POLÍTICA DE GESTÃO DE RISCOS

Aprovada em reunião do Conselho de Administração em 30/11/2021.

1. FINALIDADE

1.1. A Política de Gestão de Riscos institui diretrizes e competências para o gerenciamento dos riscos corporativos, com a finalidade de assegurar a consecução dos objetivos estratégicos, incorporar o contexto de riscos às tomadas de decisões, estimular boas práticas de governança corporativa e aprimorar o desempenho organizacional e o ambiente de controle.

1.2. Esta política não substitui outras abordagens de gerenciamento de riscos em exercício na Companhia, como o gerenciamento de riscos em nível de processo, o Programa de Prevenção de Riscos Ambientais (PPRA) e o gerenciamento de riscos nos sistemas de abastecimento de água (SAA) e esgotamento sanitário (SES), que possuem políticas, métodos e normas regulamentadoras próprias.

2. DIRETRIZES

2.1. A gestão de riscos corporativos deverá:

a) Abordar explicitamente a incerteza para aumentar a segurança quanto ao alcance dos objetivos estratégicos, mantendo-se alinhada aos contextos interno e externo da Companhia, reagindo a mudanças de forma dinâmica e interativa;
b) Fomentar o aprimoramento do ambiente de controles internos que visam a conformidade com as normas, leis e regulamentos vigentes, fazendo-se presente de forma gradual nos processos relevantes da Companhia;
c) Adicionar e preservar valor através da sinergia entre os conselheiros, diretores, gerentes e demais tomadores de decisão, de forma transparente e inclusiva, viabilizando a compreensão do gerenciamento de riscos corporativos por todos os envolvidos;
d) Melhorar continuamente a prática de gerenciamento de riscos corporativos através de ciclos de avaliação e revisões.

3. COMPETÊNCIAS

3.1. Compete ao Conselho de Administração:

a) Aprovar a Política de Gestão de Riscos;
b) Aprovar o Portfólio de Riscos Corporativos;
c) Supervisionar o cumprimento desta política.

3.2. Compete ao Comitê de Auditoria Estatutário (CAE):

a) Supervisionar as atividades desenvolvidas nas áreas de gerenciamento de riscos, controles internos e auditoria e assessorar o Conselho de Administração nesses assuntos;
b) Avaliar e monitorar exposições de risco da Companhia.

3.3. Compete à Auditoria Interna (AUD):

a) Aferir a efetividade do gerenciamento de riscos e dos controles internos.

3.4. Compete à Diretoria da Presidência:

a) Supervisionar as atividades da Assessoria de Conformidade, Controles Internos e Gestão de Riscos (ACR), disponibilizando estrutura e recursos necessários para seu adequado funcionamento.

3.5. Compete à Diretoria Executiva:

a) Monitorar continuamente os riscos aos quais a Companhia está exposta, assegurando a adequação do Mapa de Riscos Corporativos aos ambientes interno e externo e comunicando ao Conselho de Administração a ocorrência de mudanças significativas;
b) Acompanhar a implantação das ações mitigatórias e a resolução dos incidentes de riscos considerados relevantes;
c) Aprovar o Relatório Consolidado de Gestão de Riscos, para encaminhamento aos Conselhos de Administração e Fiscal, ao Comitê de Auditoria Estatutário e à Auditoria Interna;
d) Aprovar a aceitação fundamentada de riscos com grau de exposição entre os limites de apetite e a tolerância a risco, quando outras respostas não forem possíveis, convenientes ou oportunas.

3.6. Compete ao dono do risco:

a) Assegurar níveis adequados de exposição dos riscos sob sua responsabilidade, modelados ou não, comunicando à Diretoria Executiva e à Assessoria de Conformidade, Controles Internos e Gestão de Riscos (ACR) a ocorrência de incidentes de risco ou mudanças significativas nos ambientes interno e externo;
b) Modelar seus riscos corporativos, com o apoio da ACR e dos participantes indicados, e monitorar continuamente a adequação das matrizes de risco resultantes;
c) Supervisionar a implantação das ações mitigatórias e a resolução dos incidentes de risco sob sua responsabilidade.

