Política de Gestão de Riscos

1. Objetivo

Esta política tem como objetivo estabelecer diretrizes para a gestão de riscos na Tegma Gestão Logística S.A., orientando sobre as práticas necessárias para a identificação, avaliação, tratamento, comunicação e monitoramento dos riscos, contribuindo para a cultura, governança e a preservação de valor da empresa.

2. Abrangência

A Política de Gestão de Riscos é aplicável à TEGMA GESTÃO LOGÍSTICA S/A, incluindo suas empresas controladas, coligadas (no que couber) e que sejam por ela adquiridas ou criadas, todas denominadas simplesmente como “Tegma”, que deverão aderir ao disposto nesta Política, conhecendo-a e contribuindo para sua disseminação e prática.

As empresas que não possuam normativos para esta finalidade devem seguir os preceitos constantes nesta política observando suas respectivas estruturas de gestão.

3. Referências

- **ABNT NBR ISO 31000:2018** – Gestão de Riscos - Diretrizes
- **ABNT NBR ISO/IEC 27005:2023** – Tecnologia da Informação – Técnicas de Segurança – Gestão de Riscos de Segurança da Informação
- **COSO – ERM:** Committee of Sponsoring Organizations of the Treadway Commission – Enterprise Risk Management Framework;
- Modelo das **Três Linhas** do IIA 2020; e
- **IBGC** - Código de Melhores Práticas de Governança Corporativa do Instituto Brasileiro de Governança Corporativa.

4. Definições

- **Análises Qualitativas:** Análise subjetiva a itens que não são passíveis de mensuração quantitativa (métricas). Por vezes um risco é passível de quantificação, mas não deve ser o único viés adotado para análise.

- **Análises Quantitativas:** Análises que podem ser mensuradas correlacionando diretamente a sua exposição ao risco de forma quantitativa (valores, quantidades, etc.), como por exemplo riscos financeiros, de estoques, operacionais e serviços podendo resultar em perdas financeiras diretas, de forma objetiva.

- **Apetite a Risco:** predisposição a tomada de riscos, o quanto a empresa está disposta a aceitar o risco para agregar valor, atingir metas, objetivos preservar e criar valor, estando estes objetivos diretamente relacionados com a sua estratégia corporativa.

- **Área de Gestão de Riscos:** área interna responsável por identificar, avaliar, monitorar e propor estratégias para mitigar os riscos que possam impactar a organização. Atua de forma transversal, apoiando a alta liderança e demais áreas na tomada de decisão, com base em uma visão estruturada dos riscos aos quais a companhia está exposta.

- **Comitê de Auditoria:** órgão não estatutário, sem poder deliberativo ou de gestão, cuja função é assessorar o Conselho de Administração no desempenho de suas atribuições, com foco no acompanhamento e avaliação de riscos, de informações gerenciais e contábeis e de Compliance.

- **Comitê de Gestão, Gente e Governança:** órgão não estutário e de assessoramento ao Conselho de Administração da Companhia, responsável por propor diretrizes e recomendações relacionadas à política de remuneração, estrutura organizacional, práticas de recursos humanos e governança corporativa, em conformidade com as melhores práticas de mercado.

- **Comitê de Riscos**: Órgão de caráter educativo, consultivo, normativo e deliberativo, responsável por supervisionar e alinhar as práticas de gestão de riscos da Tegma reportando-se a Presidência. Atua para garantir que os riscos relevantes sejam adequadamente identificados, avaliados, monitorados e tratados, contribuindo para a tomada de decisões estratégicas, a sustentabilidade dos negócios e a conformidade com normas de governança. Sua estrutura e funcionamento estão descritos em Regimento Interno próprio.

- **Conselho de Administração:** órgão de deliberação colegiada cujas atribuições e poderes se encontram previstos no Estatuto Social e na lei. É de responsabilidade do Conselho de Administração acompanhar os Riscos envolvendo a Companhia e sua respectiva exposição, acompanhando os planos de mitigação e respectivos prazos em linha com o grau de tolerância a risco estabelecido para a adequada continuidade do negócio.

- **Controles Internos:** medidas implementadas (sistêmicas ou não) para mitigar o risco, incluindo políticas, procedimentos, práticas e estruturas que visam reduzir a probabilidade de ocorrência e/ou o impacto de eventos indesejados, além de apoiar o alcance dos objetivos da organização.

