Emissor:	Diretoria de Gestão de Riscos e Controles Internos	**Emissão em:**	29/04/26
Aprovador:	Conselho de Administração da Tupy S.A.	**Revisão até:**	28/04/31

1. Objetivo

Estabelecer princípios, diretrizes e responsabilidades para a gestão de riscos na Tupy S.A. (ou "Companhia"), a fim de orientar os processos de identificação, avaliação, tratamento, monitoramento e comunicação dos riscos relacionados à Companhia.

2. Abrangência

Esta Política aplica-se à Tupy S.A. e às sociedades controladas pela Companhia, nas quais detenha, direta ou indiretamente, participação societária majoritária, no Brasil ou no exterior. Deve ser implementada nas sociedades controladas, observando-se a legislação e regulamentação aplicáveis, bem como seus respectivos documentos constitutivos. A adoção desta Política é recomendada nas demais sociedades nas quais a Tupy S.A. possua participação societária relevante, no Brasil e nos demais países.

3. Definições

Os termos e definições, para fins desta Política, encontram-se descritos no item 10 – Anexo I que é parte integrante deste documento. Para facilitar a compreensão, os termos foram definidos nas seguintes subseções: 10.1 Sobre Riscos, 10.2 Sobre a Mitigação de Riscos, 10.3 Sobre as Partes Relacionadas à Gestão de Riscos e 10. 4 Sobre os Verbos Utilizados na Gestão de Riscos.

4. Diretrizes

4.1. Introdução

A gestão de riscos corporativos é um processo conduzido pela área de Gestão de Riscos e Controles Internos em conjunto com o Comitê Executivo, com o devido acompanhamento do Comitê de Auditoria e Riscos Estatutário. É um processo que faz parte da governança da Companhia e estabelece as diretrizes e metodologia para a identificação, avaliação, tratamento, monitoramento e comunicação dos riscos. Deve ser utilizado como fonte de informação relevante para tomada de decisão estratégica e definição dos objetivos estratégicos, além de estar presente nos ciclos de gestão da Companhia.

A gestão de riscos da Tupy S.A. adota o "Modelo de Três Linhas", recomendado pelo IIA (The Institute of Internal Auditors), conforme descrito abaixo:

4.1.1. 1ª Linha: é composta pelas áreas de negócio da Companhia, responsáveis pela gestão dos riscos sob sua alçada, bem como pela implementação das ações mitigatórias e pela execução eficaz dos controles internos associados aos seus processos.

4.1.2. 2ª. Linha: é composta pelas estruturas de Gestão de Riscos, Controles Internos e Compliance da Companhia, que devem instrumentalizar os gestores da primeira linha para o correto gerenciamento de riscos através da definição de políticas, metodologias, desenvolvimento de treinamentos e orientação, além do reporte das informações aos órgãos de governança competentes.

4.1.3. 3ª. Linha: é composta pela Auditoria Interna da Companhia, que age com um olhar independente para verificar a eficácia e conformidade da atuação das duas primeiras linhas, e reportar suas recomendações aos órgãos de governança competentes, podendo ainda atuar de forma consultiva na construção dos controles internos.

4.2. Processo de Gestão de Riscos

A TUPY S.A. reconhece que gerenciar riscos de maneira eficaz é fundamental para atingir os objetivos de negócios. Cada Negócio ou Função deverá analisar seu ambiente, definir objetivos claros e:

- Identificar os riscos que impactem o alcance desses objetivos;
- Avaliar o impacto e a probabilidade da materialização dos riscos;
- Implementar ações eficazes desenvolvidas para mitigar os riscos identificados;
- Monitorar, comunicar e reportar mudanças no ambiente de riscos;
- Reportar, em base contínua, a eficácia das ações tomadas para gerenciar os riscos identificados.

4.2.1. Tipologia dos Riscos

A Gestão de Riscos da Tupy S.A utiliza as seguintes classes de riscos em seu processo de mapeamento:

- **Riscos Estratégicos**: associados à tomada de decisões estratégicas, falhas na execução da estratégia adotada ou mudanças no ambiente externo que podem impactar o valor econômico e a perpetuidade da Companhia, manter sua vantagem competitiva e atingir seus objetivos de longo prazo;
- **Riscos Financeiros e/ou de Mercado**: associados às variações adversas em fatores que afetam a posição financeira da Companhia, como liquidez, fluxo de caixa, taxas de juros, câmbio, crédito, preços de ativos, estrutura de capital ou capacidade de cumprir obrigações financeiras, entre outros;
- **Riscos Operacionais**: associados à possibilidade de ocorrência de perdas (de produção, ativos, clientes, receitas) decorrentes de falhas, deficiências ou inadequação de processos internos envolvendo pessoas e tecnologia ou de eventos externos inesperados (ex.: catástrofes naturais);
- **Riscos Regulatórios, Legais ou de Conformidade**: associados ao descumprimento de leis, regulamentos, normas internas, padrões éticos ou obrigações contratuais. Incluem ainda riscos relacionados a mudanças regulatórias, interpretações equivocadas de requisitos legais ou falhas em processos de conformidade;
- **Riscos Socioambientais**: associados a danos ambientais ou a efeitos adversos sobre comunidades, trabalhadores ou demais partes interessadas, resultantes das atividades, operações, projetos ou relações comerciais da Companhia.

