POLÍTICA DE GESTÃO DE RISCOS

1. Objetivo

1.1. Estabelecer as diretrizes e responsabilidades na gestão de riscos, especialmente no tocante à identificação e análise dos riscos que possam afetar a empresa, bem como estabelecer controles e procedimentos para monitoramento, de forma a prevenir sua ocorrência ou minimizar seu impacto.

2. Abrangência

2.1. Este Documento Normativo aplica-se a todos os Macroprocessos, Operações de Negócio e empresas Gerdau.

3. Definições:

3.1. Riscos são fatores ou eventos incertos que podem causar impactos negativos, dificultando ou impossibilitando o cumprimento dos objetivos da Empresa.

3.2. Riscos de negócio são aqueles associados à estratégia da companhia (ambiente político e social, mercado, competidores, fusões e aquisições, disponibilidade de matérias-primas), às suas finanças (ambiente econômico, geração de caixa, endividamento, aplicação e captação de recursos financeiros, mercado de capitais, variação cambial), a *compliance* (cumprimento de leis e regulamentos), à imagem e reputação e à operação (tecnologia, modelo de gestão, cultura empresarial, capacitação e sucessão de recursos humanos).

3.3. Riscos operacionais são aqueles decorrentes da inadequação ou falha nos processos internos, pessoas ou ambiente de tecnologia, que possam dificultar ou impedir o alcance dos objetivos da empresa. Estes riscos estão associados tanto ao processo industrial como à gestão de áreas administrativas, como marketing e vendas, suprimentos, logística, saúde e segurança do trabalho, meio ambiente, tecnologia da informação, gestão de pessoas e relações sindicais.

3.4. Comitê de Riscos – comitê cuja composição é determinada pelo Conselho de Administração, adiante designado como Comitê.[1]

3.5. Gerdau Business System, adiante designado como GBS

3.6. Canal da Ética – ferramenta para relatar desvios éticos e esclarecer dúvidas relacionadas ao tema. Aos denunciantes é assegurado o anonimato, o tratamento confidencial do incidente e a inexistência de represálias.

4. Diretrizes

4.1. A empresa identifica e trata os riscos de negócio e operacionais de forma a garantir o cumprimento das metas estabelecidas em seu planejamento estratégico.

4.2. Os riscos são identificados e avaliados de acordo com a probabilidade de ocorrência e seu impacto sobre o negócio, inclusive, sobre a imagem da empresa. Cada decisão tomada leva em

[1] Composição atual do Comitê de Riscos: Diretor-Presidente, Diretor Geral de Operações, Vice-Presidente Jurídico e de Compliance, Vice-Presidente de Finanças, Controladoria & RI e Gerente da Auditoria Interna.

consideração os benefícios, os aspectos negativos e os riscos atrelados, mensurando a relação entre impacto e mitigação.

4.3. Por delegação do Conselho de Administração, o Comitê acompanha temas relevantes, abaixo listados:

4.3.1. Status das avaliações sobre os controles decorrentes da Lei *Sarbanes Oxley*;
4.3.2. Principais trabalhos de auditoria sobre riscos operacionais;
4.3.3. Estatísticas de ética e temas relevantes de *Compliance*;
4.3.4. Principais incidentes registrados no Canal da Ética, respeitados o anonimato e a confidencialidade;[2]
4.3.5. Riscos ambientais, como a destinação de resíduos e áreas potencialmente impactadas;
4.3.6. Riscos de segurança empresarial, como os riscos de perda patrimonial à empresa, bem como à segurança física dos Colaboradores nas diversas localidades em que a Gerdau atua;
4.3.7. Riscos de segurança da informação;
4.3.8. Contingências jurídicas.

4.4. O Comitê avalia a adequação dos controles dos riscos associados a cada macroprocesso e/ou operação, através da avaliação dos indicadores do GBS. Além disto, a cada dois anos ou por demanda, cada macroprocesso e/ou operação apresenta ao Comitê as respectivas práticas de gestão de riscos e o relatório de suas atividades nessa área, no último ano.

