POLÍTICA DE GESTÃO ESTRATÉGICA DE RISCOS DO GRUPO MATEUS S.A

SUMÁRIO

1. OBJETIVO

A presente “Política de Gestão Estratégica de Riscos” (“Política”) que estabelecer princípios, conceitos, regras e responsabilidades na Gestão de Riscos, buscando reduzir os níveis de exposição a perdas da Companhia que possam afetar os seus objetivos estratégicos.

2. ABRANGÊNCIA

Esta Política é aplicável à Companhia e suas controladas, bem como a todos os macroprocessos e negócios do Grupo Mateus. O descumprimento das regras definidas nesta Política está sujeito à aplicação de sanções e medidas disciplinares, em consonância com o Código de Ética e Conduta da Companhia.

3. DIRETRIZES

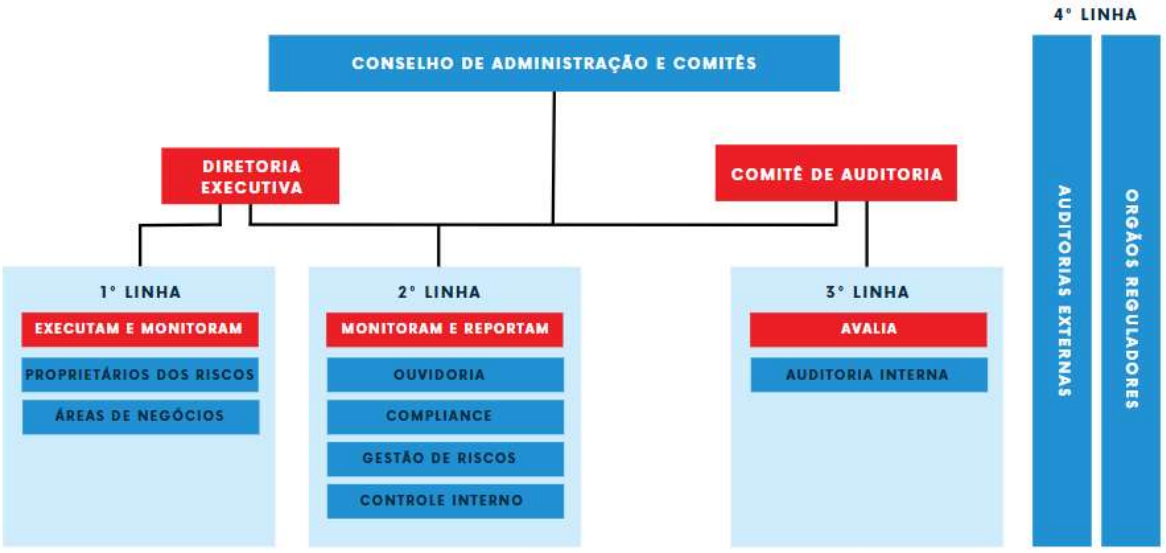
a) A Companhia assume riscos como parte da condução dos negócios. No entanto, se esses riscos não forem devidamente identificados e tratados, podem comprometer sua competitividade e sustentabilidade a longo prazo.

b) Toda decisão envolve algum nível de risco, embora não seja possível eliminá-los completamente, é essencial compreendê-los, avaliá-los e adotar ações de resposta adequadas para minimizar e antecipar possíveis perdas.

c) A estrutura de Governança Corporativa considera a atuação conjunta de todos os envolvidos nas operações possibilitando, de acordo com suas atribuições e funções, identificar, avaliar, tratar e monitorar os Riscos inerentes ao negócio da Companhia.

d) O ambiente de Governança da Companhia é composto pela Auditoria Interna, Ouvidoria, Controles Internos, Gestão de Riscos e Compliance. Estas áreas são responsáveis pelo controle, análise e avaliação da exposição aos riscos, conforme é apresentado na imagem abaixo, com o conceito das 4 linhas dos Auditores Internos do Brasil (IIA):

Figura 01. Modelo de Governança Aplicado pela Companhia



Fonte: Compliance, Riscos e Controles Internos (2025)

O **Modelo das Quatro Linhas** é utilizado para fortalecer o gerenciamento de riscos e os controles internos da Companhia. Essa estrutura distribui responsabilidades entre diferentes níveis, garantindo uma abordagem integrada e eficiente.

