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 de Gestão de Riscos Corporativos, 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 estratégia corporativa 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 devem ser priorizadas de acordo com a agregação ou preservação de valor da Companhia.

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

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 Ética da COPASA MG.

4.8 Política Anticorrupção da COPASA MG.

5 DEFINIÇÕES

5.1 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*.

5.1.1 Composição do Comitê: 01(um) superintendente de cada Diretoria, o Superintendente de Pessoas, o Procurador Jurídico, o Superintendente de *Compliance* e os Gerentes de Riscos, *Compliance* e Controles Internos.

5.2 Fatores de Risco: são ações, eventos ou processos que carregam criticidades ou fragilidades, dos quais podem decorrer impactos negativos. O plano de resposta ao risco deve ser elaborado com base nos fatores listados na matriz de risco.

5.3 Fatores de Risco de Integridade: são ações ou eventos que carregam criticidades ou fragilidades que podem levar ao favorecimento de terceiros, à solicitação ou recebimento de vantagem indevida ou ao conflito de interesses. Podem caracterizar não conformidades ou falhas nos controles, mas devem ser analisadas também sob a ótica de risco de corrupção, conforme demanda a Política Anticorrupção da COPASA MG.

5.4 Líder de *Compliance* e Riscos: pessoa com a responsabilidade para disseminar, no âmbito de sua superintendência, as políticas de *Compliance*, Controle Interno e Gestão de Riscos da Companhia.

5.5 Limites de Exposição: representa o nível máximo de exposição a riscos (probabilidade x impacto) que a Companhia está autorizada a aceitar em relação ao apetite e à tolerância.

5.5.1 Apetite a Riscos: nível de risco que uma Companhia se dispõe a aceitar para alcançar seus objetivos.

5.5.2 Tolerância a Riscos: extensão máxima do risco que a organização pode absorver ao buscar atingir seus objetivos.

5.6 Linhas de Defesa: declaração de posicionamento do Instituto de Auditores Internos – IIA Global - que relaciona funções a níveis de controle interno em uma companhia.

5.6.1 Na primeira linha de defesa encontram-se os gestores das unidades e os responsáveis diretos pelos processos, que gerenciam e tem responsabilidade sobre os riscos, pois podem implementar as ações corretivas para resolver deficiências em processos e controles. A primeira linha se encontra no nível da gestão operacional.

5.6.2 Na segunda linha de defesa encontram-se os gestores de riscos, *compliance* e controles internos, responsáveis pela verificação, monitoramento, prevenção e análise integrada dos riscos.

5.6.3 Na terceira linha de defesa está a Auditoria Interna, proporcionando uma avaliação independente quanto à adequação, suficiência e eficácia dos sistemas de controles e gestão de riscos.

5.7 Matriz de Risco: instrumento, derivado da avaliação do impacto e da probabilidade de ocorrência de eventos negativos, que expressa riscos a que a COPASA MG está submetida.

5.8 Mapa de Risco: é uma representação gráfica dos riscos que são identificados por cores correspondentes ao seu nível de criticidade.

5.9 Nível de Risco: magnitude de um risco, expressa em termos da combinação de sua probabilidade e impacto.

5.10 Perfil de Risco: é a visão consolidada dos riscos em categorias, de acordo com os processos e metodologia empregados para identificação de riscos.

5.11 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 negócios críticos.

5.11.1 Continuidade: quando a ocorrência do risco estiver ligada aos processos internos da Companhia.

5.11.2 Contingência: quando o risco impactar no atendimento direto à sociedade.

5.12 Plano de Resposta ao Risco: conjunto de ações, elaborado pelo proprietário do risco e aprovado pela respectiva Diretoria, que expressa o tratamento a ser dado ao risco.

5.13 Proprietário do Risco: é a pessoa, expressa pelo cargo ou função, ou unidade organizacional com a responsabilidade e a autoridade para gerir um risco. É quem deve elaborar e implementar o Plano de Resposta ao Risco.

5.14 Resposta ao Risco: escolha motivada da forma de tratamento ao risco, entre evitar, mitigar, compartilhar ou aceitar.

5.15 Risco: efeito das incertezas presentes em fatores ou eventos, que pode causar impactos negativos, dificultando ou impossibilitando o cumprimento dos objetivos da COPASA MG. A descrição do risco deve expressar o fato negativo que se quer evitar, bem como orientar a reflexão sobre as possíveis causas geradoras da situação e suas consequências.

