1 Objetivo

Esta política tem por objetivo estabelecer princípios, diretrizes e responsabilidades a serem observados nas atividades relacionadas à gestão dos riscos corporativos da Companhia e orientar as ações para a identificação, avaliação, tratamento, monitoramento e comunicação dos riscos.

2 Abrangência

Aplica-se à Companhia de Saneamento de Minas Gerais - COPASA MG e suas subsidiárias.

Para efeito desta Política, entende-se que o termo Companhia compreende a controladora e suas subsidiárias.

3 Princípios

3.1 A gestão de riscos deve estar alinhada com a Declaração Estratégica da Companhia.

3.2 A Companhia, incluindo seus direitos, obrigações, processos, informações e imagem, deve ser resguardada contra ameaças decorrentes de ações intencionais ou não.

3.3 Os riscos devem ser considerados em todas as decisões e a sua gestão deve ser realizada de maneira integrada.

3.4 As ações de resposta devem considerar as possíveis consequências dos riscos e ser priorizadas de acordo com a criação ou proteção de valor da Companhia e com as necessidades e expectativas das partes interessadas.

3.5 A gestão de riscos deve ser um processo contínuo, que busca envolver toda a Companhia tratando os eventos e as unidades organizacionais de forma conjunta.

3.6 Não são toleradas quaisquer decisões que exponham deliberadamente a vida humana a quaisquer riscos.

4 Referências

4.1 COSO – ERM*: Committee of Sponsoring Organizations of the Treadway Commission – Enterprise Risk Management Framework.*

4.2 Norma ABNT Standard NBR ISO 31000: 2018 – Gestão de Riscos: Diretrizes.

4.3 Caderno 19 de Governança Corporativa do IBGC – Gerenciamento de Riscos Corporativos.

4.4 Política de Divulgação de Informações e Negociação de Valores Mobiliários de Emissão da COPASA MG.

4.5 Estatuto Social da COPASA MG.

4.6 Plano de Integridade da COPASA MG.

4.7 Código de Conduta e Integridade da COPASA MG.

4.8 Política Compliance Anticorrupção da COPASA MG.

4.9 Modelo das Três Linhas do Instituto dos Auditores Internos – IIA - 2020.

5 Definições

5.1 **Apetite a Riscos:** É o nível tolerável de risco que a COPASA MG admite na busca de seus objetivos.

5.2 **Comitê de *Compliance* e Riscos**: grupo formado por empregados da Companhia com o objetivo de apoiar a Superintendência de *Compliance*, coordenadora do referido Comitê, no desempenho de suas responsabilidades relativas à gestão de riscos e *compliance*.

5.2.1 **Composição do Comitê:** 01(um) superintendente de cada Diretoria, os titulares da Superintendência de Pessoas, da Diretoria Adjunta Jurídica, da Superintendência de *Compliance* e das Unidades de Serviço de Riscos, *Compliance* e Controles Internos.

5.3 ***Committee of Sponsoring Organizations (COSO):*** organização privada sem fins lucrativos, para prevenir e evitar fraudes nos procedimentos e processos internos.

5.4 **Controle Interno:** Conjunto de métodos, procedimentos, políticas e normas adotados com o objetivo de salvaguardar ativos, verificar a adequação e o suporte dos dados contábeis e dos processos relacionados, garantir a segurança das informações, promover eficiência operacional, encorajar a aderência aos normativos e evitar fraudes, erros e crises na Companhia.

5.5 **Fatores de Risco:** são ações, eventos ou processos que carregam criticidades ou fragilidades, dos quais podem decorrer impactos negativos.

5.6 **Fatores de Risco de *Compliance*:** são ações ou eventos que carregam criticidades ou fragilidades relacionadas a eventual descumprimento de determinada obrigação legal, além de riscos de imagem e reputação da Companhia decorrentes da realização de condutas inadequadas.