- **1ª Linha:** Composta pela alta administração e pelos colaboradores, incluindo empregados, terceiros e estagiários. Esses profissionais são responsáveis por implementar e manter os controles internos durante a execução dos processos sob sua responsabilidade.
- **2ª Linha:** Envolve áreas especializadas, como Ouvidoria, Controles Internos, Gestão de Riscos e Compliance. Seu papel é identificar falhas nos controles existentes e monitorar o cumprimento das políticas e normas internas e externas.
- **3ª Linha:** Representada pela Auditoria Interna, que atua de forma independente e objetiva. Sua função é avaliar a governança, os processos de gerenciamento de riscos e a eficácia dos controles implementados, garantindo que a organização opere com segurança e conformidade.
- **4ª Linha:** Auditoria Externa e os Órgãos Reguladores podem ser considerados uma quarta linha de defesa, pois, além de atuar de forma independente, também reporta à companhia eventuais fragilidades identificadas nos controles internos financeiros. Esse monitoramento contribui para o aprimoramento da governança corporativa, permitindo que a organização implemente melhorias e mitigue riscos que possam comprometer a transparência e a integridade das suas informações financeiras. Esse modelo permite que a Companhia tenha maior transparência e controle sobre suas operações, assegurando a mitigação de riscos e a melhoria contínua da gestão.

4. PAPÉIS E RESPONSABILIDADES

Esta Política define e comunica os papéis e responsabilidades dos principais agentes envolvidos no processo de gestão de Riscos, para a construção e implantação de um modelo que capture as experiências, percepções e os melhores conjuntos de informações disponíveis para a tomada de decisão.

4.1. Conselho de Administração

a) Avaliar e aprovar a matriz de riscos estratégicos, garantindo a priorização adequada dos riscos;
b) Apoiar e acompanhar a gestão dos riscos priorizados nos fóruns de governança;
c) Fortalecer a cultura de riscos dentro da organização;
d) Revisar anualmente a estrutura e o orçamento das áreas de Gestão de Riscos e Auditoria Interna para assegurar sua efetividade;
e) Validar e aprovar as estratégias gerais de Gestão de Riscos;
f) Assegurar ao Comitê de Auditoria autonomia operacional, aprovando um orçamento próprio destinado a cobrir despesas com seu funcionamento; e
g) Receber, por meio do Comitê de Auditoria, o reporte das atividades da Auditoria Interna.

4.2. Comitê de Auditoria

a) Supervisionar as atividades das áreas de Controles Internos, Gestão de Riscos, e Auditoria Interna e Externa da Companhia;
b) Monitorar as exposições de risco da Companhia e garantir a adesão aos limites estabelecidos;
c) Avaliar a adequação dos fóruns de gestão e das diretrizes para o modelo de Gestão de Riscos;
d) Acompanhar os indicadores de risco, alinhados ao contexto de negócios e às diretrizes do Conselho de Administração;
e) Garantir que as atividades de Gestão de Riscos sejam realizadas conforme as legislações aplicáveis, políticas, normas e procedimentos internos;
f) Monitorar os Riscos Priorizados, informando periodicamente o Conselho de Administração sobre as revisões da área de Gestão de Riscos, auxiliando na avaliação dos planos de ação e no cumprimento das recomendações;
g) Aprovar e acompanhar a execução das estratégias de tratamento e monitoramento dos Riscos Priorizados;

h) Avaliar e recomendar melhorias nas políticas internas da Companhia, buscando aprimorar o controle de riscos;
i) Analisar as informações trimestrais, demonstrações intermediárias e demonstrações financeiras da Companhia.