6 DIRETRIZES

6.1 Aproveitar as oportunidades e antever as ameaças internas e externas que afetam os objetivos estratégicos, econômico-financeiros, operacionais ou de *compliance*.

6.2 Identificar e tratar os riscos de forma a oferecer garantia razoável do cumprimento das metas estabelecidas na Estratégia Corporativa da Companhia.

6.3 Classificar os riscos conforme sua natureza, a exemplo de operacional, estratégico, financeiro, de liquidez, de crédito, socioambiental, regulatório, dentre outras.

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

6.5 Identificar e avaliar os riscos de acordo com a probabilidade de ocorrência e seu impacto sobre o negócio, inclusive sobre a imagem da Empresa, e planejar as respostas aos riscos, analisando cenários, benefícios, aspectos negativos, riscos inter-relacionados e mensurando a relação entre impacto e mitigação.

6.6 A gestão de riscos deve ser dinâmica, interativa e de caráter proativo quanto aos eventos internos e externos capazes de modificar o contexto e o posicionamento da Companhia. Dessa forma, devem ser avaliadas, dentre outras, as alterações nas condições mercadológicas, em cenários econômicos, jurídico-legais, tecnológicos e operacionais que impactem nas operações, nas atividades e nos riscos da Companhia.

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

6.8 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.

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

7 RESPONSABILIDADES

7.1 Conselho de Administração

a) define a Estratégia Corporativa da Companhia para atendimento de seus objetivos de negócio;

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

c) aprova o apetite e tolerância a risco;

d) aprova os riscos estratégicos priorizados e seus respectivos planos de resposta e contingência;

e) acompanha os resultados dos processos de gerenciamento de riscos e de controles internos, por meio de relatórios executivos.

7.2 Diretoria Executiva

a) promove as condições necessárias para a efetivação dos Planos de Resposta aos Riscos;

b) aprova a metodologia de avaliação de risco corporativo, assim como as suas revisões;

c) recomenda para aprovação do Conselho de Administração os Planos de Resposta aos Riscos.

7.3 Diretores

a) indicam superintendentes para compor o Comitê de *Compliance* e Riscos;

b) opinam sobre os Planos de Resposta aos Riscos, cujos proprietários estejam a eles vinculados.

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

7.5 Auditoria Interna: provê o Conselho de Administração, o Comitê de Auditoria e as Diretorias com avaliações independentes, imparciais e tempestivas sobre a efetividade da gestão dos riscos.

7.6 Superintendência de *Compliance*

7.6.1 Unidade de Serviço de Gestão de Riscos

a) avalia e monitora, de maneira contínua, os riscos corporativos da Companhia;

b) identifica riscos, avaliando a probabilidade e o impacto de sua ocorrência;

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

d) colabora com os Proprietários dos Riscos na elaboração e implementação do Plano de Resposta aos Riscos;

e) monitora as Respostas aos Riscos corporativos, com base na execução dos Planos de Resposta aos Riscos, na evolução dos indicadores dos riscos e em análises de aderência aos controles internos estabelecidos, e dá ciência ao Diretor-Presidente;

f) coordena o processo de elaboração do Plano de Continuidade dos Negócios e do Plano de Contingência.

7.6.2 Unidade de Serviço de *Compliance* e Controles Internos

a) conscientiza os gestores sobre a importância da mitigação dos riscos e sobre as responsabilidades dos proprietários dos riscos;

b) identifica pontos de não conformidade nos processos relacionados à matriz de riscos corporativos e propõe ações para integrar os Planos de Respostas aos Riscos;

c) atua, preventivamente, nos riscos de corrupção;

d) colabora com Diretorias, proprietários de riscos e respectivas equipes na identificação dos melhores controles para mitigação dos riscos;

e) elabora análises para verificar se as atividades de rotina relacionadas ao risco guardam aderência com os controles internos estabelecidos nos Planos de Respostas aos Riscos.

7.7 Comitê de *Compliance* e Riscos

a) avalia e revisa a Matriz de Riscos Corporativos;

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

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

d) acompanha a elaboração e implementação dos Planos de Resposta aos Riscos.

7.8 Proprietários de riscos

a) participam do processo de identificação e avaliação dos riscos corporativos;

b) elaboram o Plano de Resposta aos Riscos e os relatórios de sua execução, mensurando, sempre que possível, a variação no impacto ou na probabilidade de ocorrência do efeito negativo;

c) implementam controles internos e os Planos de Resposta aos Riscos.

