

# **POLÍTICA DE GESTÃO DE RISCOS**

## **1. OBJETIVO**

Estabelecer as diretrizes e as responsabilidades para a orientação dos processos de Gestão de Riscos e Controles Internos (ERM - Enterprise Risk Management) inerentes às atividades da Auren Energia S.A. ("Auren" ou "Companhia"), incorporando a visão de riscos ao seu planejamento estratégico e à tomada de decisões, e a visão de controles internos a seus processos, em conformidade com as regulamentações aplicáveis e com as melhores práticas de mercado.

## **2. ABRANGÊNCIA**

A presente Política de Gestão de Risco ("Política") abrange a Auren e suas controladas.

## **3. REFERÊNCIAS**

- Estatuto Social;
- Norma ABNT NBR ISO 31000:2018 – Gestão de Riscos – Diretrizes;
- IBGC (Instituto Brasileiro de Governança Corporativa);
- COSO (*Committee of Sponsoring Organizations of the Treadway Commission*);
- Norma de Due Diligence de Terceiros Auren - NG.AUREN.SGC.0007;
- Modelo das Três Linhas do IIA 2020 (Institute of Internal Auditors); e
- Manual de Gestão de Continuidade de Negócios da Companhia.

## **4. DEFINIÇÕES**

### **4.1. Ações de Mitigação**

Ações que visam mitigar os riscos identificados e reduzir a exposição da Auren. Devem obrigatoriamente possuir um ou mais responsáveis pela sua implementação, prazo para conclusão e endereçar uma ou mais causas que podem levar à materialização do risco.

### **4.2. Auditoria Interna**

Área responsável por prover avaliações independentes ao Conselho de Administração, ao Comitê de Auditoria Estatutário e à Diretoria sobre a efetividade da gestão dos riscos e do ambiente de controles internos, dos processos de governança, do cumprimento das normas e regulamentos associados às operações da Companhia.

### **4.3. Appetite a Risco**

O Apetite a Risco pode ser considerado como a predisposição à tomada de riscos que a Companhia está disposta a aceitar, diante do atendimento dos seus objetivos de negócio e da geração de valor aos acionistas. A Companhia adota três níveis de apetite: conservador, moderado ou arrojado, sendo esta classificação estabelecida para cada uma das categorias de riscos qualitativas.

#### **4.4. Categoria do risco**

Categorias definidas de acordo com a os pilares da cultura, diretrizes estratégicas, compromissos ESG e sistema de gestão da Companhia. Cada categoria apresenta o respectivo nível de apetite estabelecido pelo Conselho de Administração e deve ser adotado como referência para gestão dos riscos associados.

#### **4.5. Causas do Risco**

Ocorrência ou alteração nas circunstâncias que tem o potencial de contribuir para que um risco se materialize. Cabe destacar que um mesmo risco pode conter uma ou mais causas relacionadas.

#### **4.6. Comissão de Riscos Auren (CRA)**

Órgão colegiado composto pelo 1º e 2º nível executivo da Companhia, além das áreas de segunda e terceira linhas de atuação, detalhadas ao longo do material.

#### **4.7. Comitê de Auditoria Estatutário (CAE)**

Órgão colegiado de assessoramento vinculado e com reporte ao Conselho de Administração, de caráter consultivo e com funcionamento permanente, com autonomia e independência operacional. O CAE deve pautar-se pelo atendimento aos legítimos interesses da Companhia.

#### **4.8. Conselho de Administração**

Órgão que tem como objetivo proteger e valorizar o patrimônio da Companhia, assim como maximizar o retorno do investimento e a sustentabilidade no longo prazo, baseado no Estatuto Social e nas diretrizes de seu respectivo Regimento Interno.

#### **4.9. Consequências do risco**

Resultado da materialização dos riscos identificados.

#### **4.10. Controles Internos**

Conjunto de ações, práticas e procedimentos para gerenciar riscos e aumentar a probabilidade quanto ao cumprimento dos objetivos estabelecidos pela Companhia, além de assegurar a aderência às leis e regulamentos e confiabilidade dos relatórios financeiros e gerenciais.

