1. OBJETIVO

Esta Política de Gerenciamento de Riscos ("Política") tem por objetivo estabelecer princípios, diretrizes e responsabilidades a serem observadas no processo de gerenciamento de riscos corporativos da Kepler Weber ("Companhia"), de forma a identificar, avaliar e monitorar os riscos inerentes a Companhia e ao seu setor de atuação e que possam afetar o atendimento aos seus objetivos e realização de seus negócios.

2. ABRANGÊNCIA

Esta Política aplica-se à Companhia e suas controladas, bem como a todos os colaboradores, gestores, diretores estatutários e não estatutários, membros do Conselho de Administração e Comitês.

3. DEFINIÇÕES

- **Risco:** Possibilidade de ocorrência de um evento que possa afetar o alcance dos objetivos da Companhia.
- **Risco Inerente:** Grau de risco intrínseco à operação do negócio ou à atividade, sem considerar a execução dos controles que o mitigam.
- **Apetite ao Risco:** Nível de exposição à perda que a Companhia está disposta a aceitar.
- **Gestão de Riscos:** Processo para identificar, avaliar e gerenciar potenciais eventos que possam impactar no atingimento dos objetivos da Companhia e a realização dos seus negócios.
- **Monitoramento:** Verificação, supervisão, observação crítica ou identificação da situação, executadas de forma contínua, a fim de identificar mudanças no nível de desempenho requerido ou esperado.
- **Planos de Ação:** Ações que visam criar, corrigir ou melhorar o funcionamento dos processos, sistemas e/ou estratégias da Companhia, bem como mitigar as causas dos riscos.
- **COSO ERM (Enterprise Risk Management Integrated Framework).:** Estrutura desenvolvida pela organização COSO - Committee of Sponsoring Organizations of the Treadway Commission, que estabelece metodologia internacionalmente reconhecida de Gerenciamento de Riscos.

4. GESTÃO DE RISCOS

O processo de Gestão de Riscos refere-se às práticas de identificação, avaliação e monitoramento, dos riscos inerentes à Companhia, com base em metodologia reconhecida no mercado e de forma estruturada.

O objetivo da Gestão de Riscos é conhecer e entender os riscos aos quais a Companhia está exposta e como estes impactam no atingimento das metas e cumprimento dos seus objetivos estratégicos. Este monitoramento possibilita a definição de ações preventivas ou corretivas para manter os riscos em níveis aceitáveis.

É de responsabilidade da Alta Administração e da função de Gestão de Riscos e Controles Internos a disseminação da cultura de monitoramento e inclusão dos riscos na tomada de decisão. A Gestão de Riscos deve auxiliar o processo de tomada de decisão nos diversos níveis de gestão da Companhia, contribuindo com a melhoria de desempenho, identificação de oportunidades de negócio, otimização na alocação de recursos, minimização de perdas, redução de custos, assim como na conduta do negócio no dia a dia.

5. AVALIAÇÃO GERAL DE RISCOS

A avaliação de riscos corporativos é um recurso adotado pela Companhia para mapear potenciais riscos, eventos e mensurar as possíveis perdas, assim como oportunidades geradas por eles. Esse processo é desenvolvido considerando todas as áreas da Companhia e o panorama do negócio, analisando tanto elementos internos como externos.

O objetivo da avaliação de riscos corporativos é o mapeamento dos riscos relevantes para o negócio, de modo que seja possível gerenciá-los com efetividade. Além de classificar os riscos em relação ao seu impacto e probabilidade, possibilitará que a Companhia possa priorizar os seus esforços e investimentos em ações direcionadas para os riscos de acordo com a sua criticidade.

As etapas do processo de Avaliação de Riscos Corporativos estão descritas abaixo:

5.1 Identificar os Riscos e Avaliar o Ambiente de Controle

Trata-se da identificação do conjunto de eventos, externos ou internos, que podem impactar os objetivos estratégicos da organização através de análise documental e entrevistas com todas as áreas da Companhia para o entendimento sobre o ambiente de controle relacionado a cada risco e verificação das ações mitigatórias existentes para minimizar a sua exposição.