4.3. Diretoria Executiva

a) Fixar a orientação geral dos negócios da Companhia para atender seus objetivos de negócio, de acordo com o Apetite de Risco determinado pelo Conselho de Administração;
b) Auxiliar no desenvolvimento de ações de fortalecimento da cultura de gestão de Riscos, com base no Apetite de Risco aceitável da Companhia;
c) Auxiliar na avaliação periódica da exposição da Companhia a Riscos e da eficácia dos sistemas de gerenciamento de Riscos e controles internos;
d) Implementar as estratégias e diretrizes da Companhia aprovadas pelo Conselho de Administração;
e) Executar a Política de Gerenciamento de Riscos da Companhia e, sempre que necessário, propor eventuais necessidades de revisão;
f) Contribuir para elaboração de relatórios de Riscos da Companhia.

4.4. Área de Negócios e Proprietários dos Riscos

a) Identificar os fatores de riscos e indicadores para a mensuração e monitoramento dos Riscos relacionados aos processos de negócio sob sua responsabilidade;
b) Fornecer informações precisas, íntegras e suficientes para a Modelagem de Riscos;
c) Apresentar percepção quanto à exposição ao Risco (magnitude de impacto e probabilidade de ocorrência), se possível, pautada também em indicadores de mercado;
d) Implementar os planos de ação definidos para tratamento dos Riscos sob sua responsabilidade;
e) Sugerir, avaliar, implantar e monitorar as ações com o objetivo de reduzir a exposição ao Risco sob sua responsabilidade;
f) Cumprir os limites de Riscos aprovados pelo Conselho de Administração;
g) Comunicar tempestivamente a área de Gestão de Riscos os eventos de Risco que apresentarem tendência de ocorrência e/ou eventual extrapolação de limites, para discussão nos fóruns e alçadas apropriadas;
h) Apoiar os responsáveis pelos processos na definição dos planos de ação necessários para tratamento dos Riscos, reportando-os a área de Gestão de Riscos.

4.5. Gestão de Riscos

a) Estabelecer a Política e os Procedimentos de Gestão de Riscos, garantindo um gerenciamento eficaz dos riscos;
b) Promover a adoção de boas práticas no gerenciamento de riscos, alinhadas às necessidades do negócio da Companhia;
c) Implementar treinamentos e campanhas de conscientização para reforçar a importância da Gestão de Riscos;
d) Estabelecer e aprimorar a metodologia de Gestão de Riscos, garantindo sua integração com a estratégia, tática e operações da Companhia, alinhada ao seu Planejamento Estratégico;
e) Oferecer suporte às áreas de negócio no processo de identificação, avaliação, tratamento e monitoramento dos riscos, com foco na redução da exposição aos riscos;
f) Gerenciar a Matriz de Riscos, comunicando regularmente seu status e níveis de exposição nos principais fóruns de gestão;
g) Reportar e informar ao Comitê de Auditoria sobre o status dos riscos significativos de forma tempestiva;
h) Analisar potenciais riscos com base em vulnerabilidades identificadas pelas áreas de negócio, auditoria, segurança, controles internos ou compliance;
i) Notificar os responsáveis sempre que houver variação significativa nos riscos sob sua gestão.

4.6. Ouvidoria

a) Proporcionar um meio seguro, divulgado e confidencial para que colaboradores, parceiros, clientes ou cidadãos possam reportar irregularidades, como fraudes, corrupção, assédio, discriminação, violações éticas ou legais, conforme a **NOR.JUR.003.Canal de Ouvidoria do Grupo Mateus**;
b) Realizar triagem prévia, conforme diretrizes aprovadas classificando as denúncias de acordo com a gravidade e o impacto potencial;
c) Direcionar as denúncias para as áreas competentes para que sejam devidamente investigadas, garantindo imparcialidade e rigor no processo;
d) Acompanhar o andamento das investigações e assegurar que as denúncias sejam tratadas dentro de prazos razoáveis, com respostas adequadas;
e) Implementar medidas para proteger o denunciante de possíveis retaliações, garantindo que ele não sofra consequências negativas por relatar irregularidades;
f) Manter o denunciante informado sobre o status e o resultado da investigação, quando

possível e apropriado, respeitando a confidencialidade; e

g) Elaborar relatórios periódicos com dados sobre as denúncias recebidas, investigadas e resolvidas.

