
POLÍTICA DE GESTÃO DE RISCOS CORPORATIVOS DA

COMPANHIA BRASILEIRA DE DISTRIBUIÇÃO

Aprovada em Reunião do Conselho de Administração da Companhia realizada em 06 de
fevereiro de 2020.

POLÍTICA DE GESTÃO DE RISCOS CORPORATIVOS DA COMPANHIA BRASILEIRA DE DISTRIBUIÇÃO

1. OBJETIVO

Estabelecer princípios, conceitos, diretrizes e responsabilidades na Gestão de Riscos do Grupo Pão de Açúcar (GPA) e das suas Unidades de Negócio no que tange a identificação, análise e avaliação dos riscos que possam afetar os seus objetivos estratégicos e a efetiva criação e proteção do valor do GPA.

Definir, a partir dos riscos inerentes, dispositivos de controles e de monitoramento das exposições, incorporando a visão de riscos à tomada de decisões estratégicas e em conformidade com os requerimentos legais, com as melhores práticas e metodologias de mercado aplicáveis.

2. ABRANGÊNCIA

Aplicável para todos os macroprocessos e operações de negócio do GPA.

3. DIRETRIZES

Temos como diretrizes gerais o compromisso com a proposta de valor do GPA, alinhados ao nosso código de ética e conduta para que possamos criar uma cultura de gestão de riscos que atinja a todos os seus colaboradores.

A gestão de riscos é parte do processo de Governança Corporativa do GPA, sendo parte integrante do processo decisório contribuindo para a execução da sua estratégia. Os riscos são identificados e tratados de forma a assegurar o cumprimento das metas estabelecidas no planejamento estratégico.

Para isso, a estrutura de Gestão de Riscos considera a atuação conjunta dos órgãos de governança corporativa e de gestão, de acordo com o conceito das 4 linhas de defesa, descrito na *tabela 1* abaixo:

1ª Linha	2ª Linha	3ª Linha	4ª Linha
<ul style="list-style-type: none">- A Gestão Operacional, representado pelas diretorias, gerências e demais colaboradores das unidades de negócio que atuam nas operações e tarefas do dia-a-dia.- Devem gerenciar o desempenho e os riscos assumidos de acordo com o estabelecido na política.- Implementam controles, planos de ação e prestam contas, tempestivamente, das informações	<ul style="list-style-type: none">- As áreas de controles e funções de suporte, representados pela Diretoria de Gestão de Riscos, a qual por sua vez, pode requerer o assessoramento pelas áreas internas da Companhia responsáveis por questões de <i>Compliance</i>, Controles Internos e Segurança da Informação.- Devem orientar, monitorar e avaliar a aderência aos padrões e políticas definidas e dar suporte a 1ª linha de defesa a atingir os objetivos do GPA.	<ul style="list-style-type: none">- As funções de garantia, representado pela Auditoria Interna, responsável por realizar auditorias ou revisões de práticas de Gerenciamento de Riscos e dos Controles Internos e eficácia da governança, identificando problemas e oportunidades de melhoria com independência, objetividade e autoridade para as recomendações.	<ul style="list-style-type: none">- As funções de Auditoria Externa Independente, que tem por missão profissional avaliar a qualidade dos controles internos voltados para o preparo de demonstrações financeiras. Nesse papel, a Auditoria Externa Independente é também uma linha de defesa pois tem que reportar à Companhia as fragilidades em tais controles, se encontrarem.

relacionadas à Gestão de Riscos.	- Facilitar, comunicar e monitorar as práticas de Gestão de Riscos e auxiliar na identificação de riscos segundo o Apetite a Riscos estabelecido.		
----------------------------------	---	--	--

