Política de Gestão de Riscos

Sumário

1.Área Responsável pelo Documento

Auditoria, Riscos e *Compliance*

2.Aprovações e Controle de Revisão

Revisão	Data	Elaborador	Revisor	Aprovador	Descrição das Alterações
01	30/04/2020	Mario Filipini	Sergio Kariya	REDIR/ CAFIR/ CA	Emissão Inicial
02	25/09/2023	Gerente de *Compliance*	CAFIR	CA	Revisão Geral
03	01/12/2025	Gerente de Compliance e Riscos	Presidência	CAFIR/CA	Revisão Geral

Tabela 1 – Aprovações e Controle de Revisão

3.Objetivo

Esta Política tem como objetivo orientar e estabelecer diretrizes e responsabilidades relacionadas ao processo de gestão de riscos, através da identificação, análise, priorização, tratamento e monitoramento dos riscos empresariais que possam vir a afetar os negócios da Companhia.

Adicionalmente, busca fornecer informações para apoiar o processo decisório dos negócios, baseado nos riscos empresariais, com o objetivo de apoiar o plano estratégico, na geração de valor e no crescimento sustentável da Companhia.

4.Aplicação e Público-alvo

Esta política abrange a Mills Locação, Serviços e Logística S.A, suas controladas e unidades de negócio que, direta ou indiretamente, participam do processo de Gestão de Riscos.

5.Definições

Gestão de Riscos: Avaliação e gerenciamento de incertezas que podem afetar a Companhia por meio de um enfoque estruturado de controles que alinha estratégia, processos, pessoas, tecnologia e conhecimentos, objetivando a preservação e criação de valores aos stakeholders.

Riscos: Fatores ou eventos incertos que podem causar impactos, no atingimento dos objetivos da empresa.

Controles Internos: Métodos e/ou medidas incluindo políticas, normas, procedimentos ou instruções de trabalhos adotados pela Companhia com o objetivo de salvaguardar seus ativos, adequar e suportar os dados contábeis, promover a eficiência operacional e encorajar a aderência às políticas definidas pela Companhia.

Risk Owner: Responsável por garantir que o risco seja gerenciado adequadamente e por atuar na definição e implementação dos planos de ação necessários para a mitigação dos riscos.

Apetite ao Risco: Tipo (e proporção) de riscos que uma organização está preparada, disposta a assumir e gerenciar para atingir seus objetivos, de acordo com os limites estabelecidos pelo Conselho de Administração.

Evento: Ocorrência ou alteração em um conjunto específico de circunstâncias. Os eventos podem ser de origem interna ou externa à Companhia.

Riscos prioritários: Grupo de riscos com impacto e probabilidade potencialmente elevados para o negócio. Estes riscos devem ter gestão priorizada, indicadores adequadamente estabelecidos e devem ser monitorados e sempre reportados ao CA e ao CAFIR.

Tipos de Riscos: Existem diversos entendimentos sobre as tipificações de riscos empresariais, sendo considerados como mais comuns, os de natureza, Financeira, Operacional, Estratégicos e de Conformidade ou *Compliance*.

Tratamento dos Riscos: Ações específicas para cada risco identificado. Estas ações podem ser através da eliminação, diminuição, transferência ou ainda aceite dos riscos.

Key Risk Indicator (KRI): Indicadores de riscos chaves da Companhia. Os KRI's são componentes fundamentais de uma estrutura de controle e das boas práticas de gestão de risco.

Impacto: Classificação da extensão que a Companhia pode estar exposta ou desprotegida com relação aos eventos negativos e seus efeitos, podendo ser de ordem tangível ou intangível (ex. cultura e imagem).

Probabilidade: Classificação da possibilidade de materialização do risco considerando a atual estrutura de controles da Companhia. Em algumas metodologias também utilizam a expressão vulnerabilidade para definir a possibilidade de materialização dos riscos.

Matriz de Riscos: Representação gráfica de exposição do impacto versus probabilidade dos riscos identificados pela Companhia.

COSO - Gerenciamento de Riscos: *"Committee of Sponsoring Organizations of the Treadway Commission (COSO). Internal Control – Integrated".* Comissão que estabelece o principal framework, considerado como referência, para a gestão de riscos empresariais e controles internos.

