de Investimentos;

xxiii. **Resposta ao risco:** definição do tratamento que a Companhia dará ao risco residual. Como resposta, pode-se optar por evitar, reduzir, compartilhar ou aceitar o risco;

xxiv. **Risco:** é a incerteza sobre a possibilidade de perdas ou ganhos relacionados ao rumo dos acontecimentos relativos aos objetivos estratégicos da Companhia;

xxv. **Risco corporativo**: risco que possa interromper o alcance dos objetivos e a execução da estratégia planejada;

xxvi. **Risco bruto**: é a probabilidade e o impacto de um evento de risco antes de implementada qualquer medida de controle;

xxvii. **Risco residual**: risco que permanece após a adoção de medidas para a mitigação das avaliações da probabilidade e o impacto da materialização dos riscos bruto;

xxviii. **Segregação de funções:** vedação à designação da mesma pessoa para atuação simultânea em funções mais suscetíveis a riscos, de modo a reduzir a possibilidade de ocultação de erros e de ocorrência de fraudes nos respectivos processos;

xxix. **Tolerância a risco:** percentual do apetite a risco definido pela Companhia que, quando atingido, aciona a governança para a gestão dos riscos;

7. REVISÃO

A política deve ser revisada bienalmente, a qualquer tempo sob demanda regulatória ou de mercado ou quando demandado pelo Comitê de Gerenciamento de Riscos, pela Diretoria Executiva, pelo Comitê de Auditoria Estatutário ou pelo Conselho de Administração.

As alterações realizadas neste documento devem ser encaminhadas para aprovação dos órgãos de governança citados acima.

8. DIRETRIZES

I. Disseminar, no âmbito do Programa de Integridade, a necessidade do gerenciamento de riscos e controles internos entre os empregados

para a internalização dessa cultura durante o desenvolvimento e realização das atividades e rotinas dos processos da Companhia;

II. Adotar regras de estruturas e mecanismos que abranjam a ação dos administradores e empregados, por meio da implementação cotidiana de práticas de controle interno, consoante o que estabelece o artigo 9º, Inciso I da Lei 13.303/2016;

III. Garantir que a área responsável pela verificação de cumprimento de obrigações e de gestão de riscos e controles internos corporativos (2ª linha), esteja consoante com o que estabelece o parágrafo 2º, artigo 9º da Lei 13.303/2016;

IV. Assegurar o cumprimento das normas e regulamentos e aderência às políticas e procedimentos internos;

V. Estabelecer os controles internos aos riscos, objetivos e planejamento estratégicos da Companhia;

VI. Garantir a aplicação do princípio da segregação de funções de forma que seja evitada a ocorrência de conflitos de interesses e fraudes;

VII. Apresentar o reporte aos agentes de governança por meio de relatórios periódicos de análise crítica e monitoramento de riscos e controles da Companhia;

VIII. Adotar a abordagem por linhas, que contempla a atuação integrada entre: (a) gestão dos processos, (b) controles internos, gestão de riscos e Compliance e (c) a Auditoria Interna;

IX. Garantir que na 1ª linha, a gestão dos processos seja responsável por implementar ações que assegurem a conformidade de seus processos e o adequado gerenciamento dos riscos e respectivos controles;

X. Garantir que a 2ª linha auxilie e monitore a primeira linha, no cumprimento de suas responsabilidades em conduzir a gestão com eficiência para o gerenciamento dos riscos, controles internos e conformidade dos seus processos;

XI. Garantir que a 3ª terceira linha forneça aos órgãos de governança, avaliações sobre a eficácia dos processos frente ao gerenciamento de riscos e controles internos;

XII. Fomentar que o gerenciamento de riscos se faça presente em todos os processos de gestão, planejamento, Controles Internos e Auditoria

Interna, promovendo a identificação antecipada dos riscos e a gestão tempestiva dos mesmos;

XIII. Garantir que os riscos identificados sejam analisados, classificados, priorizados e suas respostas definidas;

XIV. Garantir que a melhoria contínua do processo de gerenciamento de riscos e controles internos seja promovida por meio de ciclos de avaliações e revisões, de modo a assegurar a eficácia do gerenciamento e do monitoramento dos riscos; e

XV. Assegurar que todas as áreas gestoras dos processos forneçam todas as informações necessárias, tempestivamente, para o desenvolvimento dos trabalhos realizados pela área de Gestão de Riscos e Compliance.

