

	<b>SISTEMA INTEGRADO DE GESTÃO AGROINDUSTRIAL - SIGA</b>			
	<b>POLITICAS DE GESTÃO</b>			
Título:	POLÍTICA DE GESTÃO DE RISCOS	Código	Revisão	Página
Depto:	CORPORATIVO - ESTRUTURANTE	PO-COREST-010	0	1 de 13

ELABORAÇÃO: ANDRE LUIS DA SILVA		
VERSÃO	DESCRIÇÃO	DATA
0	ELABORAÇÃO INICIAL	03/06/2025
<div>CÓPIA</div> <div>NÃO</div> <div>CONTROLADA</div> <div>NÃO SERÁ SUBSTITUÍDA EM CASO DE REVISÃO</div>		
Nome		Cargo
ANDRÉ LUIS DA SILVA		ESPECIALISTA DE COMPLIANCE E RISCOS
FABIEDER ANDERSON LOURENÇO		ANALISTA GESTÃO DA QUALIDADE PL.
JOSÉ EDUARDO RONCHI		COORD DE GOVERNANÇA RISCOS E COMPLIANCE

		<b>SISTEMA INTEGRADO DE GESTÃO AGROINDUSTRIAL - SIGA</b>		
		<b>POLITICAS DE GESTÃO</b>		
Título:	POLÍTICA DE GESTÃO DE RISCOS	Código	Revisão	Página
Depto:	CORPORATIVO - ESTRUTURANTE	PO-COREST-010	0	2 de 13

SUMÁRIO

OBJETIVO .....	3
ABRANGÊNCIA.....	3
REFERÊNCIAS.....	3
DEFINIÇÕES.....	3
DIRETRIZES .....	4
1. Pilares estratégicos .....	4
2. Estrutura de Gestão de Riscos do Grupo .....	4
3. Categorias de Riscos .....	5
4. Metodologia de avaliação de riscos .....	6
5. Do Risk Sensing .....	10
6. Disposições gerais .....	10
RESPONSABILIDADES .....	11
ANEXOS.....	13

CÓPIA

NÃO

CONTROLADA

NÃO SERÁ SUBSTITUÍDA EM CASO DE REVISÃO

	<b>SISTEMA INTEGRADO DE GESTÃO AGROINDUSTRIAL - SIGA</b>  <b>POLITICAS DE GESTÃO</b>			
Título:	POLÍTICA DE GESTÃO DE RISCOS	Código	Revisão	Página
Depto:	CORPORATIVO - ESTRUTURANTE	PO-COREST-010	0	3 de 13

## OBJETIVO

A presente Política de Gestão de Riscos visa estabelecer e divulgar princípios, diretrizes e responsabilidades a serem observados no processo de gestão de riscos, de forma a sustentar a realização de seus objetivos estratégicos, entre outros aspectos, por meio de um processo contínuo de identificação, priorização e gestão proativa dos riscos associados a tais objetivos nas operações do Grupo ou empresas controladas pela Angelina Colombo S/A.

## ABRANGÊNCIA

Esta política se aplica a todos os acionistas, administradores, funcionários, terceiros e a todas as partes interessadas (*stakeholders*) que se relacionam com a Colombo Agroindústria ou empresas controladas pela Angelina Colombo S/A.

## REFERÊNCIAS

Código de Conduta e Ética  
 Política de Compliance  
 Política de Controles Internos  
 Regulamento de Listagem do Novo Mercado da B3 S.A. – Brasil, Bolsa, Balcão  
 Normas aplicáveis emanadas pela Comissão de Valores Mobiliários  
 COSO-ERM - *Committee of Sponsoring Organizations of Treadway Commission* (2013 e 2017)  
 ABNT NBR ISO/IEC 31.000:2018 – Gestão de Riscos  
 ABNT NBR ISO/IEC 37.000:2021 – Governança em Organizações  
 Conceito das Linhas de Responsabilidade do IIA e ISE - 2023

## DEFINIÇÕES

**Apetite a Risco:** o nível de risco que o Grupo está preparado a aceitar para atingir seus objetivos estratégicos.

**Avaliação de Eventos de Riscos:** processo de análise dos riscos relevantes para o alcance dos objetivos do Grupo e a determinação de resposta apropriada.

**Colombo Agroindústria S/A ou empresas controladas pela Angelina Colombo S/A:** empresas que detém o controle de forma direta ou indireta. Também denominada “Grupo”.

**Gestão de Riscos:** processo para identificar, avaliar, administrar e controlar potenciais eventos ou situações, para fornecer uma razoável certeza em relação ao cumprimento dos objetivos do Grupo.