REDIR: Reunião de Diretoria. Esta reunião deve ter o tema gestão de riscos com periodicidade pré-estabelecida ou sempre que necessário em função de eventos que afetem os negócios de maneira relevante.

CAFIR: Comitê de Auditoria, Finanças e Riscos, que é um órgão de assessoramento vinculado diretamente ao Conselho de Administração. Este comitê deve ter o tema gestão de riscos em sua pauta com periodicidade pré-estabelecida ou sempre que necessário em função de eventos que afetem os negócios de maneira relevante.

CE: Comite de Ética e Integridade, órgão de assessoramento vinculado ao CAFIR.

RCA: É a reunião do Conselho de Administração. O conselho deve ter o tema gestão de riscos em sua pauta com periodicidade pré-estabelecida ou sempre que necessário em função de eventos que afetem os negócios de maneira relevante.

6.Papéis e Responsabilidades

6.1 Conselho de Administração

- Aprovar a Política de Gestão de Riscos da Companhia;
- Monitorar periodicamente (ao menos uma vez ao ano), e com apoio do CAFIR e do Gerente de Riscos e *Compliance*, os riscos prioritários aos quais Companhia estiver exposta, acompanhando a evolução dos riscos de maior probabilidade e impacto e seus respectivos planos de ação; e
- Estabelecer parâmetros de apetite aos riscos, definindo quais os riscos que a Companhia está disposta a correr e considerando quais níveis máximos de exposição.

6.2 Comitê de Auditoria, Finanças e Riscos

- Aprovar a metodologia a ser utilizada para condução do processo de gestão de riscos da Companhia;
- Acompanhar de forma sistemática a gestão de riscos com o objetivo de apoiar o cumprimento de seus objetivos;

- Apoiar o Conselho de Administração em relação a comunicação sobre os riscos de maior relevância;
- Acompanhar e avaliar periodicamente (ao menos uma vez ao ano) os riscos da Companhia;
- Analisar e opinar sobre as diretrizes e políticas de gestão de riscos empresariais, principalmente na estimativa de impacto financeiro, reputacional e de *compliance;*
- Avaliar a adequação dos recursos humanos e financeiros destinados à gestão de riscos; e
- Apoiar a Área de Riscos e *Compliance* na implementação do processo de gestão de riscos.

6.3 CEO e Diretores

- Acompanhar os riscos priorizados;
- Avaliar os relatórios e resultados e prover os direcionamentos apropriados no processo de gestão de riscos;
- Patrocinar a implantação da gestão de riscos em suas respectivas áreas;
- Gerenciar os riscos inerentes às suas atividades (identificar, avaliar, reportar, monitorar e tratar);
- Definir e acompanhar os planos de ação/mitigação para redução da exposição ao risco, assim como definir o responsável e data da implantação do plano;
- Garantir que os controles internos funcionem adequadamente de forma a mitigar ou evitar a exposição à riscos; e
- Informar à Área de Riscos e *Compliance* sobre a identificação de novos riscos ou eventos que sejam relevantes e suas respectivas evoluções.

6.4 Gestor de Riscos e *Compliance*

- Realizar a análise de risco periodicamente (ao menos uma vez ao ano) e elaborar os respectivos planos de ação de mitigação;
- Coordenar as atividades de gestão de riscos, apoiando todos os envolvidos na implementação das atividades descritas nesta política;

- Buscar constantemente que a Companhia utilize boas práticas de mercado a exemplo do que que estabelece o COSO, norma ISO 31000 sobre os Princípios e Diretrizes da Gestão de Riscos e/ou outros frameworks de referência para esta atividade;
- Monitorar os riscos empresariais e os respectivos planos de mitigação;
- Realizar os ciclos de Avaliação, conforme fluxograma disposto no item 7.2;
- Interagir com a área de Auditoria Interna, informando a evolução dos principais e apoiando na definição do Plano Anual de Auditoria Interna;
- Realizar os testes de efetividade dos principais controles internos e reportar resultados com recomendações de melhorias nos controles;
- Apoiar o CA e CAFIR, mantendo-os atualizados (ao menos uma vez ao ano) sobre os principais riscos empresariais, através de reuniões formais e periódicas e ou esporádicas sempre que necessário;
- Apoiar o processo de identificação, monitoramento dos riscos e seus respectivos planos de mitigação;
- Realizar a consolidação dos riscos; e
- Disseminar a cultura de gerenciamento de riscos e controles internos na Companhia.