9. PROCESSO DE GERENCIAMENTO DE RISCOS

As atividades de gerenciamento de riscos terão como referência as boas práticas de Governança Corporativa estabelecidas pelos padrões e metodologia do Commite of Sponsoring Organization of Tradeway Commission – COSO e compõe o segundo pilar, Análise de Riscos e Ambiente de Controle, do Programa de Integridade da Sanepar.

O Processo de gerenciamento de Riscos é conduzido para garantir, com razoável certeza, que os objetivos da Companhia sejam atingidos nos aspectos estratégicos e operacionais:

I. Na identificação e mapeamento dos riscos corporativos que possam impactar o atingimento dos objetivos estratégicos da Companhia. O ponto de partida é o planejamento estratégico que subsidia a captura desses riscos para permitir a avaliação de suas criticidades (impacto e probabilidade), a identificação de ações mitigatórias já existentes, controles internos, definição de novas ações de tratamento, monitoramento e reporte;

II. As informações acima devem ser registradas em um portfólio de riscos, revisados anualmente, considerando o rumo dos

acontecimentos relacionados aos objetivos estratégicos e a mudança no agravamento do impacto ou probabilidade dos riscos;

III. O monitoramento contínuo dos riscos corporativos priorizados utiliza-se de indicadores, os quais devem ser avaliados mensalmente pelo Comitê de Gerenciamento de Riscos, trimestralmente pela Diretoria Executiva, Comitê de Auditoria Estatutário e Conselho de Administração, ou a qualquer momento em casos relevantes; e

IV. Promover o mapeamento dos processos e avaliação dos sistemas de controles internos, mediante a elaboração de fluxogramas, matrizes de riscos, de controles internos, teste de controles, entregando planos de tratamento para mitigar, com razoável certeza, os riscos e melhorar a eficiência dos processos.

V. O monitoramento contínuo dos riscos não priorizados utiliza-se de indicadores, os quais devem ser avaliados conforme periodicidade definida pelo Conselho de Administração, ou a qualquer momento em casos relevantes.

9.1. Limites de exposição

A Companhia considera os limites de exposição (apetite e tolerância) aos riscos estabelecidos dentro do perfil conservador[1], sendo eles estabelecidos de acordo com a natureza de cada risco.

9.1.1. Riscos natureza corporativa

a) O apetite a este tipo de risco é mensurado em valor financeiro e representa o impacto máximo, no horizonte de um ano, que a Companhia está disposta a assumir para atingir seus objetivos;

[1] Perfil conservador, considerando (i) o tipo de Negócio, onde a Companhia possui Contratos com os municípios, em conformidade com o publicado no 2tri/2022 75% da receita são de contratos com vencimento posterior a 2033; (ii) Perfil da Dívida com baixa alavancagem dentro das métricas dos covenants; (iii) Contratação de operação de proteção (hedge) à exposição cambial; (iv) Possui Política de Gestão de Risco, Tesouraria e Mercado.

[1] Riscos de natureza financeira são tratados na Política de Gestão de Risco, Tesouraria e Mercado, disponível no Portal de Relações com Investidores da Sanepar.

b) O apetite deve ser calculado de acordo com metodologia estabelecida, composta por 2(duas) abordagens: a quantitativa, na qual calcula-se o desvio aceito decorrente da materialização de riscos e a qualitativa, na qual é feita a ponderação do valor definido na primeira abordagem por meio da análise da Companhia sob as óticas de variação de indicadores relevantes, da estrutura de capital, do ambiente de controle, da reputação e Compliance;
c) A tolerância é um percentual do apetite a risco estabelecido que, quando atingido, aciona a Governança para a gestão dos riscos;
d) O apetite bem como a tolerância, devem ser atualizados anualmente, ou quando da ocorrência de fatos relevantes; e
e) Caso a somatória dos impactos financeiros estimados para os riscos corporativos priorizados ultrapasse a tolerância definida, a Governança deve ser acionada para reavaliar o plano de mitigação existente.

