POLÍTICA DE GERENCIAMENTO DE RISCOS CORPORATIVOS

Grendene®

[B]³ BRASIL BOLSA BALCÃO

GRENDENE S.A.

Companhia Aberta

CNPJ nº 89.850.341/0001-60 – NIRE nº 23300021118-CE

Política de Gerenciamento de Riscos Corporativos

1. Objetivo

1.1. Dado que o risco é inerente a qualquer atividade empresarial, cabe às sociedades o gerenciarem com vistas a assumir riscos calculados, reduzir a volatilidade dos seus resultados e aumentar a previsibilidade de suas atividades e se tornar mais resilientes em cenários extremos. A eficácia no gerenciamento de riscos pode afetar os objetivos estratégicos e estatutários estabelecidos pela administração e, em última análise, pode impactar a longevidade da organização.

1.2. Assim, esta Política de Gerenciamento de Riscos Corporativos ("Política") visa estabelecer diretrizes a serem observadas no processo de Gestão de Riscos Corporativos da Grendene S.A. ("Grendene" ou "Companhia"), de forma a possibilitar a identificação, avaliação, priorização e tratamento dos riscos que permeiam os processos/ negócios da Companhia.

2. Abrangência

2.1. Esta Política se aplica à Companhia e às suas controladas, assim como a todos os respectivos administradores e demais colaboradores, de forma a possibilitar a adequada identificação, avaliação, direcionamento, monitoramento e comunicação dos fatos ou eventos incertos cuja materialização possa causar impactos negativos aos negócios da Companhia e suas controladas aos quais a Companhia e suas controladas estejam ou possam estar expostas, contribuindo para o gerenciamento dos mesmos e para a tempestiva tomada de decisões e medidas aplicáveis.

2.2. Portanto, esta Política aplica-se a todos os níveis organizacionais da Grendene S.A., no Brasil e no exterior, conforme o caso.

3. Documentos de Referência

- Código de Conduta da Grendene;
- Committee of Sponsoring Organizations of the Treadway Commission – COSO ERM 2017 Gerenciamento de Riscos Corporativos – Integrado com Estratégia e Performance;
- Committee of Sponsoring Organizations of the Treadway Commission – COSO ICIF 2013 Controle Interno – Estrutura Integrada;
- Instituto Brasileiro de Governança Corporativa, IBGC – Gerenciamento de riscos corporativos: evolução em governança e estratégia (caderno 19);
- The Institute of Internal Auditors – Modelo das Três Linhas do IIA 2020: Uma atualização das três linhas de defesa.

4. Conceitos

4.1. Para efeito desta Política destacamos os seguintes termos:

a) Risco: a possibilidade de ocorrência de eventos que venham a ter impacto adverso no cumprimento dos objetivos estratégicos e dos processos de negócios da Companhia.

b) Fatores de Risco: representam as causas/ desdobramentos dos riscos identificados.

c) Gerenciamento de Riscos Corporativos: processo integrado ao planejamento estratégico e à performance operacional, visando prover garantias razoáveis em relação ao atingimento dos objetivos da Companhia, por meio da identificação, classificação, avaliação e resposta aos riscos, respeitando o apetite a risco definido pela empresa.

d) Apetite a Risco: estabelece os limites de riscos aceitáveis associados ao grau de exposição a riscos que a organização está disposta a aceitar para atingir seus objetivos empresariais e criar valor para os seus acionistas, respeitando as partes interessadas. Portanto, é o grau de exposição a riscos que a Companhia está disposta a assumir para atingir seus objetivos.

e) Resposta ao Risco: abordagem de tratamento do risco, aplicada de acordo com as diretrizes de apetite a risco definidas pela organização, ou seja, são as ações ou decisões relacionadas aos passos para evitar, transferir, mitigar ou aceitar um risco.

f) Tolerância a Riscos: Refere-se à quantidade de riscos que a Companhia (ou parte interessada) deseja absorver para a consecução de seus objetivos.

g) Controle Interno: é (ou são) o (ou conjunto de) processo(s) ou mecanismo(s) criado(s) para oferecer confiança razoável sobre o atingimento dos objetivos da Companhia, por meio da mitigação dos riscos inerentes ao negócio, incluindo, sem limitação, a criação de órgãos internos de fiscalização da Companhia (e.g., comitê de auditoria).

h) Modelo das Três Linhas: desenvolvido pelo The IIA com o intuito de apresentar os três principais papéis de atuação na gestão de risco de uma organização, anteriormente conhecido como as três linhas de defesa.