5.2 Classificar os Riscos Corporativos

Os riscos corporativos podem ser classificados conforme os 4 principais pilares abaixo:

5.2.1 Riscos Estratégicos

Os riscos estratégicos estão associados à tomada de decisão da Alta Administração e podem gerar perda substancial no valor econômico da Companhia e até mesmo a descontinuidade do negócio.
No pilar Estratégico, podemos destacar os seguintes tópicos a serem avaliados: Planejamento e Alocação de Recursos, Estrutura de Governança, Iniciativas ESG, Comunicação com o Mercado, entre outros.

5.2.2 Riscos Financeiros

Os riscos financeiros referem-se à possibilidade de prejuízos em decorrência das operações e transações financeiras da Companhia, podendo ser resultantes de gestão de fluxo de caixa ineficiente, liquidez, captação e aplicação de recursos financeiros, variação cambial, assim como o descumprimento de obrigações financeiras de contrapartes.

5.2.3 Riscos Operacionais

São riscos decorrentes de falhas de processos e controles na operação e áreas suporte da Companhia, que prejudiquem ou impossibilitem o exercício das suas atividades. Os riscos operacionais geralmente acarretam ineficiência, interrupção total ou parcial das atividades, podendo gerar impacto negativo na reputação perante o mercado, além do potencial de geração de passivos contratuais e regulatórios.
No pilar Operacional, podemos destacar os seguintes tópicos a serem avaliados: Operação Industrial, Logística, Segurança Patrimonial, Manutenção, Gestão Comercial, Recursos Humanos, Engenharia e Projetos, Supply Chain (produtos e serviços), incluindo a Gestão de Fornecedores.

5.2.4 Riscos de Compliance

Os riscos de Compliance estão associados à possíveis sanções legais ou regulatórias devido ao descumprimento de leis, acordos, regulamentos, código de conduta e políticas, que podem resultar em perda financeira e em danos reputacionais para a Companhia.

No pilar de Compliance, podemos destacar os seguintes tópicos a serem avaliados: Requisitos Legais e Regulatórios, Integridade e controles Anticorrupção, Código de Ética e Conduta.

Entre os riscos que podem permear os diversos pilares acima, podemos destacar:

5.2.5 Riscos de Tecnologia

Os riscos de Tecnologia referem-se às ameaças que podem acarretar interrupção ou indisponibilidade sistêmica em decorrência de falhas na segurança da informação, gestão de dados e acessos, gestão de mudanças, infraestrutura, falta ou obsolescência de recursos tecnológicos (ex. equipamentos, sistemas etc.), incluindo instalações.

No pilar de Tecnologia, podemos destacar os seguintes tópicos a serem avaliados: Adequação dos sistemas internos às necessidades da companhia, incidentes de cybersecurity, integridade e gestão dos dados, falha no acesso lógico aos sistemas, vazamento de dados, entre outros.

5.2.6 Riscos Socioambientais:

O risco Socioambiental consiste na exposição a perdas com incidentes envolvendo o meio ambiente e/ou a sociedade, decorrentes de atividades diretas ou indiretas da Companhia.

Os impactos sociais referem-se à saúde e segurança; ações que desrespeitem a proteção, assim como a promoção dos direitos humanos como discriminação e condições análogas à escravidão.

Os impactos ambientais são os que podem afetar também recursos naturais como o ar, cursos d´água, matas, solos e animais com a emissão de gases poluentes, resíduos, efluentes, derramamento de produtos químicos, entre outros. Já os impactos climáticos precisam ser observados com o objetivo de serem reduzidos ou compensados com a diminuição de emissão de gases do efeito estufa e captura dos gases emitidos na fabricação de equipamentos, assim como para preparar a Companhia diante de eventos que possam impactar a produção de seus clientes e consequentemente as suas vendas.

