1. OBJETIVOS

Estabelecer as diretrizes para o processo de gestão de riscos, sua abrangência, definições, fluxo de informações e a estrutura de reporte dos riscos críticos. A Política também visa atribuir responsabilidades sobre a identificação e mecanismos de tratamento, para prevenir ou minimizar o impacto dos fatores de riscos.

2. ABRANGÊNCIA

Esta Política aplica-se à Gerdau S.A., incluindo todas as suas Operações de Negócio e Processos Corporativos.

3. DEFINIÇÕES:

a) Canal de Ética: trata-se de ferramenta disponível na internet e intranet, para relatar denúncias e preocupações éticas e esclarecer dúvidas relacionadas ao tema.

b) Comitê de Riscos: é o comitê de apoio e assessoramento à Diretoria Estatutária da Gerdau S.A, composto pelo CEO, CFO, e representantes das áreas de Auditoria, Tributário, Contabilidade, Jurídico, Compliance e Operações. O Comitê de Riscos tem competência para, entre outros, assessorar a Diretoria Estatutária na identificação, gerenciamento e tratamento dos riscos da Companhia.

c) Conselho Fiscal: é o órgão fiscalizador independente da diretoria e do conselho de administração, cujos membros são eleitos pela Assembleia Geral de Acionistas. Configura-se como parte relevante do mecanismo de governança e, também, atua com funções específicas de Comitê de Auditoria.

d) Operação de Negócio ou ON: significa a divisão da estrutura organizacional das empresas da Gerdau, definidas a partir de questões geográficas, segmentos de mercado, ou associação com outras empresas.

e) Processo(s) Corporativo(s): significa cada uma das áreas internas relacionadas ao corporativo e atuação global da Gerdau, que compõem a sua estrutura organizacional e forma o seu organograma macro. Os “Processos Corporativos” da Gerdau são: Financeiro, Jurídico, Pessoas, Compliance, Tributário, Comunicação, Tecnologia da Informação, Industrial, , Auditoria Interna.

f) Riscos: são fatores ou eventos incertos que podem causar impactos, alterando, dificultando ou impossibilitando o cumprimento dos objetivos da Empresa.

This content is Public.

4. DIRETRIZES

4.1 Gestão de Riscos na Gerdau

O processo de Gestão de Riscos na Gerdau é conduzido em cada Operação de Negócio e pelos Processos Corporativos, com uma consolidação de temas prioritários. Esta abordagem visa aproveitar a expertise técnica, o conhecimento do cenário local e os aspectos específicos. Ao incluir as unidades de negócios na identificação, avaliação e gerenciamento dos seus próprios riscos, assegura-se que a gestão de riscos esteja integrada às rotinas, promovendo uma cultura proativa, alinhada às particularidades dos diversos contextos.

Cada Operação de Negócio e Processo Corporativo deve possuir uma área ou ponto focal responsável pelo tema de riscos. Promover a prática dentro da operação, com monitoramento e reporte sobre a totalidade dos seus riscos. Os riscos analisados localmente devem ser reportados sistematicamente à área de Riscos Corporativo para que a Companhia consolide os riscos relevantes e possa fazer as análises e desdobramentos necessários.

O processo de Gestão de Riscos da Gerdau deve seguir 6 etapas, conforme segue abaixo:

4.1.1 Definição do Contexto

Delimitar o escopo de identificação de um risco, analisando o contexto interno, que envolve a estrutura organizacional, processos, responsabilidades, sistemas e relações com stakeholders internos, assim como o contexto externo, envolvendo a análise do ambiente no qual a Gerdau está inserida, seja no âmbito operacional, de negócio ou corporativo.

4.1.2 Identificação e Análise

Identificar o risco pela análise dos processos existentes, consistindo na busca, reconhecimento e descrição dos riscos, considerando seus detalhes, histórico de eventos, categoria, causas e consequências.

As categorias definidas para os riscos identificados pela Gerdau e suas operações são:

(a) Estratégico: Afetam os planos de negócio e/ou os objetivos estratégicos da empresa. Estes podem ser decorrentes da falta de capacidade ou habilidade para se proteger ou adaptar as mudanças no ambiente.