Tabela 1: Linhas de defesa

4. TERMOS E DEFINIÇÕES

- 4.1. GPA:** Grupo Pão de Açúcar e suas Unidades de Negócio.
- 4.2. COAUD:** Comitê de Auditoria.
- 4.3. COMEX:** Comitê Executivo.
- 4.4. Gestão de Riscos:** Conjunto de atividades coordenadas e estruturadas a fim de alinhar o Apetite de Risco ao ciclo de tomada de decisão estratégica na busca de otimizar os resultados estabelecidos no planejamento estratégico e a efetiva criação e proteção do valor do GPA.
- 4.5. Apetite a Risco:** É o nível de risco que a companhia está disposta a aceitar, de acordo com a relação risco/retorno, para atingir seus objetivos de acordo com os limites estabelecidos pela Alta Administração.
- 4.6. Evento:** Uma ocorrência ou um conjunto de ocorrências, que podem gerar impactos afetando os resultados positiva ou negativamente.
- 4.7. Risco:** Fatores e/ou eventos que possam causar impactos negativos, comprometendo a capacidade da companhia de atingir seus objetivos estratégicos e a efetiva criação e proteção do valor do GPA.
- 4.8. Risco Inerente:** Nível de risco intrínseco à operação do negócio ou à atividade, sem considerar a execução de controles e ações diretas que reduzam as suas exposições, também chamado de risco bruto.
- 4.9. Risco Residual:** Nível de risco já considerando todos os controles e ações identificadas para redução da sua exposição.
- 4.10. Tolerância:** Os limites da variação aceitável no desempenho em relação ao alcance dos objetivos de negócio.
- 4.11. Capacidade:** A disposição de recursos que a companhia possui para atender o seu plano estratégico, como recursos de capital financeiro, tecnologias, processos e pessoas, entre outros.
- 4.12. Causas do Risco:** Fatores de risco que contribuem para que o risco eventualmente se materialize potencializando seus impactos através das consequências relacionadas.
- 4.13. Consequências do Risco:** São fatores agravantes dos resultados e impactos de um evento que possa afetar, positiva ou negativamente, a capacidade da companhia em atingir seus objetivos.
- 4.14. Probabilidade:** É a possibilidade do risco se materializar, podendo ser relatado de maneira qualitativa, quantitativa e por frequência.

4.15.Impacto: São fatores agravantes ou consequências no caso do risco se materializar, pode ser classificado em Impactos Financeiros, Negócio, Segurança Física, Segurança Alimentar, *Compliance*, Reputação e Imagem.

4.16.Controles ou Iniciativas de Mitigação: Ações executadas para redução do risco inerente, podendo ser atividades periódicas ou contínuas das Unidade de Negócios que auxiliarão no monitoramento dos níveis de exposição dos riscos.

4.17.Key Risk Indicator (KRI ou Indicadores-chave de Risco): Métricas utilizadas para medir e monitorar a exposição dos riscos relacionadas às causas do risco, auxiliando a companhia a agir de forma preventiva para reduzir os impactos da materialização dos riscos, sendo ainda um dispositivo de controle e boa prática de Gestão de Riscos.

4.18.Key Performance Indicator (KPI ou Indicadores-chave de Performance): Métricas utilizadas para medir e monitorar o desempenho e resultados dos processos, podendo ser utilizado para monitoramento de riscos.

4.19.Riscos priorizados: Lista de riscos definida de forma deliberada pela Alta Administração que descreve níveis de exposições que possam potencializar impactos elevados para o negócio, cuja gestão deve ser priorizada de forma estruturada.

5. PAPEIS E RESPONSABILIDADES

Descrevemos todas as partes interessadas que estão dentro do contexto e do ciclo de vida do processo de Gestão de Riscos com as suas respectivas responsabilidades:

Função	Responsabilidades
Conselho de Administração	<ul style="list-style-type: none">• Estabelecer as diretrizes gerais de riscos alinhadas ao contexto de negócio e do ciclo de planejamento estratégico;• Estabelecer através da capacidade e tolerância do GPA os limites aceitáveis de <i>Apetite a Riscos</i>;• Avaliar, deliberar e aprovar a matriz de riscos estratégicos e priorizados alinhados ao <i>Apetite a Riscos</i>;• Influenciar e patrocinar dentro dos fóruns de gestão o monitoramento dos riscos prioritários;• Influenciar e patrocinar a cultura de riscos dentro do GPA;• Avaliar, anualmente, a suficiência da estrutura e do orçamento da área de Auditoria Interna para o desempenho das suas funções;• Revisar e aprovar as definições gerais das estratégias de Gestão de Riscos;• Aprovar a política de riscos, suas evoluções e revisões futuras.
Comitê de Auditoria (COAUD)	<ul style="list-style-type: none">• Acompanhar as atividades da auditoria interna e da área de controles internos da companhia;• Avaliar e monitorar as exposições de risco da companhia;