**Identificação de Eventos de Riscos:** processo de busca, reconhecimento e descrição de riscos, que envolve a identificação de suas fontes, causas e consequências potenciais.

**Nível de Risco:** magnitude de um risco, expressa em termos da combinação de suas consequências e probabilidades de ocorrência.

**Proprietário de Riscos:** responsável por gerir o risco da área ou do processo.

	<b>SISTEMA INTEGRADO DE GESTÃO AGROINDUSTRIAL - SIGA</b>  <b>POLITICAS DE GESTÃO</b>			
Título:	POLÍTICA DE GESTÃO DE RISCOS	Código	Revisão	Página
Depto:	CORPORATIVO - ESTRUTURANTE	PO-COREST-010	0	4 de 13

**Resposta a Risco:** qualquer ação adotada para lidar com o risco. As respostas podem se enquadrar num destes tipos: aceitar o risco por uma escolha consciente; transferir o risco a outra parte; evitar o risco pela decisão de não iniciar ou descontinuar a atividade que dá origem ao risco.

**Risco:** possibilidade de ocorrer um evento que venha a ter impacto no cumprimento dos objetivos do Grupo.

## DIRETRIZES

### 1. Pilares estratégicos

Na condução dos negócios, o Grupo incorre em Riscos que, se não identificados e tratados de forma adequada, podem comprometer seus valores, reputação, competitividade e perenidade dos negócios.

Toda e qualquer decisão envolve determinado grau de Risco, que nunca será totalmente eliminado. Deve-se destacar que os Riscos jamais serão eliminados. O objetivo, portanto, é compreendê-los, avaliá-los e definir ações de resposta que permitam mitigar suas consequências, reduzindo e antecipando eventuais perdas.

A análise de Riscos deve suportar a tomada de decisão em todos os níveis. Para tanto, os riscos com limites aprovados devem ser considerados na elaboração de projeções, ajustando-se as metas, quando necessário, aos referidos limites.

É fundamental o entendimento e disseminação entre os órgãos e executivos envolvidos, da correta diferenciação de impactos causados por eventos e situações como:

- i. falhas de controles internos em processos;
- ii. decisões estratégicas malsucedidas; ou
- iii. falha na governança.

Este entendimento visa aperfeiçoar e fortalecer o modelo de governança corporativa do Grupo.

### 2. Estrutura de Gestão de Riscos do Grupo

A estrutura de Gestão de Riscos do Grupo considera a atuação conjunta dos órgãos de governança corporativa e de gestão, e é realizada de acordo com o modelo de 3 (três) linhas do COSO-ERM. As 3 linhas consistem em um conceito que define os papéis e responsabilidades na gestão de riscos e fortalecimento da governança, bem como a interação desses papéis em todos os níveis do Grupo, conforme indicado abaixo:

1ª Linha de Defesa: é representada pelos Proprietários de Riscos, responsáveis diretos pela execução de seus processos e detecção dos Riscos respectivos e implementação das respostas.