4.7. Compliance

a) Apoiar a identificação e análise de riscos de terceiros, com o objetivo de mitigar riscos como corrupção, fraude, conflitos de interesse e impactos negativos à imagem, garantindo a conformidade com as legislações anticorrupção e antifraude e alinhando-se à matriz de riscos priorizados;

b) Acompanhar as análises de riscos, com base nas classificações de risco estabelecidas.

c) Colaborar na elaboração e revisão de normas, políticas e procedimentos para minimizar a exposição aos riscos do negócio;

d) Apoiar no desenvolvimento de políticas, processos, normas e manuais de procedimentos;

e) Promover a cultura de Compliance, por meio de treinamentos e comunicações, garantindo o cumprimento de legislações, regulamentos e normas internas, e buscando reduzir os riscos identificados.

4.8. Controles Internos

a) Realizar a análise e avaliação dos controles internos, em colaboração com as áreas de negócio, para garantir conformidade com as regulamentações e melhores práticas;

b) Apoiar as equipes na correção de falhas e na execução de ações corretivas, tanto antes quanto após as fases do processo de auditoria, visando a melhoria contínua dos controles;

c) Contribuir na criação e atualização de documentação interna, assegurando que esteja alinhada com as diretrizes do negócio e com as necessidades da organização;

d) Realizar o mapeamento dos processos existentes, avaliar sua conformidade com as políticas internas e adequá-los às melhores práticas de mercado, garantindo eficiência e compliance;

e) Monitorar e gerenciar o acompanhamento das questões identificadas em auditorias externas, auditorias internas, controles internos e gestão de riscos, assegurando a implementação das ações corretivas dentro dos prazos estabelecidos;

f) Colaborar com a equipe de Gestão de Riscos no mapeamento e análise dos riscos contribuindo para a mitigação desses riscos e a garantia da continuidade dos negócios; e

g) Auxiliar as áreas da empresa na identificação de oportunidades de melhoria, fortalecendo os controles internos dos processos e promovendo um ambiente mais seguro e eficiente.

4.9. Gestão da Qualidade

a) Mapeamento dos processos das áreas de negócio, com identificação de riscos potenciais e oportunidades de melhoria, reportando eventuais situações de conflito de interesse à Gerência de Compliance, Riscos e Controles Internos por meio do Canal de Demandas de Compliance, disponível no Jira.
b) Assegurar que os processos das áreas de negócio estejam alinhados aos objetivos estratégicos do Grupo Mateus.
c) Elaboração de políticas, procedimentos, normativas, contribuindo com controles internos voltados à mitigação de riscos operacionais, estratégicos e regulatórios.
d) Apoio nos projetos e processos das áreas de negócio com foco na eficiência operacional e redução de riscos.

4.10. Auditoria Interna

a) Avaliações periódicas para verificar a eficácia dos processos de gestão de riscos, controles internos e governança corporativa, garantindo que estejam alinhados aos objetivos estratégicos e às melhores práticas do mercado;
b) Analisar os processos existentes, identificar lacunas ou ineficiências e propor ações corretivas e preventivas para fortalecer o ambiente de controle interno e a gestão de riscos;
c) Auditar as informações e controles desenvolvidos e monitorados pelas áreas funcionais; e
d) Elaborar e apresentar relatórios regulares ao Comitê de Auditoria (COAUD), órgão ao qual a área de auditoria interna está vinculada funcionalmente, bem como às áreas auditadas. Esses relatórios devem conter avaliações independentes, imparciais e tempestivas sobre a efetividade da Gestão de Riscos na Companhia, destacando pontos de atenção e recomendações para melhoria.