#### **4.11. Diretoria**

A Diretoria Estatutária e demais diretores da Companhia.

#### **4.12. Dono do Risco**

Gestor ou executivo responsável diretamente pela avaliação e estratégia de resposta estruturada a risco identificado em sua área de atuação. Deve pautar-se pela definição e endereçamento das ações de mitigação do risco, bem como seu monitoramento e reporte aos diferentes fóruns de Governança, mediante suporte da Gerência de Riscos de Negócio.

#### **4.13. *Due Diligence***

Processo estruturado e proativo para identificar e avaliar impactos socioambientais e econômicos das decisões, atividades e operações da Companhia ao longo de todo o ciclo de vida de um projeto ou atividade organizacional, visando evitar ou mitigar esses impactos como parte integrante da gestão de riscos da Companhia. A *due diligence* deve ser estendida a toda a cadeia de suprimentos da Companhia. Tal processo é pautado pelas diretrizes contidas na Norma Gerencial de *Due Diligence* de Terceiros.

#### **4.14. Esferas de Probabilidade**

Critérios utilizados para a análise da probabilidade da materialização do risco.

#### **4.15. Esferas de Impacto**

Critérios (qualitativos e quantitativos) utilizados para análise do impacto do risco no caso de sua eventual materialização.

#### **4.16. Exposição ao Risco/Criticidade**

Resultante da análise do risco nas esferas de probabilidade e impacto.

4.17. Ficha de Risco

Documento executivo que formaliza as informações sobre a análise, avaliação e tratamento dos riscos.

4.18. Gestão de Riscos

Conjunto de atividades coordenadas que têm como objetivo suportar a Companhia, na identificação, avaliação, tratamento, monitoramento e comunicação dos riscos.

4.19. Matriz de Risco

Conjunto de riscos identificados e classificados pela Companhia, de acordo com os critérios de análise de impacto e probabilidade.

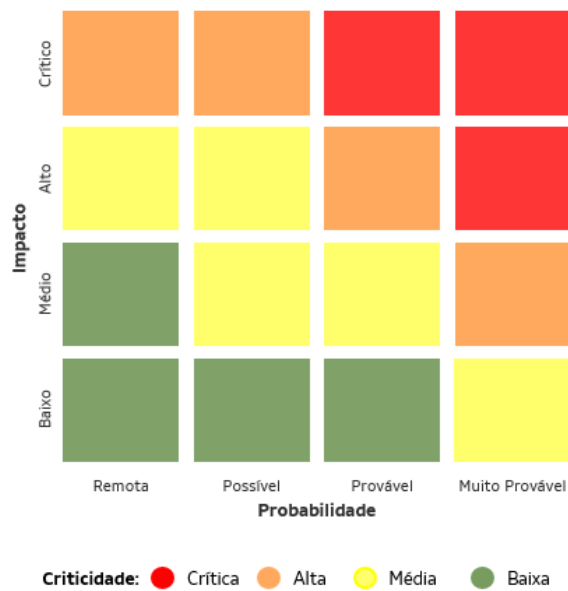


Figura 1 - Matriz de riscos

4.20. Resposta ao Risco

Ação que pode ser definida como mitigar/reduzir, aceitar, transferir/compartilhar ou evitar, atuando na probabilidade e/ou no impacto, incluindo, mas não se limitando a controles internos.

4.21. Risco

Efeito da incerteza nos objetivos da Companhia.

#### **4.22. Risco Inerente**

Visão do risco previamente a adoção de medidas de tratamento pela Companhia, como a implementação de controles internos e demais ações de mitigação.

#### **4.23. Risco Residual/Projetado**

Visão do risco posteriormente a implementação de medidas de tratamento e mitigação pela Companhia.

#### **4.24. Riscos Sistêmicos**

Riscos decorrentes do enfraquecimento ou colapso de sistemas naturais ou humanos dos quais a economia e a sociedade dependem, como por exemplo: (i) regime de chuvas e do clima; (ii) saúde pública; (iii) serviços públicos, dentre outros. Riscos sistêmicos também são decorrentes das interligações e da interdependência entre os agentes de um sistema ou mercado, no qual a insolvência ou falência de uma única entidade ou grupo de entidades pode provocar perdas e até mesmo falências em cadeia.