4.2.2. Etapas do processo de Gestão de Riscos

A metodologia adotada pela TUPY S.A., utiliza como referência a estrutura integrada de gestão de riscos sugerida pelo COSO, devidamente ajustada para as realidades da Tupy. Além disso, as etapas do processo de gestão de riscos da Companhia, seguem os preceitos estabelecidos pela ISO 31000:2018, conforme figura 1 abaixo:

Figura 1 - Processo de Gerenciamento de Riscos
Fonte: ISO 31000:2018

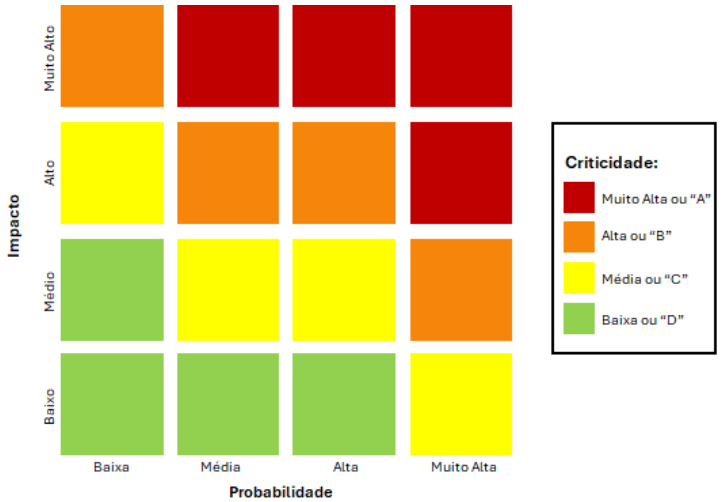
4.2.2.1. ESCOPO CONTEXTO E CRITÉRIO: A identificação dos riscos terá maior valor quando diretamente vinculada aos objetivos estratégicos. Na primeira etapa do processo de gestão de riscos, são capturados o entendimento dos objetivos estratégicos de cada negócio, levando-se em consideração os contextos interno e externo em que a Companhia está inserida. Também é necessário organizar os critérios que permitam descrever, medir e comparar riscos de forma consistente. Esses critérios ajudam a determinar o que é aceitável ou preocupante, orientando a tomada de decisões, priorização de ações e comunicação. Devem ser personalizados ao contexto da Tupy, considerando objetivos, tolerância, capacidade e requisitos regulatórios.

4.2.2.2. IDENTIFICAÇÃO DOS RISCOS: A identificação dos riscos, incluindo riscos emergentes, envolverá diferentes abordagens. O processo de identificação envolverá reuniões ou workshops dedicados a riscos em cada negócio ou poderá ocorrer, também, por meio da materialização de um evento significativo com possibilidade de novas ocorrências**.** Nesta etapa, deve-se criar uma relação e a descrição de riscos, e dos seus respectivos fatores, que possam desviar a Companhia do atingimento de seus objetivos estratégicos. Os riscos identificados (e seus respectivos fatores ficam registrados no Inventário de Riscos).

4.2.2.3. ANÁLISE DE RISCOS: Na etapa de análise de riscos, deve-se levar em consideração o impacto e probabilidade de materialização do risco, assim como de seus respectivos fatores:

- Impacto: a análise do impacto não deve levar em consideração apenas as consequências imediatas da materialização de um risco, mas também seus efeitos indiretos. Nem todos os riscos poderão ser quantificados em termos financeiros, e, para alguns riscos, critérios qualitativos serão mais adequados para a avaliação. Critérios qualitativos podem incluir, entre outros, ambientais, sociais, de conformidade, de saúde e segurança, de imagem institucional, de qualidade do produto ou de tecnologia, na forma definida na Régua de Impacto.
- Probabilidade: A avaliação da probabilidade deve levar em consideração o histórico de materialização do risco, os controles existentes que endereçam o tema, a existência e efetividade de ações mitigatórias e a opinião técnica dos especialistas sobre o tema, incluindo os donos do risco. Também deve contar com um juízo profissional estruturado, sensível às fragilidades não observáveis e às incertezas inerentes ao ambiente de negócio.

4.2.2.4. AVALIAÇÃO DE RISCOS: Nesta etapa, comparamos o nível de risco calculado durante a etapa de análise, levando-se em consideração os critérios estabelecidos na primeira etapa. Durante a avaliação, cada risco e seus fatores são classificados na Matriz de Riscos da Companhia, conforme seu grau de criticidade. Essa classificação considera o vetor formado pelas notas de probabilidade e impacto, resultando em quatro níveis, em ordem decrescente: Muito Alta ou "A" (maior criticidade para o negócio), Alta ou "B", Média ou "C" e Baixa ou "D" (menor criticidade para o negócio), conforme figura abaixo:



A matriz de riscos torna-se, portanto, uma ferramenta estratégica de priorização, permitindo direcionar esforços para a mitigação dos riscos mais relevantes, conforme os níveis de Apetite e Tolerância formalizados na Declaração de Apetite e Tolerância a Riscos da Companhia.

Um risco avaliado antes do efeito de qualquer ação mitigatória ou controle associado é chamado de Risco Inerente. Após a implementação de contramedidas parciais, obtém-se o Risco Residual Atual. Considera-se como Risco Residual Projetado aquele resultante da implementação de todas as ações mitigatórias que a Companhia estiver apta a fazer.

