MELNICK DESENVOLVIMENTO IMOBILIÁRIO S.A.
Companhia Aberta
CNPJ/ME nº12.181.987/0001-77

POLÍTICA DE GESTÃO DE RISCOS

(Aprovada em Reunião do Conselho de Administração realizada em 21/12/2021)

1. OBJETIVO

Estabelecer diretrizes e responsabilidades relacionadas a Gestão de Riscos, evidenciar a metodologia utilizada para a identificação, avaliação e monitoramento dos riscos potenciais nos negócios, visando a redução da probabilidade e/ou impacto de perdas, minimizando a um nível aceitável conforme o apetite a risco da Companhia para a preservação e crescimento de valor para a empresa.

2. CAMPO DE APLICAÇÃO

Esta Política é aplicada a todos os colaboradores da empresa, do estagiário ao Presidente, temporários ou não, bem como todas as empresas controladas, integral ou parcialmente, além dos membros do Conselho de Administração, dos Comitês e da Diretoria.

3. ESTRUTURA

A estrutura do gerenciamento de riscos da empresa se baseia no Modelo das Três Linhas, conforme figura abaixo, onde estão descritos papéis e responsabilidades de cada linha.

- **1ª linha (áreas de negócio):** Os gestores são responsáveis por gerenciar os riscos de sua área e ter propriedade sobre eles.

- **2ª linha (Gestão de Riscos, Controles Internos e Compliance):** Tem como objetivo apoiar a primeira linha, para que cumpram com suas responsabilidades, realizando o monitoramento dos riscos, fornecendo conhecimento e ferramentas adequadas para este processo.
- **3ª linha (Auditoria Interna):** Tem como objetivo uma avaliação objetiva e independente da gestão dos riscos, controles e governança da organização.

4. PROCEDIMENTOS

- A Gestão de Riscos na Companhia deve se basear na missão, visão e valores, de modo a propagar a compreensão do tema para todos os colaboradores;
- O assunto Gestão de Riscos deve ser apoiado e promovido pelo *Board* da Companhia (Conselho, Comitês e Diretoria) para todos os níveis hierárquicos, de modo a difundir a importância do tema e, consequentemente, a aderência às diretrizes e processos;
- O tema Gestão de Riscos deve estar presente em todos os processos de gestão, controles internos e auditoria interna, promovendo a identificação antecipada dos riscos e a gestão tempestiva;
- O processo de Gestão de Riscos exige o aperfeiçoamento contínuo e, caso necessário, deverá ser revisado quando da ocorrência de eventos relevantes.
- O processo de gestão de riscos é pautado em metologias internacionais, tais como ISO 31.000:2018, COSO ERM e IIA, sendo pautado nas seguintes etapas:

Adaptado da ISO 31.000:2018

4.1. Estabelecimento do contexto

Refere-se ao estudo e entendimento do (i) ambiente interno, baseado em seu Planejamento Estratégico e seus objetivos, e do (ii) ambiente externo, associadas ao ambiente macroeconômico, político, social, natural e/ou setorial em que a Companhia opera.

4.2. Identificação dos riscos

Os riscos aos quais a Companhia está exposta devem ser identificados/ revisitados anualmente (ou na ocorrência de eventos significativos ao planejamento estratégico) ou, em não tendo ocorrido eventos significativos, devem ser revisitados anualmente e ser devidamente formalizados, para posterior acompanhamento e tratamento.

4.3. Análise dos riscos

Os riscos devem ser categorizados conforme as naturezas possíveis, à saber: Estratégico, Conformidade, Financeiro,

Operacional e Cyber. A Gerência Riscos e Compliance, em conjunto com a Diretoria Executiva Financeira e Presidência, devem analisá-los a fim de verificar a existência desses riscos.

Deve ser avaliada quais esferas de impacto e probabilidade para posterior avaliação dos riscos da Companhia.

