Política de Gestão Estratégica de Riscos

Tenda

POLÍTICA DE GESTÃO ESTRATÉGICA DE RISCOS

1. OBJETIVO

O objetivo da Política de Gestão Estratégica de Riscos é estabelecer diretrizes e responsabilidades a serem observadas no gerenciamento de riscos da Companhia, assegurando que os riscos inerentes às atividades da Companhia sejam identificados, avaliados, tratados, monitorados e comunicados à Administração em tempo adequado para tomada de decisões, minimizando seu impacto através de seus controles internos e adequada governança de riscos.

Além dos objetivos acima, a Política da Tenda também tem por finalidade:

i. assegurar que os responsáveis pela tomada de decisão, em todos os níveis da Tenda, tenham acesso tempestivo a informações suficientes quanto aos riscos aos quais está exposta a organização, inclusive para determinar questões relativas à delegação, se for o caso;
ii. alocar e utilizar eficazmente os recursos para o tratamento de riscos corporativos;
iii. aumentar a probabilidade de alcance dos objetivos da organização, reduzindo os riscos a níveis aceitáveis; e
iv. agregar valor à organização por meio da melhoria dos processos de tomada de decisão e do tratamento adequado dos riscos e dos impactos negativos decorrentes da sua materialização.
v. Prestar assessoria contínua para mutuamente fiscalizar os mecanismos de controle sobre todas as atividades da organização envolvendo o tratamento de dados pessoais, incidentes de reputação digital e compliance, bem como, o tratamento dos incidentes com a finalidade de reduzir os danos.

2. CAMPO DE APLICAÇÃO

Esta política é aplicável a qualquer sociedade que seja controlada, direta ou indiretamente, pela Construtora Tenda S.A. (“Tenda”), seja por meio de titularidade da maioria ou igualdade de participação nas ações ou quotas com direito a voto, seja por meio de acordo de acionistas ou por outro meio que assegure a esta o poder de dirigir, de forma direta ou indireta, a administração de tal sociedade, incluindo toda e qualquer sociedade de propósito específico (SPE) já existente ou que venha a ser constituída sob o controle da Construtora Tenda S.A (“Empresas do Grupo Tenda”), bem como a todos os integrantes que tenham acesso a quaisquer dados pessoais detidos tratados através da Tenda, ou em seu nome.

3. DOCUMENTOS DE REFERÊNCIA

Regimento Interno do Comitê de Auditoria da Tenda

COSO ERM 2017 - Committee of Sponsoring Organizations of the Treadway Commission - Enterprise Risk Management Framework: Metodologia desenvolvida pelo COSO para o mapeamento e gerenciamento de riscos corporativos;

ISO 31000:2018 - Gestão de Riscos – Diretrizes

NBR ISO 31000:2018 – Gestão de riscos — Diretrizes

CRISC Review Manual (2019) - ISACA

The Standard for Risk Management in Portfolios, Programs, and Projects do PMI (2017)

AGR – Análise Geral de Riscos

4. DEFINIÇÕES

COSO - Committee of Sponsoring Organizations of the Treadway Commission: entidade sem fins lucrativos, dedicada à melhoria dos relatórios financeiros através da ética, efetividade dos controles internos e governança corporativa, para prevenir e evitar fraudes nas demonstrações contábeis das empresas;

Risco: Todo e qualquer evento decorrente de incertezas ao qual a Companhia está exposta e que possa impactar negativamente o alcance dos objetivos e de geração de valor estabelecidos no seu plano estratégico.

Tipos de Riscos:

(i) **Qualitativos**: quando a avaliação do Risco é realizada por meio do julgamento dos fatores de riscos, com base na experiência do avaliador. Representa uma alternativa às análises quantitativas dispendiosas, ou quando o Risco não se presta à quantificação, por não haver dados disponíveis e confiáveis;

(ii) **Quantitativos**: quando o Risco pode ser medido em valores monetários e/ou avaliação se baseia em séries de dados, permitindo o estabelecimento do percentual de probabilidade de ocorrência e a valoração do impacto no resultado da Companhia. Possibilita maior precisão por empregar técnicas de análises mais sofisticadas, com forte componente estatístico; e

(iii) **Híbridos**: quando a avaliação do Risco envolve a utilização de técnicas qualitativas e quantitativas, que se complementam.