	<ul style="list-style-type: none"> • Propor aos fóruns elegíveis definições e diretrizes para compor o modelo de Gestão de Riscos dentro da companhia; • Acompanhar e apoiar o processo de Gestão de Riscos na definição dos riscos prioritários alinhados ao contexto de negócio e as diretrizes do Conselho de Administração; • Supervisionar as atividades de Gestão de Riscos seguindo o cumprimento das legislações legais, das políticas, normas e procedimentos internos da companhia; • Avaliar, monitorar e informar periodicamente o Conselho de Administração sobre os riscos prioritários identificados pelas revisões das áreas de Gestão de Riscos auxiliando na avaliação dos planos de ação e recomendações; • Avaliar, aprovar e acompanhar a execução do tratamento e monitoramento dos riscos priorizados; • Avaliar, aprovar e recomendar à administração a correção ou aprimoramento das políticas internas da companhia; • Avaliar as informações trimestrais, demonstrações intermediárias e demonstrações financeiras da companhia.
Comitê de Governança Corporativa e Sustentabilidade	<ul style="list-style-type: none"> • Elaborar o planejamento e assegurar a operacionalização da Gestão de Riscos, considerando todas as dimensões da estrutura definida, englobando atividades estratégicas, táticas e operacionais do GPA; • Assessorar o Conselho de Administração na aplicação da metodologia de Gestão de Riscos no GPA; • Apoiar o Conselho de Administração na definição do Apetite de Risco e na definição dos riscos prioritários do GPA; • Apoiar o GPA na análise e aprovação da estratégia de Gestão de Risco; • Assessorar o Comitê de Auditoria e o Conselho de Administração sobre os níveis de exposições dos riscos; • Avaliar a eficácia do processo de Gestão de Risco no GPA; • Identificar os riscos decorrentes das mudanças estratégicas e diretivas do GPA sob decisão do Conselho de Administração.
Presidência Executiva / COMEX	<ul style="list-style-type: none"> • Promover a integração e a cultura de riscos no GPA e nos ciclos de gestão e planejamento estratégico; • Garantir a implantação de um modelo eficiente de Gestão de Riscos, alinhado aos objetivos de negócios e metas de negócio. Aplicar as diretrizes gerais estabelecidas pelo Conselho de Administração para atribuir o nível de Apetite a Risco aceitável para o GPA;

	<ul style="list-style-type: none"> • Acompanhar os riscos gerenciados no nível de cada processo e operações para garantir a efetividade das medidas de controle; • Participar dos rituais de validações e priorização dos riscos do GPA. • Acompanhar os KRIs, KPIs e as estratégias de mitigação dos riscos prioritários; • Avaliar e monitorar o tratamento dos riscos de negócio alinhados à execução do planejamento estratégico; • Avaliar, tempestivamente, a eficácia a aplicabilidade das diretrizes da política de riscos; • Avaliar e apoiar as adequações da estrutura destinada ao processo de gerenciamento, considerando recursos humanos, financeiros e tecnológicos.
Diretoria de Gestão de Riscos	<ul style="list-style-type: none"> • Definir e evoluir a metodologia de Gestão de Riscos alinhada à cadeia de valor e integrada dentro de todo o GPA; • Gerir o ciclo do processo de Gestão de Riscos no GPA cobrindo todas as Unidades de Negócio; • Garantir a gestão do fluxo de informações dentro de todas as Unidades de Negócio alinhada aos conceitos, a metodologia e aos prazos estabelecidos a cada ciclo de Gestão de Riscos; • Apoiar as Unidades de Negócio no ciclo de identificação, avaliação, tratamento e monitoramento dos riscos para auxiliá-los na redução dos níveis de exposição dos riscos; • Gerir a matriz de riscos priorizados, comunicando dentro dos principais fóruns de gestão seus status e níveis de exposições; • Suportar as áreas de negócio na identificação e avaliação do impacto dos riscos.
Dono do Risco	<ul style="list-style-type: none"> • Identificar, classificar e gerenciar os riscos das respectivas áreas de acordo com as estratégias de mitigação, em conjunto com a Diretoria de Gestão de Riscos; • Indicar o profissional que responderá como facilitador na gestão do risco junto a Diretoria de Gestão de Risco; • Assegurar a implementação dos planos de ação e acompanhamento dos KRIs (<i>Key Risk Indicador</i>); • Prestar contas dos níveis de exposição, dos planos de ações e dos indicadores que descrevem o status do risco residual para os fóruns de governança e gestão.
Facilitador Responsável /	<ul style="list-style-type: none"> • Deter o conhecimento técnico dos processos no qual os riscos estão inseridos; • Ser o responsável pela atualização das informações do mapeamento e tratamento dos riscos da sua Unidade de Negócio; • Manter as informações atualizadas tempestivamente, respeitando o calendário de planejamento do ciclo de Gestão de Riscos;