Os riscos socioambientais e climáticos podem gerar perdas financeiras e reputacionais, sanções legais ou regulatórias e indenizações por danos à terceiros e que tiveram participação direta ou indireta da Companhia envolvendo seus clientes, fornecedores, colaboradores e demais parceiros.

5.3 Avaliar os Riscos quanto ao seu Impacto e Probabilidade

Para a otimização de recursos e esforços, os riscos a serem gerenciados devem ser priorizados conforme a relevância para a Companhia, decorrente da avaliação de impacto e probabilidade conforme critérios pré-estabelecidos por esta. Desta forma, foram estabelecidos e validados os critérios apresentados nas tabelas a seguir:

5.3.1 Avaliação quanto à probabilidade de materialização do risco baseado em seu histórico e ambiente de controle:

Classificação	Probabilidade
Alta	Apesar dos controles existentes, é muito provável que o evento ocorra ou verificação de ausência de controle. O evento vem ocorrendo ou ocorreu nos últimos anos, mesmo com os controles em vigor.
Média	Apesar dos controles existentes, é possível que o evento ocorra ou verificação de controle ineficaz. O evento ocorre de tempos em tempos, e pode ter ocorrido até duas (2) vezes ao ano, mesmo com os controles em vigor.
Baixa	Apesar dos controles existentes, é possível que o evento ocorra. O evento ocorre de tempos em tempos, e pode ter ocorrido até uma (1) vez no ano, mesmo com os controles em vigor.
Remota	A ocorrência é improvável e sem histórico de materialização do risco.

5.3.2. Avaliação quanto ao impacto que uma materialização do risco poderia causar:

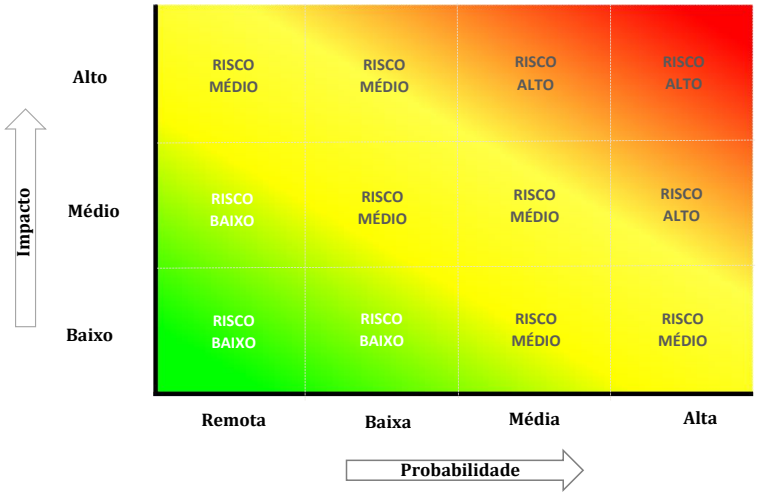
Classificação	Impacto
Alto	• Operacional: Impacto significativo na operação da Companhia. • Estratégico: Descumprimento dos objetivos e metas do negócio, impacto grave ao meio ambiente, com prejuízo ao funcionamento do ecossistema e/ou efeitos sobre a comunidade local, falha no cumprimento de requisitos de segurança do trabalho colocando a saúde e/ou vida dos profissionais em risco, exposição negativa de alta repercussão na imprensa nacional e/ou internacional. • Legal: Envolvimento de contingências, processos jurídicos que podem ocasionar em parada da operação e até inviabilizar a continuidade do negócio. • Financeiro: A ocorrência de um evento resultaria em perda financeira (acima de BRL 23 MM – ref. à mais de 5% do Patrimônio Líquido Consolidado de 2021).