i) A Primeira Linha consiste na maior parte dos colaboradores de uma empresa, que estão diretamente envolvidos com a entrega de valor para os clientes (por exemplo, comercial, logística, produção e suprimentos), incluindo as funções de apoio (como por exemplo Recursos Humanos, Tecnologia da Informação e Finanças). Ou seja, a Primeira Linha está na linha de frente do gerenciamento de riscos corporativos.

ii) Segunda Linha representa as funções especializadas em gerenciamento de riscos e que assessoram a Primeira Linha, como Gestão de Riscos, Controles Internos, Compliance, Qualidade, Saúde e Segurança do Trabalho, Segurança da Informação e Sustentabilidade.

iii) Terceira Linha visa checar a eficácia do gerenciamento de riscos corporativos, representado pela função de auditoria interna.

Figura 1: O Modelo das Três Linhas do The IIA

5. Processo de Gerenciamento de Riscos

A estrutura organizacional dos processos de gerenciamento de riscos da Companhia utiliza como parâmetro as diretrizes estabelecidas pelo Comitê de Organizações Patrocinadoras da Comissão *Treadway (Committee of Sponsoring Organizations of the Treadway Commission) – COSO*, especialmente no que diz respeito ao fluxo de identificação, avaliação, tratamento e monitoramento dos Riscos aos quais a Companhia e suas controladas estão expostas.

Nesse sentido, os objetivos devem ser estabelecidos antes da identificação das situações em potencial que poderão afetar sua realização.

Dessa forma, o processo de gerenciamento de riscos corporativos envolve a adoção, pela administração da Companhia, de um processo para estabelecer o alinhamento entre os objetivos fixados e o propósito, valores e pilares estratégicos da Companhia bem como permeia todos os processos de negócios da Grendene, visto que toda decisão tomada e atividade executada possui algum risco inerente. Para tanto, este processo é composto por 6 (seis) etapas, sendo: (i) analisar o contexto e definir o apetite a risco; (ii) identificar e classificar os riscos; (iii) avaliar e priorizar os riscos; (iv) responder aos riscos; (v) monitorar riscos e controles internos; e (vi) comunicar.

5.1 Analisar o Contexto e definir o Apetite a Risco

Esta etapa consiste no entendimento do ambiente de negócios e da estratégia da Companhia, identificando e analisando os principais riscos que podem afetar o atingimento destes objetivos estratégicos. Neste momento, a Companhia define o seu apetite a risco, que alinhado com a estratégia, estabelece os limites de exposição do negócio e serve de parâmetro para a avaliação e respostas aos riscos organizacionais.

Com o apoio do Comitê de Auditoria, o Conselho de Administração, periodicamente, realizará a análise e revisão do apetite a riscos (grau de risco aceitável) da Grendene.

5.2. Identificar e Classificar os Riscos

O entendimento dos processos de negócio e/ou de suporte é fundamental para o processo de gestão de risco e consiste em (i) mapear as atividades envolvidas no processo; (ii) entender (contemplando análise de documentação existente relacionada ao processo), identificar, classificar e registrar os riscos inerentes as atividades da Grendene, presentes nos mais diversos processos organizacionais. Para tanto, deve-se levar em consideração as avaliações históricas de materialização dos riscos, oriundas de diversas fontes (como auditorias, canal de ética, entre outros registros), bem como as mudanças no contexto de negócios analisadas na etapa anterior.

Esta identificação e classificação dos riscos deve ser conduzida pela área Governança, Riscos e Compliance - GRC (Segunda Linha), em conjunto às áreas responsáveis pelos processos organizacionais (Primeira Linha), mediante entendimento das atividades, contexto e objetivos de cada processo.

Cada risco identificado será devidamente classificado e registrado conforme as seguintes categorias:

a) Estratégico: riscos relacionados ao plano estratégico e diretrizes macro da Companhia. Podem ser relacionados tanto aos aspectos exteriores à Companhia, tais como, aspectos econômicos, políticos e sociais bem como aos aspectos interiores da Companhia, tais como, inovações, parcerias estratégicas, fusões e aquisições, entre outras questões vinculadas à estratégia da Grendene, independentemente de serem exteriores ou interiores.

b) Operacional: riscos associados à possibilidade de ocorrência de perdas (por exemplo: de produção, ativos, clientes, receitas) resultantes de falhas, deficiências ou inadequação de processos internos e pessoas.

