1. OBJETIVO

Estabelecer os princípios e diretrizes gerais que orientam o Processo de Gestão de Riscos na Rumo S.A. ("Rumo ou Companhia"), de forma integrada à estratégia, ao planejamento e à tomada de decisão. Esta política define o posicionamento institucional sobre o tema.

2. APLICAÇÃO E ABRANGÊNCIA

A Política aplica-se a todas as unidades de negócio, processos, sistemas e projetos da Rumo e suas entidades controladas. Sua adoção também é estimulada nas demais entidades nas quais a Rumo detenha participação societária, respeitando os documentos constitutivos e legislações locais aplicáveis.

3. DEFINIÇÕES E SIGLAS

- **Apetite a Risco:** o nível de exposição ao risco que a organização está disposta a aceitar para atingir seus objetivos estratégicos de negócio de curto, médio e longo prazo.
- **COSO:** Modelo de gestão de riscos e controles internos criado pelo Committee of Sponsoring Organizations of the Treadway Commission (COSO), muito usado em compliance e auditoria.
- **ISO 31000:** Norma Internacional que fornece diretrizes para estabelecer a implementação e governança de gestão de risco.
- **Temas Materiais:** São os tópicos ESG mais relevantes para a empresa e seus stakeholders, considerando seu impacto financeiro e estratégico.
- **Tratamento dos riscos:** Conjunto de iniciativas, dentre elas, mas não limitadas a (i) ações mitigatórias, (ii) controles internos, (iii) execução de projetos, (iv) desenvolvimento/aquisição de sistemas ou (vi) criação de documentos normativos, para endereçar a resposta aos riscos.

4. DIRETRIZES E REGRAS

4.1. Aspectos Gerais

A Administração da Companhia reconhece que gerenciar os riscos de maneira eficaz é fundamental para atingir os objetivos de negócio. Por isso, o Processo de Gestão de

Riscos deve ser utilizado como fonte de informação relevante para tomada de decisão estratégica e ser executado de modo a manter a exposição ao risco em níveis compatíveis com o apetite ao risco da Companhia, possibilitando a garantia de seus objetivos e metas. Como base da metodologia e estrutura de gestão, adota, entre outras, as diretrizes da ISO e COSO.

4.2. Processo de Mapeamento e Classificação

É importante que todos os colaboradores da Companhia conheçam a Política de Gestão de Risco e suas respectivas diretrizes para contribuir na identificação e mapeamento dos riscos e seus fatores frente aos objetivos de negócio. Deve ser feita de forma constante e estar integrado à cultura da Companhia.

A classificação dos riscos considera, de forma integrada, aspectos de impacto, probabilidade e capacidade de resposta, refletidos por meio de um score técnico padronizado, promovendo coerência e priorização.

A priorização dos riscos deve considerar também a sensibilidade institucional, temas materiais e alinhamento com o apetite de risco definido pela alta administração.

As ações de tratamento devem ser planejadas em três horizontes: curto (ganhos rápidos), médio (ações com orçamento aprovado) e longo prazo (estruturantes).

Os riscos mapeados podem ser aceitos, mitigados, transferidos ou evitados, conforme critérios definidos nos procedimentos técnicos e a aceitação consciente deve ser formalizada.

4.3 Gestão e Governança

4.3.1 Gestão

A gestão de riscos é um instrumento de governança corporativa, e sua efetividade depende da atuação articulada entre liderança, controles internos e riscos, processos de negócio e cultura organizacional. A estrutura de Gestão de Riscos adota, entre outras, as diretrizes do modelo de três linhas de atuação, sendo:

- 1ª Linha de Atuação: é composta pelas áreas de negócio da Companhia, representada pela Diretoria e Donos de Riscos, responsáveis direto pelos riscos que gerenciam, assim como pelas suas respectivas ações mitigatórias e controles internos associados.

- 2ª. Linha de Atuação: é composta pelas estruturas de Gestão de Riscos, Controles Internos e Compliance da Companhia, que atuam como suporte aos gestores da primeira linha para o correto gerenciamento dos riscos.

- 3ª. Linha de Atuação: é composta pela Auditoria Interna da Companhia, atuando com um olhar independente para verificar a eficácia e conformidade do modelo e reportar suas recomendações aos órgãos de governança competentes.

4.3.2 Governança

Os **Donos de Riscos**, devem identificar, classificar, tratar e monitorar os riscos sob sua responsabilidade, conforme estabelecido no procedimento de gestão de riscos baseado nesta Política.

A **Comissão de Riscos** terá como papel, ser a instância técnica de curadoria, com caráter consultivo, que apoiará a aplicação e consistência metodológica garantindo padronização, coerência das classificações e auxiliar a alta liderança na tomada de decisão e priorização de ações mitigatórias, sem substituir a responsabilidade dos donos de risco.

A **Diretoria Executiva (C-level),** deve revisar e propor apetite ao risco, bem com garantir a aderência do Processo de Gestão de Riscos como parte integrante da estratégia da Companhia durante o ciclo de Planejamento Estratégico.

A Área de **Controles Internos e Riscos**, deve revisar metodologia, orientar e suportar as áreas com ferramentas e metodologia para garantir a correta e oportuna identificação, análise, avaliação de riscos e endereçamento de planos de ação e controles mitigatórios.

O **Comitê de Auditoria,** deve assessorar o Conselho de Administração no monitoramento e recomendação da aprovação dos limites de exposição de risco da Companhia, incluindo o apetite ao risco, e na avaliação dos recursos destinados ao processo de gestão de riscos para desenvolvimento de ações que promovam mitigação dos riscos e ameaças, bem como, recomendar ajustes.

O **Conselho de Administração**, deve aprovar a Política e o apetite ao risco proposto, bem como, acompanhar a sua implementação.

4.3.3 Revisão e Reporte

Conforme cronograma determinado pela Administração, no mínimo anualmente os riscos corporativos são revisados e formalizados na Matriz de Risco Corporativos pela área de Controles Internos e Riscos junto aos Donos do Risco com o objetivo de avaliar mudança na identificação, classificação e no monitoramento das ações implementadas. Com o objetivo de garantir a transparência e rastreabilidade das decisões relacionadas à aceitação, transferência ou mitigação dos riscos. A Matriz de Riscos Corporativos deve ser apresentada ao Comitê de Auditoria para recomendação e aprovação do Conselho de Administração anualmente, conforme determinado no calendário corporativo.

5. DISPOSIÇÕES GERAIS

É importante que todos os Colaboradores (próprios e terceiros) da Companhia, incluindo os seus Administradores conheçam a Política de Gestão de Riscos e suas respectivas diretrizes.

Está política poderá ser contemplada por procedimentos e ferramentas específicas para suportar as orientações operacionais nela estabelecida.

Quaisquer situações decorrentes das informações contidas nesta Política que possam gerar conflitos internos e externos deverão ser comunicadas para área de Controles Internos e Riscos e levadas ao Conselho de Administração da Companhia que definirá as ações corretivas necessárias.

Esta Política entra em vigor na data de sua aprovação e somente poderá ser modificada conforme MDA e por deliberação do Conselho de Administração.

6. HISTÓRICO DE ALTERAÇÕES DO DOCUMENTO

Revisão	Data	Itens Alterados	Elaboradores	Aprovadores
00	29/10/2018	Original	Gerente de Auditoria e Controles Internos (Wagner de Cicco)	Conselho de Administração
01	xx/xx/2025	Revisão Geral	Comissão de Risco	Conselho de Administração