AHB LTSF MGL PA RFS RSO

Classificação	Impacto
Médio	• Operacional: Importante impacto na operação da Companhia. • Estratégico: Dificuldade para atingir os objetivos e metas do negócio, impacto ambiental restrito à operação e/ou exposição negativa de repercussão na imprensa local. • Legal: Envolvimento de contingências, processos jurídicos que podem ocasionar em parada da operação. • Financeiro: A ocorrência de um evento resultaria em perda financeira (acima de BRL 2,3 MM até BRL 23 MM – ref. à 0,5% até 5% do Patrimônio Líquido Consolidado de 2021).
Baixo	• Operacional: Baixo impacto na operação da Companhia. • Estratégico: Pouca ou nenhuma interferência no cumprimento dos objetivos e metas do negócio, impacto ambiental restrito à instalação no local do acidente ou superior à um departamento e/ou exposição negativa pontual junto a algum stakeholder, sem repercussão na imprensa. • Legal: Envolvimento de contingências. • Financeiro: A ocorrência de um evento resultaria em perda financeira (até BRL 2,3 MM – ref. ao limite de 0,5% do Patrimônio Líquido Consolidado de 2021).

5.3.3 Avaliar os Riscos Corporativos com base no *Heat Map*

Esta etapa possui como finalidade o auxílio na tomada de decisões com base nos resultados da avaliação de riscos, sobre quais riscos necessitam de tratamento e priorização para a implementação de ações corretivas e/ou mitigatórias para redução da probabilidade de materialização. O mapa de riscos corporativos permitirá uma visibilidade do posicionamento dos riscos conforme a combinação da classificação de impacto e probabilidade baseada nos critérios e nível de apetite ao risco da Companhia:



5.4 Implementar Planos de Ação para melhoria no Ambiente de Controle

Como resultado da identificação dos riscos e avaliação do ambiente de controles, deve-se verificar a aplicabilidade de discutir e alinhar com os responsáveis pelos departamentos a recomendação de ações mitigatórias e/ou corretivas para redução da exposição aos riscos. As ações devem ser priorizadas e implementadas considerando a exposição da Companhia ao risco.

5.5 Monitorar os Riscos identificados e Planos de Ação

A Avaliação de Riscos Corporativos deve ser realizada anualmente, visando a atualização e completude dos dados. Adicionalmente, os planos de ação definidos para melhoria do ambiente de controle devem ser acompanhados periodicamente, considerando-se o prazo de implementação das oportunidades de melhoria acordado com cada área, para atualização dos dados e do monitoramento dos riscos associados.

Os parâmetros de classificação de impacto e probabilidade referente à materialização dos riscos também devem ser revisados anualmente com base nos resultados da Avaliação de Riscos Corporativos.

5.5.1 Monitoramento KRI (*Key Risk Indicators*)

O monitoramento por meio dos Indicadores Chaves de Riscos é utilizado para a identificação da necessidade de implementação de ações de melhoria para redução da exposição ou quantidade de ocorrência da materialização do risco e deve ser realizado mensalmente junto às áreas de negócio identificando-se a necessidade de ações corretivas e mitigatórias de forma tempestiva.

AHB LTSF MGL PA RFS RSO

A preparação do relatório de KRIs (*Key Risk Indicators*) deve ocorrer a cada trimestre e estruturada visando a comunicação dos resultados para as áreas envolvidas, e possui os seguintes principais objetivos:

- Alertar a Alta Administração, Diretores e Gestores sobre os riscos que precisam de atenção;
- Emitir alertas quando ações corretivas se fizerem necessárias;
- Alertar a função de Gestão de Riscos e Controles Internos, além da Auditoria Interna, sobre as áreas da Companhia que necessitam de uma revisão nos controles internos.

6. LINHAS

A segregação entre as linhas é de extrema importância para garantir a independência e imparcialidade dos apontamentos da auditoria e transparência do processo. Essa necessidade é destacada no modelo de três linhas do COSO-ERM e do IIA (*Institute of Internal Auditors*).