	<ul style="list-style-type: none"> • Monitorar o status dos planos de ação junto aos responsáveis pela implementação dos dispositivos de controles.
Auditoria Interna	<ul style="list-style-type: none"> • Aferir a qualidade e a efetividade dos processos de gerenciamento de riscos, controle e governança da companhia; • Identificar e apontar oportunidades de melhorias nos processos de Controle Internos e de Gestão de Risco; • Auditar as informações e controles relacionados aos KRIs e KPIs desenvolvidos e monitorados pelas áreas funcionais; • Reportar periodicamente ao COAUD e aos seus clientes auditados os resultados de avaliações independentes, imparciais e tempestivas sobre a efetividade da Gestão de Riscos na empresa.
Colaboradores	<ul style="list-style-type: none"> • Assegurar a operacionalização da Gestão de Riscos, fazendo parte do processo de identificação, avaliação e mensuração, implementando ações preventivas e corretivas; • Participar de treinamentos que permitam a disseminação de forma consciente da cultura de Gestão de Riscos.

Tabela 2: Papéis e responsabilidades

6. PROCESSO GESTÃO DE RISCOS

O processo de Gestão de Riscos do GPA foi definido com base nas orientações do COSO – *Committee of Sponsoring Organizations of the Treadway Commission* e na norma ISO 31000: 2018 - Princípios e Diretrizes da Gestão de Riscos.

O ciclo de vida do processo é constituído de 7 etapas subsequentes e dependentes ao qual executamos com frequência anual, conforme fluxo ilustrado na *figura 1*.

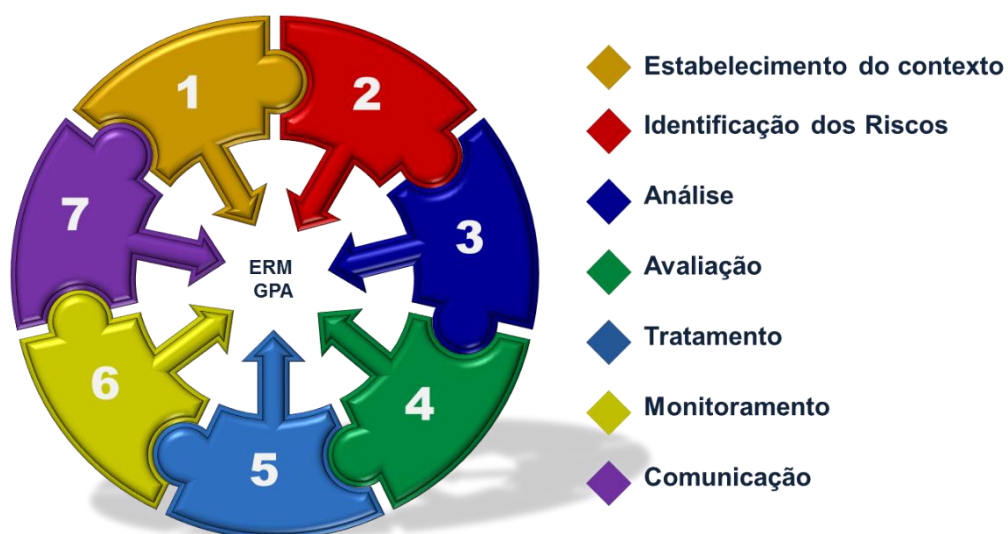


Figura 1: Etapas do processo de Gestão de Riscos GPA

6.1. ETAPAS DO PROCESSO

◆ **Etapa 1 - Estabelecimento do Contexto:**

Entender o cenário e contexto de negócio considerando fatores ligados ao planejamento estratégico de curto e longo prazo do GPA e das suas Unidades de Negócio alinhados ao ambiente em que esses objetivos são inseridos.

É uma etapa fundamental para garantir que o processo de Gestão de Riscos esteja alinhado aos ciclos de gestão e de planejamento estratégico da companhia para alinhar seus níveis aceitáveis de *Apetite a Risco*.