5.7 **Indicadores de Risco:** são os indicadores propostos pelo proprietário do risco, para acompanhamento das metas associadas ao apetite ao risco aceito pela Companhia. Esses indicadores mostram níveis de alerta para atuação dos órgãos de governança.

5.8 **Limite Crítico:** É o ponto de alerta em relação ao desempenho não tolerado, medido pelos indicadores de risco. Desvios relevantes indicam a necessidade de adoção de ações corretivas, aplicadas de maneira oportuna, suficientes para minimizar eventuais perdas e que deve ser reportado à instância superior.

5.9 **Matriz de Riscos:** é o instrumento que apresenta os riscos identificados e sua caracterização.

5.10 **Mapa de Risco:** é uma representação gráfica dos riscos, derivado da avaliação do impacto e da probabilidade de ocorrência de eventos negativos, identificados por cores correspondentes ao seu nível de criticidade.

5.11 **Nível de Criticidade do Risco:** magnitude de um risco, expressa em termos da combinação da sua probabilidade com o seu impacto. Os níveis podem ser classificados como Crítico, Alto, Médio e Baixo.

5.12 **Plano de Contingência e Plano de Continuidade dos Negócios:** processo de gestão da capacidade de uma organização de conseguir manter um nível de funcionamento adequado até o retorno à situação normal, após a ocorrência de incidentes e interrupções de operações críticas.

5.13 **Plano de Resposta ao Risco:** planejamento de ações, elaborado pelo proprietário do risco que apresenta o tratamento a ser dado ao risco.

5.14 **Ponto Focal:** empregado indicado pelo Proprietário do Risco para execução e acompanhamento de assuntos e atividades relativas ao processo de gestão de riscos.

5.15 **Proprietário de Risco:** é a pessoa, expressa pelo cargo ou função, que possui a responsabilidade e a autoridade para gerir um risco. É quem deve elaborar o plano de resposta ao risco e implementá-lo.

5.16 **Resposta ao Risco:** escolha motivada sobre o tratamento a ser aplicado ao risco, entre evitar, mitigar, compartilhar ou aceitar.

a) evitar o risco, decidindo por não iniciar ou descontinuar uma atividade que dá origem ao mesmo;
b) mitigar o risco, minimizando seu impacto e/ou probabilidade;
c) compartilhar o risco, atribuindo parte do risco a terceiros que possam capturar melhor a oportunidade em benefício da Companhia;
d) aceitar o risco, assumindo o nível de criticidade e o apetite aprovado.

5.17 **Risco:** efeito das incertezas presentes em fatores ou eventos, o qual pode causar impactos negativos, dificultando ou impossibilitando o cumprimento dos objetivos da COPASA MG.

5.18 **Risco Inteligente:** são riscos deliberadamente assumidos ou “tomados” pela Companhia, em busca de novas oportunidades ou na implementação de inovações que possibilitem a geração de valor para a COPASA MG.

5.19 **Tolerância a Riscos:** variação aceitável entre a meta e o limite crítico de indicadores dos riscos relativos aos objetivos da Companhia, considerando sua capacidade de assumir riscos.

5.20 **Três Linhas:** modelo do Instituto de Auditores Internos – IIA, o qual orienta quanto aos limites de atuação das unidades organizacionais para as ações de gestão de riscos e

controles internos, bem como em relação aos papéis dos órgãos de governança na Companhia.

6 Diretrizes

6.1 Aproveitar as oportunidades e antever as ameaças internas e externas que possam afetar os objetivos da Companhia.

6.2 Os riscos inteligentes deverão ser observados pelos Proprietários dos riscos e demais gestores da Companhia, de forma proativa visando a inovação e aproveitamento de oportunidades.

6.3 Identificar e tratar os riscos de forma a oferecer garantia razoável do cumprimento dos objetivos estabelecidos na Declaração Estratégica da Companhia.

6.4 Classificar os riscos conforme sua natureza, a exemplo de operacional, estratégico, financeiro e *compliance* e seu nível de criticidade como Crítico, Alto, Médio e Baixo.