A abordagem para esses riscos deve considerar em seu processo de identificação e mitigação, além da exposição da Companhia, o efeito que as suas atividades podem contribuir para o agravamento de tais riscos, ainda que não intencionalmente.

#### **4.25. Riscos Emergentes**

São riscos menos conhecidos e mais incertos, que estão evoluindo rapidamente devido a mudanças no ambiente externo ou interno das organizações, e que podem ter impacto significativo devido à sua natureza imprevisível e potencialmente disruptiva.

### **5. CLASSIFICAÇÃO DE RISCOS**

A Companhia está sujeita a diversos riscos que podem impactar adversamente seus negócios, os resultados de suas operações, sua situação patrimonial e financeira e/ou sua reputação frente a seus *stakeholders*. Dessa forma, os riscos podem ser classificados de acordo com as seguintes categorias:

#### **5.1. Riscos Estratégicos:**

Riscos associados a tomada de decisão com potencial de gerar perdas substanciais no valor econômico ou causar efeitos negativos à reputação, credibilidade ou à marca da Companhia perante o mercado e as comunidades onde atua.

#### **5.2. Riscos Financeiros:**

Riscos associados: (i) às operações financeiras/contábeis da Companhia; (ii) à emissão de relatórios financeiros, gerenciais, regulatórios, fiscais, estatutários e de sustentabilidade, de forma incompleta, inadequada, inexata ou intempestiva; (iii) à deterioração na capacidade de pagamento de clientes, que venham a afetar significativamente a estabilidade financeira da Companhia (Risco de Crédito); (iv) à alteração ou extinção de incentivos fiscais regionais e/ou setoriais; (v) à possibilidade de que os fluxos de caixa não sejam administrados efetivamente para maximizar a geração de caixa operacional; (vi) ao gerenciamento dos riscos e retornos específicos das transações financeiras; (vii) à desvalorização de contrato de crédito decorrente da deterioração na classificação de risco do tomador; e (viii) à volatilidade de taxas de juros e outros indicadores macroeconômicos.

### **5.3. Riscos Legais/Regulatórios:**

Riscos associados à ocorrência de modificações nas regulamentações e ações de órgãos reguladores que podem afetar significativamente a habilidade da Companhia em administrar seus negócios, os quais podem ser representados por eventual alteração da legislação trabalhista, tributária, dentre outras, e que possam afetar adversamente seus custos e competitividade. Esse risco também está associado a aplicações de sanções legais e/ou regulatórias, decorrentes de inconformidades no cumprimento de leis e regulamentações; do código de conduta ou de políticas da Companhia.

### **5.4. Riscos Operacionais:**

Risco associado à ocorrência de perdas resultantes de falhas, deficiências ou inadequação de processos internos, pessoas e sistemas, assim como de eventos externos, como catástrofes naturais, greves e atos terroristas, dentre outras. Nesta categoria, estão associados riscos relacionados a: redução, degradação ou interrupção, total ou parcial, das atividades da Companhia, segurança de barragens de usinas hidrelétricas da Companhia, redução dos recursos naturais de geração, desenvolvimento e execução de projetos, condições de saúde e segurança do trabalho de seus colaboradores e terceiros, entre outros.

### **5.5. Riscos Tecnológicos:**

Riscos associados à falha na capacidade de a Companhia garantir a salvaguarda, privacidade e confidencialidade das informações, contra eventuais ataques cibernéticos (ambientes corporativo e de automação), contemplando tentativas de comprometer a confidencialidade, integridade ou disponibilidade de dados e sistemas computacionais. São também contemplados nesta categoria de risco: falhas, indisponibilidades ou obsolescências de equipamentos, sistemas informatizados de controle, comunicação, e gestão operacional, que comprometem ou impossibilitem a continuidade das atividades regulares da organização, ao longo da sua cadeia produtiva e de valor (clientes, fornecedores, parceiros e unidades operativas), potencialmente gerando impactos nas localidades onde a Companhia possui atuação.

