GERDAU El futuro se moldea	POLÍTICA DE GESTIÓN DE RIESGOS

1. OBJETIVOS

Establecer las directrices para la gestión de riesgos, su alcance, definiciones, flujo de información y la estructura de informes de riesgos críticos. Asignar responsabilidades sobre la identificación y formas de tratamiento, para prevenir o minimizar el impacto de sus factores de riesgo.

2. ALCANCE

Esta Política se aplica a todas las empresas, Operaciones de Negocio y Procesos Corporativos de Gerdau S.A., y sus afiliadas.

Abarca todos los factores de riesgos conocidos y monitoreados por la administración de la empresa. Contempla todos los factores de riesgos conocidos y monitoreados por la administración de la compañía y que están descritos en la sección 4 del Formulario de Referencia (documento divulgado en el website de Gerdau RI y archivado en la CVM – Comisión de Valores Mobiliarios de Brasil).

3. DEFINICIONES:

a) Canal de Ética: herramienta disponible en internet e intranet, para reportar denuncias o preocupaciones éticas y aclarar dudas relacionadas al tema.

b) Comité de Riesgos: es el comité de apoyo y asesoría a la Dirección de Gerdau S.A, compuesto por el CEO, directores y gestores de las principales áreas que actúan en análisis de riesgos (ej.: Auditoría, Compliance, Finanzas, Fiscal, Contabilidad, Legal y Operaciones) y otras áreas invitadas, conforme la situación en análisis. De acuerdo a su estructura interna, el Comité de Riesgos tiene alcance para, entre otros, asesorar a la Dirección en la identificación, gestión y tratamiento de riesgos de la empresa en sus distintas clasificaciones, como riesgos de crédito, mercado, liquidez, finanzas, operacionales, regulatorios, tecnológicos, socioambiental, cambios climáticos, imagen y estratégico.

c) Consejo Fiscal: es el órgano fiscalizador independiente de la dirección y del consejo de administración, con miembros elegidos por la reunión general de inversionistas. Tiene relevancia como verificación independiente en la gobernanza corporativa y compuesto por consejeros independientes, que también actúan en funciones específicas de un Comité de Auditoria.

d) Operación de Negocio - ON: significa la división de estructura organizativa de Gerdau, definidas a partir de cuestiones geográficas, segmento de mercados, o asociaciones con otras empresas.

e) Procesos Corporativos: significa cada una de las áreas internas relacionas al Corporativo y con actuación global en Gerdau, conforme su estructura organizativa y organigrama macro. Los “Procesos Corporativos” de Gerdau son: Proceso de Finanzas; Legal; Personas; Auditoría, TI y Proceso Industrial.

f) Riesgos: son factores o eventos inciertos que pueden causar impactos, alterando, dificultando o imposibilitando el cumplimento de los objetivos de la empresa.

g) Riesgo ambiental: es la exposición de las operaciones a impactos al medio ambiente, sea por extracción de recursos naturales o por el efecto causado por los procesos productivos.

h) Riesgo de corrupción: son originados por el no cumplimiento de prácticas legales y no alineadas a las políticas y directrices de la empresa, generado por actitudes internas o externas que busquen favorecimientos ilícitos.

i) Riesgos estratégicos: son aquellos que afectan el cumplimiento de los objetivos de negocio, así como su correcta ejecución.

j) Riesgo financiero: es el relacionado al desempeño económico. Está ligado a finanzas corporativas, como, por ejemplo, rentabilidad, deudas, márgenes, liquidez, indicadores, etc.

k) Riesgos operacionales: son las ocurrencias de pérdidas causadas por falla, deficiencia o no adecuación de los procesos internos involucrando personas y sistemas relacionados directamente con la operación.

l) Riesgos regulatorios: es la capacidad de la empresa para acompañar, interpretar y anticiparse a las leyes y reglamentos en los mercados donde actúa.

m) Riesgo político: es el causado por decisiones, eventos o condiciones político-económicas que pueden afectar materialmente los resultados esperados.

n) Riesgo tecnológico: puede estar relacionado a ciber ataques, salida indebida de datos, obsolescencia de los sistemas que soportan los procesos administrativos y operaciones.

o) Riesgo de Reputación: generan daños a la imagen de la empresa, derivado de un suceso adverso, sin culpa por parte de la empresa.