Em casos em que áreas de negócio específicas venham a ter papel de gerenciamento de riscos em nível tático ou operacional, é mandatório o alinhamento à metodologia e diretrizes estabelecidas por esta Política. Exceções deverão ser apresentadas e aprovadas pela área de GRCI.

4.2.2.5. TRATAMENTO DE RISCOS: A avaliação de riscos é fundamental para a distribuição eficiente de recursos e a priorização de ações, pois oferece um panorama abrangente dos riscos significativos no contexto dos objetivos estratégicos da Companhia. Nesta etapa de tratamento de riscos, é essencial definir e implementar ações mitigatórias e/ou controles internos que respondam adequadamente a cada risco ou fator de risco identificado. É importante reforçar que a decisão sobre o tratamento de cada risco deve considerar sua avaliação em relação ao apetite de risco da Companhia. As estratégias de tratamento podem incluir:

- **Mitigar:** Reduzir a probabilidade ou impacto do risco por meio de controles internos ou ações mitigatórias.
- **Transferir:** Compartilhar ou transferir o risco para terceiros, como por meio de seguros ou outras parcerias.
- **Aceitar:** Assumir o risco quando ele estiver dentro do apetite definido pela Companhia ou quando o custo de mitigação for superior ao benefício.
- **Evitar:** Eliminar a atividade ou situação que gera o risco.

Os riscos serão tratados, de acordo com o seu nível de criticidade, conforme segue:

- **Riscos "A":** Riscos prioritários que demandam ação imediata para eliminação, transferência ou mitigação de seus fatores de origem com a elaboração de planos de ação e/ou implementação de controles internos capazes de reduzir sua criticidade. Esses riscos devem ser monitorados de forma contínua e reportados, com prioridade, às instâncias competentes de Companhia**.**
- **Riscos "B":** Riscos de criticidade alta que exigem atenção especial e demandam ações de curto prazo, para a eliminação, transferência ou mitigação de seus fatores de origem por meio da elaboração de planos de ação e/ou implementação de controles internos. Além disso, requerem o acompanhamento e reporte periódico pelos responsáveis e pelas áreas de governança.
- **Riscos "C":** Riscos de criticidade média que estão sujeitos à implementação de ações e controles internos proporcionais ao seu nível de exposição. Exigem monitoramento regular pelos seus responsáveis e a adoção de controles e indicadores consistentes, que assegurem que a exposição permaneça estável e não evolua para níveis mais elevados de criticidade.
- **Riscos "D":** Riscos de criticidade baixa que requerem a manutenção de controles internos proporcionais à sua relevância ou aos limites de tolerância definidos pela Companhia. Demandam monitoramento pelos seus responsáveis e a adoção de controles e indicadores consistentes, que assegurem que a exposição permaneça estável.

4.2.2.6. REGISTRO E RELATO: Os donos de riscos devem, periodicamente, analisar e reportar seus riscos, usando a Matriz de Riscos padrão estabelecida por esta Política, assim como eventuais materializações e suas reais consequências para a Companhia. As lições aprendidas devem ser registradas a fim de manter a melhoria contínua dos processos envolvidos e mitigar as consequências de uma nova materialização. Em casos significativos, deve-se envolver na discussão do registro do risco o Comitê Executivo e/ou o Comitê de Auditoria e Riscos Estatutário.

4.2.2.7. MONITORAMENTO E ANÁLISE CRÍTICA: Mudanças nos contextos interno e externo do negócio e as decisões tomadas no curso da implementação da estratégia alteram continuamente o perfil dos riscos de uma empresa. É essencial que essas mudanças sejam identificadas de forma tempestiva,

permitindo o mapeamento de novos riscos ou a atualização daqueles já existentes sempre que necessário e, principalmente, nos processos decisórios materiais da Companhia, conforme item 4.3.3 abaixo. Esse processo deve garantir a adequação da Matriz de Riscos da empresa, em conjunto com os órgãos de governança competentes.

4.2.2.8. COMUNICAÇÃO E CONSULTA: É necessária a comunicação, de forma ágil e contínua, com as diferentes Partes Interessadas sobre os riscos do negócio, a fim de manter alinhados o processo de gestão de riscos e a implementação da estratégia da Companhia. Desta forma, pode-se identificar informações relevantes que permitam a melhoria contínua das informações sobre os riscos identificados. Recomenda-se a adoção de uma comunicação transparente e consistente sobre os riscos, assegurando que as decisões estratégicas sejam tomadas com pleno entendimento e ponderação das ameaças e oportunidades envolvidas, bem como das medidas definidas para seu gerenciamento.

4.3. Governança de Gestão de Riscos

4.3.1. Reportes Formais do Ciclo de Monitoramento de Riscos

Os reportes periódicos devem ser realizados de forma integrada, consolidada e tempestiva, contemplando o Comitê Executivo, o Comitê de Auditoria e Riscos Estatutário e o Conselho de Administração, em conformidade com as diretrizes abaixo estabelecidas. Cabe notar que todas as matérias submetidas ao Comitê de Auditoria e Riscos Estatutário e ao Conselho de Administração devem, obrigatoriamente, ser previamente apresentadas e discutidas no Comitê Executivo.