5. PROCESSO GESTÃO DE RISCO

O processo de Gestão de Riscos da Companhia foi estruturado com base nas diretrizes do COSO (Committee of Sponsoring Organizations of the Treadway Commission) e na norma ISO 31000:2018 (Princípios e Diretrizes da Gestão de Riscos) e possui como principal finalidade:

- **Aumentar a probabilidade de realização/alcance das metas estabelecidas pela Companhia:** Garantir que os objetivos estratégicos sejam alcançados de forma consistente, por meio de uma gestão de riscos eficaz e alinhada aos propósitos do negócio.
- **Aprimorar a identificação de oportunidades e ameaças**: Fortalecer a capacidade de

antecipar e responder a cenários favoráveis e desfavoráveis, promovendo a resiliência e a competitividade da organização.

- **Atender às políticas, normas e requisitos legais e regulatórios, padronizando conceitos e práticas**: Assegurar a conformidade com as legislações aplicáveis e as melhores práticas de mercado, promovendo a uniformidade e a consistência nos processos internos.
- **Melhorar o reporte das informações ao mercado, elevando a confiança das partes interessadas**: Garantir transparência e precisão nas informações divulgadas, fortalecendo a credibilidade perante investidores, analistas de mercado, agências de crédito e demais stakeholders.
- **Garantir base confiável de dados para a tomada de decisão e planejamento**: Oferecer um fluxo dinâmico e eficiente de informações, permitindo decisões estratégicas embasadas e a prevenção ou minimização de perdas, com a participação de todos os agentes envolvidos.
- **Alocar e utilizar eficazmente os recursos, melhorando o ambiente de controles**: Otimizar a distribuição e o uso dos recursos disponíveis, fortalecendo os controles internos e promovendo a eficiência operacional.
- **Aperfeiçoar a eficácia e eficiência operacional, aumentando a resiliência das operações da Companhia**: Melhorar continuamente os processos, garantindo que as operações sejam ágeis, resilientes e capazes de se adaptar a mudanças no ambiente de negócios

5.1. Classificação dos Riscos

No processo de análise dos riscos, os riscos inerentes são documentados por meio do Dicionário de Riscos Corporativos, onde são classificados e categorizados em uma linguagem comum, considerando as características do negócio do Grupo Mateus.

O Dicionário de Riscos Corporativos contempla informações segregadas em 5 principais temas, conforme abaixo:

Figura 02. Classificação dos Riscos Aplicado pela Companhia

Fonte: Compliance, Riscos e Controles Internos (2025).

5.2. Etapas de Gestão de Riscos

O processo de Gestão de Riscos leva em consideração a identificação do perfil de exposição e tolerância a riscos (apetite ao risco), por meio da avaliação do ambiente interno e externo. Além disso, está alinhado aos objetivos e diretrizes estratégicos definidos no Plano Estratégico da

Companhia, previamente aprovados pelo Conselho de Administração. Essa abordagem garante que a gestão de riscos esteja integrada à estratégia da organização, promovendo a proteção e a criação de valor para o negócio.

5.2.1. Identificação e Mapeamento

Identificação dos riscos inerentes as atividades da Companhia e suas implicações nos objetivos (metas e resultados) projetados.

A Companhia possui um Dicionário de Riscos inerentes ao seu negócio baseada nos eventos que possam identificar vulnerabilidades e ameaças que coloquem em risco a realização dos objetivos estratégicos da Companhia.

5.2.2. Análise e Quantificação

Definição do impacto e probabilidade de ocorrência dos Riscos sobre os objetivos projetados, fornecendo a base para a avaliação de riscos e para tomada de decisões quanto ao tratamento. Representa o cálculo do nível de exposição da Companhia a determinado risco.