4.5. Anualmente, o Comitê presta contas ao Conselho de Administração quanto às atividades desenvolvidas no ano anterior.

4.6. O plano anual de auditoria é elaborado tendo como base, entre outros, os resultados dos trabalhos anteriores de auditoria, os resultados dos testes da certificação *Sarbanes-Oxley*, a compilação das entrevistas com a Alta Administração, realizadas a cada três anos, e as informações recebidas dos gestores dos processos. Neste plano consta, também, o grau de exposição a riscos de todos os processos/unidades da empresa, a partir do qual são definidos os trabalhos de auditoria do próximo ano.

4.7. Além do plano anual, a Auditoria realiza trabalhos por demanda da Alta Administração e oriundos do Canal de Ética.

4.8. As análises do Comitê devem servir de base para a elaboração das informações a serem prestadas em cumprimento de exigências legais e/ou normativas.

4.9. A divulgação externa de informações envolverá os riscos abaixo listados:

4.9.1. Riscos de Negócio – Geral
4.9.1.1. Crise/ retração econômica
4.9.1.2. Demanda cíclica

4.9.2. Riscos Políticos

[2] As denúncias podem ser encaminhadas via Canal da Ética ou, a critério do denunciante, diretamente ao Conselho Fiscal.

4.9.2.1.Políticas governamentais

4.9.3.Riscos Financeiros
4.9.3.1.Inflação
4.9.3.2.Redução do crédito para clientes
4.9.3.3.Taxa de Juros
4.9.3.4.Risco de crédito
4.9.3.5.Variação Cambial
4.9.3.6.Gerenciamento de capital (relação entre as dívidas financeiras e o capital próprio)
4.9.3.7.Risco de Liquidez
4.9.3.8.Mercado de capitais pode ser afetado por acontecimentos políticos, econômicos e sociais
4.9.3.9.Custo de capital

4.9.4.Riscos de Estratégia
4.9.4.1.Suprimentos – sucata, minério de ferro e carvão
4.9.4.2.Fusões e aquisições - integração de novos negócios
4.9.4.3.Energia
4.9.4.4.Mercado e competidores

4.9.5.Riscos de *Compliance*
4.9.6.Riscos Reputacionais
4.9.7.Riscos Operacionais
4.9.7.1.Falhas em equipamentos

4.9.8.Riscos de Recursos Humanos
4.9.8.1.Custo com demissões
4.9.8.2.Preparação de pessoas e sucessão
4.9.8.3.Cultura Organizacional e Comunicação

5. Responsabilidades

5.1. Conselho de Administração

5.1.1.Define o perfil de riscos da empresa, através dos direcionadores estratégicos e orientação geral ao CEG, e assegura a efetividade do sistema de controle de riscos.

5.2. Comitê Executivo Gerdau – CEG

5.2.1.Assegura a existência de uma estrutura adequada ao gerenciamento de riscos; identifica, avalia e trata os riscos de negócio pertinentes, quando da execução do planejamento estratégico.

5.3. Comitê de Riscos

5.3.1.Por delegação do Conselho de Administração, acompanha os riscos e contingências listados no item 4.3, acima, bem como, os riscos gerenciados no nível de cada macroprocesso e/ou operação, para verificar a efetividade dos controles existentes, e aprova o plano anual de auditoria.

5.4. Auditoria Interna

5.4.1.Identifica os riscos operacionais e respectivos controles internos dos processos. Anualmente, realiza a avaliação de riscos com o propósito de elaborar o Plano de Auditoria

para o exercício seguinte.

6. Disposições Finais

6.1. Os casos omissos, exceções, bem como, os ajustes na presente Política de Gestão de Riscos devem ser submetidos à aprovação pelo Process Owner do Macroprocesso de Ética e *Compliance* e validados pelo Conselho de Administração.

6.2. Esta Política foi aprovada em reunião do Conselho de Administração, possuindo vigência imediata.