Categorias de Riscos: Matriz utilizada para avaliação dos principais riscos inerentes ao negócio da Tenda, esses riscos são segregados em 4 (quatro) grupos, sendo:

(i) Estratégicos;
(ii) Operacionais;
(iii) Financeiros;
(iv) Regulamentar.

Fator de Risco: Fatores internos ou externos que podem originar os eventos de riscos;

Tolerância a Riscos: Quantidade de riscos que a Companhia aceita correr acima de seu apetite a risco, de forma discricionária e específica;

Assunção de Risco: Situação na qual a Companhia se dispõe a manter-se exposta a um determinado risco, considerando o apetite a risco da Companhia, e o benefício que isso pode proporcionar, conforme a capacidade econômica definida por níveis de alçadas de concessão;

Matriz de Riscos ou Mapa de Riscos: Visa estabelecer uma comparação individual dos Riscos a partir dos impactos e probabilidade de ocorrência, para fins de priorização e gestão. Deve

estar em constante evolução e deve ser atualizada anualmente na AGR – Avaliação Geral de Risco e sempre que necessário com o surgimento de novos eventos de risco.

Riscos Prioritários: São riscos com probabilidade e impacto potencialmente elevado para o negócio, cuja gestão deve ser priorizada.

Estratégias de Resposta ao Risco: É o conjunto de ações que visam dar resposta ao Risco. As opções são as seguintes: Eliminar, Compartilhar, Tratar ou Aceitar;

Limite de Risco ou Apetite ao Risco: É a exposição e/ou impacto máximo do Risco que a Companhia está disposta a aceitar, na busca dos objetivos e geração de valor. Nem todos os tipos de Riscos são passíveis de aceitação, sendo assim, os limites de aceitação deverão obrigatoriamente ser fundamentados e formalizados pelas seguintes análises:

(i) Avaliação do retorno tangível e intangível relacionado ao Limite de Risco proposto;
(ii) Capacidade da Companhia de suportar o impacto do Limite de Risco proposto;
(iii) Decisão se o risco deve ou não ser aceito conforme sua tipologia;
(iv) Viabilidade da implantação das iniciativas de mitigação (custo e esforço) versus efeito na mitigação do risco e respectivo retorno; e
(v) Disponibilidade de recursos (investimento e esforço) para implantação.

Dono do Risco (Risk Owner): Deve ser um membro do Diretoria da Companhia, que possua o maior domínio e conhecimento técnico acerca do risco correspondente, responsável pela tomada de decisão e capaz de estabelecer e gerir os planos de ação para adequar a exposição aos limites aprovados.

Atividades de Controle: políticas, procedimentos e mecanismos desenvolvidos para assegurar que eventos indesejáveis sejam prevenidos ou detectados e corrigidos;

Cultura de riscos: conjunto de padrões éticos, valores, atitudes e comportamentos aceitos e praticados, e à disseminação da gestão de riscos como parte do processo de tomada de decisão em todos os níveis;

Linhas de Gestão: Conceito que define papéis e responsabilidades no gerenciamento de riscos e fortalecimento da governança, bem como a interação desses papéis em todos os níveis da Organização. A primeira linha é representada pelos gestores das áreas e/ou negócios, responsáveis diretos pela execução de seus processos e respectivos riscos. A segunda linha são as áreas de apoio ou staff que auxiliam os gestores a executar suas atividades, dentre as áreas de apoio estão as áreas de Gestão de Riscos e Compliance, e a terceira linha é a área de Auditoria Interna, a qual tem a responsabilidade de realizar um monitoramento periódico através de uma avaliação independente do processo de governança, gestão de riscos e sistemas de controles internos que os gestores de primeira linha são responsáveis.

Auditoria interna: Fornece aos órgãos de governança e à alta administração avaliações abrangentes, baseadas no maior nível de independência e objetividade dentro da organização, devendo prover avaliações sobre a eficácia do gerenciamento de riscos e dos controles internos;

Conformidade: Ato de verificar se condutas e práticas internas estão compatíveis com as diversas regras, normativos e legislações;

Componentes dos controles internos da gestão: são os ambientes de controle interno da Tenda, a avaliação de risco, as atividades de controles internos, a informação, a comunicação e o monitoramento;

Controles internos da gestão: processo que engloba o conjunto de regras, procedimentos, diretrizes, protocolos, rotinas de sistemas informatizados, conferências e trâmites de documentos e informações, entre outros, operacionalizados de forma integrada pela direção e pelo corpo de colaboradores da empresa, destinados a enfrentar os riscos e fornecer segurança razoável de que os objetivos organizacionais serão alcançados.