As linhas estão organizadas na Companhia conforme abaixo:

1ª linha: Representada pelos colaboradores e gestores das áreas de negócios da Companhia, cuja responsabilidade é atingir os objetivos organizacionais referentes à entrega de produtos e/ou serviços aos clientes, incluindo as funções de apoio. Dentro do processo de Gestão de Riscos, sua função é conhecer e monitorar os riscos inerentes à sua responsabilidade, buscando trabalhar em conjunto com a Função de Riscos e Controles Internos para minimizar a possibilidade de materialização dos riscos e os seus impactos.

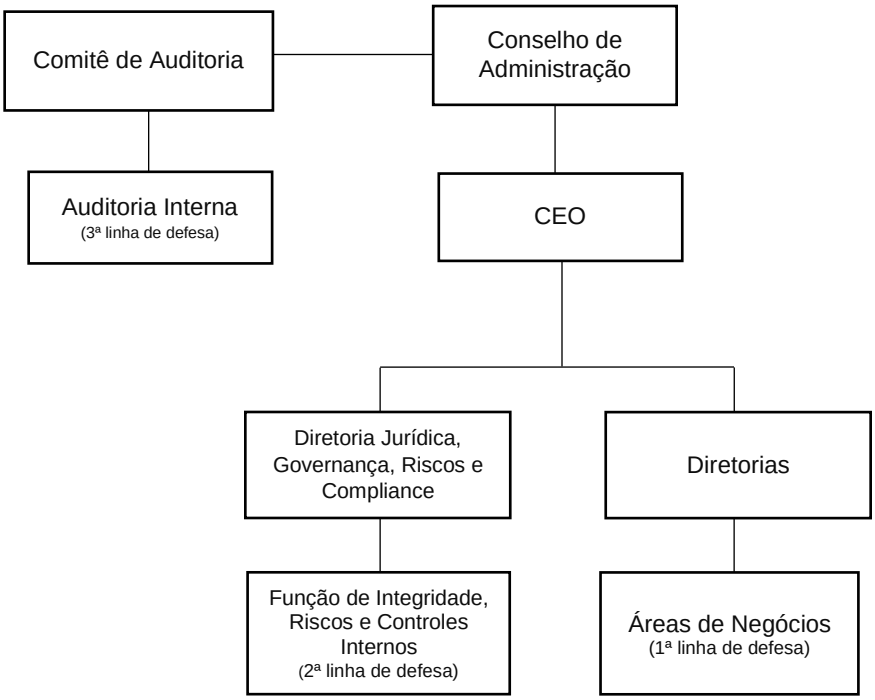
2ª linha: Representada pela Função de Riscos e Controles Internos e pela Função de Integridade, que atuam na garantia do apropriado funcionamento da primeira linha, por meio do estabelecimento de controles, na identificação de falhas de performance de controles e na identificação de desvios de políticas e procedimentos internos. A Função de Riscos e Controles Internos e a Função de Integridade são acompanhadas pelo Comitê de Auditoria e reportadas para o Conselho de Administração, e podem contar com o auxílio de outras áreas da Companhia, tais como controladoria, jurídico e auditoria interna, para o desempenho de suas atividades. Os colaboradores que exercem as Funções de Riscos e Controles Internos e a Função de Integridade não acumulam funções ou possuem relação de subordinação com áreas de negócios da Companhia.

3ª linha: Representada pela área Auditoria Interna, sua responsabilidade é realizar avaliações e assessorias independentes e objetivas sobre a adequação e eficácia da governança e do

gerenciamento de riscos. A área Auditoria Interna tem suas atividades reportadas periodicamente ao Conselho de Administração, por meio do Comitê de Auditoria, e as atribuições da Auditoria Interna são aprovadas pelo Conselho de Administração da Companhia.

7. PAPÉIS E RESPONSABILIDADES

O processo de Gestão de Riscos da Companhia está estruturado conforme organograma e descrições abaixo:



7.1 Conselho de Administração da Companhia:

O Conselho de Administração é responsável por determinar os objetivos estratégicos, os direcionamentos e o perfil de riscos da Companhia adequado ao seu apetite à riscos, relacionados a sua cultura e identidade.