4.3.1 Esferas de Impacto

A área de Riscos e Compliance deverá estruturar a **régua de Impacto** com base nos vetores qualitativos e quantitativos para que seja realizada a devida avaliação e classificação do efeito dos riscos, caso estes se materializem.

- **Critério qualitativo:** Imagem & Reputação, Saúde & Segurança, Compliance.

Os vetores qualitativos devem ser elaborados de acordo com os principais valores da Companhia e suas principais preocupações, além das informações extraídas do Planejamento Estratégico e do conhecimento dos gestores acerca do negócio

- **Critério quantitativo:** Financeiro.

O vetor quantitativo deve ser estabelecidos com base no valor calculado do Apetite a Risco, que será fracionado entre as escalas de impacto.

O impacto do risco pode ser classificado em 4 escalas, sendo elas: **muito alto, alto, médio e baixo**.

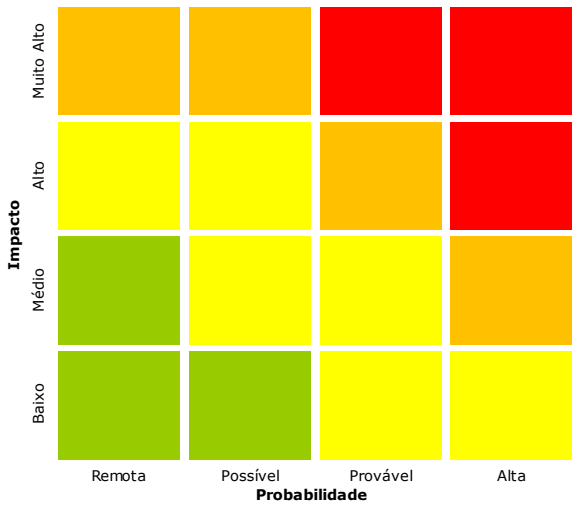
4.3.2 Esferas de Probabilidade

A área de Gestão de Riscos e Compliance baseia sua análise em dados **históricos** e na existência ou não de **mitigadores**, como sendo os critérios para avaliação e classificação da possibilidade de materialização dos riscos.

A probabilidade de materialização dos riscos pode ser classificado em quatro escalas: **quase certa, provável, possível e remota**.

4.4. Avaliação dos riscos

Os riscos e fatores identificados devem ser avaliados conforme seu impacto e probabilidade, gerando seu nível de criticidade no mapa de riscos.



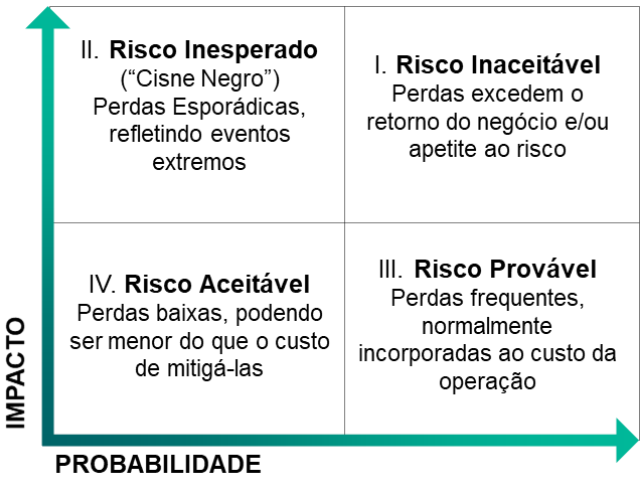
4.5. Tratamento dos riscos

Para cada risco identificado deve ser atrelado uma das respostas possíveis:

I. **Evitar** – Descontinuação das atividades que geram os riscos;
II. **Reduzir** – Adoção de medidas para reduzir a probabilidade ou o impacto dos riscos, ou, até mesmo, ambos);
III. **Compartilhar** – Redução da probabilidade ou do impacto dos riscos pela transferência ou pelo compartilhamento de uma porção do risco, ou;
IV. **Aceitar –** Nenhuma medida é adotada para mitigar a probabilidade ou o grau de impacto dos riscos.