5. DIRETRIZES

O processo de gerenciamento de riscos segue os princípios éticos da Companhia, valores e cultura, e as informações geradas pelo processo de gestão de riscos devem ser confiáveis, seguir as orientações legais, e fornecer subsídios para tomada de decisões visando a redução do grau de exposição aos riscos e priorização de ações. Cabe a administração garantir recursos aptos a operacionalização dos processos de identificação, avaliação, tratamento e monitoramento dos riscos, assim como, para garantir a proteção e o devido tratamento de dados pessoais, a fim de garantir a privacidade aos colaboradores, conselheiros, acionistas, possíveis clientes, clientes, parceiros comerciais, intermediários, consultores, prestadores de serviços, corretores, bem como todas as pessoas físicas identificadas e/ou identificáveis, no ambiente de trabalho da Tenda.

Anualmente, a Matriz de Riscos deverá ser atualizada conforme percepção de impacto e probabilidade da Diretoria Executiva e Conselho de Administração, e posteriormente validada pelo Comitê de Auditoria possibilitando a consolidação a fim de ter uma ordem de prioridade de desenvolvimento de cada Risco.

A mitigação de riscos depende de implementação de controles, sistemas e mecanismos de proteção que não possuem forma ou modelo único, e sempre deve ser priorizado aquele que mais adapte-se ao processo, estrutura e recursos disponíveis no momento de acionamento.

Todas as informações e reportes resultantes do processo de gestão de riscos devem possuir repositório e guarda adequado, de preferência diretório específico, no servidor da Companhia, com acesso restrito pela área de Auditoria Interna, responsável pelo gerenciamento de riscos. Deverão ser classificadas como informações restritas ao uso interno, e as informações cujo reporte será externo, como Formulário de Referência devem refletir a metodologia utilizada e, se necessário, informações superficiais sobre a exposição identificada no processo de gestão de riscos.

A capacitação dos empregados e agentes da Tenda, são desenvolvidas de forma continuada, por meio de soluções educacionais através de plataformas de desenvolvimento, em todos os níveis, bem como, por meio de orientações pautadas no Código de Ética.

6. CATEGORIA DE RISCOS

A Companhia categoriza seus riscos conforme as diretrizes abaixo e sempre considera os fatores externos e internos em cada categoria:

Risco Estratégico: Riscos que afetam os objetivos estratégicos, considerando ambiente interno e externo;

Risco Operacional: Riscos relacionados à operação da Companhia (processos, pessoas e tecnologia), que afetam a eficiência operacional. Podem se manifestar de diversas maneiras, como por exemplo: atos fraudulentos, interrupção do negócio, conduta incorreta de funcionários, deficiência em contratos, resultando em perdas financeiras, comerciais, multas fiscalizatórias e/ou impactos jurídicos e reputacionais.

Risco Financeiro: Está associado à exposição das operações financeiras/contábeis da Companhia e confiabilidade das demonstrações financeiras.

Risco Regulamentar: Riscos relacionados ao cumprimento de normas e legislação, considerando leis aplicáveis ao setor de incorporação/construção civil e outras legislações (ambiental, trabalhista, cível e tributário/ fiscal).

7. METODOLOGIA

A metodologia aplicada é baseada nos componentes do COSO ERM (Enterprise Risk Management), sendo subdividida nos seguintes itens: Ambiente Controlado, Fixação de objetivos, Identificação de Eventos, Avaliação de Riscos, Resposta aos Riscos, Atividades de Controle, Informações e comunicações e Monitoramento.

Governança e Cultura de riscos: A cultura de riscos deve ser disseminada em todos os níveis da Companhia e a gestão e monitoramento dos riscos não deve ser uma ação exclusiva de um único executivo ou departamento. Os gestores são responsáveis primários pela gestão cotidiana dos riscos associados à sua área ou processo de negócio e disseminação de cultura de gestão de riscos entre seus liderados.

Risco, estratégia e definição dos objetivos: a estratégia e gerenciamento de riscos deve compreender os fatores internos e externos, bem como o impacto dos riscos que possam estar em desacordo com o direcionamento definido pela Companhia e possam afetar o atendimento dos objetivos de negócios e estratégia.

Identificação, avaliação e resposta: os riscos devem ser periodicamente identificados, avaliados, priorizados e documentados de forma estruturada para que possam ser tratados adequadamente.

