Política de Gestão de Riscos

EMAE - Empresa Metropolitana de Águas e Energia

SUMÁRIO

1. OBJETIVO **3**
2. ABRANGÊNCIA **3**
3. CONCEITOS **3**
4. DIRETRIZES **4**
5. RESPONSABILIDADES **5**
5.1 CONSELHO DE ADMINISTRAÇÃO 5
5.2 COMITÊ DE AUDITORIA 5
5.3 DIRETORIA 6
5.4 COMITÊ EXECUTIVO DE RISCOS 6
5.5 ÁREA DE GESTÃO DE RISCOS 7
5.6 DONOS DOS RISCOS 7
5.7 AUDITORIA INTERNA 8
6. DISPOSIÇÕES FINAIS **8**
7. REFERÊNCIAS **8**
8. HISTÓRICO DAS ALTERAÇÕES **9**

POLÍTICA DE GESTÃO DE RISCOS

A necessidade de antecipar-se às mudanças e à complexidade dos negócios motivou as organizações buscarem maior aderência às boas práticas de Governança, Riscos e Conformidade (GRC), estabelecendo mecanismos de gestão e controle para a preservação e a geração de valor, de maneira alinhada à sua missão, visão, valores e estratégia.

A EMAE reforça seu comprometimento para a evolução de suas práticas de GRC com a identificação e o gerenciamento dos riscos corporativos que possam vir a impactar o negócio e o alcance de suas estratégias.

1. OBJETIVO

O presente documento tem por objetivo estabelecer orientações e diretrizes para a efetiva gestão dos riscos corporativos da Empresa Metropolitana de Águas e Energia e suas subsidiárias, no conjunto EMAE, que compreende as atividades de identificação, avaliação, priorização, tratamento, monitoramento e comunicação dos riscos.

Em adição, o documento visa promover uma linguagem comum de gerenciamento de riscos, com o propósito de difundir o conhecimento de Gestão de Riscos e incorporá-la na tomada de decisões da Empresa.

2. ABRANGÊNCIA

Esta política é aplicada a todos os empregados da EMAE, incluindo membros do Conselho de Administração, Conselho Fiscal, Comitês e Diretoria e todos que atuam em seu nome.

3. CONCEITOS

Sem prejuízo de outras definições específicas constantes dessa Política, os termos listados nesse capítulo terão os seguintes significados quando usados nesse documento, tanto no singular quanto no plural, assim como no feminino ou no masculino:

- **Ação Mitigatória:** ações tomadas pela Empresa visando a diminuição da exposição ao risco e mitigação da possibilidade de materialização do mesmo;
- **Apetite a Risco:** se refere a quanto de risco uma empresa está disposta a correr para alcançar a realização de sua missão e visão, e gerar valor para os acionistas;
- **Dono do Risco (*Risk Owner*):** responsável por tratar e monitorar o risco que está sob sua competência;
- **Fator de Risco:** condição que, individualmente ou combinada, possa acarretar ou ampliar a probabilidade de materialização do risco;
- **Impacto do Risco:** avaliação qualitativa e/ou quantitativa do efeito do risco na Empresa, se materializado;
- **Indicador de Risco (*KRI – Key Risk Indicator*):** instrumento de medição utilizado para monitorar e analisar a variação dos riscos estratégicos, por meio de análises de dados obtidos nos ambientes interno e externo;
- **Matriz de Riscos:** representação gráfica da exposição dos riscos estratégicos identificados pela EMAE de acordo com sua criticidade de cada risco, que é estabelecida pela avaliação de seu impacto versus sua probabilidade;
- **Perfil de Risco:** disposição da Empresa para incorrer em riscos. Exemplos de perfis de risco: conservador, moderado e agressivo.

