1 PÚBLICO ALVO

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.

2 OBJETIVOS

Esta política tem por objetivo estabelecer princípios, diretrizes, conceitos e competências a serem observados nas atividades relacionadas à gestão dos riscos e controles internos. Orientar as ações para a identificação, avaliação, tratamento, monitoramento e comunicação dos riscos e controles internos, gerando valor para a Companhia e aperfeiçoando as práticas de governança, considerando a visão de riscos na tomada de decisão.

3 REFERÊNCIAS

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

3.2 Código de Conduta e Integridade da Copasa.

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

3.4 Estatuto Social da COPASA MG.

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

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

3.7 Norma ABNT NBR ISO 31010: 2019 – Gestão de Riscos — Técnicas para o processo de avaliação de riscos.

3.8 Norma ABNT NBR ISO 31073:2022 – Gestão de riscos – Vocabulário

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

3.10 Norma ISO/TS 31050 – Gestão de riscos emergentes para aumentar a resiliência.

4 DIRETRIZES

4.1 Alinhar a gestão de riscos e controles internos com os objetivos da Companhia.

4.2 Resguardar a Companhia, incluindo seus direitos, obrigações, processos, informações e imagem, contra ameaças decorrentes de ações intencionais ou não.

4.3 Considerar as necessidades e expectativas das partes interessadas nas ações de resposta aos riscos.

4.4 Estabelecer a gestão de riscos e controles internos como um processo contínuo e integrado.

4.5 Não admitir decisões que exponham deliberadamente a vida humana a quaisquer riscos.

4.6 A gestão de riscos e controles internos deve se basear em informações atuais, rastreáveis e provenientes de fontes validadas, com registro expresso de limitações, incertezas ou lacunas de dados.

4.7 Identificar nos processos da Companhia os controles internos que apoiam a mitigação dos riscos.

4.8 Adotar o modelo das Três Linhas 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.

4.9 Assegurar que as atividades de controle sejam realizadas em todos os níveis.

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

4.11 Identificar e tratar os riscos de forma a oferecer garantia razoável do cumprimento dos objetivos da Companhia.

4.12 Classificar os riscos e os controles internos conforme sua natureza e seu nível de criticidade.

4.13 Gerenciar, de forma proativa e abrangente, os riscos associados aos processos da Companhia de forma a mantê-los em um nível tolerável de magnitude.

4.14 Identificar e avaliar os riscos de acordo com a probabilidade de ocorrência e seu impacto sobre o negócio, considerando, ainda, a interdependência entre os riscos.

4.15 Planejar as respostas aos riscos, analisando cenários, benefícios, aspectos negativos, riscos interdependentes, mensurando a relação entre impacto e mitigação.

4.16 Assegurar que a gestão de riscos seja dinâmica, iterativa e de caráter proativo frente aos eventos internos e externos capazes de modificar o contexto e o posicionamento da Companhia.

4.17 Fortalecer a gestão de riscos como parte da cultura empresarial, incorporando-a aos processos de tomada de decisão, às práticas de governança e à sustentabilidade do modelo de negócio da Companhia.

4.18 Garantir às partes interessadas transparência no processo de gestão de riscos e controles internos, assegurando o sigilo das informações e demais normas internas de segurança empresarial.

4.19 Considerar, na gestão dos riscos, aspectos de curto, médio e longo prazo, podendo ser expressos nos objetivos, metas, metodologia e monitoramento dos riscos.

5 COMPETÊNCIAS

5.1 Conselho de Administração:

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

b) aprovar a Política de Gestão de Riscos e Controles Internos, assim como suas revisões;

c) aprovar o Termo de Apetite ao Risco - TAR;

d) acompanhar os resultados dos processos de gestão de riscos e controles internos.

