# POLÍTICA DE GESTÃO DE RISCOS

# Sumário

## 1. OBJETIVO

Este documento tem por objetivo a implementação e orientação do processo de gestão de riscos do Grupo Mafra ("Grupo Mafra" ou "Grupo"), de forma a permitir a correta e tempestiva identificação de riscos, a avaliação adequada do cenário e a subsequente adoção das medidas cabíveis, bem como a correta comunicação aos responsáveis pela gestão e posterior monitoramento dos riscos encontrados.

## 2. APLICAÇÃO E PÚBLICO ALVO

A presente Política aplica-se a todos os administradores, colaboradores ou quaisquer outros envolvidos em processos internos do Grupo Mafra.

## 3. DEFINIÇÕES

- **Apetite (ou tolerância) a riscos**: grau de exposição a riscos, em sentido amplo, que o Grupo está disposto a tolerar para atingir seus objetivos empresariais

- **Controles**: Ações tomadas pela Administração, Conselhos ou outras partes para gerenciar os riscos e aumentar a probabilidade do atingimento dos objetivos e metas da Companhia. Os controles incluem políticas, regulamentos, procedimentos e métodos utilizados pelo Grupo para mitigar a materialização, o impacto ou a frequência de um risco, de forma a preveni-los, detectá-los e corrigi-los.

- **Gestão de riscos**: Conjunto de medidas práticas para identificar, avaliar, classificar, administrar, comunicar e monitorar os riscos identificados.

- **Partes interessadas**: Sócios, acionistas, clientes, credores, fornecedores de bens e serviços, parceiros externos, comunidades de entorno, autoridades, mídia, formadores de opinião, lideranças empresariais, entidades de classe, ONGs, governos e agentes regulatórios e financiadores que podem afetar ou ser afetados pelas atividades, objetivos ou políticas do Grupo.

- **Plano de Ação**: Conjunto de medidas adotadas para tratar os riscos identificados, de forma a evitar a materialização dos riscos ou reduzir a probabilidade e o impacto dessa materialização, levando esses fatores a níveis compatíveis com o apetite a riscos do "Grupo Mafra". Pode abranger quaisquer áreas da empresa e passar por criação, melhoria e/ou auditoria de processos e controles, utilização de sistemas e instrumentos específicos de identificação e proteção, entre outros.

- **Plano de Contingenciamento**: Conjunto de medidas que devem ser adotadas em caso de materialização do risco, para minimizar as consequências negativas e garantir a continuidade do negócio e das atividades executadas pela Companhia, com a definição dos responsáveis e medidas a serem adotadas.

- **Risco**: Possibilidade de que um evento ocorra e afete adversamente a realização dos objetivos da Companhia. O risco é medido em termos de impacto e probabilidade.

## 4. ESTRUTURA DE GERENCIAMENTO DOS RISCOS

No processo de gerenciamento dos riscos adota-se o modelo dos agentes de defesa, segregado em três linhas, com um papel distinto a ser desempenhado na estrutura de governança:

- **1º linha de defesa**: Gestores das áreas responsáveis pelos processos, riscos e controles inerentes ao negócio;
- **2º linha de defesa**: Área de Controles Internos, que visam suportar a prática da gestão de riscos da Companhia.
- **3º linha de defesa**: Auditoria Interna a qual possui como responsabilidade avaliar de forma independente a eficácia da gestão de riscos e controles da Companhia.


*Gráfico da Declaração de Posicionamento do The IIA* As Três Linhas de Defesa no Gerenciamento Eficaz de Riscos e Controle *publicado em 2013, adaptado da* Guidance on the 8th EU Company Law Directive, *artigo 41, da ECIIA/FERMA*

## 5. DIRETRIZES

O processo de gestão de riscos ocorre em 6 (seis) etapas, conforme descrição a seguir.

### 5.1 Etapas do gerenciamento de riscos

#### 5.1.1. Avaliação do contexto

A estruturação da classificação adequada de riscos passa necessariamente por uma prévia avaliação dos ambientes internos e externos em que as Partes Interessadas estão inseridas.