- **COSO** *Commitee of Sponsoring Organizations*: entidade sem fins lucrativos criadaem 1985 nos Estados Unidos, formada por representantes de diversas organizações de contabilidade, auditoria e executivos financeiros que, em conjunto, definem modelos conceituais tidos como referência internacional para gerenciamento de riscos corporativos, proporcionando diretrizes para aprimoramento e efetividade dos controles internos e governança corporativa.

- **Dono do Processo (Process Owner):** responsável pelo processo da Companhia. Este colaborador zela pelo ciclo de vida do processo e de seu resultado. Importante ressaltar que o Process Owner é uma atribuição e não um cargo ou função.

- **Dono do Risco (Risk Owner):** diretor responsável por garantir que o risco seja gerenciado adequadamente e por apoiar na definição e implementação dos planos de ação necessários para a remediação e/ ou minimização dos riscos.

- **Fator de Risco:** causas individuais e/ou combinadas com potencial de contribuição para

a eventual materialização de um risco.

- **Gestão de Riscos:** processo conduzido pelo Conselho de Administração, Comitê de Auditoria, Comitê de Gestão, Gente e Governança, Diretoria, Comitê de Riscos, Gestão de Riscos e demais áreas de negócio para identificar, analisar, avaliar, tratar, monitorar e comunicar potenciais eventos ou situações que possam afetar o atingimento dos objetivos e resultados da Companhia.

- **Impacto do Risco**: consequência da materialização de um risco por meio da ocorrência de um fator de risco. O impacto pode ser classificado em 5 níveis (muito baixo, baixo, moderado, alto e extremo) para 6 pilares de riscos (Financeiro, Regulatório, Operacional, Reputacional, ASG e Estratégico).

- **Probabilidade do Risco**: avaliação da chance do risco se materializar considerando o potencial de materialização do risco de acordo com os controles existentes e/ou o histórico e grau de impacto causado pela materialização do risco no passado. A probabilidade é classificada em 5 níveis: Raro, Improvável, Possível, Provável e Quase Certo.

- **Risco:** evento incerto que pode ocorrer quando uma ameaça real ou potencial encontra uma vulnerabilidade ou um conjunto de vulnerabilidades nos Controles Internos. Conforme definição do sistema de gerenciamento de risco do COSO, risco é a possibilidadede ocorrência de um evento, oriunda de fontes internas ou externas, capaz de afetaradversamente o atendimento dos objetivos da Companhia.

- **Tolerância a Risco:** o quanto a companhia tolera/suporta uma exposição em relação ao risco para que esse não lhe impacte no atingimento de suas metas.

5. Diretrizes

As diretrizes de gestão de riscos estabelecidas nesta política foram elaboradas com base em boas práticas atualizadas, alinhadas ao sistema de gerenciamento de riscos proposto pelo COSO.

As diretrizes aqui apresentadas definem e caracterizam as macroetapas do processo de Gestão de Riscos da Companhia, com a finalidade de:

- Fortalecer a Cultura da Gestão de Riscos;
- Definir papéis e responsabilidades;
- Padronizar conceitos e práticas;
- Assegurar o cumprimento dos princípios de governança; e
- Apoiar o atingimento dos objetivos e metas da Tegma e suas controladas.

Sob a gestão da Diretoria Administrativa-Financeira, a área de Gestão de Riscos tem como objetivo identificar possíveis riscos e fatores de riscos de qualquer natureza, levando em consideração os cenários externos e internos, mas não se limitando a, conforme os exemplos a seguir:

- **Financeiros:** Riscos que possam afetar as operações financeiras da Companhia como perda de receita, aumento de custos, multas, despesas que impactem o fluxo de caixa, dentre outros.

- **Regulatórios:** Riscos de sanções legais ou regulatórias, de perda financeira ou de reputação que a Tegma pode sofrer como resultados de falhas no cumprimento da aplicação de leis, normas, acordos, regulamentos, Código de Ética e Conduta, normas e procedimentos internos, dentre outros.

- **Operacionais:** Riscos relevantes nas operações que possam impactar diretamente os negócios da companhia (possíveis perdas de eficiência e eficácia das operações), podendo aumentar a probabilidade de possíveis desvios na estratégia, como interrupções ou lentidão nos processos, acidentes de trabalho, perda de ativos, gargalos logísticos, riscos tecnológicos e/ou relacionados a funcionalidades sistêmicas, dentre outros.