c) De Conformidade (*Compliance*): riscos relacionados à falta de habilidade ou disciplina da organização para cumprir com a legislação e/ou regulamentação externa (e.g., regulamentações da CVM e da B3) aplicáveis ao negócio e às normas e procedimentos internos, incluindo o código de conduta da Grendene.

d) Financeiro e de Mercado: riscos associados à exposição das operações financeiras e gestão do caixa da organização, incluindo, sem limitação, risco de liquidez, risco de crédito e riscos relacionados às oscilações de mercado (taxas de juros e câmbio, por exemplo).

e) Da Informação: riscos relacionados à perda, vazamento ou uso indevido de dados confidenciais ou pessoais, independente de culpa e/ou dolo, conforme o caso, dos envolvidos.

f) Tecnológico: corresponde a perdas e/ou danos relacionados à disponibilidade, desempenho, integridade e segurança dos sistemas da empresa, bem como falhas e/ou indisponibilidade de equipamentos informatizados.

g) Socioambiental: riscos associados às questões climáticas, meio ambiente e questões sociais.

5.3. Avaliar e Priorizar os Riscos

Os riscos, após identificados, classificados e registrados, devem ser avaliados com base em duas dimensões:

a) Probabilidade: expectativa de ocorrência do risco em determinado horizonte de tempo;

b) Impacto: severidade do resultado da materialização de um dado risco.

Para tanto, deve-se mensurar Probabilidade e Impacto dentro de 5 diferentes níveis, conforme mostrado na Figura 2, que alocarão o risco em 3 diferentes graus:

a) Risco Alto: os riscos deverão ser priorizados em curtíssimo / curto prazo através ações de mitigação e/ou implantação de controles internos;

b) Risco Médio: os riscos deverão ser priorizados em curto / médio prazo através ações de mitigação e/ou implantação de controles internos;

c) Risco Baixo: os riscos deverão ser priorizados após a implementação de ações e controles internos nos riscos avaliados como críticos e significativos.

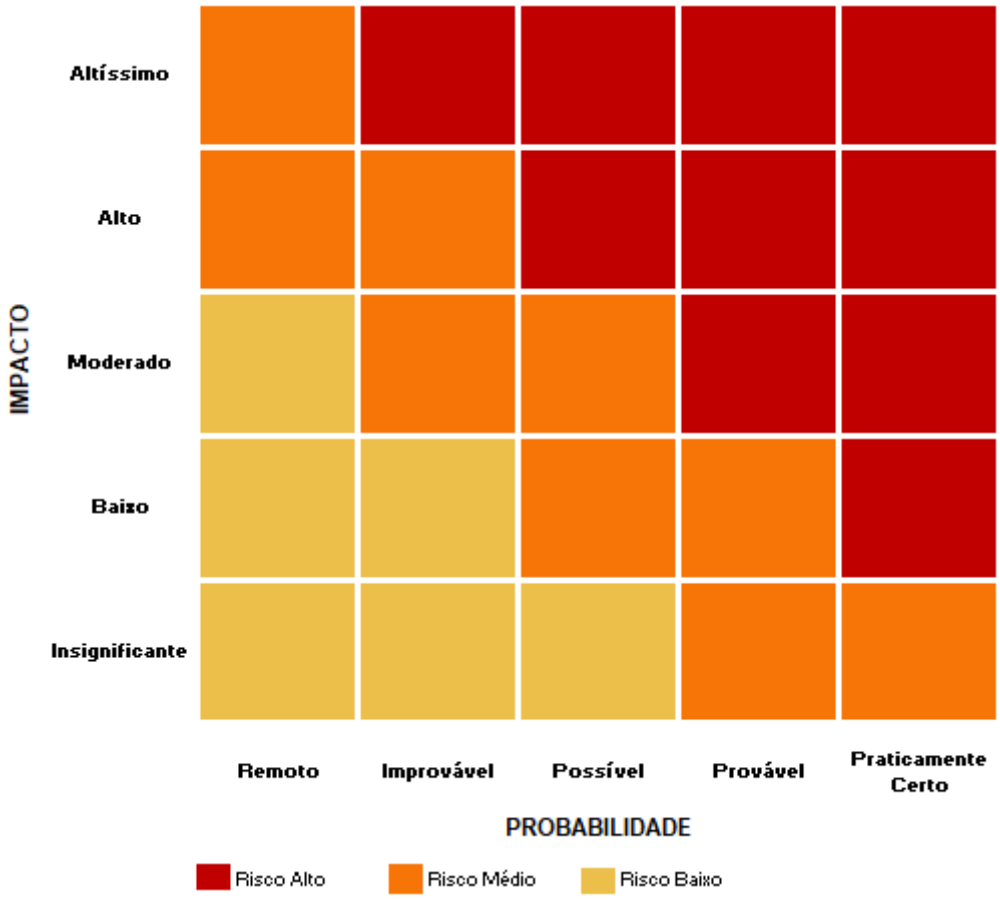

Figura 2 – Matriz de Avaliação de Riscos

Para realizar esta etapa de avaliação e priorização dos riscos deve-se levar em consideração os seguintes aspectos:

a) Independente da classificação do risco, considerar os possíveis impactos socioambientais, caso o risco se materialize;

b) Eficiência dos controles internos atuais, o que requer uma avaliação do funcionamento deles. Neste caso, pode-se verificar aspectos como: mitigação do risco, tempestividade; segregação de função; procedimentos de detecção de erros e tratamento deles; automação; entre outros;

c) Frequência em que o processo está exposto ao risco;

d) Possíveis interferências no andamento da operação da empresa, caso o risco se materialize;

e) Possíveis perdas financeiras, caso o risco se materialize;

f) Possíveis impactos negativos para a imagem da empresa perante as partes interessadas, caso o risco se materialize;

g) Possíveis autuações, condenações, perda de benefícios ou embargos, caso o risco se materialize.

5.4. Responder aos Riscos

Com base na avaliação realizada na etapa anterior, as respostas deverão se encaixar nos 4 (quatro) tipos de tratamento listados abaixo:

Evitar: descontinuação das atividades que geram os riscos. Nenhuma alternativa é aceitável ou viável para reduzir o impacto ou probabilidade de ocorrência do risco, justificando abandonar o negócio ou processo que gera o risco.

Mitigar: adoção de medidas para reduzir a probabilidade de ocorrência ou o impacto dos riscos.

Transferir: redução da probabilidade de ocorrência ou impacto dos riscos pela transferência ou pelo compartilhamento de uma porção do risco através de contratação de seguros, hedge, associações, terceirização de uma atividade, dentre outros.

Aceitar: nenhuma medida é adotada para afetar a probabilidade de ocorrência ou impacto dos riscos, contudo, o evento deverá ser monitorado por controles para reavaliação periódica.

Os controles internos compreendem as respostas “mitigar” e “transferir”, portanto, precisam ser avaliados, melhorados ou implantados (caso não existam). Ou seja, os controles internos têm papel fundamental na gestão dos riscos corporativos, devendo serem mapeados e gerenciados pela empresa, assim como os riscos aos quais eles objetivam mitigar.

5.5 Monitorar Riscos e Controles Internos

Uma vez avaliados os riscos e revisados/ implantados os controles internos, o processo passará por ciclos de monitoramento, com o objetivo de verificar a eficácia dos controles internos e, por consequência, a avaliação dos riscos.

Os riscos e os controles internos definidos serão consolidados em uma matriz de riscos e matriz de controles internos da Grendene, visando facilitar o monitoramento e sua gestão.

Em relação aos riscos, a empresa, periodicamente, realizará revisões, podendo alterar o grau do risco, bem como incluir novos riscos detectados (riscos emergentes). Nesta etapa, deve-se identificar alterações nos ambientes externos e internos e aprimorar a análise de eventos e o processo de avaliação de riscos.

Em relação aos controles internos, o monitoramento será realizado por meio de testes com base na matriz de controles internos da empresa (definindo amostras e coletando evidências dos controles internos), de acordo com calendário preestabelecido.

5.6 Comunicar

Esta última etapa tem por objetivo desenvolver uma cultura de transparência, responsabilização e conscientização dos riscos, além de garantir uma comunicação clara, objetiva e tempestiva a todas as partes interessadas, emitindo comunicados, relatórios, entre outras ações.

6. Responsabilidades

Como o processo de gerenciamento de riscos corporativos permeia todos os processos de negócios, todos os colaboradores da Grendene são responsáveis pela gestão dos riscos da Companhia, desde a definição de estratégias e projetos, como na execução de suas funções no dia a dia.