- **Plano de Ação:** conjunto de medidas a serem adotadas pela Empresa para diminuir o impacto ou probabilidade de materialização do risco inerente a um nível que esteja em consonância com o apetite a risco da Empresa.
- **Plano de Trabalho de Gerenciamento de Riscos:** documento elaborado pela Gestão de Riscos contendo o planejamento periódico (exemplo anual) das atividades a serem executadas, reportadas e apresentadas, prazos, recursos necessários e responsáveis.
- **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 inerente e do residual, ações mitigatórias existentes, resposta(s) ao risco e planos de ação e de contingências, se aplicável;
- **Resposta ao Risco:** definição do tratamento que a Empresa dará ao risco residual. Como resposta, pode-se optar por evitar, reduzir, compartilhar ou aceitar o risco;
- **Risco:** é a incerteza sobre a possibilidade de perdas ou ganhos relacionados ao rumo dos acontecimentos relativos aos objetivos da Empresa;
- **Risco Estratégico:** risco que possa interromper o alcance dos objetivos e a execução da estratégia planejada;
- **Risco Inerente:** risco intrínseco da atividade na Empresa;
- **Risco Residual:** risco que se mantém após a adoção de iniciativas e esforços para redução dos impactos ou probabilidade de materialização dos riscos inerentes;
- **Tolerância a Risco:** percentual do apetite a risco definido pela Empresa que, quando atingido, aciona a governança para a gestão dos riscos.

4. DIRETRIZES

- As atividades de Gestão de Riscos devem considerar o alinhamento da estratégia da EMAE com sua missão, visão e valores, bem como as implicações do plano adotado;
- A Gestão de Riscos da EMAE deve ser vinculada ao diretor-presidente e liderada por diretor estatutário indicado pelo Conselho de Administração, devendo o estatuto social prever as atribuições da área, bem como estabelecer mecanismos que assegurem atuação independente;
- O Conselho de Administração e a Diretoria devem promover a Gestão de Riscos na Empresa, assegurar a prática das diretrizes e o engajamento aos procedimentos de gerenciamento de riscos;
- O gerenciamento de riscos deve fazer parte da cultura da EMAE, permeando os processos de gestão, controles internos, conformidade e auditoria interna, promovendo a identificação antecipada dos riscos e a sua gestão tempestiva;
- Os riscos identificados devem ser analisados, classificados, priorizados e ter sua estratégia de tratamento e monitoramento definida;

- As tomadas de decisão da EMAE devem considerar os riscos envolvidos, visando a preservação e a criação de valor da Empresa;
- A melhoria contínua do processo de gerenciamento de riscos deve ser promovida por meio de ciclos anuais de avaliação e revisões independentes, a fim de assegurar a eficácia do gerenciamento dos riscos;
- O processo de gerenciamento de riscos ocorre por meio da captura dos riscos associados ao planejamento estratégico, negócio e processos da EMAE, avaliando sua criticidade (impacto e probabilidade), identificando as ações mitigatórias e controles internos existentes e, posteriormente, definindo seu tratamento, monitoramento e reporte;
- Os riscos devem ser registrados em um portfólio e matriz, que devem ser revisados anualmente ou a qualquer momento, considerando os acontecimentos relacionados às estratégias e à mudança na probabilidade dos riscos e na eventualidade da sua materialização o impacto; e
- O monitoramento contínuo dos riscos requer a utilização de indicadores, os quais devem ser avaliados e reportados, pelo Comitê Executivo de Riscos, periodicamente ao Comitê de Auditoria e Conselho de Administração.

5. RESPONSABILIDADES

5.1 Conselho de Administração

- Definir o perfil de riscos da Empresa;
- Aprovar a política de Gestão de Riscos;
- Aprovar o apetite a risco da Empresa e tolerância;
- Implementar e supervisionar os sistemas de gestão de riscos e de controle interno estabelecidos para a prevenção e mitigação dos principais riscos a que esteja exposta a Empresa, inclusive os riscos relacionados à integridade das informações contábeis e financeiras e os referentes à ocorrência de corrupção e fraude;
- Avaliar periodicamente o portfólio dos riscos associados ao planejamento estratégico e as ações mitigatórias reportadas pelo Comitê Executivo de Riscos;
- Aprovar a matriz de riscos e os respectivos planos de resposta e contingência; e
- Acompanhar os resultados do processo e performance de gerenciamento dos riscos.