- **Reputacional:** Riscos relacionados à percepção pública e confiança dos *stakeholders*, seja por práticas contínuas ou acidentes e eventos inesperados.

- **ASG (Ambiental, Social e Governança):** Possíveis impactos que a atividade traga ao meio ambiente, decorrentes da atividade do dia a dia ou acidentes, assim como impacto social, governança e ética, observando o que a companhia faz para mitigá-los bem como planos de recuperação caso haja mitigação do risco.

- **Estratégicos:** Riscos associados às decisões estratégicas da alta administração da Companhia que visam atingir seus objetivos de negócios, assegurando a capacidade ou habilidade da Tegma em proteger-se ou adaptar-se às mudanças do ambiente que ela esteja inserida.

A gestão de riscos deve ter interfaces com as áreas de Controles Internos, Gestão de Riscos, Compliance, Segurança da Informaçao, Privacidade de Dados, Controladoria e Auditoria Interna, unindo esforços para a identificação antecipada de riscos e a gestão conservadora e tempestiva.

Os riscos identificados devem ser aprofundados por meio da análise de seus fatores e da avaliação da criticidade (impacto x probabilidade), seguida do estabelecimento de estratégias para seu tratamento e monitoramento. Com base na identificação e avaliação, a área de Gestão de Riscos realizará a análise detalhada e comunicará os riscos aos donos dos riscos. Posteriormente, os riscos serão monitorados e registrados em uma matriz de riscos ou ferramenta equivalente, disponibilizada pela área de Gestão de Riscos, com o objetivo de acompanhar continuamente sua evolução e efetividade das ações adotadas.

Bimestralmente os riscos e suas respectivas tratativas serão apresentados para a Comitê de Riscos, trimestralmente aos Comitês de Auditoria e de Gestão, Gente e Governança, e semestralmente ao Conselho de Administração.

A melhoria contínua do processo de gestão de riscos deve ser alcançada através do monitoramento contínuo, permitindo um gerenciamento dos riscos de forma adequada e o aperfeiçoamento do processo através de ciclos de avaliação e revisão frequentes.

6. Processo de Gestão de Riscos

6.1 Identificação de Riscos

A identificação de riscos deve reconhecer e descrever os principais riscos aos quais a Companhia está exposta, sejam de natureza estratégica ou operacional, considerando as possíveis alterações em seu ambiente de negócios.

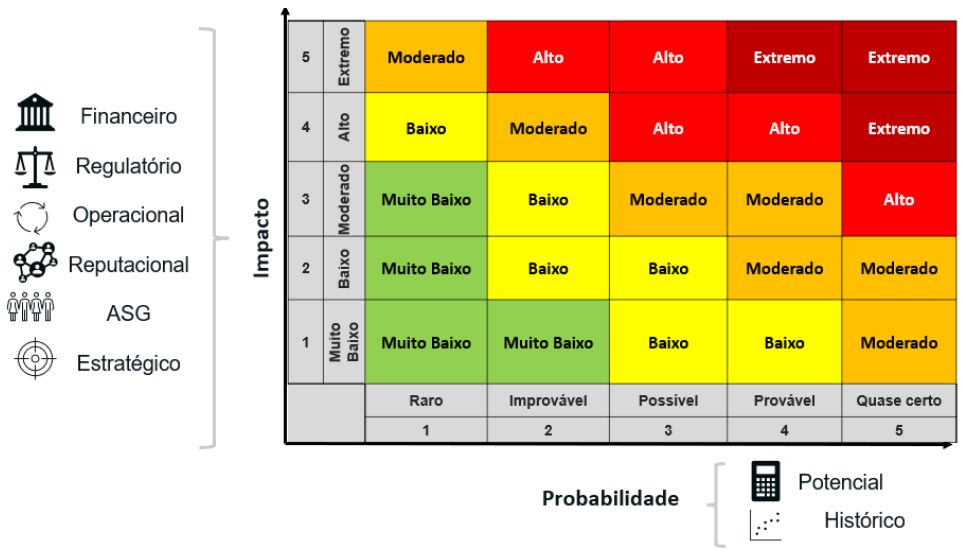
Devem ser identificados os fatores de risco que possam impactar o cumprimento dos objetivos estratégicos da Tegma, independentemente de serem fontes internas ou externas.