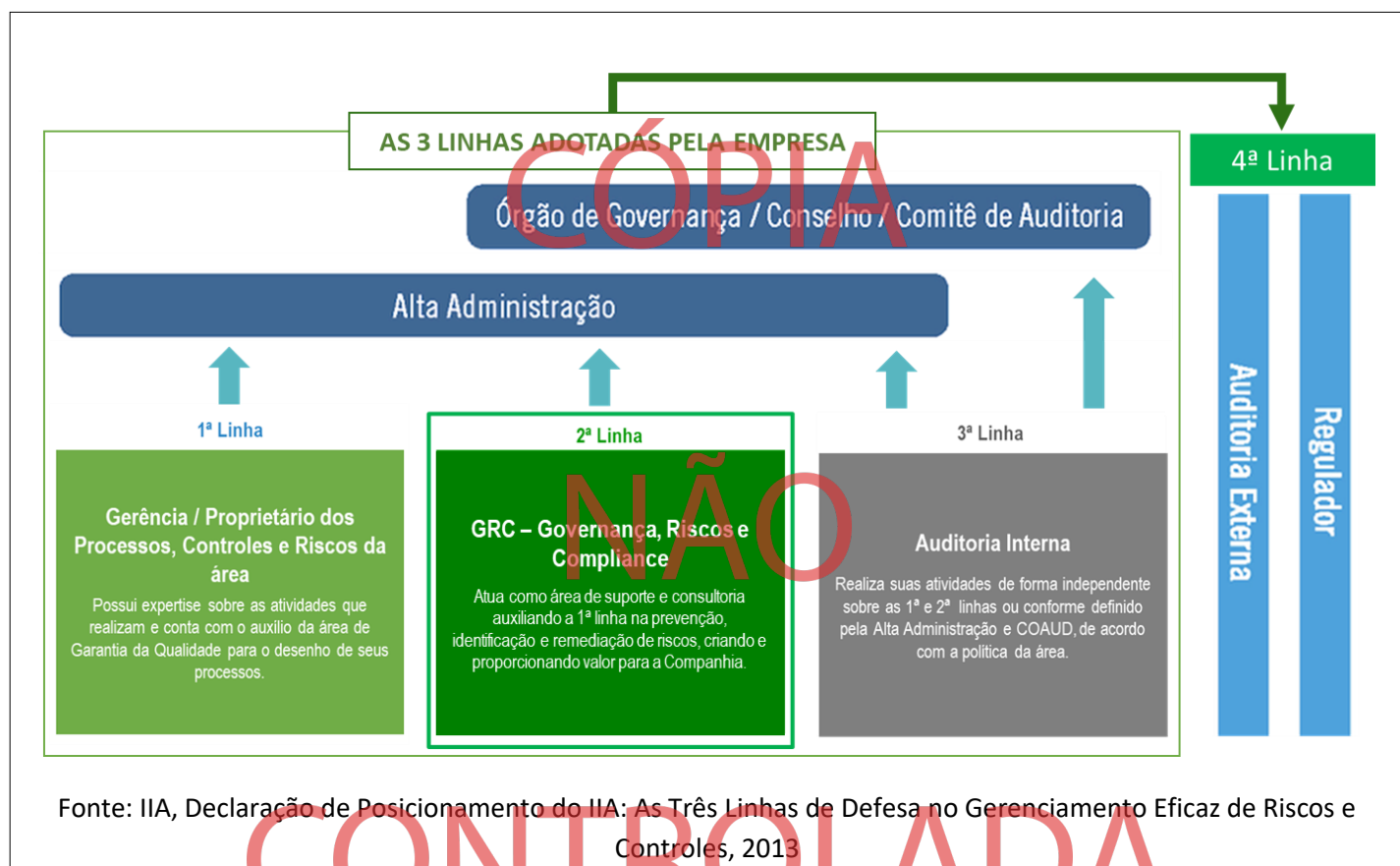
2ª Linha de Defesa: é representada pela área de GRC (Governança, Riscos e Compliance), que atuam na garantia do apropriado funcionamento da primeira linha, por meio do estabelecimento de controles, na identificação de falhas de performance de controles e na identificação de desvios de políticas e procedimentos internos. A área de GRC integra-se à Gerência Jurídica e de Compliance da companhia, fazendo parte de suas atividades e responsabilidades.

3ª Linha de Defesa: é representada pela área de Auditoria Interna, que atua no fornecimento de avaliações independentes à administração, especialmente pela realização de testes nas operações e nos controles

	<b>SISTEMA INTEGRADO DE GESTÃO AGROINDUSTRIAL - SIGA</b> <b>POLÍTICAS DE GESTÃO</b>			
Título: Depto:	<b>POLÍTICA DE GESTÃO DE RISCOS</b> <b>CORPORATIVO - ESTRUTURANTE</b>	Código <b>PO-COREST-010</b>	Revisão <b>0</b>	Página <b>5 de 13</b>

internos e no suporte à área de GRC para identificação de desvios operacionais e financeiros decorrentes de falhas e/ou fraudes. Em que pese integrar-se à Gerência Jurídica e de Compliance, a Auditoria Interna fará reportes diretamente ao Conselho de Administração da Companhia.

Neste sentido, o processo de Gestão de Riscos do Grupo está estruturado conforme organograma e descrições abaixo:



**Parágrafo único:** Na figura acima, de acordo com as melhores práticas de Governança Corporativa, apresentamos os Órgãos Reguladores e Auditorias Externas como 4ª Linha de Defesa/Responsabilidade, sendo o primeiro, com caráter sancionador.

**NÃO SERÁ SUBSTITUÍDA EM CASO DE REVISÃO**

### 3. Categorias de Riscos

As principais categorias de riscos aos quais o Grupo busca proteção estão elencadas a seguir:

**Riscos Estratégicos:** são aqueles que podem impactar na missão, metas ou nos objetivos do Grupo, em busca de criação, proteção e crescimento de valor e incluem os riscos concorrenciais, riscos políticos e riscos de imagem/reputacionais. São causados por mudanças no ambiente externo, tais como político e econômico, mercado, competidores, fusões e aquisições, disponibilidade de recursos, inovações e portfólio de produtos e/ou serviços.