4.3.1.1. Comitê de Auditoria e Riscos Estatutário

Periodicidade	Conteúdos a Reportar:
Anual	1) Relatório Anual de GRCI 2) Plano Anual de GRCI 3) Atualização da DAR e das Réguas de Impacto e Probabilidade
Semestral	1) Avaliação de Riscos Emergentes
Trimestral	1) Reavaliação do inventário de riscos da companhia, incluindo: • Evolução dos riscos críticos • Situação dos planos de mitigação • Mudanças no perfil de risco e eventos relevantes 2) Informações sobre controles internos e status de implementação
Extraordinário	1) Escalonamento imediato de riscos críticos novos ou alterações súbitas na exposição 2) Análise de Risco em Projetos Específicos

4.3.1.2. Conselho de Administração

Periodicidade	Conteúdos a Reportar:
Anual	1) Relatório Anual de GRCI 2) Plano Anual de GRCI 3) Atualização da DAR e das Réguas de Impacto e Probabilidade
Semestral	1) Avaliação de Riscos Emergentes 1) Reavaliação do inventário de riscos da companhia • Evolução dos riscos críticos • Situação dos planos de mitigação • Mudanças no perfil de risco e eventos relevantes 2) Informações sobre controles internos e status de implementação
Extraordinário	1) Escalonamento imediato de riscos críticos novos ou alterações súbitas na exposição 2) Análise de Risco em Projetos Específicos

4.3.2. Governança para Riscos Emergentes

A identificação e atualização dos Riscos Emergentes devem ser conduzidas de forma contínua, integradas ao processo corporativo de Gestão de Riscos, considerando sinais, tendências, inovações, eventos externos relevantes e fatores internos que possam alterar o perfil de risco da Companhia.

4.3.2.1. Priorização dos Riscos Emergentes: Os Riscos Emergentes identificados devem ser avaliados e priorizados com base, no mínimo, nos seguintes critérios corporativos:

- **Magnitude Potencial:** Avaliação multidimensional do impacto, conforme régua corporativa;
- **Velocidade:** Tempo estimado para o risco afetar a Companhia, considerando a rapidez de evolução;
- **Horizonte Temporal:** Classificação em curto (≤ 12 meses), médio (1–3 anos) e longo prazo (> 3 anos);
- **Incerteza/Confiança:** Grau de evidência disponível, desde hipóteses com baixa confiabilidade até sinais fortes e consistentes;
- **Pervasividade:** Amplitude do efeito, considerando o número de plantas, mercados, regiões ou unidades impactadas;
- **Preparação Atual:** Avaliação das lacunas de controles, respostas, planos de ação ou capacidade organizacional frente ao risco identificado.

4.3.2.2. Responsabilidades e Escalonamento: A área de GRCI é responsável por coordenar o processo corporativo de monitoramento e análise de Riscos Emergentes, garantindo sua integração aos processos de reporte e tomada de decisão. Riscos considerados prioritários devem ser escalonados às instâncias competentes, incluindo Comitê Executivo, Comitê de Auditoria e Riscos Estatutário e Conselho de Administração, quando aplicável.

4.3.2.3. Atualização e Revisão Periódica: Os Riscos Emergentes devem ser revisados no mínimo anualmente, ou sempre que eventos externos ou internos alterarem de forma material seu potencial de impacto, velocidade, probabilidade ou pervasividade**.**

4.3.3. Inclusão de Análise de Riscos nos Processos Decisórios da Companhia

A análise de risco é obrigatória em todos os Processos Decisórios materiais, isto é, aqueles que excedam o Apetite ao Risco da Companhia, conforme registrado na DAR, ou que resultem em impacto classificado como Alto ou Muito Alto, de acordo com as réguas (quantitativa e qualitativa) de avaliação de impacto estabelecidas. Essa obrigatoriedade aplica-se a decisões com potencial impacto Financeiro, Estratégico, Operacional, Regulatório ou Socioambiental, entre outros.

5. Divulgação e Treinamento

5.1. Esta Política será arquivada e publicada nos repositórios oficiais da Companhia em atendimento aos públicos interno e externo.

5.2. Cabe à área de Gestão de Riscos e Controles Internos (GRCI) promover ações necessárias para disseminação e treinamento desta Política.

6. Papeis e Responsabilidades

6.1. Conselho de Administração (CA):

- Revisar e aprovar as diretrizes gerais da estratégia de gestão de riscos da Tupy S.A., incluindo esta Política e sua implementação (metodologia, processos, sistemas, e mecanismos de reporte);
- Revisar e aprovar no mínimo anualmente as Réguas de Impacto e de Probabilidade;
- Assegurar que os processos decisórios materiais que lhe forem submetidos para deliberação incorporem, de forma consistente, uma análise de riscos documentada e aderente à metodologia de gestão de riscos da Companhia.
- Validar anualmente a atualização do Mapa Integrado de Riscos e dos Temas de Riscos Prioritários, bem como as ações de mitigação decorrentes da estratégia de resposta a riscos da Companhia;
- Deliberar sobre o Apetite e Tolerância a Riscos da Tupy S.A. e aprovar a respectiva Declaração de Apetite a Riscos, revisando-as no mínimo, anualmente;
- Supervisionar o processo de gestão de riscos, assegurando que os mecanismos e recursos adotados suportem o alcance dos objetivos estratégicos da Companhia.