5.2 Comitê de Auditoria

- Apoiar a cultura de Gestão de Riscos;
- Assessorar o Conselho de Administração na definição do apetite a risco aceitável da Empresa;
- Conhecer o plano de trabalho da Gestão de Riscos;

- Avaliar periodicamente o portfólio dos riscos estratégicos e as ações mitigatórias reportadas pelo Comitê Executivo de Riscos;
- Assessorar o Conselho de Administração na aprovação dos riscos a serem priorizados e de suas respectivas estratégias de tratamento, que podem incluir planos de ação e contingência;
- Acompanhar, avaliar, monitorar e, quando necessário, fazer recomendações sobre mudanças na avaliação da criticidade dos riscos; e
- Analisar as avaliações independentes anuais do processo de Gestão de Riscos e reportar os resultados e planos de ação ao Conselho de Administração.

5.3 Diretoria

- Participar do processo de Gestão de Riscos da EMAE (metodologia, processos, sistemas, política, padrões e mecanismos de reporte, dentre outros) e garantir que estão alinhadas às práticas da Empresa e às boas práticas;
- Disseminar a cultura de Gestão de Riscos;
- Conhecer o apetite a risco da EMAE;
- Participar do processo de elaboração do portfólio dos riscos associados ao planejamento estratégico e conhecer os riscos priorizados;
- Conhecer o portfólio de riscos dos processos sob sua gestão; e
- Promover ciclos de avaliação e revisões independentes ao processo de gerenciamento de riscos (agentes internos ou externos), com periodicidade anual, de modo a assegurar a eficácia do gerenciamento e do monitoramento dos riscos.

5.4 Comitê Executivo de Riscos

- Deliberar sobre o processo de Gestão de Riscos da EMAE (metodologia, processos, sistemas, política, padrões e mecanismos de reporte, dentre outros) e garantir que estão alinhadas às práticas da Empresa e às boas práticas;
- Disseminar a cultura de Gestão de Riscos;
- Revisar e validar o método do cálculo do apetite a risco;
- Deliberar sobre o plano de trabalho de Gestão de Riscos e encaminhar para conhecimento do Comitê de Auditoria;
- Revisar e acompanhar o portfólio de riscos estratégicos;
- Identificar e definir as respostas aos riscos;
- Apresentar os riscos estratégicos e ações mitigatórias ao Comitê de Auditoria e ao Conselho de Administração;
- Submeter à avaliação do Comitê de Auditoria os riscos estratégicos a serem priorizados e de seus respectivos tratamentos;

- Obter junto ao Conselho de Administração a aprovação dos riscos estratégicos a serem priorizados e de seus respectivos tratamentos;
- Aprovar os donos dos riscos;
- Avaliar os planos de ação sugeridos pelos donos dos riscos; e
- Monitorar as variações de criticidade dos riscos priorizados e reportar aquelas significativas ao Comitê de Auditoria e Conselho de Administração.