**Riscos Operacionais:** são aqueles que envolvem a operação, sistemas, processos, controles internos, clientes, receitas e outros ativos do Grupo que podem implicar perdas financeiras, danos de reputação e imagem, declínio dos resultados do Grupo.

	<b>SISTEMA INTEGRADO DE GESTÃO AGROINDUSTRIAL - SIGA</b>  <b>POLITICAS DE GESTÃO</b>			
Título:	POLÍTICA DE GESTÃO DE RISCOS	Código	Revisão	Página
Depto:	CORPORATIVO - ESTRUTURANTE	PO-COREST-010	0	6 de 13

**Riscos Financeiros:** são aqueles decorrentes de efeitos não esperados no cenário econômico, político e nas tendências de mercado que podem ter reflexo no comportamento do consumidor, na taxa de juros, inflação, investimentos financeiros, dentre outros. Dentre eles, podemos citar: perdas financeiras devido a aplicações financeiras equivocadas; perdas financeiras em operações com derivativos objetivando hedge, dentre outros.

**Riscos Socioambientais:** são os riscos relacionados a questões ambientais, como a contaminação de água e solo, manutenção de áreas de preservação permanente e reserva nativa legal e questões socioambientais, como riscos de perdas decorrentes de efeitos negativos das atividades e operações do Grupo sobre a sociedade.

**Riscos Regulamentares:** são os riscos relacionados a eventuais descumprimentos das legislações vigentes no ordenamento jurídico brasileiro, as quais o Grupo está submetido e que podem gerar danos ou perdas aos negócios do Grupo. Dentre eles, podemos citar: atividades executadas em desacordo com políticas, normas e procedimentos do Grupo, falhas no monitoramento de alteração/criação de leis e regulamentações, sanções/multas devido à transmissão de informações incorretas para órgãos regulatórios, dentre outros.

**Riscos Reputacionais:** são os riscos que impactam diretamente na imagem, reputação e percepção do Grupo perante o mercado, seus colaboradores, parceiros comerciais e fornecedores. Esses riscos podem decorrer dos Riscos Regulamentares, operacionais, socioambientais, entre outros.

#### 4. Metodologia de avaliação de riscos

A metodologia foi dividida em cinco etapas e pode ser vista no esquema abaixo:



##### Etapa 1: Análise de Ambiente e de Fixação de Objetivos

O ambiente de controle está relacionado aos controles informais, que estão vinculados aos valores das pessoas do Grupo e são igualmente importantes para gerar um ambiente de controle saudável.

	<b>SISTEMA INTEGRADO DE GESTÃO AGROINDUSTRIAL - SIGA</b>  <b>POLÍTICAS DE GESTÃO</b>			
Título:	POLÍTICA DE GESTÃO DE RISCOS	Código	Revisão	Página
Depto:	CORPORATIVO - ESTRUTURANTE	PO-COREST-010	0	7 de 13

A análise do ambiente tem a finalidade de colher informações para apoiar a identificar de eventos de riscos, bem como contribuir para a escolha de ações mais adequadas para assegurar o alcance dos objetivos de processo.

Os objetivos devem ser divulgados a todos os componentes do Grupo, antes da identificação dos eventos que possam influenciar nos seus atingimentos. Eles devem estar alinhados à missão do Grupo e devem ser compatíveis com o Apetite a Riscos.

## Etapa 2: Identificação de Eventos de Risco

Esta etapa tem por finalidade identificar e registrar tanto os eventos de riscos que comprometem o alcance do objetivo do processo, assim como as causas e efeitos/consequências de cada um deles. Considere também o resultado da análise do Ambiente e de Fixação de Objetivos – 1ª Etapa.

**Eventos:** são situações em potencial – que ainda não ocorreram – que podem causar impacto na consecução dos objetivos do processo, caso venham a ocorrer. Podem ser positivos ou negativos, sendo que os eventos negativos são denominados riscos, enquanto os positivos, oportunidades.

**Causas:** condições que dão origem à possibilidade de um evento ocorrer, também chamadas de fatores de riscos e podem ter origem no ambiente interno e externo.

**Risco:** possibilidade de ocorrência de um evento que venha a ter impacto no cumprimento dos objetivos.

**Consequência:** o resultado da materialização de um evento de risco sobre os objetivos do processo.

Por meio da identificação de eventos de riscos, pode-se planejar a forma de tratamento adequado e qual o tipo de resposta a ser dada a esse risco, destacando que os eventos de riscos devem ser entendidos como parte de um contexto, e não de forma isolada. Abaixo, destacamos os componentes do evento de risco:



O processo de identificação de riscos requer a participação de colaboradores com conhecimento do processo, visão holística dos negócios do Grupo nos seus diferentes níveis.