6.2. Comitê de Auditoria e Riscos Estatutário (CAE):

- Assessorar o Conselho de Administração no desempenho de sua atuação no tocante à Gestão de Riscos da Tupy S.A., nos termos desta Política;
- Supervisionar a adequação dos processos de gestão de riscos, assegurando a atualização do Mapa Integrado de Riscos e dos Temas de Riscos Prioritários, bem como a efetividade das ações de mitigação e dos controles previstos na estratégia de resposta a riscos da Companhia;
- Analisar e recomendar a aprovação do Apetite e Tolerância ao Risco e da respectiva Declaração de Apetite a Riscos;
- Avaliar e monitorar as exposições de Risco da Tupy S.A.;
- Recomendar a aprovação da presente Política e suas eventuais alterações.

6.3. Comitê Executivo

- Avaliar e propor ao Conselho de Administração a presente Política e suas alterações;
- Assegurar que os processos decisórios materiais a serem aprovados incorporem, de forma consistente, uma análise de riscos documentada e aderente à metodologia de gestão de riscos da Companhia.
- Garantir a aplicação desta Política em toda a Companhia, incorporando as práticas de gestão de riscos e controles internos ao planejamento estratégico e ao processo decisório;
- Monitorar a adequação dos processos de gestão de riscos, avaliando a atualização do Mapa Integrado de Riscos e dos Temas de Riscos Prioritários;
- Aprovar a governança estabelecida pela área de GRCI para acompanhar a efetividade das ações mitigatórias e dos controles internos;
- Propor o Apetite e Tolerância a Riscos ao Conselho de Administração e recomendar sua revisão sempre que houver alteração de cenário relevante;
- Promover a cultura de gerenciamento de Riscos na organização e o fortalecimento das 1ª e 2ª Linhas da Companhia, assegurando os mecanismos e recursos necessários ao processo;
- Comunicar à área de GRCI sobre a identificação de novos riscos ou informações relevantes em relação aos riscos já existentes, garantindo atualização e alinhamento contínuo;
- Aprovar o Regimento Interno do Comitê de Riscos e Controles Internos;
- Aprovar o Plano Anual da área de GRCI;
- Avaliar o Relatório Anual de GRCI;
- Indicar a necessidade de avaliações independentes do processo de gerenciamento de riscos e controles internos (agentes internos ou externos), de modo a assegurar sua eficácia.

6.4. Comitê de Gestão de Riscos e Controles Internos

- Apoiar o Comitê Executivo da Tupy S.A. no acompanhamento do Mapa Integrado de Riscos, bem como emitir recomendações preventivas referentes aos potenciais riscos pautados em suas reuniões;
- Emitir recomendações visando a melhoria contínua da estratégia e do processo de Gestão de Riscos da Companhia;
- Monitorar a exposição aos riscos e avaliar a eficácia das ações mitigatórias e dos controles internos;
- Acompanhar indicadores e relatórios sobre riscos corporativos;
- Executar as demais atribuições referentes à gestão de Riscos previstas no seu Regimento Interno.

6.5. Vice-Presidência Executiva de Finanças e Administração

- Elaborar e aprovar junto às instâncias pertinentes políticas e outros documentos normativos para a devida gestão de riscos financeiros e de mercado, sempre em linha com as diretrizes desta Política;
- Integrar o Comitê de Gestão de Riscos e Controles Internos (CGRCI) contribuindo para a avaliação de riscos que possam ter impactos financeiros para a companhia;
- Suportar a área de GRCI através de recursos, sistemas e processos assegurando a devida implementação desta Política e disseminação da cultura de gestão de riscos na companhia.

6.6. Gestão de Riscos e Controles Internos -GRCI (2ª Linha)

- Elaborar e propor ao Comitê Executivo esta Política e suas alterações, para posterior encaminhamento ao Comitê de Auditoria e Riscos Estatutário;

- Desenvolver e apoiar na implementação das políticas, metodologias, processos e ferramentas para o gerenciamento de riscos;
- Elaborar, em conjunto com as Áreas de Negócio (1ª linha), a análise de riscos documentada e aderente à metodologia de gestão de riscos da Companhia, para os processos decisórios materiais que serão submetidos ao Comitê Executivo e ao Conselho de Administração.
- Coordenar o processo corporativo de monitoramento e análise dos Riscos Emergentes, assegurando sua integração aos processos de reporte e tomada de decisão;
- Coordenar o processo de gestão de riscos, assegurando a atualização do Mapa Integrado de Riscos e dos Temas de Riscos Prioritários;
- Estabelecer a governança para acompanhar a efetividade das ações mitigatórias e dos controles internos, com definição clara de donos de riscos, controles e processos, além de regras objetivas para prazos de implementação e critérios de postergação;
- Elaborar a definição de Apetite e Tolerância a Riscos da Companhia e propor ao Comitê Executivo a Declaração de Apetite a Riscos, para posterior encaminhamento ao Comitê de Auditoria e Riscos Estatutário;
- Monitorar os níveis de exposição potencial dos principais riscos identificados, reportando-os periodicamente ao Comitê Executivo e ao Comitê de Auditoria e Riscos Estatutário;
- Apoiar a 1ª Linha na identificação, avaliação, monitoramento e reporte dos seus respectivos riscos;
- Auxiliar a 1ª Linha no desenho e implementação de ações mitigatórias, controles internos ou indicadores de risco para o devido gerenciamento de suas exposições;
- Elaborar, anualmente, o plano de trabalho para o gerenciamento de riscos, submetendo-o à aprovação do Comitê Executivo e reportando-o ao Comitê de Auditoria e Riscos Estatutário;
- Disseminar a cultura de gerenciamento de riscos na Companhia por meio de treinamentos e iniciativas estruturadas de comunicação interna voltadas à conscientização e alinhamento;
- Atender às recomendações do Comitê de Auditoria e Riscos Estatutário e do Comitê Executivo referentes aos riscos identificados e ao processo de gestão de riscos.