Compete ao Conselho de Administração, no âmbito desta Política:

- Avaliar e definir a estrutura operacional para gestão de riscos e o seu respectivo orçamento;
- Definir o formato, periodicidade de reporte das informações requeridas para acompanhamento;

- Definir e revisar periodicamente os limites de exposição referentes ao nível de apetite ao risco da Companhia;
- Monitorar de forma periódica a efetividade do processo de Gestão de Riscos e fornecer orientações para o seu aprimoramento constante;
- Monitorar de forma contínua os Riscos que podem impactar o atingimento das metas e objetivos do negócio, assim como os planos de ação de melhoria em resposta aos riscos;
- Fornecer à Diretoria e Gestão, quando necessário, sua percepção do grau de exposição aos riscos que a Companhia está exposta e influência na priorização dos riscos a serem tratados;
- Assegurar, ao Comitê de Auditoria, autonomia operacional, aprovando-lhe orçamento próprio destinado a cobrir despesas com seu funcionamento;
- Receber, diretamente ou por meio do Comitê de Auditoria, o reporte das atividades da Auditoria Interna, avaliando, ao menos anualmente, se a estrutura e orçamento desta são suficientes ao desempenho de suas funções.

7.2 Comitê de Auditoria

É o órgão autônomo de assessoramento vinculado ao Conselho de Administração, que visa auxiliar no acompanhamento e avaliação da efetividade do processo de Gestão de Riscos.

Compete ao Comitê de Auditoria, no âmbito desta Política:

- Aprovação sobre o Plano Anual de Auditoria Interna;
- Opinar na contratação e destituição dos serviços de auditoria independente.;
- Acompanhar e avaliar o processo de Gestão de Riscos, assim como o cumprimento de seus objetivos e recomendar soluções de aprimoramento, se aplicável;
- Acompanhar as atividades da Auditoria Interna e da função de Riscos e Controles Internos da Companhia;
- Avaliar e monitorar as exposições de Risco da Companhia.

7.3 Função de Integridade, riscos e controles internos

A Função de Integridade, riscos e controles Internos é responsável por implementar as políticas de Compliance e Gerenciamento de Riscos, de acordo com a metodologia de Gestão de Riscos e monitoramento contínuo junto às áreas. Compete a Função de Integridade, riscos e controles internos, no âmbito desta Política:

- Zelar pela aplicação do Código de Ética e Conduta da Companhia;

- Elaborar o plano de implantação dos procedimentos e diretrizes do Código de Ética Conduta, bem como das demais políticas de integridades; e
- Estabelecer os processos gestão de riscos da Companhia;
- Realizar periodicamente a revisão e atualização da Avaliação Geral de Riscos, em período mínimo bienal, incluindo a elaboração do Mapa de Riscos Corporativos;
- Validar e comunicar os resultados da Avaliação Geral de Riscos, assim como os planos de ação de melhorias para implementação com os gestores das áreas de negócio;
- Elaborar reporte com os resultados da Avaliação Geral de Riscos e comunicá-los ao Conselho de Administração, por meio do Comitê de Auditoria;
- Auxiliar as áreas de negócio no desenvolvimento de processos e controles para gestão de riscos, inclusive aplicando treinamentos quando necessários para apoiá-los;
- Acompanhar a execução, e implementação dos planos de ação junto às áreas de negócio;
- Realizar o monitoramento, avaliar, consolidar os dados relacionados aos KRIs junto às áreas.

7.4 Diretorias

A Diretoria, enquanto órgão colegiado, é responsável pelo monitoramento dos riscos que podem comprometer os objetivos e metas relacionadas à sua área de atuação.