## 6. DIRETRIZES

### 6.1. Conceitos Gerais

Em linha com o compromisso para preservação de valor e construção sustentável do negócio, o processo de gestão de riscos faz parte de uma abordagem mais ampla, denominada Resiliência Corporativa, que considera a preparação e capacidade da Companhia em atuar sob as óticas preventiva e reativa.

Na ótica preventiva, a Companhia conta com as etapas de gestão de riscos detalhadas nesta política, suportadas pelo Modelo de Três Linhas de Atuação representadas pelas seguintes áreas:

**1ª Linha de atuação (áreas de negócio da Companhia):** Cabe aos integrantes dessa Linha identificar, tratar, monitorar e reportar os riscos inerentes às atividades sob sua gestão. Também é a 1ª Linha que executa, no dia a dia, ações mitigatórias e controles internos definidos em resposta aos riscos envolvidos nas operações sob sua gestão.

**2ª Linha de atuação (Gestão de Riscos de Negócio e Controles Internos):** responsável pela organização e estruturação do processo de Gestão de Riscos, atuando no desenvolvimento e padronização de procedimentos e sistemas que permitam identificar, avaliar, monitorar e tratar riscos. Atua tanto no apoio aos gestores e colaboradores na identificação, tratamento e monitoramento de riscos e elaboração de ações mitigatórias, quanto junto à alta administração, reportando-lhe (de forma independente) informações e indicadores sobre o processo de Gestão de Riscos.

**3ª Linha de atuação (Auditoria Interna):** deve exercer uma atuação imparcial, independente e autônoma, voltada ao monitoramento e aferição da conformidade, qualidade e efetividade da Gestão de Riscos. Sempre que julgar pertinente, a Auditoria Interna deve recomendar aos órgãos aplicáveis melhorias e/ou planos de ação para o adequado tratamento de riscos (auditando a implementação desses planos posteriormente), bem como reportando os respectivos resultados.

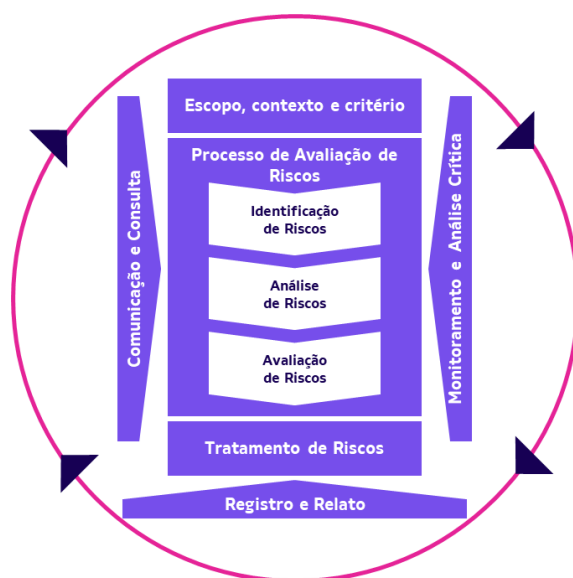
Sob a ótica reativa, a Companhia conta com um fluxo de acionamento e planos de resposta estruturados para responder à materialização de potenciais riscos decorrentes de fatores externos ou internos, conforme detalhado no Manual de Gestão de Continuidade de Negócios.

## 6.2. Processo de Gestão de Riscos

O processo de Gestão de Riscos da Auren é baseado nas diretrizes estabelecidas pelo IBGC, COSO ERM e ABNT NBR ISO 31000:2018, especialmente no que diz respeito às etapas do processo, as quais possuem os seguintes objetivos:

- Garantir que a gestão de riscos seja integrada às atividades da Companhia;
- Envolver todos os participantes da estrutura organizacional nas diversas etapas do processo;
- Padronizar conceitos e práticas;
- Suportar o processo de tomada de decisão;
- Auxiliar as áreas de negócio no processo de redução da exposição aos riscos;
- Contribuir com a transparência da Companhia para os diversos stakeholders: acionistas, analistas de mercado, agências de crédito, órgãos reguladores, entre outros.