Os riscos são categorizados de acordo com sua natureza e origem, conforme Categorias de Riscos. Para tanto, é necessário descrever os processos de identificação, avaliação e tratamento dos riscos, são eles:

(i) **Identificação**: O processo de captura e identificação de riscos consiste na utilização de ferramentas e metodologia COSO ERM (Enterprise Risk Management) para estabelecer as matrizes de riscos e controles e mantê-las constantemente atualizadas. A Companhia deve estar atenta para o surgimento de novos riscos e/ou riscos denominados emergentes, que assim que identificados, devem ser avaliados, incorporados ao processo de gestão de riscos e, dependendo de sua criticidade, imediatamente reportados e tratados.

Podemos definir que a abordagem da Companhia para identificar os principais riscos de negócio é composta por três fases:

1. **Análise Geral de Riscos (AGR)**: Identificação e avaliação dos riscos de negócio da Companhia através de uma matriz de riscos corporativos, cujo conteúdo é atualizado anualmente por meio de entrevistas para obtenção de percepções sobre os atuais riscos dos negócios e avaliação do plano de auditoria e dos ciclos testes de controles internos do ano anterior, abordando os 4 grupos de riscos: estratégico, regulamentar, financeiro e operacional.

2. **Avaliação final e priorização de riscos**: O Modelo de Classificação de Processos (MCP), define os processos da Companhia em três principais categorias: processos corporativos, processos operacionais e processos de apoio. Ao final deste processo, são estabelecidos os riscos prioritários, bem como o plano anual de auditoria interna, com objetivo de que estes riscos sejam avaliados de maneira recorrente no ano subsequente.

3. **Execução do plano anual de auditoria e testes recorrentes de controles internos**: A Matriz de Riscos é avaliada de forma recorrente, através dos trabalhos de auditoria interna, que são planejados através de cronograma estruturado. As revisões da auditoria interna têm como principal objetivo a avaliação dos controles internos e execução de testes transacionais dos processos classificados como prioritários. As eventuais exceções identificadas nos trabalhos geram planos de ação para mitigação dos riscos associados. Os relatórios, bem como os planos de ação são validados e reportados formalmente para a Diretoria e Comitê de Auditoria.

(ii) **Avaliação**: Os riscos devem ser avaliados de acordo com seu impacto e probabilidade de ocorrência, considerando as premissas abaixo. A classificação final do risco será definida em função da combinação entre o resultado da probabilidade e impacto.

a. Impacto considera a análise dos riscos em relação ao possível impacto nas operações da Companhia. O critério para definição do impacto será aplicado de acordo com premissas qualitativas e quantitativas, as quais se encontram representadas no quadro abaixo:

Impacto	Peso Atribuído	Métricas de Avaliação de Impacto
Alto	5	1.1 Impacto financeiro acima de **R$ 8 milhões**. 1.2 Continuidade dos negócios pode ser afetada. 1.3 Ausência /desalinhamento entre a estratégia, os valores/missão e os processos de negócios. 1.4 Comprometimento da imagem perante ao mercado/sociedade. 1.5 Não atendimento aos requerimentos mínimos estabelecidos pelos órgãos reguladores. 1.6 Falhas e/ou erros relevantes nas Demonstrações Financeiras que requeiram revisão imediata. 1.7 Eventos que necessitem ser reportados ao Conselho de Administração e Comitês da Companhia. 1.8 Atos ilegais 1.9 Perda de alianças-chave (Caixa Econômica) para o negócio 1.10 Óbitos ou afastamentos em decorrência de acidentes de trabalho.
Significativo	4	2.1 Impacto financeiro entre **R$ 8 milhões e R$ 4 milhões**. 2.2 Grande relevância interna nos processos de negócios. 2.3 Falhas e/ou erros relevantes nas Demonstrações Financeiras que requeiram revisão a médio prazo. 2.4 Eventos que necessitem ser discutidos e avaliados pela Diretoria e Presidência. 2.5 Comprometimento do *market share*. 2.6 Falhas na segurança de dados e informações. 2.7 Impacto na rentabilidade dos projetos.
Moderado	3	3.1 Impacto financeiro entre **R$ 4 milhões e R$ 2 milhão**. 3.2 Falhas e/ou erros relevantes nas Demonstrações Financeiras que requeiram revisão no longo prazo. 3.3 Eventos que necessitem ser discutivos e avaliados pela(s) Gerência(s). 3.4 Relevância interna nos processos de negócio. 3.5 Dificuldades para atender às necessidades dos clientes.
Baixo	2	4.1 Impacto financeiro entre **R$ 2 milhões e R$ 1 milhão.** 4.2 Baixa relevância nos processos de negócio. 4.3 Processo não relevantes nas Demonstrações Financeiras. 4.4 Sem impacto no valor da marca. 4.5 Eventos que necessitem ser discutidos e avaliados pelo(s) Coordenador(es).
Insignificante	1	5.1 Impacto financeiro até **R$ 1 milhão.** 5.2 Sem relevância na participação de mercado. 5.3 Eventos que necessitem ser discutivos e avaliados pelos Analistas.