	<b>SISTEMA INTEGRADO DE GESTÃO AGROINDUSTRIAL - SIGA</b>  <b>POLITICAS DE GESTÃO</b>			
Título:	POLÍTICA DE GESTÃO DE RISCOS	Código	Revisão	Página
Depto:	CORPORATIVO - ESTRUTURANTE	PO-COREST-010	0	8 de 13

A técnica a ser utilizada na identificação de eventos de risco deve ser a que melhor se adapta ao processo de avaliação. Dentre as principais técnicas estão: questionários e checklist (lista de itens a serem verificados ou executados); workshop (oficina) e brainstorming (tempestade de ideias); inspeções e auditorias; fluxogramas; diagrama de causa e efeito, *bow-tie* (laço de gravata, técnica de gestão de riscos), etc.

### **Etapas 3: Avaliação de Eventos de Riscos e Controles**

Esta etapa tem por finalidade avaliar os eventos de riscos identificados considerando os seus componentes (causas e consequências). Os eventos devem ser avaliados sob a perspectiva de probabilidade e impacto. Normalmente as causas se relacionam à probabilidade de o evento ocorrer e as consequências ao impacto, caso o evento se materialize.

A avaliação de riscos deve ser feita por meio de análises quantitativas e qualitativas ou da combinação de ambas e, ainda, quanto à sua condição de inerentes (risco bruto, sem considerar qualquer controle) e residuais (considerando os controles identificados e avaliados quanto ao desenho e a sua execução).

Risco inerente: é o risco a que o Grupo está exposto sem considerar quaisquer ações gerenciais que possam reduzir a probabilidade de sua ocorrência ou seu impacto.

Risco residual: é o risco a que o Grupo está exposto após a implementação de ações gerenciais para o tratamento do risco.

Controles internos: são o conjunto de regras, procedimentos, diretrizes, protocolos, rotinas de sistemas informatizados, conferências e trâmites de documentos e informações, entre outros, destinados a enfrentar os riscos e fornecer segurança razoável na consecução da missão do Grupo.

A realização desta etapa ocorrerá em duas sub-etapas (1ª Mensuração do risco inerente e 2ª Avaliação dos controles de resposta aos eventos de risco), sendo todas elas utilizando a Planilha Matriz de Riscos e Controles e ferramenta sistêmica.

### **Etapas 4: Resposta a risco**

Atividades de controles são as políticas e os procedimentos estabelecidos e executados para reduzir os riscos que o Grupo tenha optado por responder, também denominadas de procedimentos de controle. As atividades de controles devem estar distribuídas por toda o Grupo, em todos os níveis e em todas as funções. Incluem uma gama de controles internos preventivos e detectivos (corretivos e compensatórios), bem como a preparação prévia de planos de contingência/continuidade em resposta a possíveis materializações de eventos de riscos.

Em alguns casos a atividade de controle aborda diversos riscos e as vezes são necessárias diversas atividades para resposta a apenas um risco.

Conhecido o nível de risco residual, deve ser verificada qual estratégia a ser adotada para responder ao evento de risco. A escolha da estratégia dependerá do nível de exposição a riscos previamente estabelecidos em confronto com a avaliação que se fez do risco na Matriz de Riscos e Controles. Em função do nível de risco residual, tem-se sugestão de medida correspondente a ser adotada.

Os tipos de respostas são os seguintes:



	<b>SISTEMA INTEGRADO DE GESTÃO AGROINDUSTRIAL - SIGA</b>  <b>POLITICAS DE GESTÃO</b>			
Título:	POLÍTICA DE GESTÃO DE RISCOS	Código	Revisão	Página
Depto:	CORPORATIVO - ESTRUTURANTE	PO-COREST-010	0	9 de 13

**Aceitar:** O Grupo decide, deliberadamente, não tomar nenhuma medida em relação ao risco. A sua probabilidade e impacto são tão baixos que não justificam a criação de controles para mitigação, ou os controles existentes já resguardam boa parte de suas consequências. Conviver com o evento de risco mantendo práticas e procedimentos existentes. Para este cenário, onde os riscos são classificados como "Altos e Críticos", é necessário monitorar seu apetite e, caso entre em patamar de estresse, designar e acompanhar o plano de ação junto a área responsável.

**Evitar/Eliminar:** Alterar ou reduzir escopos/requisitos, ou não iniciar ou descontinuar atividades/processos para eliminar o objeto sujeito ao risco, eliminando a ameaça na origem. Exemplos: Cancelar um projeto; suspender a produção de matéria-prima em uma determinada área ou região, ou fornecedor.