4. DIRECTRICES:

4.1 Identificación y tratamiento de Riesgos:

4.1.1 La estructura de Gestión de Riesgos en Gerdau es descentralizada, para capturar y potencializar la gestión del conocimiento técnico y perfil de los profesionales de cada área. Los responsables por la gestión de riesgos deben identificar y tratar los que puedan afectar los objetivos de la empresa. Hay una consolidación de informaciones de riesgos críticos de las ON´s y Procesos Corporativos para reporte al Comité de Riesgos Corporativo.

4.1.2 Siempre que algún riesgo represente una probabilidad de materialización con impacto relevante, es obligación del responsable por la ON o Proceso Corporativo, establecer controles para mitigación o seguimiento de su avance, así como, reportar el estatus a sus superiores y demás áreas involucradas.

4.1.3 Los riesgos deben ser identificados y evaluados considerando la probabilidad de ocurrencia y su impacto para el negocio, leyes e imagen de la empresa. Las acciones de mitigación deben ser compatibles con el grado de exposición a los riesgos.

4.1.4 Para los riesgos operacionales, considerando el análisis del costo del control contra la exposición a los riesgos, deben establecerse conforme el “Modelo de las Tres Líneas”, definido por el órgano global e independiente *“The Institute of Internal Auditors”.*

1ª línea: ambiente de controles con actividades de rutina y de control, procedimientos, niveles de aprobación, bloqueos sistémicos, restricción de accesos, conciliaciones.
2ª línea: actividades de gestión, seguimiento de resultados, análisis de procesos, prestaciones de cuentas, gestión de los controles internos, y
3ª línea: realización de auditorías internas y/o externas en todos los procesos.

4.1.5 En la primera línea abarca todos los procesos críticos de las ON´s y Procesos Corporativos, y deben tener sus rutinas formalizadas en Directrices, con definiciones de procedimientos, responsabilidades y límites para aprobación necesarios para mitigar los riesgos operacionales, financieros, regulatorios, ambientales, fraude o imagen.

4.1.6 En la segunda línea, además de la actuación de los gestores de los procesos en el seguimiento de sus riesgos, existen otras áreas de apoyo para mejoras en el ambiente de control:

- El área de Controles Internos es responsable en analizar el ambiente de control, procesos y riesgos, evaluar alteraciones, realizar evaluaciones en conformidad con ley Sarbanes Oxley (SOX) proponer mejoras y reportar resultados.
- El área de *Compliance* debe garantizar un programa de integridad y conformidad de las actividades con exposición de riesgos relacionados con las directrices éticas, incumplimiento de leyes, reglas, normas y prácticas anticorrupción. La actividad es compuesta por capacitaciones de diseminación del Código de Ética y Conducta, de las Directrices, monitoreo de registros, Canal de Ética, y evaluaciones periódicas.

4.1.7 La empresa tiene un Canal de Denuncias anónimo y confidencial, disponible y divulgado a todos los empleados y terceros. Las ocurrencias son gestionadas por el área de Compliance, investigadas por áreas responsables y los temas relevantes son reportados para la Alta Administración.

4.1.8 En la tercera línea, la Auditoría Interna realiza su trabajo de evaluación de controles de manera independiente, a partir de planes anuales de trabajo, considerando, entre otros, mapear y analizar los riesgos, los resultados de auditorías anteriores, el resultado de las evaluaciones de la certificación SOX (Sarbanes-Oxley), histórico de riesgos en otras localidades, y las informaciones recibidas de los gestores de procesos.

4.1.9 La evaluación de los riesgos debe estar presente en todos los análisis de procesos de la empresa, y considerados para eventual divulgación externa de información. Es responsabilidad de los gestores de los procesos tener atención a estos riesgos, internos o externos, y que puedan representar pérdidas, comprometer la imagen, afectar planes de negocio o sostenibilidad económica.

4.1.9.1 Principales riesgos a considerar:
a) **Riesgos de escenario económico:** crisis / retracción económica; demanda cíclica.
b) **Riesgos Políticos:** Políticas de gobierno; riesgos sociales; cambios en leyes y reglamentaciones.
c) **Riesgos Financieros:** inflación, tasa de interés; riesgo de crédito, variación cambiaria; gestión de capital (relación entre deuda financiera y el capital propio); riesgos de liquidez, exposición al mercado de capitales; costo financiero.
d) **Riesgo de Estrategia:** Fusiones y adquisiciones, desinversiones; nuevos negocios; mercado y competidores; barreras comerciales; confidencialidad de la información.
e) **Riesgos de Reputación:** Comunicación; imagen; relacionamiento con stakeholders.
f) **Riesgos Ambientales:** leyes ambientales; pasivos ambientales; relacionamiento con la comunidad.
g) **Riesgos Operacionales y Tecnológicos:** riesgos de suministro de materiales; energía; equipamientos y capacidad productiva; Gestión de costos; Sistemas de Información y Control.
h) **Riesgos de Recursos Humanos**: Sucesión; retención; cultura y ambiente laboral; movimientos sindicales.
i) **Riesgos Regulatorios:** cumplir leyes y reglas; ética y compliance.