É constituída de um ciclo anual de alinhamentos executivos com os donos do processo e a Alta Administração para compor um mapa de referências que irá auxiliar nas próximas etapas para identificar os riscos que estão mais alinhados ao contexto do negócio.

Para estabelecer os cenários que devem apoiar essa etapa consideramos dois fatores influenciadores, são eles:

- **Fatores Externos:** Econômicos, Meio ambiente, Políticos e Sociais.
- **Fatores Internos:** Infraestrutura, Recursos Humanos, Processos e Tecnologias.

◆ **Etapa 2 – Identificação dos Riscos:**

A abordagem de identificação de riscos é top-down, partindo de entrevistas com os principais executivos das Unidades de Negócio, tendo em vista os principais processos pelos quais são responsáveis.

O produto gerado nessa etapa é uma lista abrangente de riscos baseada nos eventos que possam identificar vulnerabilidades e ameaças que coloquem em risco a realização dos objetivos estratégicos do GPA.

Nesta etapa também deve ser definido o dono e o responsável por cada um dos riscos identificados, assim como uma descrição que orientará as próximas etapas do mapeamento.

◆ **Etapa 3 – Análise:**

Realizamos uma análise mais detalhada dos riscos identificados, incluindo atributos importantes para dar clareza e respaldo qualitativo e quantitativo para gerar variáveis que possam classificar de forma holística o universo de riscos para atuarmos de forma mais assertiva nas suas priorizações.

Definimos, entre outros, as suas causas ou fatores de risco e seus efeitos, classificando seus fatores agravantes para que possamos gerar uma lista de riscos abrangente e relevante para prosseguir com o mapeamento.

Levantamos informações para obter dados que possam descrever a probabilidade e impactos dos riscos, gerando assim uma matriz qualitativa para descrever de forma executiva o universo de riscos com base nas suas classificações, como segue descrito na *figura 2*.

PROBABILIDADE	PROVÁVEL	BAIXO	MÉDIO	ALTO
	POSSÍVEL	BAIXO	MÉDIO	ALTO
	REMOTA	BAIXO	MÉDIO	ALTO
		IMPACTO		

Figura 2: Matriz de Riscos Qualitativa

Classificamos os riscos dentro dessa matriz qualitativa, seguindo os seguintes critérios:

- **Classificação Alta ou Risco Alto (Vermelho):** Representam uma ameaça potencial aos negócios do GPA e devem ser tomadas ações prioritárias para reduzir ou eliminar o componente de risco.
- **Classificação Média ou Risco Médio (Amarelo):** Representam uma ameaça, podendo ser monitorados e gerenciados através de medidas de controles preventivas que possam manter o grau de exposição ou aceitação do risco.
- **Classificação Baixa ou Risco Baixo (Verde):** Representam uma ameaça aceitável com grau de impactos menores não havendo necessidade de monitoramento contínuo e podendo ser aceito.

◆ Etapa 4 – Avaliação:

Avaliamos os riscos inerentes e seus potenciais impactos de materialização para a realização dos objetivos do GPA.

Com o suporte da Alta Administração, dos executivos e dos líderes de processos avaliamos os eventos dentro das perspectivas de probabilidade ou frequência e impactos. Buscamos variáveis para combinar métodos de avaliação qualitativos e quantitativos.

Consideramos, entre outras, variáveis para classificação de impactos que auxiliam na melhor classificação dos riscos, utilizando o gradiente de alto, médio e baixo para cada variável.

Por fim, combinando todas as variáveis de avaliação, definimos a criticidade dos riscos identificados, o que nos permite construir um mapa de priorização, partindo dos riscos de maior exposição para os de menor exposição.

Esse mapa auxilia o GPA e as suas Unidades de Negócio a obter um maior grau de alinhamento do planejamento estratégico com o nível aceitável de Apetite a Riscos da companhia.

◆ Etapa 5 – Tratamento:

A fase de tratamento de riscos envolve identificar os dispositivos de controle existentes dentro do processo para classificarmos a sua efetividade como medida de prevenção e como fator redutor do grau de exposição (Fator Mitigatório) que irá auxiliar na atribuição do risco residual.

Para os processos que requerem um maior grau de efetividade dos controles ou que não possuem fatores de mitigação efetivos, formalizamos nessa etapa a implementação de um ou mais planos de ação para mitigar os fatores de risco.

Para cada plano de ação, atribuímos responsáveis e cronogramas de implementação para garantir a eficácia e eficiência dos planos e assim reduzir o nível de risco residual.