Posteriormente, os riscos identificados devem passar por uma priorização, para que a Companhia imponha seus esforços de maneira faseada.

Para assessorar na priorização temos a matriz de priorização, que aglomera os riscos conforme a perda atrelada à materialização de cada um:



Os riscos de cada quadrante possuem as seguintes características:

I. **Risco Inaceitável** – Demandam ações prioritárias para implementar mitigadores, visando eliminar ou reduzir sua classificação de impacto e/ou de probabilidade;

II. **Riscos Inesperado** – São aqueles classificados como impacto alto e probabilidade baixa. Devem ser monitorados e quantificados regularmente para direcionar as estratégias de mitigação e, por consequencia, os planos de ação;

III. **Risco Provável** – Demandam definições dos níveis aceitáveis de perda por Risco, evitando que o grau de impacto suba ao longo do tempo, ou;

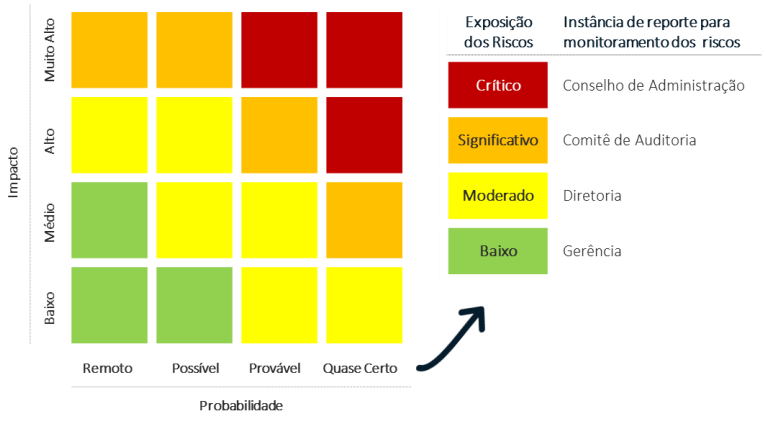
IV. **Risco Aceitável** – São aqueles classificados como baixo impacto e probabilidade, não demandando monitoramento contínuo.

Para cada risco priorizado devem ser identificadas as ações mitigatórias existentes e, no caso de ausência delas, devem ser estabelecidos planos de ação para a devida implementação.

4.6. Monitoramento dos riscos

Verificação, supervisão e observação crítica, executadas de forma contínua, acerca dos planos de ação e elaboração de reportes periódicos à Alta Administração.

Os riscos serão reportados às instâncias aplicáveis, conforme quadro abaixo:



4.7. Comunicação e divulgação aos envolvidos sobre as etapas do processo

Processo contínuo que permeia toda a Gestão de Riscos da Companhia, visando fornecer, compartilhar ou obter