6.5 Gerenciar, de forma proativa e abrangente, os riscos associados aos processos estratégicos, de negócio e de suporte, de forma a mantê-los em um nível tolerável de magnitude.

6.6 Identificar e avaliar os riscos de acordo com a probabilidade de ocorrência e seu impacto econômico-financeiro, operacional, regulatório, reputacional, *compliance* ou socioambiental sobre o negócio, considerando, ainda, a interdependência entre os riscos.

6.7 Planejar as respostas aos riscos, analisando cenários, benefícios, aspectos negativos, riscos inter-relacionados e mensurando a relação entre impacto e mitigação.

6.8 A gestão de riscos deve ser dinâmica, iterativa e de caráter proativo quanto aos eventos internos e externos capazes de modificar o contexto e o posicionamento da Companhia.

6.9 Fortalecer a gestão de riscos como parte da cultura empresarial da COPASA MG.

6.10 Garantir a administradores, investidores e demais partes interessadas um fluxo contínuo, transparente e adequado de informações associadas aos principais riscos e seu processo de gestão na COPASA MG, respeitando o grau de sigilo das informações, bem como os procedimentos corporativos, políticas, diretrizes e demais normas internas de segurança empresarial e da informação.

6.11 Assegurar o monitoramento e a análise crítica do próprio gerenciamento de riscos como parte integrante de um processo contínuo de melhoria da governança corporativa.

6.12 O Proprietário do Risco na avaliação, definição e implementação das ações de tratamento do risco, em conjunto com o Ponto Focal, deve promover ampla discussão com todas as áreas envolvidas.

7 Responsabilidades

7.1 Conselho de Administração

a) definir a estratégia da Companhia para atendimento de seus objetivos de negócio, promovendo a integração das práticas de gestão de riscos ao processo decisório;

b) aprovar a Política de Gestão de Riscos Corporativos, assim como suas revisões;

c) aprovar os indicadores e apetite aos riscos com níveis de criticidade Alto e Crítico;

d) aprovar a análise residual dos riscos;

e) acompanhar os resultados dos processos de gerenciamento de riscos, por meio de relatórios executivos.

7.2 Diretoria Executiva

a) aprovar a metodologia de gestão de riscos, assim como as suas revisões;

b) aprovar a Matriz de Riscos Corporativos;

c) aprovar os Planos de Resposta aos Riscos com níveis de criticidade Alto e Crítico;

d) promover as condições necessárias para a implementação dos Planos de Resposta de todos os riscos corporativos;

e) recomendar para aprovação do Conselho de Administração, os indicadores e apetite dos riscos com níveis de criticidade Alto e Crítico;

f) aprovar os indicadores e apetite dos demais riscos.

7.3 Diretoria proprietária do risco

a) ser responsável, juntamente com o Proprietário do Risco, por identificar, monitorar e mitigar os riscos corporativos;

b) indicar superintendentes para compor o Comitê de *Compliance* e Riscos;

c) recomendar para aprovação os indicadores e apetite dos riscos;

d) recomendar para aprovação os Planos de Resposta dos riscos com nível de criticidade Alto e Crítico e aprova os demais planos.

7.4 Comitê de Auditoria: supervisionar as atividades de gestão de riscos, *compliance* e controles internos.

7.5 Auditoria Interna: prover o Conselho de Administração, o Comitê de Auditoria e as Diretorias com avaliação e assessoria independentes, objetivas, imparciais e tempestivas sobre a adequação, eficácia da governança, do gerenciamento de riscos e controles internos, para apoiar o atingimento dos objetivos organizacionais, promover e facilitar a melhoria contínua.

