1. OBJETIVO

A Política de Gestão da EMAE tem como objetivo estabelecer diretrizes para a identificação, avaliação, tratamento, monitoramento e comunicação de riscos, bem como para a implementação de controles internos eficazes. Esta política visa garantir a integridade dos processos operacionais e estratégicos da Companhia, promovendo a mitigação de riscos e a conformidade com as melhores práticas de governança corporativa e sustentabilidade.

2. ABRANGÊNCIA

Esta política se aplica aos membros do Conselho de Administração, diretores, membros do Conselho Fiscal, membros de comitês, empregados, colaboradores, estagiários, prestadores de serviços, fornecedores, parceiros, bem como a todos que atuem em nome da EMAE e suas subsidiárias integrais, direta ou indiretamente.

3. PRINCÍPIOS

A gestão de riscos da Companhia está fundamentada nos seguintes princípios:

- **Responsabilidade e Transparência**: a gestão de riscos deve ser realizada de forma clara e acessível, garantindo que todas as partes envolvidas compreendam os riscos e suas medidas de mitigação.
- **Integridade e Sustentabilidade**: a gestão de riscos deve preservar a integridade operacional da Companhia, alinhando-se aos princípios de sustentabilidade econômica, ambiental e social.
- **Conformidade**: garantir que todas as operações e controles estejam em conformidade com as legislações aplicáveis.

4. DEFINIÇÕES

4.1. Risco

A possibilidade de que um evento ou condição afete negativamente a realização dos objetivos estratégicos, operacionais, financeiros, ambientais ou de conformidade da Companhia.

4.2. Gestão de Riscos

Processo sistemático de identificação, avaliação, tratamento, monitoramento e comunicação dos riscos que possam impactar a Companhia.

4.3. Controle Interno

Conjunto de políticas, processos e práticas implementadas para mitigar riscos, assegurar a

conformidade e promover a eficiência operacional.

5. DIRETRIZES

5.1. Gestão de Riscos Integrada à Governança Corporativa

A gestão de riscos será integrada ao sistema de governança corporativa da Companhia. O Conselho de Administração supervisionará a eficácia da gestão de riscos, assegurando que os mecanismos implementados estejam em consonância com a estratégia e os objetivos organizacionais.

5.2. Identificação e Avaliação de Riscos

A identificação de riscos será realizada continuamente por meio de um processo estruturado que envolva mapeamento de processos, análise de cenários e auditorias. A avaliação dos riscos será conduzida utilizando uma matriz de riscos baseada nos critérios de probabilidade de ocorrência e impacto potencial, conforme recomendado pela ISO 31000:2018 e pelo COSO ERM.

5.3. Controles Internos

Os controles internos serão desenhados e implementados para mitigar os riscos identificados, garantindo a conformidade com as normativas aplicáveis e assegurando a eficiência operacional. Esses controles incluem:

- Controles preventivos: medidas adotadas para evitar a ocorrência de riscos.
- Controles detectivos: mecanismos que permitem a identificação de erros ou irregularidades após sua ocorrência.
- Controles corretivos: ações que visam corrigir as consequências de um risco já materializado.

A eficácia dos controles internos será avaliada periodicamente, garantindo que atendam aos objetivos estratégicos da Companhia e estejam alinhados às boas práticas de mercado.

5.4. Tratamento de Riscos

Os riscos serão tratados com base na criticidade, utilizando as seguintes estratégias:

- Mitigar: implementação de ações para reduzir o impacto e/ou a probabilidade de ocorrência de um risco.
- Transferir: transferência parcial ou total do risco para terceiros, por meio de contratos ou seguros.
- Aceitar: aceitação do risco quando seu impacto for considerado de baixo nível e os custos de mitigação superem os benefícios.
- Evitar: alteração de processos ou atividades para eliminar o risco.

5.5. Monitoramento e Revisão de Riscos e Controles

O monitoramento contínuo dos riscos e dos controles internos será conduzido por meio de auditorias e revisões periódicas. As áreas de riscos e auditoria trabalharão em conjunto para identificar oportunidades de melhoria no sistema de gestão de riscos. O desempenho dos controles internos será avaliado conforme os critérios estabelecidos, assegurando que estejam funcionando conforme o desenho previsto.

5.6. Comunicação e Consulta

A comunicação sobre os riscos e os controles será realizada de forma transparente e contínua. As informações sobre os principais riscos e suas respectivas medidas de controle serão divulgadas às partes interessadas por meio de relatórios periódicos, garantindo a consulta e o feedback dos colaboradores, gestores e conselhos envolvidos no processo.

5.7. Plano de Continuidade de Negócios (PCN)

A EMAE deve manter um Plano de Continuidade de Negócios (PCN) devidamente estruturado e revisado periodicamente, com o objetivo de assegurar a continuidade das atividades críticas da Companhia em situações de crise ou interrupções inesperadas. O PCN deve:

- Identificar as operações e processos críticos para o funcionamento da EMAE;
- Estabelecer estratégias e procedimentos para mitigar impactos e restaurar as operações no menor tempo possível;
- Definir responsabilidades claras para a execução do plano, com a criação de uma equipe de resposta a emergências e crises;
- Incluir medidas de redundância tecnológica, operacionais e de pessoal;
- Promover a realização de testes e simulações periódicas para assegurar a eficácia e a prontidão do plano.