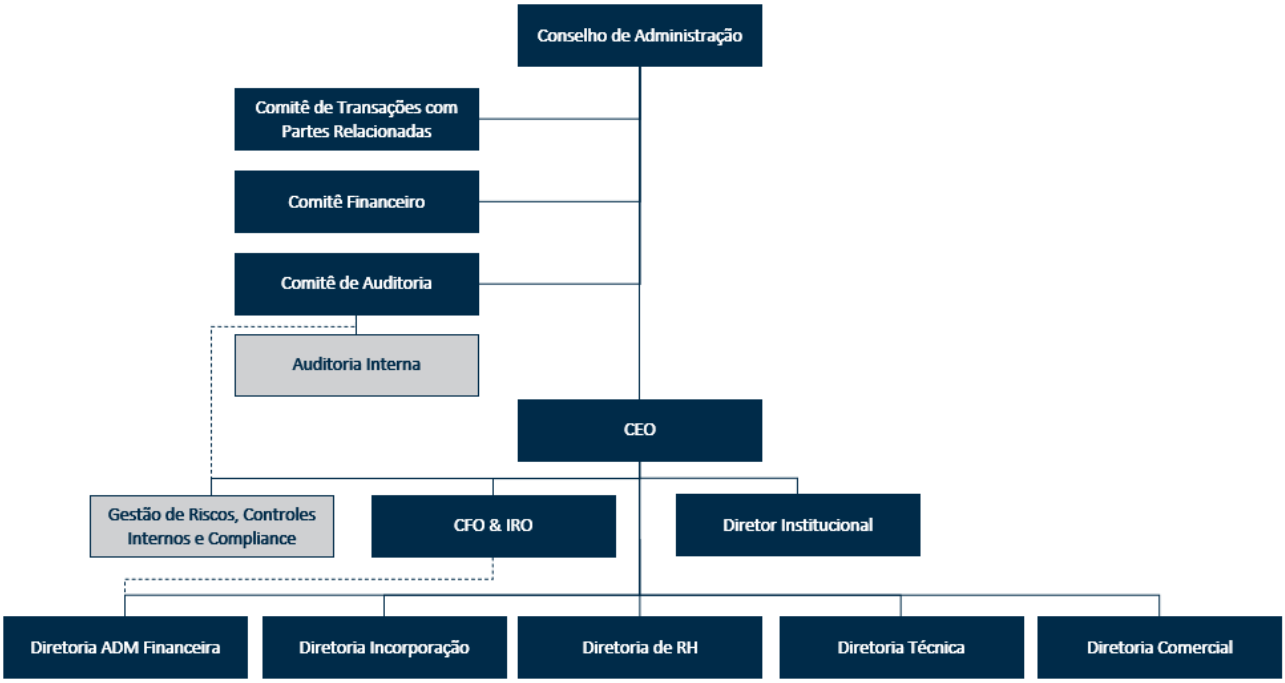
informações contribuindo para que o ambiente corporativo reflita os valores e a cultura de riscos desejada pela organização;

4.8. Estabelecimento de governança

Busca reforçar a necessidade da supervisão deste processo por parte da Alta Administração e difundir uma cultura voltada ao gerenciamento de riscos.

5. PAPÉIS E RESPONSABILIDADES

O organograma a seguir representa a estrutura corporativa da Companhia:



As áreas envolvidas no gerenciamento de riscos da Companhia possuem as seguintes atribuições:

5.1 Conselho de Administração

- Apoiar e multiplicar a disseminação da cultura de Gestão de Riscos;
- Avaliar a análise realizada das diretrizes estratégicas (Plano Estratégico P2A, metas, etc), sob a ótica de Gestão de Riscos;
- Avaliar e aprovar exceções às diretrizes estabelecidas deliberadas pelo Comitê de Auditoria;
- Deliberar sobre a Política de Gestão de Riscos e suas eventuais revisões;
- Deliberar sobre os limites de exposição a riscos (apetite e tolerância);
- Avaliar periodicamente o portfólio dos riscos estratégicos e as ações mitigatórias reportadas;
- Deliberar quais os riscos a serem priorizados pela Companhia com base na recomendação do Comitê de Auditoria;
- Acompanhar os resultados do processo e da performance do gerenciamento de riscos estratégicos.

5.2 Comitê de Auditoria

- Apoiar e multiplicar a disseminação da cultura de Gestão de Riscos;
- Deliberar sobre os padrões para o processo de gerenciamento de riscos (metodologia, processos, sistemas, política, mecanismos de reporte, dentre outros) e solicitar ajustes, se necessário;
- Reportar ao Conselho de Administração as exceções às diretrizes de Gestão de Riscos apresentadas e discutidas neste Comitê;
- Validar o planejamento da Gerência de Riscos, Controles Internos e Compliance, solicitar ajustes se necessário e acompanhar a execução do trabalho;