Compete à Diretoria, no âmbito desta Política:

- Promover a integração da gestão de riscos com os processos das áreas de sua responsabilidade; e
- Acompanhar o monitoramento dos riscos inerentes aos processos das áreas de sua responsabilidade e alinhar junto com a função de Riscos e Controles Internos as ações de implementação de ações corretivas e mitigatórias aplicáveis para redução à exposição dos riscos inerentes às suas respectivas áreas de atuação e ao negócio.

7.5 Áreas de Negócio

As Áreas de Negócio são os responsáveis pelo monitoramento dos riscos relativos aos objetivos e metas aplicáveis aos processos das áreas, assim como pelas atividades de controles de cada processo.

Compete aos colaboradores e gestores das Áreas de Negócios, no âmbito desta Política:

- Monitorar os riscos inerentes aos processos, assim como o nível de maturidade do ambiente de controles existentes na área de sua responsabilidade e acompanhar a exposição aos riscos, com base nos Indicadores-Chave de Riscos;
- Executar as ações de acordo com a resposta aos riscos pertinentes à respectiva área, conforme alinhado com a função de Gestão de Riscos e Controles Internos; e
- Comunicar à Diretoria as atualizações em relação aos planos de ação, à materialização dos riscos, ao ambiente de controle, assim como o surgimento de riscos emergentes.

7.6 Auditoria Interna:

A área de Auditoria Interna é responsável por auxiliar na verificação da efetividade dos controles, das políticas e normas estabelecidas na Companhia, com atribuições aprovadas pelo Conselho de Administração. A estrutura e o orçamento considerado suficiente para o desempenho das funções, são avaliados e aprovados pelo Conselho de Administração ou Comitê de Auditoria ao menos uma vez por ano.

Compete à Auditoria Interna, no âmbito desta Política:

- Elaborar o Plano Anual de Auditoria interna com base na priorização estabelecida com base nos resultados da Avaliação Geral de Riscos e submetê-lo à aprovação do Comitê de Auditoria;
- Avaliar a confiabilidade das informações e eficiência das operações;
- Avaliar a efetividade da sistemática de Controles Internos e reportar para o Comitê de Auditoria;
- Reportar os resultados das auditorias ao Comitê de Auditoria; e
- Aferir a qualidade e a efetividade do processo de Gestão de Riscos e dos processos de governança, da adequação dos controles e do cumprimento das normas e regulamentos associados aos negócios da Companhia, de forma independente, imparcial e tempestiva.

8. REFERENCIAL TEÓRICO

- Diretrizes de governança corporativa do estatuto social da Companhia.
- COSO – ERM: Committee of Sponsoring Organizations of the Treadway Commission – Enterprise Risk Management Framework.
- Modelo das Três Linhas do IIA 2020.

- Guia de Orientação para Gerenciamento de Riscos Corporativos IBGC (Instituto Brasileiro de Governança Corporativa) 2007.
- ABNT NBR ISO 31.000 / 2018: Gestão de Riscos – Princípios e diretrizes.
- Regulamento de Listagem do Novo Mercado da B3 S.A. – Brasil, Bolsa, Balcão.
- Resolução nº 59 da CVM (Comissão de Valores Mobiliários).

9. APROVAÇÃO, VIGÊNCIA E REVISÃO

A presente Política passa a vigorar após a aprovação em reunião do Conselho de Administração da Companhia, realizada em 15/03/2023, em 15 dias a contar da publicação no site corporativo https://www.kepler.com.br/governanca/politicas-kw, onde pode ser consultada.

A Companhia pode, por sua mera liberalidade ou em razão de alterações legislativas, a qualquer momento, e deve, a cada 2 (dois) anos, revisar os termos da presente política, sendo que em caso de alteração será submetida a nova aprovação.

10. CONTROLE DE ALTERAÇÕES

REVISÕES	DESCRIÇÃO DAS ALTERAÇÕES	DATA
00	Elaboração do documento	14/02/2014
01	Revisão periódica	28/07/2020
02	Revisão periódica	09/09/2021
03	Adequações Regulamento Novo Mercado	15/03/2023
04	Diligência Regulamento Novo Mercado	05/07/2023