5.5 Área de Gestão de Riscos

- Propor diretrizes para o gerenciamento de riscos da EMAE (metodologia, processos, sistemas, política, padrões e mecanismos de reporte, dentre outros);
- Disseminar a cultura de Gestão de Riscos, bem como os papéis e responsabilidades de todos os envolvidos no processo;
- Estabelecer e manter atualizada a política de Gestão de Riscos, assim como padrões e mecanismos de reporte próprios de informações;
- Elaborar e revisar periodicamente o plano de trabalho da Gestão de Riscos;
- Propor critérios para identificação, avaliação e classificação dos riscos que a Empresa está sujeita;
- Coordenar e monitorar o processo de identificação e avaliação dos riscos;
- Calcular e atualizar o apetite a risco anualmente ou quando eventos relevantes ocorrerem;
- Atuar em conjunto com o Comitê Executivo de Riscos, Comitê de Auditoria e Conselho de Administração na discussão sobre a definição do apetite a risco aceitável da Empresa;
- Elaborar, revisar e atualizar o portfólio de riscos sempre que houver atualizações na estratégia ou quando eventos relevantes ocorrerem;
- Auxiliar na definição dos donos dos riscos;
- Assessorar o dono do risco na definição do plano de ação e de contingência e na criação de indicadores e níveis de exposição dos riscos;
- Acompanhar eventuais mudanças na criticidade dos riscos e reportá-las ao Comitê Executivo de Riscos;
- Elaborar reportes acerca da Gestão de Riscos ao Comitê Executivo de Riscos, Comitê de Auditoria, Conselho de Administração e Fiscal; e
- Manter os colaboradores envolvidos com as atividades de gestão de riscos devidamente capacitados na metodologia adotada pela EMAE.

5.6 Donos dos Riscos

- Elaborar as fichas de riscos e atualizá-las sempre que necessário;

- Implantar os planos de ação necessários para a mitigação dos riscos, envolvendo as demais áreas, em linha com o plano de tratamento aprovado pelo Comitê Executivo de Riscos, Diretoria Colegiada e Conselho de Administração;
- Desenvolver indicadores para monitorar a exposição dos riscos sob sua responsabilidade;
- Realizar periodicamente a revisão técnica do risco, dos seus fatores, da sua criticidade (impacto versus probabilidade) e da resposta, considerando alterações em ações mitigatórias existentes, conclusão dos planos de ação e de contingência e resultados das avaliações dos processos (ambiente de controle) relacionados ao risco; e
- Efetuar reportes periódicos à Gestão de Riscos sobre o acompanhamento do risco sob sua responsabilidade (mudanças significativas na probabilidade e/ou impacto do risco ou em qualquer outra característica e caso identifique riscos não mapeados).

5.7 Auditoria Interna

- Executar ciclos de avaliação e revisões independentes ao processo de gerenciamento de riscos (agentes internos ou externos), com periodicidade anual, de modo a assegurar a eficácia do gerenciamento e do monitoramento dos riscos e reportar à Diretoria e ao Comitê de Auditoria;
- Prestar apoio operacional à Gestão de Riscos; e
- Conhecer o mapa de riscos corporativos e considera-lo no planejamento dos trabalhos de auditoria interna da EMAE.

6. DISPOSIÇÕES FINAIS

Os Administradores devem, anualmente, participar de treinamento sobre a Política de Gestão de Riscos.

A política será anualmente avaliada e revisada ou sempre que demandado pela Gestão de Riscos, Diretoria, Comitê de Auditoria ou Conselho de Administração. As alterações realizadas neste documento deverão ser submetidas para validação pelo Comitê de Auditoria e, posteriormente, para aprovação do Conselho de Administração.

7. REFERÊNCIAS

- Estatuto Social EMAE;
- COSO-ERM: Committee of Sponsoring Organizations of the Treadway Commission (Comitê das Organizações Patrocinadoras - ERM) - *Enterprise Risk Management Framework*;
- ISO 31000;
- Código Brasileiro de Governança Corporativa;

- Lei nº 13.303, de 30 de junho de 2016 (Lei das Estatais);
- Deliberação CODEC nº 02, de 27 de junho de 2018;
- Instrução CVM 552;
- Instrução CVM 586; e
- Regulamento do Novo Mercado.

8. HISTÓRICO DAS ALTERAÇÕES

VERSÃO	DATA DE APROVAÇÃO	DATA DE VIGÊNCIA	DESCRIÇÃO DAS ALTERAÇÕES
03	06/12/2023	06/12/2023	Sem alterações
02	25/10/2022	25/10/2022	Revisão ortográfica e gramatical.
01	08/12/2021	08/12/2021	Inclusão de texto no item 2 aumentando a abrangência da Política.
00	18/03/2020	18/03/2020	Implantação da Política