6.7. Áreas de Negócio (1ª Linha)

- Identificar, avaliar, monitorar e reportar os seus respectivos riscos seguindo as diretrizes desta Política e aplicando a metodologia de Gestão de Riscos da Companhia;
- Definir, implementar e executar as ações mitigatórias, controles internos e indicadores de risco para o devido gerenciamento de suas exposições;
- Elaborar, em conjunto com a área de GRCI, a análise de riscos documentada e aderente à metodologia de gestão de riscos da Companhia, para os processos decisórios materiais que serão submetidos ao Comitê Executivo e ao Conselho de Administração.
- Informar tempestivamente a área de GRCI sobre riscos, potenciais ou materializados, bem como sobre mudanças significativas no contexto interno ou externo do negócio que possam alterar a avaliação e exigir adequações no tratamento dos riscos;
- Certificar (*sign-off*), anualmente ou sob demanda, que os riscos relacionados aos processos sob sua responsabilidade estão devidamente identificados, avaliados e registrados no sistema de gestão de riscos;
- Responder aos órgãos de governança, quando solicitado, o status dos riscos sob sua responsabilidade.

6.8. Auditoria Interna (3ª Linha)

- Realizar avaliações independentes para assegurar a efetividade dos processos de gerenciamento de riscos da Companhia, à luz da presente Política;
- Avaliar, por meio de testes independentes, a efetividade dos controles implementados para mitigação de riscos (ToE);
- Reportar os resultados das avaliações de controle interno e o acompanhamento das correções das deficiências de controles internos;
- Incorporar a Matriz de Riscos na elaboração do Plano de Auditoria Interna, garantindo alinhamento aos riscos do negócio.

6.9. Governança Corporativa

- Assegurar que os processos decisórios materiais a serem deliberados pelo Conselho de Administração e pelos Comitês de Assessoramento estejam instruídos por análise de riscos documentada e aderente à metodologia de gestão de riscos da Companhia.

7. Documentos de Referência

7.1. Estatuto Social da Tupy S.A.
7.2. Norma ABNT NBR ISO 31000:2018;
7.3. COSO ERM – Enterprise Risk Management: Integrating with Strategy and Performance (2017)
7.4. Modelo das Três Linhas do IIA (The Institute of Internal Auditors);

8. Histórico de Revisões

8.1. Histórico

Versão	Data	Principais Alterações
003	06/22	Inclusão dos conceitos de 3 linhas de defesa e de Apetite a Riscos, além de outros ajustes em papeis e responsabilidades.
004	03/26	Revisão completa da Política: estrutura de tópicos, definições, conteúdo técnico, papeis e responsabilidades.

9. Aprovações

Área	Atribuição
Gestão de Riscos e Controles Internos	Elaboração
Compliance	Revisão
Jurídico	Revisão
Governança Corporativa	Revisão
Vice-Presidência Executiva de Finanças	Revisão
Comitê Executivo	Revisão
Comitê de Auditoria e Riscos Estatutário	Revisão
Conselho de Administração	Aprovação

10. Anexo I - Termos e Definições usados na Gestão de Risco da Tupy S.A.

Os termos abaixo listados, para fins desta Política, terão os significados atribuídos a seguir:

10.1. Sobre Riscos:

10.1.1. Risco: É a possibilidade de ocorrência de um evento que possa impactar negativamente (ou positivamente) os objetivos da organização. Em outras palavras, risco é a combinação da probabilidade de um evento acontecer e o impacto que ele pode causar;

10.1.2. Fator de Risco: É um elemento ou condição que aumenta a probabilidade de ocorrência de um risco. Pode ser interno (como falhas de processo, falta de controles) ou externo (como mudanças regulatórias, crises econômicas). Um mesmo risco pode conter um ou mais fatores relacionados.

10.1.3. Evento de Risco: É a materialização do risco, ou seja, quando o evento que estava apenas como possibilidade realmente ocorre.

10.1.4. Consequência de Risco: É o resultado ou impacto gerado pela materialização de um risco, ou seja, os efeitos que o evento de risco causa nos objetivos da organização.

10.1.5. Criticidade do Risco: Classificação do risco de acordo com suas avaliações de impacto e probabilidade.

10.1.6. Impacto: É a magnitude das consequências que um evento adverso pode gerar sobre os objetivos da organização, caso ocorra. Pode ser mensurado de forma qualitativa ou quantitativa.

10.1.7. Probabilidade: É a chance ou a frequência estimada de ocorrência de um evento de risco dentro de um determinado período ou contexto. É normalmente expressa em termos qualitativos ou quantitativos e utilizada junto com o impacto para determinar o nível do risco.

10.1.8. Risco Inerente: Risco associado ao negócio antes do efeito de qualquer ação, controle ou contramedida. Trata-se da exposição bruta da organização ao risco.