- **PROBABILIDADE:** Chance de materialização do risco considerando o grau de maturidade e eficácia dos controles internos e histórico do risco (se já materializado).

Figura 03. Métricas para definição da probabilidade

Probabilidade	Aspectos
Extrema	As linhas de defesa da Organização são insuficientes para minimizar o risco, em função da ausência de controles chave ou recorrência de problemas.
Alta	As linhas de defesa da Organização são insuficientes para minimizar o risco, em função da ineficácia de controles existentes, ou recorrência de problemas.
Média	Os controles existentes não operam de forma padronizada ou são ineficientes e podem não minimizar o risco.
Baixa	Os controles existentes minimizam o risco.

Probabilidade			
Extremo	Alto	Médio	Baixo
É esperado que o evento ocorra na quase totalidade das circunstâncias	Evento pode ocorrer na maioria das circunstâncias	Evento possui possibilidade razoável de ocorrer	Evento pode ocorrer em circunstâncias raras
Entre 91% e 100%	Entre 51% e 90%	Entre 11% e 50%	Entre 1% e 10%

Fonte: Compliance, Riscos e Controles Internos (2025)

- **IMPACTO:** Análise dos riscos quanto à possível influência nas operações da Companhia (grau de severidade).

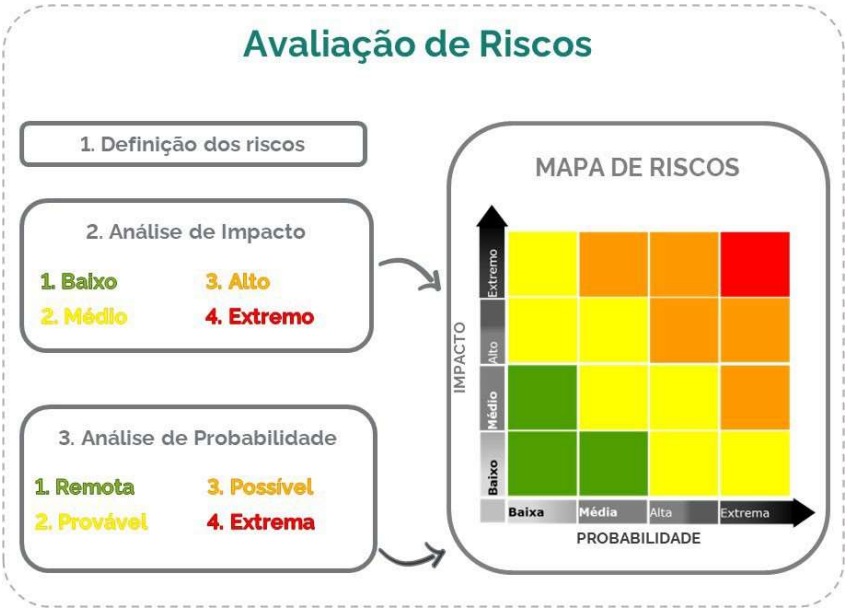
Figura 04. Métricas para definição do impacto

Impacto	Aspectos
Extremo	Impacto financeiro crítico e/ou grave crise de imagem e/ou incapacidade de operar.
Alto	Impacto financeiro muito importante e/ou Alto impacto na imagem e/ou Alto impacto na capacidade de operar.
Médio	Impacto financeiro moderado e/ou impacto moderado na imagem e/ou impacto moderado na capacidade de operar.
Baixo	Impacto financeiro baixo e/ou impacto baixo na imagem e/ou impacto baixo na capacidade de operar.