- Discutir e revisar a Política de Gestão de Riscos, solicitar ajustes se necessário e recomendá-la ao Conselho de Administração;
- Discutir e revisar a definição dos limites de exposição a riscos (apetite e tolerância) aceitável pela Companhia, solicitar ajustes se necessário e recomendá-los ao Conselho de Administração;
- Discutir a proposta dos riscos estratégicos a serem priorizados pela Companhia, solicitar ajustes se necessário e efetuar recomendação ao Conselho de Administração;
- Recomendar ao Conselho de Administração a resposta aos riscos priorizados, considerando: Evitar, Reduzir, Compartilhar e Aceitar;
- Acompanhar os reportes periódicos sobre os riscos priorizados e outros eventuais temas relevantes e reportá-los ao Conselho de Administração;

5.3 Presidente – CEO e Diretoria Executiva Responsável pela área de Riscos, Controles Internos e Compliance

- Promover a integração da Gestão de Riscos com os ciclos de revisão do planejamento estratégico;
- Apoiar e multiplicar a disseminação da cultura de Gestão de Riscos;
- Revisar os padrões para o processo de gerenciamento de riscos (metodologia, processos, sistemas, política, mecanismos de reporte, dentre outros), garantir que estão alinhadas às práticas da Companhia/ do tema/ do mercado e submeter para revisão e deliberação do Comitê de Auditoria e Conselho de Administração, respectivamente;
- Revisar a Política de Gestão de Riscos, solicitar ajustes se necessário e submeter para revisão e deliberação do Comitê de Auditoria;
- Revisar a definição do limite de exposição a riscos (apetite e tolerância) avaliando o que é aceitável pela Companhia, solicitar ajustes se necessário e submeter para revisão e deliberação do Comitê de Auditoria;
- Tomar conhecimento, discutir, validar, e avaliar o portfólio de riscos estratégicos e posteriormente os riscos operacionais.
- Avaliar os planos de ação sugeridos pelos donos dos riscos;
- Monitorar as variações de criticidade dos riscos priorizados e reportar as variações significativas ao Comitê de Auditoria;
- Deliberar o planejamento da Gerência de Riscos e Compliance, solicitar ajustes se necessário, acompanhar a execução do mesmo e submeter para validação do Comitê de Auditoria;
- Acompanhar os indicadores chaves e reportar desvios ao Comitê de Auditoria.

5.4 Área de Gestão de Riscos e Compliance

- Apoiar e multiplicar a disseminação da cultura de Gestão de Riscos;
- Atuar como segunda linha;
- Propor os padrões para o processo de gerenciamento de riscos (metodologia, processos, sistemas, política, mecanismos de reporte, dentre outros) e revisá-los sempre que necessário;
- Elaborar o planejamento da Gerência de Riscos, Controles Internos e Compliance anualmente;
- Propor a Política de Gestão de Riscos e atualizá-la sempre que necessário;
- Efetuar o cálculo dos limites de exposição à riscos (apetite e tolerância) anualmente e atualizá-lo quando eventos relevantes ocorrerem;
- Atuar em conjunto com a Diretoria Executiva Responsável pela área de Riscos, Controles Internos e Compliance na discussão sobre a definição do limite de exposição à riscos (apetite e tolerância) aceitável pela Companhia e apresentar os resultados ao Comitê de Auditoria, para avaliação e recomendação do Conselho de Administração;
- Propor, em conjunto com os Diretores Executivos da 1ª linha, a régua de impacto e probabilidade, para classificação da criticidade dos riscos e atualizá-la sempre que necessário;
- Implementar o processo de identificação e avaliação dos riscos junto aos Diretores Executivos da 1a. linha;
- Elaborar e atualizar o mapa de riscos sempre que houver atualizações no planejamento estratégico ou quando eventos relevantes ocorrerem;
- Estimular as demais áreas da Companhia a gerenciar e assumir riscos, levando-se em consideração os limites de exposição a riscos (apetite e tolerância) aprovados pelo Conselho de Administração; visando o alcance da estratégia e objetivos da Companhia;
- Assessorar o dono do risco na definição do plano de ação e na criação de indicadores de exposição dos riscos;
- Assessorar o dono do risco na definição, desenho e implementação dos controles internos necessários para: (i) para mitigar riscos existentes; e (ii) gerar informações confiáveis para alimentar os indicadores de exposição de riscos;
- Receber dos Donos dos Riscos comunicado sobre eventuais mudanças nos riscos (descrição, fatores, criticidade –