9.1.2. Riscos de natureza operacional

a) O apetite a riscos de natureza operacional é estabelecido com base na criticidade dos riscos identificados na avaliação do sistema de controles internos dos processos;
b) Para os riscos avaliados como “Significativo” e “Crítico”, deve-se obrigatoriamente estabelecer planos de tratamento para mitigar a probabilidade e impacto de materialização;
c) Para os riscos avaliados como “Moderados”, é recomendável a elaboração de planos de tratamento e monitoramento das ações e controles existentes para conservação ou redução deste nível;
d) Para os riscos avaliados como “Baixos” deve-se manter e monitorar as ações e controles existentes para conservação deste nível; e
e) Para os riscos de Compliance identificados na avaliação dos processos, deverão ter planos de ações definidos, independentemente de sua criticidade, a fim de mitigá-los. Demais exceções, devem ser discutidas pela Diretoria Executiva e aprovadas pelo Conselho de Administração.

10. ESTRUTURA

a) A área responsável pela verificação de cumprimento de obrigações e de gerenciamento de riscos e controles internos corporativos (2ª linha), deve ser vinculada ao diretor presidente e liderada por diretor estatutário, devendo o Regimento Interno da Diretoria Executiva definir as atribuições da área, bem como estabelecer estruturas e mecanismos que assegurem atuação independente, consoante o que estabelece o parágrafo 2º, artigo 9º da Lei 13.303/2016.
b) A Diretoria Adjunta de Governança, Riscos e Compliance é responsável pela garantia de aplicação dessa política. Para tanto, os gestores dos processos impactados pelos riscos, devem prestar todas as informações necessárias, tempestivamente, para o desenvolvimento dos trabalhos realizados.
c) O orçamento e a estrutura dos processos de Gerenciamento de Riscos e Controles Internos devem ser avaliados pela Auditoria Interna, a fim de atestar se estão adequados às atividades e ao porte da Companhia.

11. RESPONSABILIDADES

11.1. Conselho de Administração

a) Aprovar diretrizes para o processo integrado de gerenciamento de riscos e controles internos da Sanepar (metodologia, processos, sistemas, política, padrões e mecanismos de reporte, dentre outros);
b) Aprovar o apetite e tolerância a risco;
c) Aprovar os riscos corporativos priorizados e seus respectivos planos de resposta e contingência;
d) Avaliar periodicamente o portfólio dos riscos corporativos e suas ações mitigatórias;
e) Acompanhar os resultados dos processos de gerenciamento de riscos e de controles internos, por meio de relatórios executivos;
f) Avaliar e validar a estrutura de controles internos e gerenciamento de riscos estabelecida para garantir o tratamento dos riscos; e

g) Aprovar o plano de trabalho de gerenciamento de riscos e controles internos da DAGRC-Diretoria Adjunta de Governança, Riscos e Compliance.

11.2. Comitê de Auditoria Estatutário

a) Supervisionar os processos de gestão de riscos e controle interno, relatórios financeiros e contábeis, e auditorias independente e interna;
b) Assessorar o Conselho de Administração para a aprovação ou para a modificação dos riscos estratégicos e de seus respectivos planos de mitigação e contingência, bem como do apetite ao risco e da definição de diretrizes para o processo de gestão de riscos
c) Assessorar o Conselho de Administração na avaliação e monitoramento da matriz de riscos estratégicos da Companhia, com os riscos priorizados, seus respectivos planos de resposta e contingência;
d) Assessorar o CA para a aprovação e implementação do plano anual dos trabalhos de gestão de riscos, implementar e supervisionar os sistemas de gestão de riscos e de controle interno estabelecidos para a prevenção e mitigação dos principais riscos a que está exposta a Companhia, inclusive os riscos relacionados à integridade das informações contábeis e financeiras e os relacionados à ocorrência de corrupção e fraude;

11.3. Diretoria Executiva

a) Promover o processo de gerenciamento de riscos e de controles internos da Sanepar (metodologia, processos, sistemas, política, padrões e mecanismos de reporte, dentre outros) e garantir que estejam alinhados às boas práticas de gestão, inclusive ao planejamento estratégico da Companhia;
b) Assegurar a aplicação das diretrizes e a aderência ao gerenciamento de riscos e aos procedimentos de controles internos;
c) Deliberar sobre os procedimentos de gerenciamento de riscos e controles internos e suas atualizações;
d) Revisar e validar o valor do apetite e tolerância a risco;