O ambiente interno é conjunto de fatores controlados pelo Grupo que pode de alguma forma aumentar ou reduzir riscos, ou o impacto de riscos materializados, tais como mas não limitados à existência e observância de processos e controles internos, estrutura de

governança e compliance, políticas, regulamentos e procedimentos, situação econômico-financeira, entre outros.

O ambiente externo é o conjunto de fatores alheios ao Grupo e não controlados por ele que pode de alguma forma aumentar ou reduzir riscos, ou o impacto de riscos materializados, tais como mas não limitados ao contexto político, jurídico, cultural, ambiental, econômico ou social em que o Grupo está inserido, bem como as percepções e valores de terceiros com os quais o Grupo tenha qualquer tipo de relação, comercial ou não.

### 5.1.2. Identificação dos riscos

É necessário que se identifique, formalize e documente, periodicamente e de forma estruturada, os riscos a que o Grupo está sujeito, de forma a permitir o tratamento adequado desses riscos segundo o Plano de Ação estabelecido. Nesse processo, devem ser considerados todos os tipos de riscos, entre os quais:

- **Estratégicos**: Riscos associados à tomada de decisões pela alta administração do Grupo cuja materialização pode gerar perda substancial de valor econômico do Grupo ou de empresa dele integrante, de capital ou de participação de mercado, como consequência de planejamento e/ou decisões falhos, usualmente relacionados a estratégias de negócio/participação no mercado, investimentos, sucessão, inovação e competição;

- **Financeiros**: Riscos cuja materialização possa gerar perdas financeiras para o Grupo ou de empresa dele integrante, prejudicando ou inviabilizando a atividade do Grupo e/ou empresa mediante a redução dos recursos financeiros necessários à realização das atividades da empresa. Envolve, entre outros, os riscos de liquidez, de mercado (riscos decorrentes de variação de preços de ativos e passivos, em razão da variação de taxas de juros, variações cambiais, preço de mercadorias e insumos e outros) e de crédito (não recebimento de valores devidos por terceiros).

- **Regulatórios/legais**: Riscos cuja materialização gere sanções legais ou regulatórias, e possível perda financeira (multas, impedimentos de atuação e outros) e/ou de reputação, decorrentes de descumprimento de leis, acordos, políticas, regulamentos, etc., ou de alterações nas normas pertinentes, previstas ou não, que possam comprometer atividades do Grupo ou de empresa dele integrante.

- **Riscos Operacionais**: Referem-se às possíveis perdas de eficiência e eficácia das operações da organização por razões ligadas à própria infraestrutura do Grupo ou de empresa dele integrante, tais como pessoas, processos, estrutura física e/ou tecnológica.

- **Riscos de imagem/reputação**: Riscos decorrentes de eventos que possam gerar em Partes Interessadas perda de confiança na idoneidade e/ou integridade do Grupo ou de empresa dele integrante, ou na capacidade destes de cumprir com seus compromissos.

- **Riscos socioambientais**: Riscos cuja materialização possa gerar dano ou inviabilização econômica do Grupo ou de empresa dele integrante (ações de reparação, multas, interdição, etc.), em razão de danos ao meio ambiente, pessoas ou regiões onde o Grupo ou empresa dele integrante atue.

### 5.1.3. Análise e avaliação de riscos

Essa etapa envolve a identificação dos riscos, suas causas, possíveis consequências, áreas afetadas e probabilidade de geração efetiva de consequências.

Identificadas essas características, os riscos devem ser priorizados conforme a razão entre i) a probabilidade de concretização do dano num dado intervalo de tempo e ii) o impacto da concretização do risco, assim entendido o dano concreto decorrente da materialização do risco, tal como o valor de indenizações e multas devidos, o impacto dessas no fluxo de caixa, o impacto no meio ambiente, o eventual dano à imagem/reputação (e suas consequências financeiras) etc.