impacto e/ou probabilidade, etc) e nos planos de ação estabelecidos para mitigação dos riscos priorizados e, se necessário, solicitar ajustes.

- Acompanhar eventuais mudanças na criticidade dos riscos e reportá-las a Diretoria Executiva Responsável pela área de Riscos, Controles Internos e Compliance e ao Comitê de Auditoria;
- Estruturar KRIs, com base em indicadores das áreas, a fim de monitorar a variação e o(s) resultado(s) do(s) risco(s)
- Efetuar reportes periódicos a Diretoria Executiva Responsável pela área de Riscos, Controles Internos e Compliance e ao Comitê de Auditoria sobre toda e qualquer mudança atrelada aos riscos (ex: criticidade dos riscos), sobre o tratamento do riscos identificado e sobre o status dos planos de ação para a mitigação dos mesmos.
- Treinar a Companhia sobre o tema Gestão de Riscos, criando agentes multiplicadores.

5.5 Auditoria Interna

- Monitorar e avaliar, de forma independente e imparcial, a qualidade e efetividade do processo de gerenciamento de riscos e dos controles internos da Companhia, realizando as recomendações de melhorias que entender adequadas;
- Verificar a conformidade do processo de gerenciamento de riscos com a Política de Gestão de Riscos e demais políticas, normas e diretrizes adotadas pela Companhia;
- Avaliar a adequação dos controles internos existentes para: (i) para mitigar riscos existentes; e (ii) gerar informações confiáveis para alimentar os indicadores de exposição de riscos;
- Recomendar a adoção de planos de ação, acompanhar e auditar a sua implementação e a efetividade dos tratamentos propostos;
- Elaborar e disponibilizar, ao término de cada trabalho, relatórios e informações ao Comitê de Auditoria, para subsidiar o acompanhamento da efetividade do sistema de controles internos de gerenciamento de riscos da Companhia.

5.6 Donos dos Riscos (Áreas de Negócio)

- Apoiar e multiplicar a disseminação da cultura de Gestão de Riscos;
- Atuar como primeira linha;
- Seguir as diretrizes da Companhia para do processo de Gestão de Riscos;
- Atualizar, em conjunto a Gestão de Riscos, as fichas de riscos, sempre que houver atualizações no planejamento estratégico ou quando eventos relevantes que afetem os riscos e/ou sua exposição ocorrerem. Não tendo ocorrido nenhum desses fatores, deve ser realizada revisão das fichas de risco com periodicidade mínima anual. Essa revisão deve incluir, no mínimo, a descrição do risco, dos seus fatores, da criticidade do risco (impacto versus probabilidade), da resposta ao risco e das demais informações do risco. Para isso, devem ser consideradas as alterações em ações mitigatórias existentes, a conclusão dos planos de ação e os resultados das avaliações dos processos (ambiente de controle) relacionados ao risco;
- Tratar os riscos sob sua responsabilidade, sugerindo resposta ao riscos e garantindo a implementação de controles de acompanhamento e tomada de ações necessárias para a mitigação dos riscos críticos, juntamente com o envolvimento de outras áreas, quando necessário;
- Implementar KRIs a fim de monitorar a variação e o(s) resultado(s) do(s) risco(s) sob sua responsabilidade e monitorar seus indicadores de área e reportar eventuais desvios de ambos à Gerência de Riscos, Controles Internos e Compliance;
- Definir, desenhar e implementar os controles internos necessários para (i) para mitigar riscos existentes; e (ii) gerar informações confiáveis para alimentar os indicadores de exposição de riscos;
- Efetuar reportes periódicos à Gerência de Riscos e Compliance sobre o monitoramento do risco de sua responsabilidade (mudanças significativas na probabilidade e/ou impacto do risco ou em qualquer outra característica) e eventuais riscos não mapeados;
- Efetuar reportes periódicos à Gerência de Riscos, Controles Internos e Compliance sobre o desenvolvimento dos planos de ação para a mitigação dos riscos;
- Garantir a guarda de toda documentação suporte referente à conclusão dos planos de ação.