5.2 Comitê de Auditoria:

a) monitorar a qualidade e a integridade dos mecanismos de controle interno da Companhia;

b) avaliar e monitorar as exposições da Companhia a riscos;

c) apreciar a Política de Gestão de Riscos e Controles Internos, assim como suas revisões, anteriormente à apreciação do Conselho de Administração;

d) apreciar o apetite a riscos da Companhia, anteriormente à apreciação pelo Conselho de Administração;

e) acompanhar os resultados dos processos de gestão de riscos e controles internos.

5.3 Diretoria Executiva:

a) aprovar a metodologia e recomendar para o Conselho de Administração a aprovação da Política de Gestão de Riscos e Controles Internos, assim como suas revisões;

b) aprovar a estruturação dos riscos da Companhia;

c) recomendar para aprovação do Conselho de Administração o apetite aos riscos;

d) acompanhar os resultados dos processos de gestão de riscos e controles internos;

e) garantir que a cultura de gestão de riscos e controles internos seja integrada em todos os níveis da Companhia.

5.4 Diretoria proprietária do risco

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

b) indicar membros para composição do Comitê de *Compliance* e Riscos, de preferência proprietário de risco;

c) propor o apetite aos riscos e recomendar para a Diretoria Executiva;

d) aprovar e apoiar a elaboração dos indicadores e Planos de Resposta aos riscos sob sua responsabilidade;

e) promover as condições necessárias para a implementação dos indicadores e Planos de Resposta aos riscos;

f) apoiar na elaboração das ações necessárias caso haja violação de limite crítico dos indicadores de riscos;

g) reportar para a Diretoria Executiva aspectos e considerações sobre os riscos e controles de sua respectiva área sempre que considerar pertinente.

5.5 Superintendência de *Compliance*

5.5.1 Gerência de Riscos e Controles Internos

a) mapear, avaliar e monitorar os controles associados aos riscos nos processos, identificando pontos críticos;

b) auxiliar as unidades nas atividades de identificação, implantação e adequação de controles internos, destacando os controles-chave dos processos da Companhia;

c) assegurar a revisão periódica e atualização do sistema de controles internos pelos proprietários dos riscos, monitorando sua efetividade;

d) alinhar a estrutura dos controles internos aos riscos e aos objetivos estratégicos da Companhia;

e) coordenar e apoiar as unidades envolvidas e os proprietários de risco na identificação, avaliação, análise e tratamento dos riscos;

f) realizar monitoramento, análise crítica, comunicação, consulta, registro e relato dos riscos;

g) desenvolver, melhorar e disseminar a metodologia e boas práticas para a gestão de riscos e controles internos;

h) apoiar metodologicamente, o proprietário do risco e demais áreas envolvidas, na elaboração, implementação e monitoramento dos Planos de Resposta e indicadores de riscos;

i) dar ciência, em conjunto com o proprietário, ao Comitê de *Compliance* e Riscos sobre a violação de limite crítico, bem como as ações corretivas para retorno do indicador ao nível tolerado;

j) realizar reportes periódicos sobre os processos de gestão de riscos e controles internos para acompanhamento da alta administração, mensalmente para a Diretoria Executiva e trimestralmente para o Comitê de Auditoria e Conselho de Administração;

k) utilizar os relatórios emitidos pela Auditoria Interna como subsídio para a melhoria contínua e a retroalimentação do processo de gestão de riscos e controles internos;

l) disseminar a cultura de gestão de riscos e controles internos em todos os níveis da Companhia.

5.6 Comitê de *Compliance* e Riscos

a) apoiar na implementação e revisões da metodologia de gestão de riscos e controles internos;

b) participar do fortalecimento da cultura empresarial no que se refere a gestão de riscos e controles internos;

c) opinar sobre a proposta de riscos, indicadores e apetite aos riscos;

d) acompanhar a elaboração e implementação dos planos de resposta aos riscos e controles internos;

e) acompanhar as violações de limites críticos dos indicadores.