8 PARÂMETROS PARA A METODOLOGIA

8.1 A Unidade de Gestão de Riscos deverá elaborar e revisar documento descrevendo a metodologia a ser adotada para a identificação, avaliação, respostas e monitoramento dos riscos corporativos.

8.2 São requisitos da metodologia

a) avaliação periódica dos riscos quanto a sua probabilidade e impacto, utilizando análises qualitativas baseadas em critérios previamente definidos, de modo que a combinação entre a probabilidade e impacto determinará o nível do risco;

b) existência de elementos que permitam determinar o perfil de risco da Companhia;

c) observância da interdependência de riscos, verificando de que forma materializações de determinados eventos de riscos podem desencadear outros;

d) priorização e tratamento dos riscos conforme o nível de criticidade;

e) elaboração de plano de resposta aos riscos;

f) previsão de monitoramento do processo com a finalidade de reavaliar o impacto e probabilidade de ocorrência dos riscos ou a própria metodologia;

g) observância da comunicação, de forma clara e objetiva a todos as partes interessadas, dos resultados de todas as etapas do processo de gestão de riscos, de forma a contribuir para o entendimento da situação atual e da efetividade dos planos de resposta aos riscos;

h) atuação em consonância com o conceito de linhas de defesa, de forma a deixar clara a responsabilidade de cada unidade organizacional no gerenciamento e na gestão de riscos e controles da Companhia.

8.3 A metodologia deverá ser elaborada considerando o contexto da Companhia, bem como os objetivos estratégicos, cultura empresarial, valores éticos, competências de seus colaboradores, além do ambiente externo no qual está inserida.

9 LIMITES DE EXPOSIÇÃO

9.1 A companhia considera os limites de exposição (apetite e tolerância) aos riscos estabelecidos dentro do perfil conservador, sendo eles estabelecidos de acordo com natureza de cada risco:

9.1.2 Riscos natureza estratégica:

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.

O apetite deve ser calculado de acordo com metodologia estabelecida, composta por duas abordagens:

a) quantitativa: na qual calcula-se o desvio aceito decorrente da materialização de riscos;

b) qualitativa: na qual é feita a ponderação do valor definido na abordagem quantitativa, por meio da análise da Companhia sob as óticas de variação de indicadores relevantes, da estrutura de capital, do ambiente regulatório, da reputação e *Compliance*.

A tolerância é um percentual do apetite a risco estabelecido que, quando atingido, aciona a Governança para a gestão dos riscos.

O apetite bem como a tolerância, devem ser atualizados anualmente, ou quando da ocorrência de fatos relevantes.

Caso a somatória dos impactos financeiros estimados para os riscos estratégicos priorizados ultrapasse a tolerância definida, a Governança deve ser acionada para reavaliar o Plano de Resposta existente.

9.1.3 Riscos de natureza operacional:

O apetite a riscos de natureza operacional é estabelecido com base na criticidade dos riscos identificados no mapeamento dos processos.

Para os riscos avaliados como “Crítico” ou “Catastrófico” deve-se obrigatoriamente estabelecer Planos de Resposta para mitigar a probabilidade e impacto de materialização.

Para os riscos avaliados como “Sério” é recomendável a elaboração de planos de tratamento e monitoramento das ações e controles existentes para conservação ou redução deste nível.

Para os riscos avaliados como “Moderado” ou “Baixo” deve-se manter e monitorar as ações e controles existentes para conservação neste nível.

Os riscos de *Compliance* identificados na avaliação dos processos deverão ter planos de ação definidos, independentemente de sua criticidade, a fim de mitigá-los.

Para os riscos de natureza operacional que atingirem o limite de tolerância será necessário elaborar os denominados Planos Contingência e de Continuidade, bem como todos os desdobramentos, suficientes para sua mitigação, deverão ser providenciados pelos proprietários de riscos.

Situações excepcionais devem ser discutidas pela Diretoria Executiva e aprovadas pelo Conselho de Administração.

10. DISPOSIÇÕES FINAIS

10.1 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.

10.2 Esta Política, aprovada pelo Conselho de Administração em reunião realizada em 30/07/2020, entra em vigor a partir desta data.

Informações de Controle:

Versão 0 (Instituição): aprovada pelo Conselho de Administração, em reunião de 23/06/2014.

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.

Unidade Gestora do Documento: Superintendência de *Compliance*.

Instância de Revisão: Diretoria Executiva.

Instância de Aprovação: Conselho de Administração.