### 5.1.4. Tratamento dos riscos e determinação do Plano de Ação

O tratamento dos riscos identificados nas atividades desempenhadas pelo Grupo será priorizado conforme criticidade.

O tratamento de riscos é responsabilidade da 1° linha de defesa, cabendo às áreas de negócio o gerenciamento dos riscos, de forma que quando identificado um novo risco que não esteja coberto por controles que mitiguem a sua materialização, esse risco deverá ser reportado para a área de Controles Internos para adoção de medidas que configurem o seu gerenciamento para adequá-los ao apetite a riscos do Grupo, conforme alternativas a seguir1:

- **Evitar**: Não correr os riscos, determinando a descontinuação das atividades que os geram, sejam eles decorrentes da produção de um bem específico, da manutenção de uma linha de negócios ou de processos da empresa. Essa alternativa deve ser aplicada quando não houver alternativa viável ou suficiente para reduzir o impacto ou a probabilidade de ocorrência de risco que possa ter consequências relevantes e /ou irreversíveis, justificando a descontinuação;

- **Aceitar**: Não adotar nenhuma providência para reduzir a probabilidade ou o impacto do risco. Essa alternativa deve ser aplicada quando o custo do gerenciamento/mitigação não compensar, se comparado com o impacto possível. Nesse caso, o risco deverá ser monitorado continuamente, para garantir novo tratamento adequado caso haja mudança na situação que possa aumentar o impacto e/ou probabilidade do risco – gerando alteração de sua criticidade;

- **Reduzir**: Determinar medidas para reduzir a probabilidade de concretização do risco e/ou seu impacto em caso de concretização. Essa alternativa deve ser

1As alternativas aqui listadas são adaptações do Enterprise Risk Management Framework do COSO (Committee of Sponsoring Organizations of the Treadway Commission) COSO é formado por representantes da American Accounting Association, American Institute of Certified Public Accountants, Financial Executives Internationl, Institute of Managements Accountants e pelo Institute of Internal Auditors, ao qual está ligado a AUDIBRA – Instituto dos Auditores Internos do Brasil, através da FLAI – Federação latino-americana de Auditores Internos

aplicada quando a redução da probabilidade ou do impacto forem suficientes para tornar o risco assumível, segundo o apetite a riscos do Grupo;

- **Compartilhar**: Determinar medidas para reduzir a probabilidade de concretização do risco e/ou seu impacto em caso de concretização mediante transferência e/ou compartilhamento de parte do risco por meio de seguros, hedge, associações, terceirização de atividades e outros.

Após determinar em conjunto com as áreas responsáveis e/ou afetadas as estratégias de tratamento a serem adotadas, o Plano de Ação será documentado e comunicado às áreas envolvidas, para assegurar a efetivação tempestiva das medidas determinadas.

A área de Controles Internos irá dar suporte às áreas na elaboração dos Planos de Ação que corrigem as falhas de controle identificadas na causa raiz e mitigam os riscos afetados.

> **IMPORTANTE**: Em caso de identificação de risco prioritário, conforme Mapa de Riscos, deve ser elaborado preventivamente Plano de Contingenciamento a ser adotado caso concretizado o risco, que não deve se limitar ao contingenciamento financeiro, mas sim abranger todas as medidas cabíveis em todas as esferas.

### 5.1.5. Monitoramento de riscos

O monitoramento de riscos é o acompanhamento dos riscos identificados e priorizados e da efetividade da implementação dos processos de gestão de riscos do Grupo e das medidas de tratamento de riscos determinadas.

O monitoramento deve ser realizado pela 1° linha de defesa, buscando avaliar de forma continua a eficácia de seus controles e melhoria no gerenciamento de seus riscos. A área de Controles Internos (2º linha de defesa) apoiará as áreas de negócio no monitoramento dos riscos, com o objetivo de contribuir para o atingimento dos objetivos e metas da companhia.