Na figura a seguir demonstra-se as etapas do processo de gestão de riscos, baseado na ISO 31000:2018:



**Figura 2** - Processo de Gestão de Riscos conforme Norma ISO 31.000:2018

## 6.3. Escopo, contexto e critério

É a primeira etapa do processo de Gestão de Riscos. Contempla a captura e o entendimento dos objetivos estratégicos de curto, médio e longo prazo, bem como o ambiente/contexto (interno e externo) em que a Companhia está inserida e a diversidade de critérios de risco e esferas de impacto.

## 6.4. Identificação de Riscos

A etapa de identificação de riscos é um processo contínuo, onde deve-se reconhecer, descrever e registrar os riscos aos quais a Companhia está exposta. Esta identificação dar-se-á através de

entrevistas e análises com os principais executivos de cada área de negócio e, também, a partir dos fóruns de Planejamento Estratégico da Companhia. Neste momento é definida a categoria do risco, que será utilizada para realizar o vínculo ao apetite a risco, dando insumos para a etapa de avaliação do risco (descrita na seção 6.6 desta Política).

Cabe destacar que a identificação dos riscos também pode ocorrer quando da ocorrência de um evento de risco operacional significativo para os negócios, sendo assim, necessário agregá-lo ao processo de gestão de riscos da Companhia.

## 6.5. Análise de Riscos

A análise dos riscos é feita considerando as esferas de impacto (sob a ótica qualitativa e quantitativa) e de probabilidade, sendo o resultado de tal análise exposto no Mapa de Riscos da Companhia.

## 6.6. Avaliação de Riscos

A etapa de avaliação dos riscos envolve comparar a criticidade do risco resultante da etapa de análise do risco, sob as óticas das esferas de probabilidade e impacto e, a seguir, avaliar se sua classificação está aderente ao respectivo apetite da Categoria de Risco.

## 6.7. Tratamento de Riscos

Esta fase envolve primeiro a definição da resposta ao risco, com base em sua aderência ao respectivo apetite e, posteriormente, a definição junto ao dono do risco e demais áreas envolvidas sobre as ações de mitigação.

As seguintes opções de resposta ao risco podem ser consideradas na etapa de tratamento:

- **Mitigar:** Reduzir a exposição aos riscos (tanto em impacto quanto em probabilidade) a partir da implementação de ações de mitigação e estruturação do ambiente de controles internos;
- **Aceitar:** Aceitar os impactos e consequências do risco sem a tomada de ações de redução do impacto e probabilidade;
- **Transferir/compartilhar:** Contratação de apólices de seguro, entre outros. Requer que um terceiro esteja disposto e tenha capacidade para assumir responsabilidade do risco; ou
- **Evitar:** Interromper a atividade de negócio que está expondo a Companhia ao risco em questão.

## **6.8. Comunicação e Consulta**

A comunicação, durante todas as etapas dos processos de gestão de riscos e de controles internos, deve atingir todas as partes interessadas, sendo realizada de maneira clara e objetiva, respeitando as boas práticas de governança exigidas pelo mercado.

## **6.9. Monitoramento e Análise Crítica**

Sem prejuízo às responsabilidades atribuídas a cada parte no processo de Gestão de Riscos, cabe à Diretoria de Riscos e Controles Internos, coordenar o processo e monitorar a execução das ações de mitigação, bem como a maturidade e efetividade do ambiente de controles internos.

Durante o processo de monitoramento dos riscos e controles internos deve-se também detectar mudanças no contexto interno e externo à Companhia, bem como os efeitos de tais mudanças nos riscos já formalizados, devendo estes serem refletidos no Mapa de Riscos da Companhia e reportados à Alta Administração e seus demais fóruns de Governança.

Deve-se também garantir a identificação de riscos sistêmicos e riscos emergentes pertinentes às atividades da Companhia, seja sob a perspectiva dos impactos de tais riscos para os negócios, seja a contribuição da Companhia para o eventual agravamento às localidades onde a mesma opera.