b. A probabilidade, por sua vez, considera uma análise dos riscos em relação à magnitude em que a Companhia está exposta ou desprotegida, considerando: (i) Efetividade dos controles internos; (ii) Nível de influência da gestão em relação ao fator de risco; (iii) Velocidade em que o risco pode ser materializar; (iv) Histórico de ocorrências de materialização do risco, entre outros. Abaixo o quadro de probabilidade de ocorrência adotada pela Companhia:

Probabilidade de Ocorrência	Peso Atribuído	Range de Posibilidade de Ocorrência
Quase Certo	**100**	Esperado ocorrer na maioria das vezes (acima de 80%)
Provável	**80**	Provável que ocorra em grande parte das vezes (acima de 50% até 80%)
Possível	**50**	Pode ocorrer em algum momento (acima de 20% até 50%)
Pouco Provável	**20**	Poderia ocorrer em circunstâncias excepcionais (acima de 5% até 20%)
Remoto	**5**	Poderia acontecer em circunstâncias raras (até 5%)

Sendo assim, para a etapa de análise, os riscos devem ser classificados individualmente e associados na matriz de impacto versus probabilidade no quadrante adequado, conforme a classificação efetuada sob os aspectos dos eixos Impacto e Probabilidade

Tenda – Matriz de Impacto x Probabilidade

Impacto	Peso	Matriz de Impacto x Probabilidade				
Alto	5	5%	20%	50%	80%	100%
Significativo	4	4%	16%	40%	64%	80%
Moderado	3	3%	12%	30%	48%	60%
Baixo	2	2%	8%	20%	32%	40%
Insignificante	1	1%	4%	10%	16%	20%
Peso Probabilidade		5 Remoto	20 Pouco Provável	50 Possível	80 Provável	100 Quase Certo
% Ocorrência		1% - 5%	6% - 20%	21% - 50%	51% - 80%	+80%

Classificação do Risco	Range Percentual
Crítico	80,00 à 100,00%
Alto	50,00 à 79,99%
Significativo	40,00 à 49,99%
Moderado	05,00 à 39,99%
Baixo	0,01 à 04,99%

A partir da classificação do risco, a Companhia endereça para a respectiva área o material que permitirá o oportuno entendimento das exposições sofridas, dos planos de ação e contingência, com a finalidade de minimizar os riscos e os prazos de conclusão das ações, além de eventuais medidas para evitar eventos futuros.

(iii) **Resposta**: Os riscos identificados devem ser gerenciados de forma adequada e a definição de resposta deve ser realizada de acordo com a sua criticidade. A ação de resposta deve considerar a relação entre impacto e probabilidade, custos e benefícios para que o risco seja adequadamente mitigado. Na companhia são empregadas quatro possibilidades para resposta ao Risco:

a. Eliminar: eliminar totalmente o Risco, protegendo os objetivos da empresa dos impactos associados ao Risco;

b. Compartilhar: compartilhar o risco a terceiros por meio de contratos de seguros, terceirização de operações e atividades;

c. Tratar/Mitigar: reduzir parcialmente a exposição ou adotar ações pontuais visando minimizar potenciais impactos; e

d. Aceitar: assumir os impactos potenciais do risco e respectivas oportunidades.