5.7 Proprietário de risco

a) identificar e avaliar os riscos e controles internos;

b) garantir a execução dos controles internos existentes e implementar melhorias identificadas;

c) definir, estruturar e monitorar os indicadores, implementando ações para o atingimento das metas estabelecidas;

d) reportar tempestivamente, o resultado dos indicadores, falhas de controles-chave e eventos materializados para a Gerência de Riscos e Controles Internos;

e) propor a definição do apetite aos riscos;

f) elaborar, implementar e monitorar os Planos de Resposta aos Riscos;

g) indicar, orientar e dar suporte ao empregado que atua como Ponto Focal do risco;

h) reportar, tempestivamente ao Diretor Proprietário, a violação do limite crítico dos indicadores, constando as justificativas de violação e as ações corretivas para retorno do resultado ao nível tolerado.

5.8 Ponto focal

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

b) fazer o devido alinhamento do acompanhamento dos riscos e controles internos com o proprietário do risco.

5.9 Auditoria Interna

a) avaliar a adequação da governança, do gerenciamento de riscos e dos controles dos processos, sistemas, áreas, operações ou localidades da Companhia;

b) emitir recomendações para o aprimoramento da governança, da gestão de riscos, dos controles internos e da performance dos processos, sistemas, áreas, operações ou localidades, dentre outras pertinentes aos trabalhos realizados;

c) subsidiar o processo de gestão de riscos e controles internos com informações, por meio dos relatórios de Auditoria Interna;

d) participar das reuniões do Comitê de *Compliance* e Riscos, visando contribuir com as discussões sobre o processo de gestão de riscos e controles internos, a título de consultoria, de forma a preservar sua objetividade e independência.

6 PARÂMETROS PARA A METODOLOGIA

A metodologia adotada pela Copasa para a identificação, avaliação, resposta, monitoramento e definição do apetite aos riscos e controles internos está apresentada no Manual de Gestão de Riscos e Controles Internos, cuja responsabilidade pela elaboração e revisão cabe à Gerência de Riscos e Controles Internos e aprovação pela Diretoria Executiva.

7 DISPOSIÇÕES FINAIS

7.1 A Superintendência de *Compliance* será responsável pela promoção da capacitação para a alta administração a respeito desta Política.

7.2 Esta Política, aprovada pelo Conselho de Administração em reunião realizada em 29/07/2026, entra em vigor a partir desta data.

Informações de Controle:

Versão 0 (Instituição): aprovada pelo Conselho de Administração, em reunião de 29/07/2026.

Unidade Gestora do Documento: Superintendência de *Compliance*.

Instância de Revisão: Diretoria Executiva.

Instância de Aprovação: Conselho de Administração.

ANEXO I - DEFINIÇÕES

Apetite a Riscos: nível de risco que a Companhia está disposta a buscar, reter ou assumir para alcançar seus objetivos.

Causa: condição ou origem que aumenta a probabilidade do fator de risco. Alvo do controle preventivo.

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 ao *compliance,* gestão de riscos e controles internos.

Committee of Sponsoring Organizations (COSO): organização privada sem fins lucrativos que desenvolve estruturas de referência global para implementação de controles internos efetivos, gestão de riscos e prevenção de fraudes corporativas.

Consequência: resultado de um fator de risco (evento) que afeta os objetivos.

Controles Internos: processo efetuado para fornecer garantia razoável em relação a prevenção e mitigação dos fatores de riscos para a realização dos objetivos.

Controle-chave: controle ou conjunto de controles com a maior capacidade de mitigar o risco correspondente, reduzindo significativamente a sua probabilidade de ocorrência ou o seu impacto.

Fatores de Risco: são os eventos com a possibilidade de materialização do risco. É a unidade em que se avalia a exposição, se desenham os controles e se medem os indicadores de risco. Redigem-se sempre como uma ocorrência.

Indicadores de Risco: indicadores que medem a exposição da Companhia a um fator de risco, sinalizando níveis de alerta em relação ao apetite ao risco.