Cabe destacar que também faz parte desta etapa do processo a revisão do impacto financeiro de curto, médio e longo prazo dos riscos de negócios em relação ao apetite ao risco, conforme aprovado pelo Conselho de Administração.

## **7. RESPONSABILIDADES**

### **7.1. Conselho de Administração**

- Aprovar a Política de Gestão de Riscos e acompanhar sua implementação;
- Aprovar o Apetite a Riscos da Companhia proposto pela Diretoria executiva;
- Validar os riscos identificados da Companhia, assim como a resposta aos riscos críticos e altos não aderentes ao apetite; assim como as suas respectivas causas, respostas, ações mitigatórias e controles, quando aplicável;
- Supervisionar o processo de Gestão de Riscos a partir das informações apresentadas pela Diretoria de Riscos e Controles Internos, membros do Comitê de Auditoria Estatutário e demais órgãos da governança;
- Garantir a avaliação, ao menos anual, do processo e sistemas de Gestão de Riscos; e
- Zelar para que a Diretoria de Riscos e Controles Internos possua recursos, ferramentas adequadas para identificar, analisar, avaliar e tratar os riscos de negócio.

## **7.2. Comitê de Auditoria Estatutário (CAE)**

- Avaliar a política, conceitos e metodologias adotados no processo de Gestão de Riscos;
- Acompanhar de forma sistemática a gestão dos riscos e o cumprimento dos seus objetivos;
- Supervisionar as iniciativas da Diretoria de Riscos e Controles Internos;
- Avaliar a efetividade e a suficiência dos sistemas de controles e de gestão dos riscos de negócios;
- Assegurar-se de que a Companhia desenvolva o processo de Gestão de Riscos conforme previsto nesta Política e em demais normativos correlatos e melhores práticas de mercado;
- Apoiar a Diretoria na avaliação, discussão e revisão da classificação dos riscos, sua criticidade e respectivos planos de mitigação;
- Assessorar o Conselho de Administração na supervisão do processo de Gestão de Riscos da Companhia; e
- Analisar e recomendar a aprovação do apetite e do processo de gestão dos riscos ao Conselho de Administração.

## **7.3. Diretoria**

- Recomendar, ao menos a cada 2 (dois) ciclos de Planejamento Estratégico, ou a partir de eventos significantes, o Apetite aos Riscos para revisão do Comitê de Auditoria e aprovação do Conselho de Administração;
- Reportar ao Conselho de Administração e ao Comitê de Auditoria os riscos envolvidos na implementação da estratégia da Companhia a cada ciclo de Planejamento Estratégico ou a partir da ocorrência de eventos significantes;
- Avaliar a assertividade dos processos de gestão de riscos e de controles internos por meio dos reportes periódicos, discutindo e validando, no colegiado ou por vice-presidência, as avaliações apresentadas pelos donos dos riscos e definindo o posicionamento frente aos riscos, de acordo com o apetite aprovado pelo Conselho de Administração;
- Patrocinar e garantir a implantação da gestão de riscos em todas as áreas de negócio;
- Validar a definição e acompanhamento das ações mitigatórias para redução da exposição ao risco, assim como definir o responsável e o prazo para implantação dessas ações;
- Definir diretrizes, recursos e metas que garantam o bom funcionamento da gestão de riscos;
- Aprovar a matriz de riscos de negócio e definir os respectivos donos dos riscos;
- Supervisionar se as lideranças da Companhia estão respondendo aos riscos conforme ações de mitigação definidas;
- Avaliar as deficiências reportadas pelas auditorias interna e externa, de acordo com o grau de criticidade, tomando as ações necessárias para suas mitigações;
- Aprovar a Política de Gestão de Riscos da Companhia, o Regimento Interno da Comissão de Riscos e normas específicas acerca dos processos de gestão de riscos e controles internos; e
- Informar à área de Riscos e Controles Internos sobre a identificação de novos riscos ou eventos que sejam relevantes, e suas respectivas evoluções.