6. DISPOSIÇÕES FINAIS

A Gerência de Riscos, Controles Internos e Compliance se mantem à disposição para esclarecer eventuais dúvidas sobre o tema Gestão de Riscos e para estabelecer procedimentos necessários para divulgação deste documento, a ser realizada

através de todos os meios, fóruns e âmbitos disponíveis, priorizando os meios de comunicação internos como espaço de disseminação a todos os colaboradores, bem como às demais partes interessadas.

Quaisquer exceções às diretrizes estabelecidas neste documento devem ser submetidas para conhecimento da Gerência de Riscos e Compliance para devido endereçamento do item, conforme governança estabelecida.

7. GLOSSÁRIO

Ação mitigatória/ Mitigador: Medida adotada pela Companhia que proporciona uma redução da sua exposição ao risco e que busca atenuar a possibilidade de materialização do risco. São atividades periódicas ou contínuas mudanças em práticas já existentes buscando direcionar mitigação de um risco específico. Podem ser divididas em: Ações, políticas, TI/Sistema, Controles ou projetos.

Apetite a risco: Grau de exposição aos riscos que a organização está disposta a aceitar na busca e na realização de sua missão.

COSO (Committee of Sponsoring Organizations of the Treadway Commission): Organização reconhecida mundialmente por promover diretrizes relacionadas a aspectos críticos de governança corporativa, ética nos negócios, controles internos, gerenciamento de ricos corporativos e discussão de fraude.

Dono do Risco: O dono do risco é o gestor do risco e das suas consequências para a Companhia. Cabe a ele também fazer gestão das ações mitigatórias, KPI´s e planos de ação juntamente as equipes responsáveis. O Dono do Risco é uma pessoa indicada pelo Presidente e aprovada pelo Comitê de Auditoria.

Esferas de impacto: Critério quantitativos e/ou qualitativos de avaliação de impacto de risco.

Exposição ao risco: Classificação do risco de acordo com as avaliações de probabilidade e impacto e suas consequências.

Fator de risco: Ocorrência de evento ou alteração de um conjunto específico de circunstâncias que contribuem para que eventualmente um risco se materialize. O mesmo risco pode conter um ou mais fatores relacionados.

Nota 1: Um fator pode consistir em uma ou mais ocorrências, e pode ter várias causas.

Nota 2: Um fator pode consistir na não ocorrência de alguma coisa.

Ficha de Risco: Documento executivo que formaliza os riscos e fatores de riscos identificados e que consolida as informações disponíveis sobre eles.

Impacto de Risco: Trata-se, em nível qualitativo e/ou quantitativo, das consequências no caso da materialização dos fatores de riscos. O impacto do risco e analisado em diferentes esferas que podem ser revisadas a cada ciclo de avaliação.

Incerteza: Estado, mesmo que parcial, da deficiência de informações relacionadas à um fato - sua compreensão, seu conhecimento, sua consequência ou sua probabilidade. A incerteza pode se transformar em ameaça ou em oportunidade para a empresa.

Indicadores chave (KPIs): Métricas utilizadas para monitorar e avaliar como o risco se comporta. Fornece alertas quanto a exposição ou potencial de perda futura e para avaliar a aderência e evolução das atividades de Gestão de Riscos na Companhia.