10.1.9. Risco Residual Atual: Risco remanescente após a implantação de algumas ações mitigatórias e atividades de controle no atual momento de identificação e avaliação do risco.

10.1.10. Risco Residual Projetado: Risco, em sua forma futura, após a implementação total de ações mitigatórias e atividades de controle, dentro dos objetivos da Companhia.

10.1.11. Risco Emergente: risco decorrente de mudanças rápidas, inesperadas ou disruptivas no ambiente econômico, socioambiental, tecnológico, político ou competitivo. Pode apresentar elevado grau de incerteza, baixa evidência inicial e dinâmica acelerada, dificultando sua identificação, avaliação e monitoramento.

10.1.12. Risco Prioritário: É o risco que após sua avaliação recebe a classificação “A”. Um risco prioritário demanda ação imediata para eliminação, transferência ou mitigação de seus fatores de origem com a elaboração de planos de ação e/ou implementação de controles internos capazes de reduzir sua criticidade. Esses riscos devem ser monitorados de forma contínua e reportados, com prioridade, às instâncias competentes de Companhia.

10.1.13. Apetite ao Risco: Nível e tipo de risco que a Companhia está disposta a assumir para atingir seus objetivos estratégicos de curto, médio e longo prazos.

10.1.14. Tolerância ao Risco: é a variação aceitável em torno do limite definido pelo apetite ao risco, expressa por métricas objetivas e mensuráveis. Essas métricas monitoram a margem de desvio de um valor alvo e acionam medidas corretivas para restabelecer o risco dentro do patamar previamente estabelecido.

10.1.15. Capacidade de Risco: Limite máximo de tolerância ao risco, superior ao apetite, que a Companhia pode suportar para atingimento de seus objetivos estratégicos e manter a continuidade dos negócios. Diferente do apetite (que é uma escolha), a capacidade é um limite real imposto pelas condições da empresa.

10.1.16. Declaração de Apetite a Riscos (ou Risk Appetite Statement - RAS): Documento interno e estratégico que estabelece a escala de apetite aos riscos que uma organização está disposta a aceitar para atingir seus objetivos. É usualmente identificado pela sigla “RAS” (abreviatura de sua nomenclatura na língua inglesa).

10.2. Sobre a Mitigação de Riscos:

10.2.1. Gestão de Riscos: Conjunto de atividades coordenadas para a identificação, avaliação, tratamento, monitoramento e comunicação dos riscos do negócio, executadas de acordo com política e metodologia aprovadas.

10.2.2. Resposta ao Risco: Definição da forma de tratamento ao risco.

10.2.3. Tratamento de Riscos: Conjunto de iniciativas destinadas a endereçar os riscos identificados, incluindo, mas não se limitando a: (i) implementação de ações mitigatórias e de contingência, (ii) fortalecimento de controles internos, (iii) execução de projetos específicos, (iv) desenvolvimento ou aquisição de sistemas, (v) elaboração de documentos normativos; (vi) cenarização, simulações e treinamento.

10.2.4. Ações Mitigatórias (plano de ação): uma ação (ou conjunto de ações) endereçada para a redução das exposições ao Risco que deve estar vinculada ao(s) fator(es) de risco que causa(m) as exposições. Deve, ainda, possuir responsáveis por sua implantação, prazo de conclusão e, em seu conjunto, demonstrar capacidade de reduzir a exposição ao risco, evidenciando a redução, até o nível residual projetado.

10.2.5. Controles Internos: conjunto de políticas, procedimentos e práticas implementadas pela Companhia para a redução do seu grau de exposição a riscos, manutenção da conformidade às normas e regulamentações vigentes, bem como garantia da confiabilidade dos relatórios financeiros e gerenciais.

10.2.6. Dono de Risco: Pessoa, tipicamente pertencente à área de negócio (1ª Linha de Atuação), responsável por gerenciar um risco específico, garantindo que ele seja identificado, avaliado, monitorado e tratado de acordo com as diretrizes da organização. O dono do risco deve assegurar que as ações necessárias para mitigação ou resposta sejam implementadas, acompanhar sua evolução e reportar sua situação aos níveis adequados de governança.

10.2.7. Dono de Controle: Pessoa responsável por garantir que um controle interno seja corretamente implementado. Deve assegurar que o controle atenda ao objetivo para o qual foi criado, monitorar sua eficácia, propor melhorias e demonstrar sua tempestiva execução através de evidências documentadas. Eventualmente o Dono de Controle pode acumular as funções de Dono de Risco devendo, nesses casos, assegurar simultaneamente a gestão adequada do risco e a efetividade dos controles a ele associados.

10.2.8. Régua de Impacto: Instrumento multidimensional que estabelece uma escala padronizada para mensurar a severidade (impacto) das consequências de um risco caso ele se materialize.

10.2.9. Régua de Probabilidade: Instrumento que estabelece uma escala padronizada para mensurar a chance de ocorrência de um risco, com critérios objetivos que indicam frequência ou percentual estimado.

10.2.10. Registro de risco: Documento que formaliza e consolida todas as informações relativas ao risco e seus fatores, abrangendo a identificação, avaliação e o respectivo tratamento.

10.2.11. Mapa Integrado de Riscos (ou "Mapa"): Instrumento que contém o conjunto de temas de Riscos que necessitam ser avaliados e monitorados, organizados por categorias, de acordo com a taxonomia estabelecida em documento normativo interno.