6.5 *"Risk Owner"*

- Responsáveis pela identificação, elaboração de planos de mitigação e tratamento dos riscos; e
- Responsáveis pela eficácia dos controles internos relacionados aos riscos sob sua responsabilidade.

7.Diretrizes

As diretrizes aqui apresentadas definem as principais (de forma macro) etapas do processo de Gestão de Riscos Empresariais da Companhia, a saber:

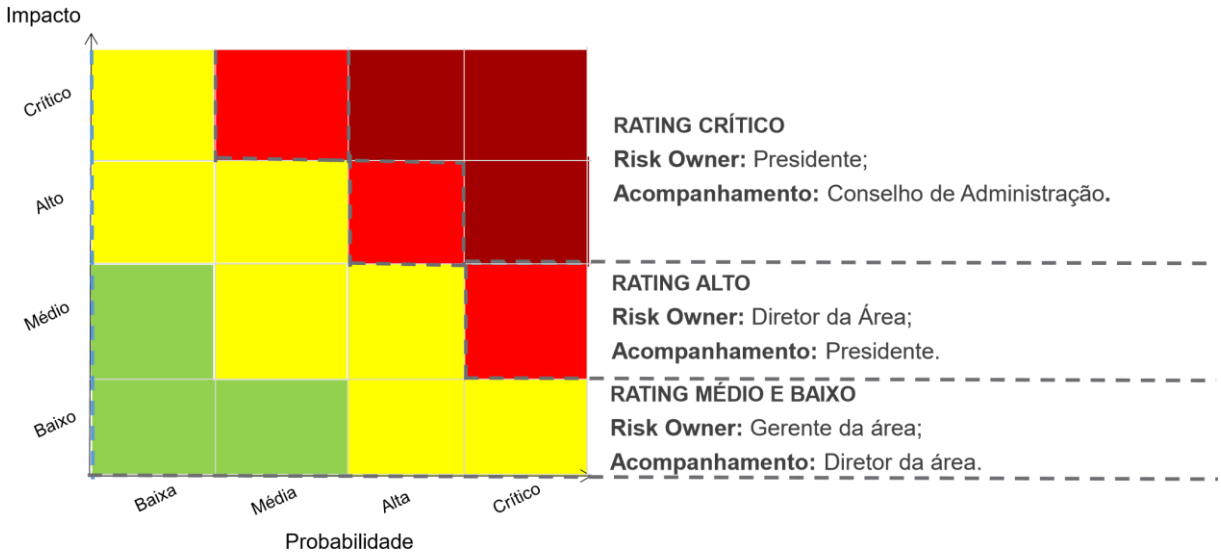
- Fortalecer a Cultura da Gestão de Riscos Empresariais.
- Definir papéis e responsabilidades.
- Padronizar conceitos e práticas.
- Assegurar que os princípios da governança e controles internos sejam seguidos; e

- Possibilitar o alcance dos objetivos e metas da Companhia.

7.1 Matriz de Riscos / Classificação

O processo de Gestão de Risco resultará na Matriz de Risco abaixo. A classificação dos Riscos identificados é produto da relação de Impacto e Probabilidade.

Sua elaboração e atualização depende da realização periódica dos ciclos de avaliação, conforme item 7.2.



Legenda:

Baixo **Alto**

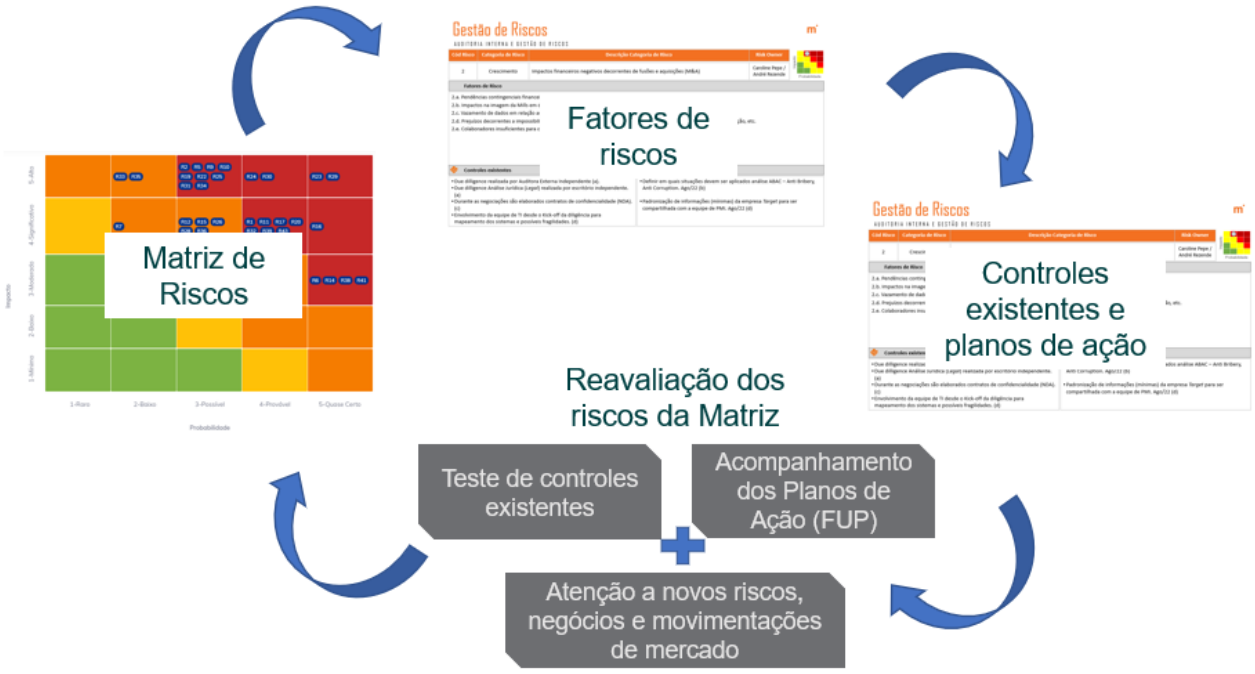
Médio **Muito Alto**

7.2 Ciclos de Avaliação

Os ciclos de avaliação dividem-se em:

(i) identificar e atualizar os riscos e respectivos fatores de riscos, bem como os controles capazes de mitigar ou evitar os riscos e respectivos planos de ação; e

(ii) realizar os testes de efetividade dos controles reportados no ciclo (i), reportar e recomendar melhorias e atualizar a matriz de riscos conforme resultados dos testes de efetividade, como segue:



Os ciclos de avaliação serão realizados periodicamente, ao menos, uma vez por ano ou em períodos menores, a depender das características do risco identificado.

8.Prevenção a Fraude, Suborno e Corrupção

A Mills está comprometida com o cumprimento de todo o conteúdo da Lei Anticorrupção 12.846/13 e do Decreto nº 11.129/22, além de todas as leis e as regulamentações aplicáveis em vigor, relacionadas ao combate à prática de suborno e corrupção. A Mills exige que todos os seus administradores, colaboradores e prestadores de serviço conduzam todas as suas atividades com integridade e nos mais elevados padrões éticos.

9.Sanções e Penalidades

O cumprimento deste normativo é exigido a todo o público-alvo definido acima, a violação e a não observância aos preceitos nela descrita, pode acarretar a aplicação de medidas disciplinares conforme a Política de Consequência ou conforme deliberação do Comitê de Ética e Integridade.

10. Referências

Estatuto da Mills.

Regulamento do Novo Mercado – B3	A companhia possui ações listadas na Bolsa de valores (B3) Novo Mercado, logo, segue o respectivo regulamento que versa sobre a adoção da área de Gestão de Riscos, bem como a estruturação de sua política.
COSO – *"Committee of Sponsoring Organizations of the Treadway Commission"*	Comissão que estabelece o principal framework, considerado como referência, para a gestão de riscos empresariais e controles internos.

11. Anexos

PR- ARC – 002 – Procedimento da área de Auditoria, Riscos e Compliance.

12. Aprovação e Vigência

Esta Política de Gestão de Riscos, foi elaborada em 30 de abril de 2020, pela Área de Riscos e *Compliance* e tem a vigência a partir da data de sua publicação e de suas revisões devidamente aprovadas pelas alçadas competentes. E será revisado periodicamente, sendo passível de alteração ou atualização sempre que constatada a sua necessidade.

As eventuais omissões e as dúvidas de interpretação do conteúdo deste documento, serão objeto de análise e decisão do Aprovador.

***