Esse processo deve ser conduzido em conjunto com as áreas de negócio e a Diretoria Executiva, com o apoio da área de Gestão de Riscos, responsável por aplicar a metodologia vigente e assegurar a consistência do processo.

6.2 Avaliação dos Riscos

Os riscos serão avaliados levando em consideração seus aspectos quantitativos e qualitativos, bem como ocorrências passadas (histórico), a exposição da companhia, sua quantificação, além da efetividade dos controles internos dentre outras variáveis.

Após tal avaliação serão classificados em um mapa para referência junto aos demais riscos, conforme modelo abaixo:



Cada aspecto de impacto de riscos (financeiro, regulatório, operacional, reputacional, ASG e estratégico) possui uma régua definindo o que são os diferentes níveis de impacto, desde muito baixo até o extremo, assim como uma régua de probabilidade de raro até quase certo, considerando o potencial e histórico. As definições e os critérios aplicáveis estão estabelecidos no documento interno que regulamenta a **Régua de Probabilidade e Impacto**.

O impacto consolidado é calculado com base em metodologia interna da Companhia, que considera a média ponderada para os parâmetros definidos e o peso de cada impacto.

6.3 Tratamento dos Riscos

Com base nos resultados de avaliação, o dono do risco deve definir a estratégia de tratamento, escolhendo uma das opções a seguir:

- Evitar: a estratégia/operação/atividade que gera o fator de risco deverá ser

descontinuada.

- Mitigar: implementar ações para diminuir a probabilidade de ocorrência e/ou o impacto do risco, até um nível aceitável segundo o apetite ao risco da Companhia.

- Conviver/Aceitar: consiste na decisão de manter a exposição ao risco, considerando que:
  i. está alinhada ao apetite de risco da empresa;
  ii. o custo ou esforço para mitigar o risco supera os benefícios esperados; ou
  iii. trata-se de um risco de origem externa, inerente à atividade da Tegma, cuja exposição não pode ser significativamente reduzida.

A decisão de conviver com o risco pressupõe o monitoramento contínuo de sua exposição e dos possíveis impactos.

6.3.1. Planos de Ação

Serão elaborados planos de ação sempre que houver necessidade de medidas corretivas ou preventivas, com foco na melhoria contínua dos controles internos e na mitigação dos riscos.

Os planos de ação para mitigação de riscos serão propostos pelos seus respectivos donos dos processos e deverão ser validados e monitorados pela área de Controles Internos. A aprovação de todos os planos de ação caberá à Diretoria Executiva.

Os riscos e fatores de risco classificados com criticidade extrema ou alta deverão ter seus planos de ação compartilhados com o Comitê de Auditoria ou com o Comitê GGG, conforme a natureza do evento, e comunicados ao Conselho de Administração.

A área de Gestão de Riscos deverá ser informada, de forma tempestiva e estruturada, sobre o andamento e a conclusão dos planos de ação relacionados a riscos com potencial impacto nos objetivos estratégicos da Companhia, garantindo visibilidade e alinhamento com os processos de monitoramento e reporte de riscos.

6.4 Monitoramento dos Riscos

No processo de monitoramento, a área de Gestão de Riscos deve:

- Acompanhar a evolução dos riscos registrados, avaliando mudanças na probabilidade, impacto e nível de exposição;
- Monitorar a efetividade das estratégias de tratamento adotadas, com base nos indicadores de Riscos (KRI's - Key Risk Indicators) e evidências fornecidas pelas áreas responsáveis;
- Alertar tempestivamente alta administração sobre riscos com potencial impacto relevante nos objetivos estratégicos ou no apetite ao risco da Companhia;
- Detectar e registrar riscos emergentes, considerando mudanças no ambiente interno e externo;
- Atualizar periodicamente a matriz de riscos com base nas análises de cenário, novos eventos, desvios ou reavaliações críticas;
- Promover ciclos periódicos de revisão e validação dos riscos junto às áreas e Diretoria.

6.5 Comunicação dos riscos

A comunicação, durante todas as etapas dos processos de gestão de riscos, deve atingir todas as partes interessadas, sendo realizada de maneira clara e objetiva, respeitando as boas práticas de governança corporativa.