### 5.1.6. Comunicação dos riscos

Os riscos devem ser comunicados de forma clara e objetiva, com todas as informações relevantes possíveis, a todas as partes afetadas e/ou responsáveis, e, principalmente, às responsáveis pela determinação e efetivação das medidas de tratamento de riscos.

Igualmente, uma vez determinadas as medidas a serem adotadas para tratamento dos riscos, essas deverão ser comunicadas de forma precisa e célere às áreas responsáveis pela implementação das medidas determinadas.

## 6. PAPÉIS E RESPONSABILIDADES

**Compete ao Conselho de Administração:**

- Aprovar a Política de Gerenciamento de Riscos da Companhia e futuras alterações, conforme necessário;
- Aprovar o Apetite e Mapa de Riscos da Companhia;

**Compete ao Comitê de Auditoria, Gestão do Risco, Compliance e de Recursos Humanos:**

- Recomendar a aprovação a Política de Gerenciamento de Riscos da Companhia e futuras alterações, conforme necessário;
- Recomendar a aprovação do Apetite e Mapa de Riscos da Companhia;
- Manifestar-se sobre as sugestões de alteração da estrutura operacional de gerenciamento de Riscos e aprovar eventuais sugestões de alterações, caso entenda necessário.
- Garantir a implementação da Política, com suas estratégias e diretrizes, conforme aprovadas pelo Conselho de Administração;
- Manter o Conselho de Administração atualizado sobre monitoramento e exposição a riscos;

**1º linha de defesa (gestores de processo):**

- Gerir os riscos inerentes aos processos sob sua responsabilidade a partir da identificação, avaliação, monitoramento e tratamentos aos riscos, com a participação das demais áreas a serem envolvidas, conforme divisão de competências aqui estabelecida;
- Reportar tempestivamente as informações à 2º linha (área de Controles Internos) sobre os riscos inerentes ao processo que ainda não estejam cobertos por controles que mitiguem sua probabilidade de ocorrência e/ou impacto.
- Implementar e monitorar seus planos de ação para tratamento das deficiências identificadas em seus respectivos processos.
- Reportar a ocorrência de materialização dos riscos para a 2º linha (área de Controles Internos) de imediato para tratamento elaboração dos Planos de Ação.

**2º linha de defesa (Área de Controles Internos):**

- Suportar a 1º linha no gerenciamento dos riscos inerentes aos negócios da Companhia;
- Manter a Política de Gerenciamento de Riscos da Companhia atualizada;
- Avaliar vulnerabilidade do ambiente de controles dos processos da Companhia através dos testes de efetividade;
- Monitorar a implementação dos planos de ação para as falhas identificadas;
- Realizar a asseguração da implementação dos planos de ação para as falhas identificadas (Follow-up);
- Elaborar o relatório de consolidação de riscos e reportá-los periodicamente ao Comitê de Auditoria, Gestão do Risco, Compliance e de Recursos Humanos.

## 7. APROVAÇÕES

| Elaboração | Revisão | Aprovação |
|---|---|---|
| Controles Internos; e<br>Jurídico. | Maio de 2021 | Comitê de Auditoria, Gestão do Risco, Compliance e de Recursos Humanos; e<br><br>Conselho de Administração |

## ANEXO I - Declaração de ciência e concordância

# TERMO DE COMPROMISSO

Eu, _____, inscrito no CPF sob o nº _____, portador do RG nº _____, declaro que obtive acesso a Política de Gestão de Risco do Grupo Mafra e estou ciente de todos os seus termos, com os quais tenho total concordância e me comprometo a cumpri-los durante a minha prestação de serviços para qualquer empresa que componha o Grupo Mafra.

Declaro estar ciente de que eventual violação de minha parte a qualquer regra estabelecida nessa política, poderá culminar na aplicação de sanções com base no Código de Conduta, sem prejuízo de eventuais sanções legais.

Por ser verdade, assino o presente termo.

Local/data:_____

_____

Assinatura