6.1 Conselho de Administração

Monitorar periodicamente os principais riscos da Grendene reportados pelo Comitê de Auditoria;

Supervisionar periodicamente os processos do Gerenciamento de Riscos Corporativos da Grendene, incluindo a exposição aos riscos, a eficácia dos controles internos e a conformidade (Compliance);

Definir o apetite a risco para a Companhia em função das diretrizes, objetivos e projetos estratégicos;

Garantir que a Grendene possua uma estrutura adequada e compatível com sua complexidade (e tamanho) de Auditoria, Governança, Riscos e Compliance;

Zelar pela independência da área de Governança, Riscos e Compliance - GRC;

Definir e aprovar as atribuições da auditoria interna;

Aprovar a política de gerenciamento de riscos, incluindo eventuais alterações e revisões;

Tratar os assuntos omissos desta Política.

6.2 Comitê de Auditoria

Supervisionar as atividades, a efetividade, evolução e estrutura do gerenciamento de riscos corporativos da Grendene, bem como sugerir melhorias ao Conselho de Administração;

Monitorar e avaliar a exposição ao risco da Grendene, e, quando necessário, recomendar alterações na matriz de riscos e/ou nos níveis de apetite a risco da Companhia;

Definir e gerenciar o processo de comunicação e reportes da gestão de riscos corporativa da Grendene;

Revisar periodicamente esta política e, se for necessário, submeter sugestões de alteração ao Conselho de Administração.

6.3 Diretoria Executiva

Acompanhar e patrocinar o processo de gerenciamento de riscos corporativos, apoiando nas ações e conscientização da liderança da Grendene, com base no modelo das Três Linhas do The IIA;

Garantir a integração da gestão de riscos corporativos no processo de concepção, monitoramento e revisão da estratégia da Companhia.

6.4 Colaboradores (Primeira Linha)

Realizar o gerenciamento de riscos no dia a dia de suas atividades, identificando, avaliando e implantando ações de mitigação, bem como apoiar as ações conduzidas pelas áreas especialistas em gestão de riscos na empresa;

Reportar eventos ou situações que representem riscos à Grendene às áreas de gestão de riscos e/ou seu gestor;

Participar ativamente de todas as ações de disseminação da cultura de gestão de riscos, incluindo comunicados e treinamentos.

6.5 Governança, Riscos e Compliance - GRC (Segunda Linha)

Coordenar o processo de Gerenciamento de Riscos Corporativos da Grendene, identificando, classificando, avaliando e respondendo aos riscos, em conjunto com as áreas de negócios responsáveis pelos processos escopo da análise e considerando o apetite a risco definido pelo Conselho de Administração;

Consolidar e manter atualizada a matriz de riscos da Companhia, monitorando constantemente o ambiente de riscos e reportando ao Comitê de Auditoria novos riscos identificados;

Elaborar e manter atualizada a matriz de controles internos, avaliando os controles e assessorando as áreas de negócios no fortalecimento do ambiente de controles internos da Grendene;

Desenvolver e aplicar a metodologia do gerenciamento de riscos corporativos, com base nas melhores práticas de mercado e em conformidade com as leis e normas externas e políticas e procedimentos internos;

Conduzir ações de disseminação de uma cultura de transparência, responsabilização e conscientização dos riscos na Grendene;

Reportar periodicamente as atividades de gestão de riscos corporativos ao Comitê de Auditoria da Grendene.

6.6 Auditoria Interna (Terceira Linha)

Examinar, de forma independente, imparcial e tempestiva, a efetividade e qualidade do processo de gerenciamento de riscos corporativos da Grendene, registrando as fragilidades e fazendo recomendações para a melhoria e ajustes no referido processo;

Avaliar o ambiente e a matriz de controles internos da empresa, testando e apontando a efetividade dos controles existentes e recomendando melhorias, considerando a eficácia da mitigação dos riscos envolvidos;

Por meio do monitoramento e avaliação do processo de gestão de riscos e controles internos, identificar e apontar possíveis riscos ainda não mapeados pela organização;

Acompanhar a implantação das recomendações pontuadas no processo de auditoria/ avaliação do processo de gestão de riscos e do ambiente de controles da Grendene;

Fornecer informações e reportes à alta gestão e ao Comitê de Auditoria sobre a efetividade da gestão de riscos e controles internos da companhia, bem como o atendimento às normas e exigências legais.

7. Disposições Gerais

As omissões desta Política e eventuais dúvidas de interpretação serão decididas em reunião do Conselho de Administração.

A presente Política foi implementada em 24 de fevereiro de 2022 e revisada em 29 de fevereiro de 2024 pelo Conselho de Administração da Companhia vigorando por prazo indeterminado, podendo ser extinta ou modificada a qualquer tempo, desde que aprovada pelo Conselho de Administração.

Farroupilha, RS, 29 de fevereiro de 2024.

Renato Ochman
Secretário
****