A resposta ao risco identificado deve ser efetuada de acordo com as alçadas definidas pela criticidade do risco mapeado, representadas na tabela abaixo:

Classificação do Risco	Alçadas de Resposta ao Risco	Tomada de Decisão
Crítico	CEO + Diretor da Área responsável pelo Processo	A decisão de resposta ao Risco deve ser discutiva e tratada pelo CEO em conjunto com a(s) Diretoria(s) Executiva(s) responsável(is) pelo processo gerador do risco.
Alto	Diretor da Área responsável pelo Processo	A decisão de resposta ao Risco deve ser discutida e tratada pela(s) Diretoria(s) Executiva(s) responsável(is) pelo processo gerador do risco
Significativo		
Moderado	Gerente da Área responsável pelo Processo	A decisão de resposta ao Risco deve ser discutida e tratada pela(s) Gerência(s) responsável(is) pelo processo gerador do risco
Baixo		

As ações que forem geradas com base nas respostas ao risco, pela decisão de "Eliminar", "Tratar", "Compartilhar", serão acompanhadas pela área de Gestão de Riscos através de compromisso firmado pelas partes, e deverão seguir os prazos para implementação de Planos de Ação de acordo com a criticidade do risco, seguindo as premissas da tabela abaixo:

Classificação do Risco	PDA com envolvimento de melhorias e/ou recursos atreladas uso de Tecnologia da Informação?	Prazo para Implementação de Ação ao Risco Identificado
Crítico	**SIM**	Implementar plano de ação com prazo máximo de até **120 dias** após a emissão do relatório de Auditoria ao Comitê de Auditoria.
	NÃO	Implementar plano de ação com prazo máximo de até **30 dias** após a emissão do relatório de Auditoria ao Comitê de Auditoria.
Alto	**SIM**	Implementar plano de ação com prazo máximo de até **150 dias** após a emissão do relatório de Auditoria ao Comitê de Auditoria.
	NÃO	Implementar plano de ação com prazo máximo de até **60 dias** após a emissão do relatório de Auditoria ao Comitê de Auditoria.
Significativo	**SIM**	Implementar plano de ação com prazo máximo de até **180 dias** após a emissão do relatório de Auditoria ao Comitê de Auditoria.
	NÃO	Implementar plano de ação com prazo máximo de até **90 dias** após a emissão do relatório de Auditoria ao Comitê de Auditoria.
Moderado	**SIM**	Implementar plano de ação com prazo máximo de até **180 dias** após a emissão do relatório de Auditoria ao Comitê de Auditoria.
	NÃO	Implementar plano de ação com prazo máximo de até **90 dias** após a emissão do relatório de Auditoria ao Comitê de Auditoria.
Baixo	**SIM**	Implementar plano de ação com prazo máximo de até **210 dias** após a emissão do relatório de Auditoria ao Comitê de Auditoria.
	NÃO	Implementar plano de ação com prazo máximo de até **120 dias** após a emissão do relatório de Auditoria ao Comitê de Auditoria.

Para o risco que o responsável (de acordo com o quadro de alçadas de assunção/apetite ao risco) optar por "Aceitar", este deverá preencher e assinar eletronicamente o formulário "F.001-GRC -Termo de Assunção de Risco", documentando perante a área de Gestão de Riscos, e demais Órgãos de Governança da Companhia que está ciente da exposição aos riscos mapeados, bem como aceitando as consequências que a situação pode acarretar para a Companhia futuramente.

8. CONSIDERAÇÕES ADICIONAIS

Informação e comunicação: As informações utilizadas para gerenciamento dos riscos devem ser íntegras e corretas, representando a situação atual das operações da Companhia. Os riscos da Companhia devem ser comunicados e conhecidos por todos os envolvidos em seu gerenciamento e monitoramento, devem ser reportados tempestivamente. O processo de comunicação dos riscos deve ser claro e eficiente, o conteúdo das informações deve ser suficiente para tomada de decisão apropriada.

Monitoramento: Deve haver monitoramento constante para evitar que a exposição da Companhia aos riscos aumente e impeça a continuidade de negócios. O adequado monitoramento consiste no acompanhamento do ambiente de controle da Companhia e ações de resposta aos riscos.

A estrutura de controle interno deve ser avaliada periodicamente, verificando a eficiência dos controles existentes e influências decorrentes de potenciais mudanças no ambiente interno e/ou externo da Companhia.

As ações de melhorias (planos de ação), bem como sua efetividade devem ser acompanhadas, garantindo o atingimento do propósito inicial, prazo de implementação, e eficiência para redução do risco.

9. RESPONSABILIDADES

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

A Diretoria, o Comitê de Auditoria e o Conselho de Administração da Companhia devem compreender as práticas, permitindo o cumprimento adequado de suas responsabilidades no processo e fortalecendo os níveis de governança corporativa.