e) Avaliar o plano de trabalho de gerenciamento de riscos e controles internos da DAGRC e encaminhá-lo para análise do CAE e aprovação do Conselho de Administração;
f) Revisar e aprovar o portfólio de riscos corporativos;
g) Acompanhar e gerir todos os riscos corporativos do portfólio;
h) Definir os donos dos riscos;
i) Avaliar os planos de ação sugeridos pelos donos dos riscos e aprovar eventuais postergações de prazos;
j) Encaminhar ao Conselho de Administração, para aprovação, os riscos corporativos priorizados e seus respectivos planos de ação e contingência;
k) Deliberar sobre os resultados dos processos de gerenciamento de riscos e de controles internos;
l) Indicar a necessidade de avaliações independentes do processo de gerenciamento de riscos e controles internos (agentes internos ou externos), de modo a assegurar sua eficácia;
m) Garantir o desenvolvimento contínuo dos profissionais atuantes em gerenciamento de riscos e controles internos da Companhia;
n) Assegurar autonomia aos agentes de controles internos da Sanepar no exercício de suas atividades, garantindo o acesso a documentos, sistemas de informação e pessoas, e demais elementos necessários ao exercício de suas atividades;
o) Assegurar o alinhamento entre o plano de negócio, planejamento estratégico e de investimentos e o Gerenciamento de Riscos e Controle Interno, visando o adequado tratamento dos riscos; e
p) Designar focais da diretoria, considerando a competência e o perfil adequados para o desempenho da atribuição.

11.4. Comitê de Gerenciamento de Riscos

a) Avaliar as variações de criticidade dos riscos e quando essas forem significativas, reportá-las à Diretoria Executiva, ao Comitê de Auditoria Estatutário e ao Conselho de Administração;

b) Analisar, propor e deliberar sobre diretrizes e estratégias dos processos de gerenciamento de riscos e controles internos;
c) Quando necessário, analisar e apresentar pontos de melhoria no processo de gerenciamento de riscos e controles internos (metodologia, processos, sistemas, política, padrões e mecanismos de reporte, dentre outros);
d) Subsidiar a Diretoria na definição do apetite e tolerância a risco;
e) Avaliar e recomendar para a diretoria executiva o plano de trabalho de gerenciamento de riscos;
f) Acompanhar mensalmente o resultado das ações mitigatórias e dos indicadores de riscos propostos para o tratamento dos riscos corporativos priorizados;
g) Acompanhar trimestralmente o resultado das avaliações dos sistemas de controles internos dos processos;
h) Avaliar e recomendar recursos necessários para a execução dos processos de gerenciamento de riscos e controles internos;
i) Zelar pelo cumprimento da Política de Gerenciamento de Riscos e Controles Internos;
j) Posicionar sobre as atividades do Comitê, quando demandado pela Diretoria Executiva, Comitê de Auditoria Estatutário e Conselho de Administração;
k) Analisar e recomendar sobre portfólio e planos de tratamento de riscos corporativos sempre que houver atualizações;
l) Analisar e propor priorização de riscos corporativos; e
m) Analisar e recomendar sobre planos de tratamento resultantes das avaliações dos sistemas dos controles internos dos processos.

11.5. Área de Gerenciamento de Riscos e Controles Internos

a) Propor e revisar diretrizes para os processos de Gerenciamento de Riscos e Controles Internos (metodologia, processos, sistemas, política, portfólio de riscos, padrões e mecanismos de reporte, dentre outros);
b) Disseminar conhecimentos sobre gestão de riscos e controles internos aos empregados, de modo a fortalecer essa cultura na Companhia;