4.1.9.2 Para estos riesgos, las áreas impactadas deben realizar el monitoreo de la exposición, a través de seguimiento de escenarios e informaciones externas; implantar indicadores de control; contratar análisis técnico especializado siempre que sea necesario; profundizar los análisis de las causas de variaciones en los resultados; diagnosticar el ambiente interno; garantizar el cumplimiento de políticas, procedimientos y estructura de gobernanza de Gerdau.

4.1.9.3 Los gestores de las ON`s y Procesos Corporativos son responsables en considerar todos estos riesgos en sus herramientas de control, definición de planificaciones (DOFA – análisis de escenarios), seguimiento de presupuestos, desglose de resultados y evaluaciones de escenarios futuros.

4.1.9.4 En las evaluaciones de nuevos negocios, venta de operaciones, cambios relevantes en las rutinas y objetivos, revisiones de planificaciones, es necesario que el gestor responsable garantice el correcto análisis e impacto que los nuevos escenarios puedan presentar.

5 ESTRUCTURA ORGANIZACIONAL EN LA GESTIÓN DE RIESGOS:

De conformidad con las definiciones del inciso 4.1.1., a continuación, se establece los órganos de la empresa que están involucrados en el proceso de evaluación de los resultados.

5.1 Comités de las Operaciones de Negocios y Procesos Corporativos

Las Operaciones de Negocio, responsables por la operación industrial, centros de acopio, puertos, centros de distribución y los Procesos Corporativos posen Comités, compuestos por gestores responsables por reporte y tratamiento de temas y riesgos críticos. Además, son responsables por la gestión de los riesgos de sus operaciones, garantizando el tratamiento necesario. Son ejemplos: Comité de Operación de Negocio, Comité de Crédito, Comité Financiero, Comité de Inversiones, Comité Industrial, etc.

5.2 Comité de Riesgos

El Comité de Riesgos es responsable por evaluar la consolidación de los riesgos críticos evaluados y tratados conforme al inciso 5.1. El Comité de Riesgos debe garantizar que todas las Operaciones de Negocio y Procesos Corporativos realicen sus análisis y que los riesgos críticos estén controlados. Además de estas evaluaciones, el Comité posé la atribución de evaluar periódicamente algunos señalizadores de riesgos reportados por la Auditoria Interna, Compliance, Seguridad de la Información y Legal:

- Status de evaluación de controles bajo la Ley SOX (Sarbanes-Oxley);
- Principales trabajos de auditoría interna sobre riesgos operaciones;
- Avances y tratamiento de las denuncias del canal de ética;
- Programa de Integridad y temas de Compliance;
- Riesgos de imagen;
- Riesgos de seguridad de la información;
- Contingencias legales;
- Eventuales otros riesgos identificados que necesiten reporte al Comité de Riesgo.

5.3 Consejo Fiscal (Comité de Auditoría)

Órgano fiscalizador independiente, actúa en ciertas ocasiones específicas como Comité de Auditoría, con atribuciones definidas en el artículo 13 del Estatuto Social de la Empresa, así como, verificar los avances de trabajo de las auditorías internas y externas, resultados de evaluaciones SOX, y en su caso, apoyando en el tratamiento de la gestión de riesgos.

5.4 Comité de las Operaciones:

Estructura de apoyo operativo en la gestión de algunos procesos de la empresa, involucrando más de un área, responsable por evaluar los resultados, revisar causas de variaciones y presentar perspectivas de escenarios futuros, basado en variables internas y externas. Son ejemplos: Comités de Operaciones, Comité de Estrategia y Sostenibilidad, Comité de Crédito, Comité de Remuneración, Comité Industrial, etc.

Esta política de Gestión de Riesgos ha sido revisada y aprobada en reunión del Consejo de Administración de la compañía el 04 de mayo de 2022.

****