(b) Financeiro: Associados aos temas de avaliação das incertezas relacionadas às operações financeiras, que incluem a gestão do fluxo de caixa, gestão cambial, investimentos financeiros, empréstimos, crédito etc.

(c) Operacional: Relacionado ao exercício das atividades da Companhia, devido a possíveis eventos de falhas, deficiências ou inadequações de processos internos e externos envolvendo pessoas, sistemas, unidades industriais e áreas de negócio.

(d) Legal/Regulatório: Relacionados ao ambiente regulatório, decorrentes de eventuais descumprimentos de legislação e regulamentação, desvios de conduta e da documentação orientadora. Abrangem os aspectos dos esforços feitos pela empresa para tratar do componente ético.

This content is Public.

Os riscos devem ser identificados de acordo com uma hierarquização pré-definida e que suporta a divisão das responsabilidades nos diversos níveis da organização.

4.1.3 Avaliação

O propósito da avaliação e priorização de riscos é compreender a sua relevância, analisando de acordo com as métricas estabelecidas pela Gerdau para definição do grau de probabilidade e impacto.

A avaliação é baseada em métricas únicas para toda a Gerdau, aprovadas pelo Comitê de Riscos e validada pelo Conselho de Administração. As métricas consideram os seguintes níveis distintos de impacto e probabilidade:

- Níveis de probabilidade: Muito Alta, Alta, Média, Baixa, muito baixa.
- Níveis de impacto: Os riscos são avaliados em Catastrófico, Crítico, Sério, moderado e Brando. Para classificação nestes níveis de impacto existem 6 dimensões independentes para análise, sendo elas: Saúde e segurança, Meio ambiente, Aspectos legais/Regulatório, Imagem, Qualidade e Financeiro.

O resultado da análise dos riscos entre probabilidade e impacto é representado na matriz de riscos ou heatmap, conforme Figura a seguir. Nesta representação, tem-se a magnitude do risco expressa nos 25 quadrantes, resultante da combinação entre o impacto (consequência do evento) e a probabilidade de ocorrência da causa/evento. Os níveis estabelecidos e a representação por cores são utilizados como critérios de priorizações de ações sobre os riscos.

Resultado		Probabilidade				
		(1) Muito baixa	(2) Baixa	(3) Média	(4) Alta	(5) Muito Alta
Impacto	(5) Catastrófico	GR3	GR2	GR1	GR1	GR1
	(4) Crítico	GR3	GR3	GR2	GR1	GR1
	(3) Sério	GR4	GR3	GR3	GR2	GR1
	(2) Moderado	GR4	GR4	GR3	GR3	GR2
	(1) Brando	GR4	GR4	GR4	GR3	GR3

Sempre que algum risco representar uma probabilidade de materialização com impacto GR1, é obrigação do responsável pela ON ou Processo Corporativo estabelecer controles e ações para mitigar ou monitorar seu avanço, bem como, reportar o status para níveis superiores e demais áreas impactadas com acompanhamento do plano de ação.

4.1.4 Tratamento

O propósito do tratamento de riscos é dar a tratativa mais adequada para o risco, direcionando seu endereçamento. Trata-se de um processo composto por: formular e selecionar opções para tratamento do risco, planejar e implementar o tratamento do risco, avaliar a eficácia deste tratamento e decidir se o Risco Residual é aceitável, e se não for aceitável, realizar tratamento adicional.

As alternativas para tratamento dos riscos são monitorar, evitar, reduzir, transferir ou aceitar, devendo ser priorizadas conforme a criticidade do risco. Através de planos de ação, define-se as opções de tratamento, ações necessárias, responsáveis e datas, a fim de possibilitar o monitoramento das suas execuções.

This content is Public.

4.1.5 Monitoramento

No monitoramento deve ocorrer o acompanhamento da evolução do risco ao longo do tempo, verificando se as ações adotadas pela Companhia foram eficientes assim como o efeito de eventuais mudanças no ambiente interno e/ou externo em sua avaliação.