c) Elaborar e revisar periodicamente o plano de trabalho de gerenciamento de riscos;
d) Coordenar e monitorar o processo de revisão do portfólio de riscos corporativos, bem como a avaliação dos sistemas de controles internos;
e) Atuar em conjunto com a Diretoria Executiva, Comitê de Auditoria Estatutário e Conselho de Administração, na discussão sobre a definição do apetite e tolerância a risco da Companhia;
f) Monitorar o alinhamento entre o Plano de Negócio, planejamento estratégico e de investimentos e o Gerenciamento de Riscos e Controle Interno, visando o adequado tratamento dos riscos;
g) Elaborar, revisar e atualizar o portfólio de riscos sempre que houver atualizações no Mapa Estratégico da Companhia ou quando eventos relevantes ocorrerem;
h) Auxiliar na definição dos donos dos riscos;
i) Auxiliar o dono e facilitador na definição dos indicadores de riscos, ações de tratamento e planos de contingências;
j) Acompanhar mudanças na criticidade dos riscos corporativos e reportá-las ao Comitê de Gerenciamento de Riscos e à Diretoria Executiva;
k) Elaborar relatórios com os resultados dos processos de gerenciamento de riscos e de controles internos;
l) Reportar mensalmente os resultados ao Comitê de Riscos e trimestralmente à Diretoria Executiva, Comitê de Auditoria Estatutário e Conselho de Administração;
m) Garantir o alinhamento entre os riscos operacionais e os corporativos;
n) Monitorar a realização dos planos de tratamento resultantes da avaliação dos sistemas de controles internos;
o) Auxiliar os gestores, focais e os agentes de controles internos no desenvolvimento dos trabalhos de avaliação dos sistemas de controles internos;
p) Assegurar que as recomendações relacionadas a riscos e controles internos, oriundas de Auditoria Interna, Auditoria Externa, Órgãos fiscalizadores e Controladores Externos, sejam incorporadas ao mapeamento dos processos e aos planos de tratamento.

11.6. Donos dos Riscos Corporativos

a) Indicar o facilitador do risco, considerando competência e perfil adequados para os papéis e para auxiliar nas garantias abaixo;
b) Garantir a elaboração das fichas de riscos e suas atualizações, sempre que necessário;
c) Desenvolver indicadores para monitorar a variação e os resultados do risco sob sua responsabilidade;
d) Assegurar a implantação de ações necessárias para a mitigação dos riscos, juntamente com o envolvimento de outras áreas;
e) Acompanhar o repasse mensal feito à área de Gerenciamento de Riscos dos dados e análises críticas necessárias, bem como a atualização do impacto financeiro, para as elaborações dos relatórios de riscos;
f) Informar à área de Gerenciamento de Riscos, eventuais mudanças significativas na probabilidade e/ou impacto do risco ou em qualquer outra característica e, caso identifique, riscos não mapeados;
g) Efetuar, quando demandados, reportes aos órgãos de governança sobre o desenvolvimento dos planos de ação para a mitigação dos riscos e dos planos de contingências;
h) Promover sistemática de debates e discussões desdobradas em seus fóruns de atuação e junto as suas gerências, de modo a assegurar a eficácia do gerenciamento e do monitoramento dos riscos;
i) Realizar a revisão técnica do risco, dos seus fatores, da criticidade do risco (impacto versus probabilidade) com apoio da área de gerenciamento de riscos, considerando alterações em ações mitigatórias existentes, conclusão dos planos de ação e de contingência; e
j) Identificar e definir as respostas aos riscos (evitar, mitigar, compartilhar ou aceitar).

11.7. Facilitadores de Riscos Corporativos

a) Apoiar o Dono do Risco em suas atribuições e atividades;

b) Fornecer informações ao Dono do Risco para revisão técnica do risco, dos seus fatores, da criticidade do risco (impacto versus probabilidade) e da resposta, considerando alterações em ações mitigatórias existentes e propostas e plano de contingência;
c) Elaborar reportes sistemáticos para que o Dono do Risco apresente à Área de Gerenciamento de Riscos e Controles Internos e ao Comitê de Gerenciamento de Riscos, o acompanhamento do risco sob sua responsabilidade;
d) Subsidiar o Dono do Risco, para reporte à área de Gerenciamento de Risco e Controles Internos, eventuais mudanças significativas na probabilidade e/ou impacto do risco ou em qualquer outra característica e, caso identifique, riscos não mapeados;
e) Participar, quando necessário, de reuniões promovidas pela área de Gerenciamento de Riscos e Controles Internos.
f) Atuar junto ao Dono do Risco, na implementação das ações necessárias para mitigação dos riscos, garantindo o envolvimento e as adequadas entregas das áreas intervenientes; e
g) Acompanhar e reportar ao Dono do Risco, para sua validação, os resultados e as análises críticas dos indicadores de riscos, das ações mitigatórias, bem como a atualização do impacto financeiro, conforme calendário pré-determinado pela área de Gerenciamento de Riscos e Controles interno.