7. Papéis e Responsabilidades

A Tegma adota o Modelo das Três Linhas, recomendado pelo Institute of Internal Auditors (IIA), como base para sua estrutura de gerenciamento de riscos. Esse modelo é composto por:

- **Primeira linha de atuação**: Representada pelos diretores, gestores e demais colaboradores das áreas operacionais e administrativas, responsáveis por identificar, avaliar e gerenciar os riscos no desempenho de suas atividades. Também cabe a essa linha implementar e acompanhar os controles internos e executar os planos de ação definidos para a mitigação dos riscos sob sua responsabilidade.

- **Segunda Linha de atuação**: Composta pelas áreas de Gestão de Riscos, Controles Internos, Segurança da Informação, Privacidade de Dados e Compliance, que inclui o Canal de Confidencial como um importante mecanismo de governança. Essas áreas são responsáveis por desenvolver políticas, metodologias e ferramentas de gestão de riscos, oferecer suporte técnico às áreas, promover a cultura de riscos e monitorar a efetividade das práticas adotadas pela primeira linha.

- **Terceira Linha de atuação**: Representada pela Auditoria Interna, que atua de forma independente e objetiva, reportando-se diretamente ao Comitê de Auditoria. É responsável por avaliar a eficácia da estrutura de governança, dos controles internos e do gerenciamento de riscos, abrangendo as atividades da primeira e da segunda linhas.

Além das três linhas, a estrutura de governança da Tegma conta com o suporte da estrutura Conselho de Administração, Comitês e Diretoria Executiva, que exercem papéis fundamentais no processo decisório e no acompanhamento da gestão de riscos.

7.1 Conselho de Administração:

- Aprovar a Política de Gestão de Riscos;
- Aprovar o cronograma de reportes e suas eventuais revisões, mediante proposta da Diretoria Executiva e recomendação do Comitê de Auditoria;
- Determinar o apetite ao risco, com base em proposta da Diretoria Executiva e opinião do Comitê de Auditoria;
- Supervisionar os processos de gestão de riscos, por meio de reportes regulares da Diretoria Executiva, avaliados previamente pelo Comitê de Auditoria, com foco na efetividade do processo e nas respostas aos riscos

7.2 Comitê de Auditoria:

- Acompanhar e avaliar os riscos apresentados pela área de Gestão de Riscos, por meio do Mapa de Riscos da Tegma;
- Avaliar a adequação dos modelos de aferição dos riscos citados no item acima, bem como dos testes de aderência e validação dos modelos utilizados;
- Analisar e opinar sobre as diretrizes e políticas de gestão de riscos, especialmente quanto

à estimativa de perdas financeiras em cenários normais e de estresse;
- Analisar as avaliações independentes anuais do processo de Gestão de Riscos em sintonia com os pareceres da Auditoria Interna e Externa e reportar os resultados e planos de ação ao Conselho de Administração;
- Apoiar na disseminação da cultura de gestão riscos realizada pela área de Gestão de Riscos; e
- Opinar sempre que necessário sobre a Política de Gestão de Riscos e suas atualizações, conforme recomendações da Diretoria Executiva.

7.3 Comitê de Gestão, Gente e Governança

- Assessorar o Conselho de Administração quanto a práticas de governança corporativa que fortaleçam a cultura de gestão de riscos;
- Propor diretrizes de estrutura organizacional e alocação de funções que favoreçam a
- segregação de responsabilidades, o fortalecimento dos controles internos e a eficácia do gerenciamento de riscos;
- Avaliar e recomendar políticas de remuneração e incentivos alinhadas ao apetite ao risco e aos objetivos estratégicos da Companhia;
- Avaliar a adequação dos recursos humanos e financeiros destinados à gestão de riscos, em linha com as recomendações e análises da Diretoria Executiva;
- Promover e apoiar iniciativas voltadas à cultura organizacional e ao comportamento ético, reconhecendo seu impacto na identificação e mitigação de riscos;
- Acompanhar a evolução da maturidade da gestão de riscos sob a ótica de governança e pessoas, propondo melhorias quando necessário;
- Colaborar com os demais comitês e áreas da Companhia na integração dos aspectos de riscos à estratégia, à governança e às práticas de gestão de pessoas;
- Opinar sobre revisões da Política de Gestão de Riscos, principalmente sobre os aspectos relacionados à estrutura organizacional, governança ou cultura corporativa.