Nesse contexto, as responsabilidades são distribuídas da seguinte forma:

Conselho de Administração:

(i) Definir os objetivos estratégicos da companhia, que nortearão o trabalho de identificação dos riscos da organização;
(ii) Acompanhar as ações de gerenciamento dos riscos conforme direcionamento de negócios da Companhia;
(iii) Validar os ciclos de revisão do sistema de controle de riscos e sua eficácia;
(iv) Determinar o apetite e tolerância aos riscos;
(v) Validar documentação de informações públicas sobre o modelo de gestão de riscos e transparência de informações prestadas ao Público interno e externo; e
(vi) Disponibilizar e alocar os recursos necessários para a gestão de risco.

Comitê de Auditoria:

(i) Acompanhar e recomendar sobre a aceitação das respostas aos riscos;
(ii) Auxiliar a Administração na definição das diretrizes de gestão de riscos, métricas de mensuração da tolerância e apetite aos riscos;
(iii) Acompanhar ações de implementação de planos de ação mitigatórios;
(iv) Reportar suas conclusões ao Conselho de Administração;
(v) Aprovar o dicionário de riscos, linguagem comum dos riscos e fortalecer a cultura de gestão de riscos;
(vi) Acompanhar as ações de gerenciamento dos riscos conforme apetite da Companhia;
(vii) Acompanhar e estimular o desenvolvimento de estruturas e mecanismos de proteção de riscos;
(viii) Propor alterações na Política de Gestão de Riscos e submetê-las ao Conselho de Administração; e
(ix) Assegurar a operacionalização dos mecanismos e controles relacionados ao gerenciamento de riscos;

Diretoria:

(i) Atualizar a Matriz de Riscos sempre que ocorrer a revisão do plano estratégico ou AGR – Avaliação Geral de Riscos e tempestivamente com o surgimento de fatores de risco emergentes;
(ii) Estabelecer priorização dos Riscos a partir do impacto e probabilidade;

(iii) Acompanhar periodicamente a evolução da exposição aos Riscos considerando os limites aprovados pelo Conselho de Administração;
(iv) Adotar Riscos avaliados como ferramenta de orientação da revisão ou construção do plano estratégico; e
(v) Disseminar a cultura da gestão de Risco em toda Companhia.

Gestão de Riscos:

(i) Mapear processos e auxiliar na identificação dos riscos (operacionais e financeiros, por exemplo), além de garantir os respectivos controles para mitigar os riscos identificados;
(ii) Acompanhar e sugerir melhorias de controles internos nas áreas operacionais;
(iii) Reportar inconsistência ou desatualização de desenhos de fluxos de processos, normas e procedimentos cujas alterações podem agravar o ambiente de controles;
(iv) Identificar novas oportunidades e processos aptos à priorização a partir dos resultados do processo de riscos em execução, bem como ampliar o ambiente de testes substantivos ou monitoramento contínuo a partir da identificação de novos riscos ou agravamento de riscos já identificados;
(v) Após a implementação dos planos de ação, validar se todas as ações propostas foram implementadas como planejado;

Donos dos Riscos ou Áreas de negócios:

(i) Identificar, em conjunto com a área de Gestão de Riscos os fatores e indicadores para a mensuração e monitoramento dos Riscos;
(ii) Fornecer informações precisas, íntegras e suficientes para análise;
(iii) Apresentar percepção quanto à exposição ao Risco (magnitude de impacto);
(iv) Sugerir, avaliar, implantar e monitorar as ações com o objetivo de reduzir a exposição ao Risco sob sua responsabilidade;
(v) Cumprir os limites de Riscos aprovados pelo Conselho de Administração;
(vi) Comunicar tempestivamente os eventos de risco que apresentarem tendência de ocorrência e/ou eventual extrapolação de limites; e
(vii) Dar cumprimento ao plano de ação.

10. ELABORADOR

Coordenador de Gestão de Riscos

11. APROVADORES

Gerente de Gestão de Riscos
Comitê de Auditoria
Conselho de Administração

12. RESPONSÁVEL

Gerente de Gestão de Riscos

13. TABELA DE REVISÃO

REVISÃO	DATA	HISTÓRICO
00	03/10/2018	Aprovação final da Política
01	13/10/2021	Revisão Geral do Documento
02	15/06/2023	Revisão Geral do Documento
03	02/08/2023	Revisão Geral do Documento
04	08/05/2025	Revisão Geral do Documento