Inventário de Riscos: é o instrumento que apresenta os riscos identificados e sua caracterização.

Limite Crítico: É o valor-limite tolerado definido nos indicadores de risco.

Matriz de Riscos: é uma representação gráfica dos riscos, derivado da avaliação do impacto e da probabilidade, identificados por cores correspondentes ao seu nível de criticidade.

Natureza de risco: classificação atribuída aos agrupamentos de riscos, que considera sua origem e tipificação de forma organizada.

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.

Plano de Resposta ao Risco: planejamento de ações mitigatórias elaborado pelo proprietário do risco.

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

Proprietário de Risco: pessoa com a responsabilização e a autoridade para gerenciar riscos intrínsecos aos processos da Companhia.

Resposta ao Risco: escolha motivada sobre o tratamento a ser aplicado ao risco, entre evitar, mitigar, compartilhar ou aceitar, devendo estar expresso no Termo de Apetite ao Risco - TAR.

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, atribuir formalmente parte da responsabilidade, custos e benefícios a terceiros;

d) aceitar o risco, quando posicionado dentro do apetite aprovado; posições acima do apetite exigem deliberação formal da instância competente.

Risco: efeito das incertezas nos objetivos.

Termo de Apetite ao Risco (TAR): documento que consolida o apetite, a tolerância e os limites de exposição da Companhia, aprovado pelo Conselho de Administração e revisado anualmente ou mediante mudança material de contexto.

Tolerância a Riscos: nível de disposição da Companhia em suportar o risco.

Modelo das Três Linhas do Instituto dos Auditores Internos - IIA: orienta quanto aos limites de atuação das unidades organizacionais para as ações de gestão de riscos e controles internos, se organizando em papéis e responsabilidades em três níveis distintos:

a) 1ª Linha: Responsáveis diretos pelos processos

Papel: Liderar e dirigir ações (incluindo gestão de riscos) e aplicação de recursos para atingir os objetivos da organização; manter um diálogo contínuo com o órgão de governança e reportar: resultados planejados, reais e esperados, vinculados aos objetivos da organização; e riscos; estabelecer e manter estruturas e processos apropriados para o gerenciamento de operações e riscos (incluindo controle interno); e garantir a conformidade com as expectativas legais, regulatórias e éticas.

b) 2ª Linha: Áreas de gestão de riscos e controles internos, segurança da informação e *compliance*.

Papel: Fornecer expertise complementar, apoio, monitoramento e questionamento quanto à gestão de riscos, incluindo: o desenvolvimento, implantação e melhoria contínua das práticas de gestão de riscos (incluindo

controle interno) nos níveis de processo, sistemas e entidade; o atingimento dos objetivos da gestão de riscos, como: conformidade com leis, regulamentos e comportamento ético aceitável; controle interno; segurança da informação e tecnologia; sustentabilidade; e avaliação da qualidade; fornecer análises e reportar sobre a adequação e eficácia da gestão de riscos (incluindo controle interno).

c) 3ª Linha: Auditoria Interna

Papel: Mantém a prestação de contas primária perante o órgão de governança e a independência das responsabilidades da gestão; comunica avaliação e assessoria independentes e objetivas à gestão e ao órgão de governança sobre a adequação e eficácia da governança e da gestão de riscos (incluindo controle interno), para apoiar o atingimento dos objetivos organizacionais e promover e facilitar a melhoria contínua; reporta ao órgão de governança prejuízos à independência e objetividade e implanta salvaguardas conforme necessário.

Violação do limite crítico: é o desvio em relação ao resultado tolerado do limite crítico aprovado para cada indicador, apontando a necessidade de adoção de ações corretivas de curto e médio prazos, a serem aplicadas de maneira oportuna, suficientes para minimizar eventuais perdas, e retornar o resultado do indicador ao nível tolerado.