**Mitigar/Reduzir:** Atuar para reduzir a probabilidade e/ou impacto do risco, de modo que mesmo que ele ocorra, o problema gerado é menor e mais fácil de corrigir. Significa restringi-los a um determinado nível aceitável, tornando-o menor ou mesmo removendo-o da lista dos principais riscos. Adotar medidas para reduzir a probabilidade e/ou impacto dos riscos.

**Transferir/Compartilhar:** Pode ser feito através de contratação de seguros ou de cláusulas específicas e garantias em contratos, ou, ainda, através da terceirização de atividades das quais o Grupo não tem suficiente domínio. Transferir ou compartilhar parte do risco, reduzindo a probabilidade e/ou impacto. Exemplos: seguro, transações de hedge ou terceirização da atividade.

Caso se opte por aceitar o risco, devem ser estabelecidas métricas de monitoramento para possibilitar sua reclassificação conforme eventuais alterações ao longo do tempo. . Caso o tratamento escolhido para o risco seja reduzir, devem ser definidos planos de ação para mitigar o nível de exposição.

As ações para responder os eventos de riscos devem ser compatíveis com a tolerância a riscos, considerar a relação custo-benefício, refletir se o efeito da resposta afeta a probabilidade ou o impacto, ou ambos, e elaborar um plano de implementação de controles.

#### **Etapas 5: Informação, Comunicação e Monitoramento**

O fluxo das comunicações deve permitir que informações fluam em todas as direções e que os direcionamentos estratégicos alcancem toda o Grupo. A comunicação ocorre por meio dos níveis de relacionamento delineados conforme fóruns e comitês pertinentes, além do reporte à Alta Gestão.

Para que o gerenciamento de riscos seja efetivo, cada gerente é responsável por realizar o monitoramento das tratativas dadas aos riscos identificados e reportá-las a sua diretoria a cada dois meses.

A Matriz de Riscos e Controles será o meio de monitoramento do processo de Gestão de Riscos e Controles Internos do Grupo, sendo esta revisada no mínimo anualmente, na identificação de novos eventos ou na necessidade de melhorias. Além dele, o Relatório de Implementação do Plano de Controles, construído na periodicidade definida pelas instâncias de gerentes, será de suma importância para o acompanhamento dos trabalhos realizados pelo Grupo.

Os controles operacionais devem ser continuamente avaliados no que diz respeito ao seu desenho e operação.

	<b>SISTEMA INTEGRADO DE GESTÃO AGROINDUSTRIAL - SIGA</b>  <b>POLÍTICAS DE GESTÃO</b>			
Título:	POLÍTICA DE GESTÃO DE RISCOS	Código	Revisão	Página
Depto:	CORPORATIVO - ESTRUTURANTE	PO-COREST-010	0	10 de 13

## 5. Do Risk Sensing

*Risk Sensing* é uma prática proativa de identificação e monitoramento de riscos emergentes (ou seja, que ainda não se materializaram, mas podem surgir no futuro) por meio da análise contínua de dados internos e externos. Ele utiliza ferramentas como análise preditiva, inteligência artificial, big data, mineração de texto e monitoramento de mídia para antecipar ameaças e oportunidades, muitas vezes antes que elas sejam perceptíveis pelos métodos tradicionais de gestão de risco.

Desta forma, a abordagem:

- Provoca uma vigilância contínua e antecipatória de riscos.
- Baseia-se em tecnologia e dados, incluindo fontes estruturadas (relatórios, sistemas internos) e não estruturadas (notícias, redes sociais, relatórios de terceiros, etc.).
- Foca em riscos emergentes e externos, como mudanças regulatórias, climáticas, tecnológicas, geopolíticas ou sociais.

O *Risk Sensing* é feito de forma contínua ou periódica, e não apenas durante avaliações anuais ou em auditorias. Exemplos:

- Continuamente, via ferramentas automatizadas que monitoram sinais de alerta (ex: notícias de sanções a fornecedores, riscos ESG em cadeias de suprimento, protestos trabalhistas etc.).
- Periodicamente, como parte de ciclos de revisão estratégica, planos de continuidade de negócios ou auditorias internas.

Ele é especialmente útil em momentos de:

- Planejamento estratégico e orçamentário.
- Transformações organizacionais.
- Expansões para novos mercados.
- Mudanças regulatórias ou geopolíticas intensas.