5.8. Plano de Contingência

O Plano de Contingência da EMAE deve detalhar as medidas imediatas a serem adotadas em situações de emergências que ameacem a continuidade das operações. Este plano deve:

- Incluir cenários de risco que possam causar a interrupção das atividades essenciais, como desastres naturais, falhas tecnológicas ou incidentes de segurança;
- Descrever os procedimentos de resposta imediata para proteger ativos críticos, incluindo medidas para garantir a segurança dos colaboradores, do meio ambiente e das instalações;
- Estabelecer mecanismos de comunicação interna e externa para assegurar o fluxo de informações em momentos de crise;
- Garantir a integração com as estratégias de continuidade de negócios e a coordenação com outras áreas da Companhia.

5.9. Revisão e Atualização do Plano de Continuidade e do Plano de Contingência

Ambos os planos devem ser revisados periodicamente e sempre que houver mudanças significativas nos riscos ou nas operações da Companhia. Além disso, devem ser alinhados às melhores práticas de governança corporativa aplicáveis.

6. RESPONSABILIDADES

6.1. Conselho de Administração

- Supervisionar a gestão de riscos e controles internos, assegurando que o sistema esteja integrado à estratégia da Companhia e em conformidade com os princípios de governança corporativa.
- Aprovar, acompanhar periodicamente sua execução, e, em caso de crises ou emergências, garantir uma resposta adequada para os Planos de Continuidade de Negócios (PCN) e dos Planos de Contingência.
- Supervisionar a implementação e a eficácia dos Planos de Continuidade de Negócios (PCN) e dos Planos de Contingência, garantindo que eles sejam alinhados às estratégias de longo prazo da Companhia e em conformidade com as melhores práticas de governança corporativa.

6.2. Comitê de Auditoria

- Revisar e recomendar ao Conselho de Administração as políticas e práticas de gestão de riscos, além de monitorar a eficácia dos controles internos e assegurar a implementação das ações corretivas necessárias.
- Revisar periodicamente a eficácia dos planos de continuidade e contingência, assegurando que as revisões ocorram de maneira regular e que as lições aprendidas em testes e eventos reais sejam incorporadas. Além disso, deve monitorar se os planos estão em conformidade com as regulamentações aplicáveis e as melhores práticas de governança corporativa.

6.3. Diretoria

- Implementar e monitorar a Política de Gestão de Riscos, assegurando que os riscos identificados sejam tratados de acordo com as diretrizes estabelecidas.
- Coordenar o desenvolvimento e a execução do Plano de Continuidade de Negócios e do Plano de Contingência.
- Designar as áreas e os gestores responsáveis pela gestão e implementação dos planos, assegurar que os recursos necessários estejam disponíveis, e garantir que testes e simulações sejam conduzidos regularmente para validar a prontidão dos planos.

6.4. Área de Gestão de Riscos

- Propor diretrizes e coordenar o processo de identificação, avaliação e monitoramento

dos riscos.
- Atualizar a Política de Gestão de Riscos.
- Definir e ajustar o apetite ao risco, em conjunto com o Comitê Executivo de Gestão de Riscos, Comitê de Auditoria e Conselho de Administração.
- Elaborar relatórios regulares sobre os riscos e garantir que os colaboradores envolvidos no processo estejam capacitados na metodologia adotada, além de monitorar e reportar alterações na criticidade dos riscos.
- Coordenar o desenvolvimento e a execução do Plano de Continuidade de Negócios e do Plano de Contingência.
- Identificar e avaliar riscos que possam impactar a continuidade das operações.
- Realizar testes e simulações periódicas, revisar e atualizar os planos, conforme necessário.
- Promover treinamentos para os envolvidos nos Planos de Continuidade de Negócios (PCN) e nos Planos de Contingência.
- Elaborar relatórios e coordenar a comunicação interna e externa durante crises, reportando à Diretoria e ao Conselho de Administração.

6.5. Área de Controle Interno

Responsável por garantir a eficiência dos processos e controles, bem como garantir que os objetivos estratégicos, operacionais, financeiros e de conformidade sejam alcançados, por meio de monitoramento constante dos controles, para garantir seu correto funcionamento, evitando fraudes, erros ou desvios, bem como avaliar riscos e auxiliar a implementação de medidas preventivas. A área busca garantir a conformidade com leis, regulamentos e normas, revisando periodicamente políticas e procedimentos internos, além de implementar mecanismos para prevenir e detectar irregularidades, promovendo a integridade e transparência dentro da EMAE.

6.6. Colaboradores

- Identificar e reportar riscos, além de seguir as políticas e procedimentos de controle interno estabelecidos.
- Tomar conhecimento de suas funções específicas dentro dos Planos de Continuidade de Negócios e Planos de Contingência, especialmente aqueles alocados em áreas críticas da Companhia.
- Participar de treinamentos e estar preparados para executar suas funções no caso de incidentes ou interrupções.

7. REVISÃO

Esta política será revisada anualmente, ou sempre que necessário, para garantir sua conformidade com as melhores práticas de mercado e com a evolução das atividades da Companhia. A melhoria contínua será assegurada por meio de auditorias e revisões periódicas do processo de gestão de riscos e controles internos.

8. REFERÊNCIAS BIBLIOGRÁFICAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO 31000:2018 – Gestão de riscos – Diretrizes**. Rio de Janeiro: ABNT, 2018.

COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION. **COSO Enterprise Risk Management – Integrating with Strategy and Performance**. 2017.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO 22301:2020** – **Segurança e resiliência – Sistemas de gestão de continuidade de negócios – Requisitos**. Rio de Janeiro: ABNT, 2020.