Dentro desse processo, aplicamos alternativas de respostas para os riscos, conforme *tabela 3*:

Eliminar	Reduzir ou Mitigar	Transferir	Aceitar
Adotar ações que altere ou elimine um processo ou um projeto, protegendo os objetivos do negócio dos impactos deste risco	Adotar medidas de controle para reduzir a probabilidade e/ou o impacto de um risco até um nível aceitável de acordo com o apetite a riscos	Adotar ações que reduzam a probabilidade e/ou o impacto do risco pela transferência total ou pelo compartilhamento de uma parte do risco	Nenhuma medida é adotada para afetar a probabilidade e/ou o impacto do risco, pois está dentro do nível aceitável de Apetite a Risco

Tabela 3: Alternativas de resposta para os riscos

◆ **Etapa 6 – Monitoramento:**

Constituída de um ciclo dinâmico e contínuo, sendo fundamental para garantir de forma tempestiva, preventiva e reativa ações que auxiliem em minimizar impactos em caso de materialização dos riscos.

Os colaboradores envolvidos em cada área devem ter a capacidade e competência para identificar, avaliar, priorizar, monitorar e gerir os seus riscos, considerando todas as mudanças dentro do ambiente interno e externo, para que possam obter maior grau de controle dos seus processos para atingir seus objetivos firmados no tratamento dos riscos (*Ver tabela 3*).

O processo de monitoramento dos riscos é constituído de duas frentes principais, são elas:

- **Planos de Ação:** Deve ser realizado pelas Unidades de Negócio de acordo com as responsabilidades definidas pelos donos dos riscos com periodicidade que pode variar de mensal, bimestral, trimestral, semestral, chegando até a anual, dependendo das necessidades de Gestão do Risco.
- **Medida de Controles:** Utilizamos métricas e indicadores ao qual chamamos KRI. Essas métricas e indicadores estão relacionados aos fatores de risco e aos fatores de medidas de prevenção. Durante a fase de tratamento dos riscos, identificamos essas métricas de acordo com os dispositivos de controle, definindo os limites aceitáveis que descrevam de forma indutiva se os indicadores apontam tendências ou desvios que possam materializar os riscos para que atribuam gatinhos para as Unidade de Negócio tomar ações de reversão dos eventos e consequentemente dos impactos.

◆ **Etapa 6 – Comunicação:**

Cumprimos um ritual frequente de alinhamentos que tem como objetivo desde a disseminação da cultura de Gestão de Riscos através de *workshop*, treinamentos e / ou de rituais de prestação de contas com os donos dos riscos e com os principais fóruns de gestão do GPA, como Conselho de Administração, Comitê Executivo e Comitê de Auditoria.

Para cumprir esse ritual de comunicação definimos um plano que desenvolve formatos de comunicação de acordo com o público alvo, onde descreva a frequência, os envolvidos e a responsabilidade dentro do contexto.

6.2. CLASSIFICAÇÃO DOS RISCOS

Adotamos 4 classificações de riscos dentro do processo, são eles:

- **Estratégicos:** Riscos que afetam a estratégia ou os objetivos estratégicos do GPA. Estão ligados a cenários de incertezas e/ou oportunidades e estão no foco prioritário da Alta Administração.
- **Operacionais:** Riscos decorrentes da inadequação ou falha na gestão de processos internos, de pessoas ou tecnologias que possam dificultar ou impedir o alcance dos objetivos.
- **Compliance:** Riscos que estão dentro do contexto legal ou regulatório, ligados à corrupção pública ou privada, crimes e a fraudes.
- **Tecnologia da Informação (TI):** Riscos relacionados ao uso, operação e influência da tecnologia da informação dentro do GPA que possam gerar vulnerabilidades que uma vez exploradas afetam a operação e resultados da companhia.

7. VIGÊNCIA E APROVAÇÃO

Essa política tem vigência a partir da sua aprovação e publicação, podendo ser revisada sempre que houver necessidade.

8. PENALIDADES

O descumprimento desta política é considerado falta grave, passível de aplicação das sanções administrativas, cíveis, penais e/ou trabalhistas cabíveis, a serem avaliadas pelo Diretor Executivo da área e pelo Comitê de Ética.

A presente Política foi aprovada em Reunião do Conselho de Administração da Companhia realizada em 06 de fevereiro de 2020.