Tem como finalidade:

- Antecipar riscos que ainda não impactaram a empresa diretamente.
- Dar vantagem competitiva por meio da agilidade na resposta.
- Informar decisões estratégicas com dados atualizados e preditivos.
- Melhorar a resiliência organizacional, ajustando planos de mitigação.
- Fortalecer a cultura de risco, envolvendo lideranças e áreas-chave.
- Complementar a matriz de riscos tradicional, que é mais estática e baseada no histórico.

## 6. Disposições gerais

Em caso de conflito entre as disposições desta Política e da legislação vigente, prevalecerá o disposto na legislação vigente.

**Parágrafo único:** Qualquer violação às legislações pode resultar em penalidades civis e criminais para a Companhia, seus funcionários ou terceiros. Qualquer violação à esta política pode causar a adoção de medidas disciplinares, administrativas ou outras medidas permitidas por lei.

	<b>SISTEMA INTEGRADO DE GESTÃO AGROINDUSTRIAL - SIGA</b>  <b>POLITICAS DE GESTÃO</b>			
Título:	POLÍTICA DE GESTÃO DE RISCOS	Código	Revisão	Página
Depto:	CORPORATIVO - ESTRUTURANTE	PO-COREST-010	0	11 de 13

## RESPONSABILIDADES

### Compete ao Conselho de Administração:

- (i) Promover a disseminação da cultura de gestão de riscos no Grupo, juntamente com a Diretoria Executiva.
- (ii) Definir os objetivos estratégicos, as diretrizes e o perfil de riscos do Grupo, adequado e aderente aos seus negócios.
- (iii) Fornecer periodicamente sua percepção do grau de exposição a Riscos que o Grupo está exposta e influenciar na priorização dos riscos a serem tratados.
- (iv) Validar e aprovar anualmente o cálculo do Apetite a Risco.
- (v) Avaliar em pauta prévia, mudanças ou atualizações em cada Risco.
- (vi) Assegurar ao Comitê de Riscos, Finanças e Auditoria (CRFA) autonomia operacional, lhe aprovando orçamento próprio destinado a cobrir despesas com seu funcionamento.
- (vii) Receber, por meio do CRFA, o reporte das atividades da Auditoria Interna, avaliando, ao menos anualmente, se a estrutura e orçamento desta são suficientes ao desempenho de suas funções.

### Compete ao CRFA:

- (i) Reporte aos temas relacionados à Gestão de Riscos ao Conselho de Administração, dada sua autonomia e vinculação.
- (ii) Avaliar e monitorar as exposições de Risco para desenvolvimento de ações que promovam redução de riscos e ameaças.
- (iii) Recomendar ao Conselho de Administração a avaliação de políticas, limites e planos de ação.
- (iv) Avaliar, monitorar e recomendar à Diretoria Executiva a correção ou aprimoramento das políticas internas do Grupo.
- (v) Monitorar o cumprimento desta Política e avaliar a performance frente aos limites de Risco aprovados.
- (vi) Opinar na contratação e destituição dos serviços de auditoria independente.
- (vii) Sugerir aprimoramentos ao processo de gestão de Riscos, apontando as causas e responsabilidades, sempre que julgar necessário.
- (viii) Acompanhar as atividades da área de Governança, Riscos e Compliance e reportá-las ao Conselho de Administração.
- (ix) Possuir meios para receber e tratar informações acerca do descumprimento de dispositivos legais e normativos aplicáveis à Colombo Agroindústria S/A, além de regulamentos e códigos internos, inclusive estabelecer procedimentos específicos para proteção do prestador e da confidencialidade da informação.

### Compete à Diretoria Executiva:

- (i) Aprovar esta Política e acompanhar o processo de Gestão de Riscos.
- (ii) Apoiar na cultura e gerenciamento dos riscos dentro de suas esferas de responsabilidade, conforme as tolerâncias a risco estabelecidas, alinhadas ao Apetite a Risco do Grupo.
- (iii) Analisar, avaliar e acompanhar os riscos sob responsabilidade dos Proprietários dos Riscos.
- (iv) Disponibilizar os recursos necessários para a execução do processo de Gestão de Riscos.
- (v) Assegurar a implementação dos planos de ação elaborados pelos Proprietários dos Riscos.