ISO 31.000:2018: Norma crida com o objetivo de estabelecer uma padronização na Gestão de Riscos entre as empresas, bem como das melhores práticas e abordagens para sua implantação.

Linhas: Conceito que divide o ambiente corporativo em 3 partes: **(i) Primeira Linha**, que representa as áreas de negócio, os responsáveis pela execução dos processos e riscos operacionais; **(ii) Segunda Linha**, que representa áreas de gestão que suportem a Primeira Linha para garantir que seja apropriadamente desenvolvida e posta em prática e para que opere conforme intencionado; **(iii) Terceira Linha**, que visa avaliar forma como a primeira e a segunda linhas alcançam seus objetivos de gerenciamento de riscos e controle e identificar possíveis desvios ao processo estabelecido, decorrente de falhas/fraudes. Este conceito estabelece atribuições para cada uma das linhas e demonstra a importância da interação desses papéis na Organização;

Mapa de risco: Demonstração gráfica com base na análise geral dos riscos e de auto avaliação da administração, onde são analisados os riscos da empresa, considerando impacto e probabilidade para sua materialização.

Natureza do risco: Podem ser quatro tipos, à saber: “Estratégico”, “Regulamentar” (também conhecido como “Conformidade”), “Operacional”, “Financeiro” ou “Cyber”. Estas designações são maneiras de categorizar os objetivos da Companhia em blocos e consequentemente, os riscos atrelados a estes objetivos.

Plano de Ação: Proposta de melhoria ou correção de desvios de fatores de riscos identificados, com a finalidade de redução da probabilidade e/ou do impacto de materialização de risco a um limite que seja aceito pela Companhia.

Ponto Focal: O ponto focal é o vínculo entre a equipe de Gestão de Riscos, o Dono do Risco e o responsável Técnico pelo risco. O Ideal é que haja um ponto focal para cada dono de risco e que ele esteja hierarquicamente abaixo do dono, de modo a evitar a descentralização de informações.

Probabilidade: Nível qualitativo ou quantitativo que caracteriza a chance do fator de risco se materializar.

Resposta ao risco: Definição do tratamento que a Companhia dará ao risco, podendo optar por evitar, reduzir, compartilhar ou aceitar o risco.

Risco: É a possibilidade de ocorrência(s) de evento(s), gerando incerteza sobre a possibilidade de perda(s) ou ganho(s), que afete(m) o rumo dos acontecimentos relativos aos objetivos estratégicos da Companhia.

Risco Inerente: É o risco existente antes de ser tratado quando a sua probabilidade e impacto.

Risco Residual: É o risco remanescente após a Administração ter tomado ações/medidas para reduzir a probabilidade de ocorrência e/ou para mitigar seu impacto.

Tolerância ao risco: Refere-se à uma parte do apetite a risco definido pela Companhia que, quando atingido, chega ao limite estabelecido pela Even.

Tratamento de risco: Seleção, formalização e implementação de uma ou mais ações mitigatórias dos fatores de risco, que serão monitoradas pelo dono do risco. A decisão sobre a estratégia adotada para trata cada risco depende principalmente do grau de apetite a risco da empresa. Medidas de tratamento de risco devem obrigatoriamente reduzir a probabilidade e/ou impacto do risco.

8. DOCUMENTOS DE REFERÊNCIA

- COSO – ERM (*Committee of Sponsoring Organizations of the Treadway Commission – Enterprise Risk Management Framework*)
- ISO (*International Organization for Standardization*) 31.000:2018
- IIA (The Institute Of Internal Auditors)
- Estatuto Social Melnick
- Regimentos do Conselho de Administração e do Comitê de Auditoria
- Instrução CVM (Comissão de Valores Mobiliários) 552
- Instrução CVM (Comissão de Valores Mobiliários) 586

Este documento foi elaborado pela Gerência de Riscos e *Compliance*, passou pela revisão da Diretoria Administrativa Financeira, foi recomendado pelo Comitê de Auditoria e aprovado pelo Conselho de Administração.