Para estes riscos, cabe às áreas impactadas realizarem o monitoramento da exposição, por meio de acompanhamento de cenários e informações externas; implantação de indicadores de controle; contratação de análises técnicas quando necessário; aprofundar as causas de variações nos resultados; mapeamento de clima interno; fazer cumprir as políticas, procedimentos e a estrutura de governança da Gerdau.

4.1.6 Reporte

Os gestores das Operações de Negócio e Processos Corporativos são responsáveis em considerar todos estes riscos em suas ferramentas de controle, acompanhamento de orçamento/investimentos e desdobramento de resultados.

Os reportes seguem as linhas de liderança, Diretoria, Comitês, Conselho de Administração e Conselho Fiscal.

5 RESPONSABILIDADES

Seguindo a definição do "Modelo das Três Linhas", definido pelo órgão independente *The Institute of Internal Auditors* - IIA, os riscos são geridos pela 1ª linha de defesa da Companhia, consolidados pela 2ª linha e avaliados e testados de forma independente pela 3ª linha. O modelo é detalhado conforme abaixo e está alinhado com o modelo de gestão definido pela Gerdau:

a) 1ª linha: composto pelas áreas operacionais da Companhia e seus líderes diretos. São os donos de riscos, responsáveis pelo controle, identificação, análise, avaliação e monitoramento dos riscos. Possuem a responsabilidade direta pela execução da Gestão de Riscos.
b) 2ª linha: formada pelas áreas de Gestão de Riscos Locais, Riscos Corporativos, Controles Internos e Compliance, as quais suportam os donos de riscos, na criação de regras (políticas, diretrizes, procedimentos), auxílio da implementação das políticas, definindo metodologias, indicadores de riscos e identificação de controles internos capazes de mitigar os riscos identificados pela 1ª linha.
c) 3ª linha: formada pela área de Auditoria Interna, que realiza análise independente e tem como objetivo avaliar o ambiente de controle da companhia, inclusive identificando riscos adicionais não mapeados, suportar o processo com novos inputs e direcionar os esforços para atuar em riscos relevantes reportando à Diretoria Estatutária e ao Comitê de Riscos suas considerações sobre o gerenciamento dos riscos, tendo em vista o resultado dos seus trabalhos de auditoria.

A seguir constam as responsabilidades das instâncias envolvidas no processo de gerenciamento de riscos:

5.1 Comitês das Operações de Negócio e de Processos Corporativos

Os riscos mapeados pelos responsáveis pelas Operações de Negócio da Companhia e pelos Processos Corporativos possuem comitês compostos por um grupo de gestores responsáveis pelo reporte e tratamento dos assuntos e riscos críticos. Além disso, são responsáveis por gerir os riscos das suas operações, garantindo o tratamento adequado. São exemplos: Comitê das Operações de Negócio, Comitê de Crédito, Comitê de Finanças, Comitê de Investimentos, Comitê Industrial etc.

This content is Public.

Suas principais atribuições são:

- Avaliar e priorizar os riscos dos negócios de acordo com o grau de criticidade/exposição, necessidade de investimentos e de tratamentos;
- Estabelecer Diretrizes para tratamento sistêmico dos riscos, ou seja, que considere ações que abranjam toda a Operação ou Processo;
- Aprovar investimentos para fins de tratamento do risco, de acordo com sua alçada, para o tratamento dos Riscos do Negócio, levando em consideração as diretrizes da Companhia;
- Aprovar e acompanhar o tratamento dos Riscos do Negócio, quando pertinentes, através de seus planos de ação.