7.6 Superintendência de *Compliance*

7.6.1 Unidade de Serviço de Gestão de Riscos

a) coordenar, de maneira contínua, a avaliação e monitoramento dos riscos corporativos da Companhia;

b) coordenar a identificação dos riscos, avaliando a probabilidade e o impacto de sua ocorrência;

c) revisar a metodologia de avaliação de risco corporativo, submetendo-a à aprovação da Diretoria Executiva;

d) colaborar com os Proprietários dos Riscos na elaboração e implementação dos Planos de Resposta aos Riscos;

e) monitorar a execução dos Planos de Resposta aos Riscos, a evolução dos indicadores e dar ciência ao Conselho de Administração;

f) coordenar o processo de elaboração de Planos de Continuidade dos Negócios ou de Planos de Contingência relativos aos riscos corporativos.

7.6.2 Unidade de Serviço de *Compliance* e Controles Internos

a) identificar pontos de não conformidade nos processos relacionados aos riscos;

b) atuar, preventivamente, nos riscos de *compliance*;

c) identificar e avaliar, em conjunto com o proprietário, os principais controles que mitigam os riscos elencados na Matriz de Riscos Corporativos, buscando melhorá-los ou sugerindo a criação de outros, quando necessário.

7.7 Comitê de *Compliance* e Riscos

a) avaliar e opinar sobre a revisão da Matriz de Riscos Corporativos;

b) participar do processo de aplicação da metodologia para a definição dos riscos;

c) participar do fortalecimento da cultura empresarial no que se refere a *compliance* e a gestão de riscos;

d) opinar sobre a definição dos indicadores e apetite aos riscos;

e) acompanhar a elaboração e implementação dos Planos de Resposta aos Riscos;

f) opinar sobre a análise residual dos riscos.

7.8 Proprietário de risco

a) identificar e avaliar os riscos corporativos;
b) definir, estruturar e monitorar os indicadores, implementando ações para o atingimento das metas estabelecidas;
c) propor o apetite aos riscos;
d) elaborar, implementar e monitorar os controles internos e o Planos de Resposta aos Riscos;
e) Indicar, orientar e dar suporte ao empregado que atua como Ponto Focal, na avaliação e implementação de ações relativas ao risco sob sua responsabilidade.

7.9 Ponto focal

a) atuar como referência para disseminar e tratar dos assuntos de gestão de riscos;

b) apoiar o proprietário de risco na implementação e acompanhamento das ações de tratamento e indicadores dos riscos, garantindo o cumprimento dos prazos e qualidade das tratativas no âmbito da sua atuação;

c) responder às Unidades envolvidas no processo de gerenciamento de riscos.

8 Parâmetros para a Metodologia

A metodologia adotada pela COPASA MG para a identificação, avaliação, respostas, monitoramento e definição do apetite aos riscos está apresentada no Manual de Gestão de Riscos Corporativos, cuja responsabilidade pela elaboração e revisão cabe à Unidade de Serviço de Gestão de Riscos.

9 Disposições Finais

9.1 A Superintendência de *Compliance* será responsável pela promoção da capacitação aos administradores a respeito desta Política, nos termos do Inciso VI, do § 1º, do Artigo 9º da Lei 13.303/2016.

9.2 Esta Política, aprovada pelo Conselho de Administração em reunião realizada em 25/05/2023, entra em vigor a partir desta data.

Informações de Controle:

Versão 0 (Instituição): aprovada pelo Conselho de Administração, em reunião de 26/03/2014.

Versão 1: aprovada pelo Conselho de Administração, em reunião de 08/03/2018.

Versão 2: revisão sem alteração de conteúdo, conforme CRC 006/20.

Versão 3: aprovada pelo Conselho de Administração, em reunião de 30/07/2020.

Versão 4: revisão, sem alteração de conteúdo, aprovada pelo Conselho de Administração, em reuniões de 26/08/2021 e 15/12/2021.

Versão 5: revisão, aprovada em reunião do Conselho de Administração de 25/05/2023.

Unidade Gestora do Documento: Superintendência de *Compliance*.

Instância de Revisão: Diretoria Executiva.

Instância de Aprovação: Conselho de Administração.