3.7. Compete à Assessoria de Conformidade, Controles Internos e Gestão de Riscos (ACR):

a) Elaborar trimestralmente o Relatório Consolidado de Gestão de Riscos, contendo o Mapa de Riscos Corporativos atualizado e demais informações requeridas pela alta administração acerca do gerenciamento de riscos corporativos e outros assuntos correlatos;
b) Conduzir a modelagem dos riscos corporativos junto aos donos dos riscos e demais participantes, conforme priorização do Mapa de Riscos Corporativos, facilitando a identificação e análise de fatores de risco e a definição de respostas apropriadas;
c) Coordenar a elaboração e monitorar os planos de ação para mitigação dos riscos que estiverem acima dos níveis aceitáveis;
d) Aprimorar continuamente o processo de gerenciamento de riscos corporativos, difundir conhecimentos e incentivar a adoção de boas práticas de gerenciamento de riscos e controles internos, visando evoluir a maturidade a risco da Companhia;
e) Manter atualizadas e integradas as informações a respeito do Portfólio de Riscos, ações mitigatórias, indicadores, incidentes e matrizes dos riscos modelados e disponibilizá-las aos interessados.

4. TERMOS E DEFINIÇÕES

4.1. Ação mitigatória: plano de ação proposto para reduzir o grau de exposição de um fator de risco, podendo envolver também a elaboração de planos de contingência, indicadores de risco, atividades de controle, monitoramento etc.

4.2. Apetite a risco: quantidade de risco, estabelecida de modo amplo, que a Companhia está disposta a aceitar na consecução dos objetivos estratégicos.

4.3. Capacidade de risco: quantidade de risco que a Companhia consegue suportar na consecução dos objetivos estratégicos. Os riscos que ultrapassam essa quantidade são qualificados como muito elevados.

4.4. Dono do risco: diretor executivo que tem mais conhecimento e afinidade com o risco, mesmo que o risco também envolva outras diretorias.

4.5. Fator de risco: é a causa de um risco; um evento que, se ocorrer, pode materializá-lo. Um fator de risco pode possuir subfatores.

4.6. Grau de exposição do risco: medida calculada com base na probabilidade e no impacto do risco, que auxilia na priorização dos riscos e na tomada de decisão em relação à resposta mais apropriada.

4.7. Mapa de Riscos: painel que contém o posicionamento dos riscos de acordo com o grau de exposição, representando visualmente a distribuição dos riscos com base na probabilidade e no impacto.

4.8. Matriz de Riscos: estrutura detalhada de fatores e subfatores de um risco corporativo, abrangendo também as estimativas de probabilidade, impacto, grau de exposição e as respostas a risco, vinculadas às ações mitigatórias.

4.9. Modelagem de risco: processo aplicado individualmente a um risco corporativo em que são combinadas as técnicas de gerenciamento de riscos à expertise dos participantes em suas áreas específicas, resultando na sua Matriz de Riscos e dando início ao gerenciamento integrado de seus fatores e ao monitoramento das ações mitigatórias.

4.10. Objetivos estratégicos: objetivos amplos de contexto corporativo, envolvendo a realização da missão e visão da Companhia e seus desdobramentos em objetivos dentro do Planejamento Estratégico.

4.11. Plano de contingência: ação mitigatória previamente planejada que visa reduzir o impacto caso um ou mais fatores de risco se materializem, comumente utilizadas quando o impacto residual permanece elevado.

4.12. Portfólio de Riscos: documento que contém o conjunto dos principais riscos que a Companhia está exposta, as escalas padronizadas de avaliação de riscos e a declaração de apetite a risco.

4.13. Processo de gerenciamento de riscos corporativos: sistemas, métodos, procedimentos, papéis (funções), escalas e demais componentes que operacionalizam a Política de Gestão de Riscos.

4.14. Resposta a risco: decisão inerente a todos os fatores de riscos avaliados, tomada observando o grau de exposição em contraste ao apetite a risco, podendo ela ser aceitar, reduzir, entre outras possibilidades previstas no processo de gerenciamento de riscos corporativos.

4.15. Riscos corporativos: incertezas inerentes aos objetivos estratégicos da Companhia.
4.16. Tolerância a risco: quantidade de risco, acima do apetite a risco e abaixo da capacidade de risco, que a Companhia pode necessitar aceitar na consecução de seus objetivos estratégicos.

5. DISPOSIÇÕES GERAIS

5.1. Esta política será revisada anualmente ou sempre que necessário.

6. REFERÊNCIAS

ABNT ISO/TR 31004:2015. Gestão de Riscos: guia para implementação da ABNT NBR ISO 31000.
ABNT NBR ISO 31000:2018. Gestão de Riscos: diretrizes.
Committee of Sponsoring Organizations of the Treadway Commission (COSO). Gerenciamento de Riscos Corporativos: estrutura integrada. 2004.
Committee of Sponsoring Organizations of the Treadway Commission (COSO). Gerenciamento de Riscos Corporativos: integrado com estratégia e performance. 2017.
Instituto Brasileiro de Governança Corporativa (IBGC). Gerenciamento de Riscos Corporativos: evolução em governança e estratégia. 2017.
Lei Federal 13.303/2016 (Lei das Estatais).