11.8. Gestores de Processos

Atuar, em conjunto com os Donos do Riscos e/ou Facilitadores dos riscos corporativos, na implementação das ações necessárias para mitigação desses riscos, garantindo seu envolvimento e as adequadas entregas na condição de área interveniente;

a) Designar o focal do processo, considerando a competência e o perfil adequados para o desempenho da atribuição;
b) Dar suporte e condições para a execução da avaliação dos sistemas de controles internos referentes aos processos sob sua responsabilidade;

c) Validar as matrizes de riscos, controles internos e o plano de tratamento gerados na avaliação dos sistemas de controles internos;
d) Implementar planos de tratamento para mitigação dos riscos inseridos nos processos sob sua responsabilidade, sempre respeitando os níveis de competência e empregando medidas proporcionais ao risco, observando a relação custo-benefício de forma a agregar valor à Companhia; e
e) Comunicar área de gerenciamento de riscos e controles internos quando da alteração de legislação ou procedimentos, no processo em que está inserido, visando ação corporativa.

11.9. Focal da Diretoria

a) Atuar junto aos gestores e focais dos processos, mediante suporte da área de Gerenciamento de Riscos e Controles Internos, na execução do mapeamento e da avaliação dos sistemas de controles internos;
b) Alinhar as demandas estratégicas, pertinentes à sua diretoria, às atividades operacionais de controles internos na empresa, a partir do treinamento recebido sobre a metodologia a ser aplicada; e
c) Participar, quando necessário, de reuniões promovidas pela área de Gerenciamento de Riscos e Controles Internos.

11.10. Focal do Processo

a) Apoiar o gestor do processo em suas atribuições e responsabilidades, reportando fatos relevantes referente as atividades de controles internos;
b) Implantar ou atualizar os controles internos e documentos normativos (inclusive fluxograma), quando da alteração de legislação ou procedimentos, no processo em que está inserido, mitigando os riscos e garantindo o Compliance;
c) Alinhar as demandas, pertinentes ao seu processo, às atividades operacionais de controles internos na empresa, a partir do treinamento recebido sobre a metodologia a ser aplicada;

d) Acompanhar e reportar ao gestor, para sua validação, os resultados e as análises críticas para subsidiar o monitoramento dos planos de ações de controles internos; e

e) Participar, quando necessário, de reuniões promovidas pela área de Gerenciamento de Riscos e Controles Internos.

12. RESPONSABILIZAÇÕES

A não aderência às responsabilidades dispostas na presente Política deve ser examinada pela área de Gerenciamento de Riscos e Controles Internos e encaminhadas para avaliação do Comitê de Gerenciamento de Risco, o qual submeterá à Diretoria Executiva para as providências a serem adotadas para fins de apuração de eventuais responsabilidades de acordo com o Regulamento Disciplinar.

13. DISPOSIÇÕES FINAIS

Esta Política entra em vigor na data de sua aprovação final pelo Conselho de Administração.

14. HISTÓRICO

Política de Gerenciamento de Riscos e de Controles Internos		**Versão**	6ª	
Área Gestora		Gerência de Governança, Riscos e Compliance		
Sigilo		Público Externo		
Versão	**Data**	**Responsável**	**Aprovador**	**Descrição da Alteração**
1ª	07/11/2017	Gerência de Controle Interno e Auditoria – GCIA	Conselho de Administração	Emissão Inicial
2ª	07/05/2019	Gerência de Governança, Riscos e Compliance – GGRC	Conselho de Administração	Inclusão da referência: Política de Controle Interno Corporativo
3ª	23/07/2020	Diretoria Adjunta de Governança Riscos e Compliance – DAGRC	Conselho de Administração	Alteração de estrutura e inclusão do tópico referente ao apetite a risco
4ª	12/08/2021	Diretoria Adjunta de Governança Riscos e	Conselho de Administração	Adequação a terminologia do controle interno e

		Compliance – DAGRC		alinhamento ao novo estatuto da Companhia.
5ª	07/12/2022	Diretoria Adjunta de Governança Riscos e Compliance – DAGRC	Conselho de Administração	Adequação de terminologia e revisão da política para bianual.
6ª	19/12/2024	Diretoria Adjunta de Governança Riscos e Compliance – DAGRC	Conselho de Administração	Adequação de texto e alinhamento ao regimento interno do Comitê de Auditoria Estatutário e revisão da política para bianual.