### Compete à área de GRC (Governança, Riscos e Compliance):

	<b>SISTEMA INTEGRADO DE GESTÃO AGROINDUSTRIAL - SIGA</b>  <b>POLITICAS DE GESTÃO</b>			
Título:	POLÍTICA DE GESTÃO DE RISCOS	Código	Revisão	Página
Depto:	CORPORATIVO - ESTRUTURANTE	PO-COREST-010	0	12 de 13

Referente às atividades de Gestão de Riscos e Controles Internos:

- (i) Elaborar e manter atualizada esta Política.
- (ii) Fornecer metodologia e ferramentas com a finalidade de identificar, avaliar e gerenciar riscos.
- (iii) Dar suporte aos Proprietários dos Riscos na identificação, análise, avaliação, tratamento e monitoramento dos riscos.
- (iv) Atualizar no mínimo anualmente o Apetite a Risco.
- (v) Promover através de treinamentos a competência em gestão de riscos, além de buscar melhorias no procedimento de gestão de riscos de forma contínua e sugerir melhorias de controles internos nas áreas operacionais.
- (vi) Orientar a integração da gestão de riscos com outras atividades de gestão.
- (vii) Monitorar a evolução dos Riscos Prioritários e dos planos de ação.
- (viii) Buscar melhorias no processo de Gestão de Riscos de forma contínua.
- (ix) Reportar-se ao CRFA quanto a questões relacionadas a Gestão de Riscos e Controles Internos.

Referente às atividades de Compliance e Privacidade de Dados:

- (i) Tomar as medidas necessárias para garantir a aplicação e divulgação do Código de Conduta e, inclusive, fiscalizar e avaliar o seu cumprimento e eficácia.
- (ii) Propor novas normas ou políticas relacionadas ao programa de Compliance ou a revisão das já existentes, e fiscalizar e avaliar o seu cumprimento e eficácia.
- (iii) Avaliar a concessão de brindes, presentes, hospitalidades ou entretenimento.
- (iv) Avaliar as doações e patrocínios realizados pelo Grupo.
- (v) Conduzir treinamentos periódicos acerca das condutas, princípios, conceitos e procedimentos previstos no Código de Conduta e Ética, para sensibilizar colaboradores e stakeholders sobre a importância da integridade, promovendo o acultramento de compliance e sua incorporação no dia a dia da organização.
- (vi) Acompanhar a implementação dos planos de ação relacionados à Compliance.
- (vii) Realizar o monitoramento periódico do Programa de Compliance e Integridade e coordenar as melhorias de processos para mitigar o Risco de Compliance.

**Compete à Auditoria Interna:**

- (i) Reportar temas relacionados à Gestão de Riscos ao Conselho de Administração por meio do CRFA (Comitê de Riscos, Finanças e Auditoria).
- (ii) Aferir a qualidade e a efetividade do processo de Gestão de Riscos e dos processos de governança e da adequação dos controles, de forma independente, imparcial e tempestiva.
- (iii) Fornecer relatórios periódicos ao Conselho de Administração, por meio do CRFA, a fim de garantir que os processos e estrutura de Gestão de Riscos estejam sendo devidamente obedecidas, apresentando recomendações práticas e monitorando a adoção e eficácia das ações corretivas propostas.

**Compete aos Proprietários dos Riscos:**

- (i) Ser e agir efetivamente como Proprietários dos Riscos e principais responsáveis pela Gestão de Riscos de suas áreas.
- (ii) Cumprir o Apetite a Risco aprovado anualmente pelo Conselho de Administração.
- (iii) Gerenciar (identificar, avaliar, tratar e reportar) os Riscos.

	<b>SISTEMA INTEGRADO DE GESTÃO AGROINDUSTRIAL - SIGA</b>  <b>POLITICAS DE GESTÃO</b>			
Título: Depto:	<b>POLÍTICA DE GESTÃO DE RISCOS</b> <b>CORPORATIVO - ESTRUTURANTE</b>	Código <b>PO-COREST-010</b>	Revisão <b>0</b>	Página <b>13 de 13</b>

- (iv) Anualmente ou tão logo identificar que um dos riscos mapeados pode ser considerado como prioritário, deve reportar, em tempo hábil, à área de GRC para que possa validar se é de fato um risco prioritário.
- (v) Elaborar planos de ação para adequar as exposições aos limites aprovados.
- (vi) Definir os responsáveis pelos planos de ação.
- (vii) Definir os prazos para finalização dos planos de ação.
- (viii) Acompanhar a execução e assegurar a implementação dos planos de ação.
- (ix) Monitorar os riscos não priorizados e reportar tempestivamente caso haja alteração relevante que possa mudar sua classificação para crítico.
- (x) Reportar a qualquer momento evento ou alterações na avaliação do risco e evolução dos planos de ação ao responsável por Gestão de Riscos da sua unidade.

### ANEXOS

Não há

NÃO  
  
CONTROLADA  
  
NÃO SERÁ SUBSTITUÍDA EM CASO DE REVISÃO