#### **7.4. Comissão de Riscos**

- Avaliar e validar a matriz de riscos da Companhia, bem como a estratégia de resposta e priorização dos riscos;
- Discutir e acompanhar o nível de exposição dos principais riscos e respectivas ações de mitigação;
- Validar as informações dos riscos e sugerir alterações, sempre que necessário; e
- Atuar de forma ativa na gestão e monitoramento dos riscos frente ao apetite instituído pelo Conselho.

#### **7.5. Gerência de Gestão de Riscos de Negócio**

Responsável por coordenar o processo de Gestão de Riscos da Companhia e garantir o correto fluxo de informações e reporte, exercendo as seguintes responsabilidades:

- Executar o processo de gestão de riscos, conforme aprovado pelo Conselho de Administração, bem como atender as recomendações e determinações do Comitê de Auditoria Estatutário, Comissão de Riscos e/ou da Diretoria;
- Convocar e coordenar semestralmente as reuniões da Comissão de Riscos;
- Propor o Regimento Interno da Comissão de Riscos e garantir seu cumprimento e atualização;
- Desenvolver, aplicar e disseminar a estratégia, a metodologia e a cultura de gestão de riscos, em conformidade com regulamentações vigentes e melhores práticas do mercado;
- Implantar as ferramentas para a gestão de riscos na Companhia, bem como gerir e garantir seu funcionamento;
- Monitorar o status e a implantação das ações de mitigação;
- Apresentar e reportar à Diretoria, à Comissão de Riscos, ao Comitê de Auditoria Estatutário e ao Conselho de Administração a avaliação dos riscos, ações de mitigação e perspectiva de adequação aos respectivos apetites, quando aplicável;
- Assegurar a manutenção e cumprimento da Política de gestão de riscos;
- Assessorar as áreas na identificação, análise, avaliação e definição das ações de mitigação;
- Identificar novos riscos que sejam relevantes e suas respectivas evoluções; e
- Conduzir o processo de revisão e submeter para aprovação da Diretoria e demais Órgãos de Governança sempre que necessário, ou no máximo a cada dois anos, a Política de Gestão de Riscos e o Apetite a Riscos (qualitativo e quantitativo).

#### **7.6. Área de Negócio /Dono do Risco**

- Atuar como primeira linha de defesa, na gestão dos riscos inerentes às suas atividades, identificando-os, avaliando-os, tratando-os e monitorando-os, além de garantir a execução correta dos controles e a documentação das evidências necessárias;

- Prover a área de riscos com todas as informações necessárias, de forma íntegra e fidedigna;
- Informar à área de controles internos, de forma tempestiva, a necessidade de atualização dos controles de sua responsabilidade;
- Implementar os planos de mitigação dos riscos e demais planos definidos para remediação das deficiências apontadas pelas auditorias interna e externa;
- Informar a área de Riscos, sobre a identificação de um risco materializado ou potencial, seja de sua área ou de outras que venha a observar, bem como suportar na análise do risco sob as óticas das esferas de probabilidade e impacto e na definição e implementação das ações de mitigação; e
- Quando solicitado, reportar e responder aos órgãos de governança (Diretoria, Comissão de Riscos, Comitê de Auditoria Estatutário, Conselho de Administração etc.) os riscos sobre sua responsabilidade e eventuais deficiências significativas de controles.

## **7.7. Controles Internos**

- Desenvolver e manter a metodologia e as boas práticas para avaliação do ambiente de controles internos dos processos relacionados aos riscos de negócio;
- Estruturar o sistema de gestão e supervisão dos controles internos de forma compatível com as atividades da Companhia, garantindo as segregações e controles necessários para mitigar eventuais conflitos na condução de seus negócios;
- Propor e desafiar as áreas de negócio quanto a melhor aderência da estrutura de controles internos aos objetivos da Companhia, aos normativos internos, a complexidade e a estratégia de resposta aos riscos de negócio;
- Avaliar continuamente os riscos dos processos e o ambiente de controles;
- Apoiar as áreas de negócio na elaboração de planos de ação necessários para a implementação do adequado ambiente de controles internos;
- Reportar os resultados obtidos na avaliação do ambiente de controles internos aos donos dos processos, à Diretoria e ao Comitê de Auditoria Estatutário e demais fóruns, quando aplicável;
- Disseminar a cultura sobre a importância da manutenção e preservação do ambiente de controles internos e a responsabilidade das áreas de primeira linha de atuação; e
- Identificar, a partir da matriz de riscos, os processos de negócio que necessitam de revisão ou reestruturação dos controles interno, bem como eventuais necessidades de atualização a partir dos planos de mitigação efetivamente implementados.