	Impacto Financeiro			
Ebtida Ajustado (2023)	**Extremo**	**Alto**	**Médio**	**Baixo**
% do Ebtida Ajustado	Acima de 5%	De 2,5% a 5%	De 1,25% a 2,5%	Até 1,25%

Fonte: Compliance, Riscos e Controles Internos (2025)

Figura 05. Modelo de mapa de calor



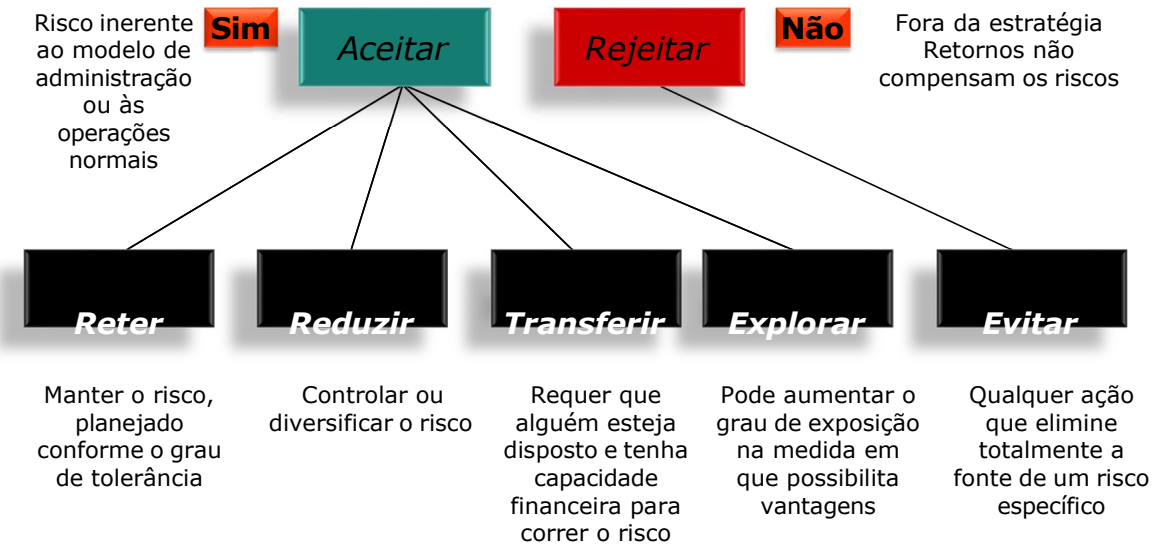
Fonte: Compliance, Riscos e Controles Internos (2025)

5.2.3. Avaliação, Priorização e Tratamento:

Definição de plano de ação e tratamento a ser dado a cada Risco, de acordo com a sua classificação, considerando as Estratégias de Resposta ao Risco.

Recomendação de soluções para mitigar os riscos com o objetivo de reduzir a sua exposição para zona mais adequada.

Figura 06. Métricas para tratamento dos riscos



Fonte: Compliance, Riscos e Controles Internos (2025)

5.2.4. Monitoramento:

Processo de verificação e supervisão da adequação dos controles estabelecidos, executado de forma contínua, a fim de avaliar mudanças de cenário, objetivos e respostas necessárias.

O monitoramento sobre o nível de exposição aos riscos se ocorre através da medição de Indicadores de Riscos (KRI-Key Risk Indicators) que sinalizam de forma preventiva o nível de exposição versus o apetite da Companhia, disparando ações de mitigação sempre que os limites de tolerância forem ultrapassados.

6. VIGÊNCIA

Esta Política está disponível para consulta oficial na plataforma *Pops e Políticas* do Maestro e no site www.ri.grupomateus.com.br. Entra em vigor na data de sua aprovação e somente poderá ser modificada por deliberação do Conselho de Administração da Companhia.

7. DOCUMENTOS DE REFERÊNCIA

Princípios e Diretrizes da Gestão de Riscos ISO 31000:2018

Diretrizes de Governança Corporativa do Estatuto Social da Companhia

Regulamento de Listagem do Novo Mercado da B3 S.A. – Brasil, Bolsa, Balcão CVM

Código de Ética e Conduta do Grupo Mateus-

Benchmarking do mercado, principalmente com relação ao setor

Committee of Sponsoring Organizations of Treadway Commission (COSO-ERM)

8. ANEXOS