7.4 Diretoria Executiva

- Implementar e assegurar a execução da Política de Gestão de Riscos em suas áreas de atuação;
- Garantir a alocação de recursos adequados para a implantação de controles internos eficazes e estratégias de mitigação;
- Promover e incorporar a cultura de gestão de riscos nas operações sob sua responsabilidade;
- Aprovar normas, propor o nível de apetite a riscos específicos em suas respectivas áreas;
- Conhecer e aplicar a régua de impacto e probabilidade, conforme diretrizes corporativas;
- Participar do processo de construção e atualização da matriz de riscos;
- Aprovar a matriz de riscos e indicar os riscos a serem priorizados;
- Gerenciar os riscos inerentes às suas atividades, conforme os critérios de impacto e probabilidade estabelecidos;
- Definir, acompanhar e garantir a implementação de planos de ação e/ou contingência, estabelecendo responsáveis e prazos;
- Aprovar as respostas de tratamento aos riscos;
- Definir e monitorar indicadores-chave de risco (KRIs) para acompanhar a variação e os resultados dos riscos sob sua responsabilidade
- Comunicar à área de Gestão de Riscos a identificação de novos riscos ou eventos

relevantes, bem como sua evolução.

7.5 Gestão de Riscos:

- Coordenar e definir as diretrizes para o processo de gestão integrada de riscos da Tegma, assegurando alinhamento às melhores práticas de mercado e às normas aplicáveis;
- Elaborar e manter atualizada a Política de Gestão de Riscos;
- Elaborar e realizar plano de trabalho, incluindo orçamento, recursos (humanos e tecnológicos) e prazos, a fim de viabilizar a execução do processo de Gestão de Riscos de maneira eficiente;
- Promover a integração do processo de gestão de riscos com o planejamento estratégico da Companhia;
- Disseminar a cultura de gestão de riscos em todas as áreas, garantindo sua compreensão e adoção;
- Elaborar, revisar e propor alterações nos critérios da régua de Impacto e Probabilidade (histórico e potencial), conforme mudanças relevantes no ambiente interno ou externo;
- Estruturar e aplicar treinamentos conceituais e metodológicos sobre gestão de riscos para todos os envolvidos no processo;
- Coordenar, em conjunto com as áreas, o processo de identificação, avaliação, atualização e monitoramento da Matriz e do Mapa de Risco, considerando riscos emergentes e interdependências;
- Monitorar e consolidar os indicadores de risco (KRIs), e emitir reportes periódicos ao Comitê de Riscos;
- Propor revisões da Matriz de Riscos diante de mudanças no planejamento estratégico, em periodicidade mínima anual, ou sempre que ocorrerem mudanças materiais no ambiente da Companhia;
- Comunicar formal e tempestivamente ao Presidente, à Diretoria Administrativo-Financeira, ao Comitê de Auditoria e ao Conselho de Administração sobre riscos e fatores de riscos classificados como altos ou extremos, assim como sobre riscos com endereçamentos em atraso.

7.6 Controles Internos:

- Mapear os processos-chave da Companhia com os respectivos donos, identificando os controles existentes;
- Apoiar na definição, documentação e estruturação dos controles internos;
- Avaliar a eficácia e eficiente dos controles através de aplicação de testes de aderência em relação aos riscos identificados, reportando às áreas responsáveis eventuais falhas ou ausência de controles, e recomendando planos de ação corretivos;
- Monitorar e acompanhar a implementação dos planos de ação;
- Consolidar e reportar periodicamente à Gestão de Riscos, à Presidência, à Diretoria e ao Comitê de Auditoria os resultados dos testes de desenho e efetividade, deficiências identificadas e o status dos planos de ação.

8. Disposições Gerais

Todos os colaboradores da Tegma devem cumprir esta política, comunicando à área de Gestão de Riscos quaisquer riscos ou alterações na exposição aos riscos em suas operações ou áreas corporativas.

Esta política está alinhada às demais políticas da Tegma e pode ser complementada por documentos normativos específicos, desde que respeitem seus princípios e diretrizes.

Devem ser observados os dispositivos legais, regulatórios e acordos jurídicos vigentes aplicáveis ao tema.

Ficam revogados quaisquer documentos ou disposições que contrariem esta política. Casos omissos serão decididos pelo Conselho de Administração da Companhia.

9. Aprovação e Vigência

Esta Política foi revisada e aprovada pelo Conselho de Administração em reunião realizada em 18 de dezembro de 2025 e entra em vigor a partir desta data.