## **7.8. Auditoria Interna**

- Desenvolver, de forma coordenada com o Conselho de Administração e Comitê de Auditoria, Plano Plurianual de Trabalho, de forma a executar de forma sistemática, revisões da efetividade dos controles internos mantidos pela Companhia;

- Fornecer opiniões independentes ao Conselho de Administração, por meio do Comitê de Auditoria Estatutário, sobre o processo de gestão de riscos, a efetividade dos controles internos e a governança corporativa, recomendando ações de melhorias, quando aplicáveis; e
- Verificar a conformidade do processo de Gestão de Riscos com as políticas e normas adotadas pela Companhia.

## **7.9. Compliance - Ética e Integridade**

- Conduzir Compliance Risk Assessment de forma periódica, visando suportar a Companhia na identificação, avaliação, tratamento e reporte dos principais riscos de Ética e Integridade aos quais a Companhia está exposta;
- Mobilizar demais áreas da Companhia para o endereçamento das ações de mitigação dos riscos de Ética e Integridade identificados, por meio de sugestão de medidas para mitigação de riscos levantados, bem como promover o desenvolvimento de comunicações e treinamentos internos sobre ética e integridade corporativa;
- Prover à Diretoria de Riscos e Controles Internos informações, dados e recomendações para atualização do mapa de riscos de negócio da Companhia, a partir do Compliance Risk Assessment;
- Conduzir as atividades de *Due Diligence* de Ética e Integridade Terceiros, com base nas diretrizes da Norma Gerencial de *Due Diligence* de Terceiros da Companhia;
- Estruturar e definir diretrizes, com o suporte de demais áreas da Companhia, no que tange à gestão dos riscos de ética e integridade apontados através dos procedimentos de identificação de riscos do departamento; e
- Gerenciar o canal de denúncias Linha Ética, recebendo e endereçando os relatos recebidos, assim como conduzir as investigações internas, recomendar medidas disciplinares ou de remediação para deliberação na comissão de Conduta da Companhia. Acompanhar a aplicação de tais medidas e garantir que os desvios sejam reportados internamente para aprimoramento do programa de ética e integridade e sugerir medidas para mitigação dos riscos apurados em decorrência dos relatos advindos da Linha Ética.

## **8.DISPOSIÇÕES GERAIS**

### **8.1. Alteração**

Esta Política poderá ser alterada sempre que necessário, por deliberação do Conselho de Administração ou por proposta da Diretoria de Riscos e Controles Internos.

### **8.2. Conflito**

No caso de conflito entre as disposições desta Política e do Estatuto da Companhia, prevalecerá o disposto no Estatuto. No caso de conflito entre as disposições desta Política e da legislação ou regulamentação vigentes, prevalecerá o disposto na legislação ou regulamentação, conforme aplicável.

### **8.3. Autonomia das disposições**

Caso qualquer disposição desta Política venha a ser considerada inválida, ilegal ou ineficaz, essa disposição será limitada, na medida do possível, para que a validade, legalidade e eficácia das disposições remanescentes não sejam afetadas ou prejudicadas.

### **8.4. Vigência e Divulgação**

A presente Política de Gestão de Riscos entrará em vigor na data de sua aprovação pelo Conselho de Administração e permanecerá em vigor pelo prazo indeterminado, devendo ser revisada, pelo menos, a cada dois anos, ou até que haja deliberação em sentido contrário. Esta Política será divulgada na forma prevista na legislação e regulamentação aplicáveis.\*\*\*