5.2 Área de Gestão Riscos Corporativos

- Definir metodologias, diretrizes e ferramentas de gestão de riscos.
- Elaborar o planejamento e assegurar a operacionalização sistêmica da gestão de riscos,
- considerando todas as dimensões da estrutura definida, englobando atividades estratégicas, táticas e operacionais.
- Validar o escopo dos trabalhos de gestão de riscos e suas atribuições com as Operações, Comitês, Diretoria e Conselho de Administração.
- Monitorar os riscos identificados, em parceria com as demais áreas da Companhia.
- Assessorar as Operações de Negócio e os Processos Corporativos na identificação e avaliação dos diversos tipos de riscos, assim como suportar na definição dos planos de ação.
- Monitorar os riscos identificados, em parceria com as demais áreas da Companhia.
- Reportar as informações relevantes decorrentes do processo de gestão de riscos aos
- públicos de interesse, incluindo o Comitê de Riscos e Conselho de Administração da Companhia;
- Disseminar, continuamente, a cultura de gestão de riscos na Companhia;
- Assegurar a manutenção da política de gestão de riscos, assim como as diretrizes e documentos internos, a fim de verificar o seu cumprimento.

5.3 Comitê de Riscos

O Comitê de Riscos é responsável por avaliar a consolidação dos riscos provenientes das Operações de Negócio e dos Processos Corporativos. Cabe a este Comitê garantir que os responsáveis pelos riscos realizem as suas análises e que os críticos (GR1) estejam sendo tratados adequadamente. Além disso, outras responsabilidades são atribuídas a este comitê:

- Supervisionar o processo como um todo, verificando se a Companhia possui mecanismos internos e metodologias revisadas e bem estabelecidas para fins de gerenciamento dos riscos;
- Aprovar e avaliar constantemente os parâmetros de avaliação de riscos (régua de impacto e probabilidade) assim como monitorar as exposições de riscos da Companhia;
- Avaliar seus recursos humanos e financeiros destinados para o processo estão aderentes;
- Monitorar os riscos e seus níveis, suportar os processos e Operações de Negócios na condução e priorização dos planos de ação;
- Assessorar o Conselho de Administração (CA) no que tange ao processo de gestão de riscos da Companhia, informando sobre a evolução da metodologia, reportando riscos críticos.

Além da avaliação deste sumário de riscos da Companhia, possui como atribuições avaliar periodicamente outros sinalizadores de riscos provenientes das informações fornecidas pela Auditoria Interna, *Compliance,* Segurança da Informação e Jurídico:

This content is Public.

- Status das avaliações sobre os controles decorrentes da Lei Sarbanes Oxley;
- Principais trabalhos de auditoria sobre riscos operacionais;
- Evolução e tratamento das denúncias do canal da ética;
- Programa de Integridade e temas de Compliance;
- Contingências jurídicas.

5.4 Diretoria Estatutária

- Executar as diretrizes constantes na Presente política.
- Atuar de forma comprometida no gerenciamento de riscos, através do conhecimento, compreensão e acompanhamento dos principais riscos da Companhia.
- Promover a cultura do gerenciamento de riscos na Companhia e o fortalecimento da 1ª e 2ª linha de Defesa.
- Propor o apetite de risco ao Conselho de Administração.
- Manter uma estrutura organizacional adequada para operar e gerenciar de forma razoável os riscos em que a Companhia está sujeita.
- Ratificar a priorização dos riscos a serem tratados.

5.5 Conselho de Administração

- Supervisionar o desenvolvimento da arquitetura de gerenciamento de risco;
- Validar os aspectos estratégicos do processo de gestão de riscos, assim como avaliar e monitorar as exposições de riscos da Companhia;
- Considerar em suas análises e tomadas de decisões os reportes recebidos do Comitê de Riscos, no que tange ao processo de gestão de riscos da Companhia.

5.6 Conselho Fiscal (Comitê de Auditoria)

O Conselho Fiscal é o órgão fiscalizador independente, atuando em certas funções específicas de um Comitê de Auditoria, tendo entre suas atribuições aquelas descritas no Estatuto Social da Companhia, bem como, com funções de acompanhamento dos resultados dos trabalhos das auditorias internas e externas, resultados dos testes realizados para atingimento da Certificação SOX e, quando necessário, apoiar na definição de metodologia e melhorias no processo de gestão de riscos.

Esta Política foi revisada e aprovada em reunião do Conselho de Administração da Companhia em 26 de outubro de 2026.

****

This content is Public.