10.2.12. Matriz de Riscos: Representação gráfica da avaliação dos graus de criticidade dos riscos da Companhia considerando as análises de impacto e probabilidade.

10.2.13. Inventário de Riscos: conjunto estruturado e atualizado de todos os fatores de riscos identificados pela organização, independentemente de sua categoria, origem ou nível de criticidade. O Inventário de Riscos consolida, em um repositório único, as informações essenciais de cada fator de risco — como descrição, causas, impactos, responsáveis, controles associados, avaliações (inerente e residual), ações de tratamento e status de monitoramento.

10.2.14. Dicionário de Riscos: documento corporativo que padroniza a taxonomia, isto é, a descrição e a classificação dos riscos da organização, definindo de forma consistente seus conceitos, categorias e subcategorias. Seu objetivo é garantir uniformidade na identificação, avaliação, registro e comunicação de riscos, evitando interpretações divergentes entre áreas e fortalecendo a comparabilidade, a rastreabilidade e a qualidade das informações utilizadas no processo de gestão de riscos.

10.2.15. KRI (Key Risk Indicator ou Indicador Chave de Risco): Métrica específica utilizada para monitorar a evolução da exposição a um risco, sinalizando tendências ou mudanças que possam indicar aumento da probabilidade ou do impacto. Funciona como um alerta antecipado, permitindo ações preventivas antes que o risco se materialize.

10.2.16. KPI (Key Performance Indicator ou Indicador Chave de Performance): Métrica quantificável usada para avaliar o desempenho de processos, projetos ou áreas em relação aos objetivos estratégicos da organização. Permitem monitorar resultados, identificar desvios e apoiar a tomada de decisão.

10.3. Sobre as Partes Interessadas na Gestão de Riscos

10.3.1. Conselho de Administração (CA): Órgão formado por membros eleitos pelos acionistas da Companhia, podendo haver conselheiros independentes. Responsável por fixar a orientação geral dos negócios da Companhia, controlar e fiscalizar o seu desempenho.

10.3.2. Comitê de Auditoria e Riscos Estatutário (CAE): Órgão de assessoramento do Conselho de Administração formado por membros do CA e por conselheiros independentes. Dentre as suas diversas responsabilidades estão a de: acompanhar as atividades da auditoria interna e da área de gestão de riscos e controles internos da Companhia; e avaliar e monitorar as exposições de risco da Companhia**.**

10.3.3. Comitê Executivo: Órgão formado por Diretor Presidente e Diretores Vice-presidentes (estatutários ou não). O Comitê Executivo é responsável por executar as medidas necessárias para alcançar os objetivos da empresa previstos no estatuto social.

10.3.4. Gestão de Riscos e Controles Internos (GRCI): Área responsável por garantir que os riscos que possam impactar os objetivos estratégicos da organização sejam identificados, avaliados, monitorados e mitigados. Atua como facilitadora e provedora de diretrizes, metodologias e governança para que as áreas de negócio atuem diretamente na gestão dos seus riscos e na execução eficaz dos controles internos, fortalecendo a cultura de conformidade e gestão de riscos em toda a empresa.

10.3.5. Auditoria Interna: Área responsável por avaliar, conforme seus princípios e diretrizes, a efetividade da gestão de riscos nos processos da Companhia, das ações mitigatórias de risco, dos controles internos e da conformidade às normas e legislações dos mercados em que a Companhia opera.

10.3.6. Comitê de Gestão de Riscos e Controles Internos (CGRCI): órgão interno de assessoramento ao Comitê Executivo com a finalidade de analisar, identificar, propor, monitorar e dar pareceres sobre aspectos que abranjam o sistema de gerenciamento de riscos e controles da Companhia.

10.4. Sobre Verbos utilizados na Gestão de Riscos:

Verbo	Descrição
Aceitar	Assumir o risco conscientemente quando está dentro do apetite ou quando o custo da mitigação não se justifica.
Acompanhar	Verificar a execução e eficácia de planos de ação e controles.
Analisar	Estudar detalhadamente as causas, efeitos e fatores que influenciam um risco.
Avaliar	Julgar a natureza e características do risco, considerando impacto, probabilidade e velocidade.
Classificar	Organizar riscos por categoria, grau de severidade, origem ou impacto.
Comunicar	Compartilhar informações relevantes sobre riscos com públicos internos e externos.
Consolidar	Agrupar informações sobre riscos para visão integrada.
Controlar	Aplicar e manter mecanismos (políticas, processos, sistemas) que limitem o risco.

Escalar	Acionar níveis superiores de governança quando o risco excede limites definidos.
Evitar	Eliminar o risco por meio da descontinuação de atividades, processos ou exposições.
Identificar	Reconhecer, localizar e descrever riscos, causas e eventos que possam impactar objetivos.
Mapear	Representar processos, riscos e controles de forma estruturada.
Mensurar	Quantificar riscos, considerando métricas qualitativas ou quantitativas de impacto/probabilidade.
Mitigar	Desenvolver e implementar ações para reduzir a probabilidade e/ou impacto de riscos.
Monitorar	Acompanhar continuamente o comportamento do risco, controles e indicadores associados.
Planejar	Definir estratégias, ações, cronogramas e responsáveis relacionados ao tratamento dos riscos.
Priorizar	Determinar quais riscos devem ser tratados primeiro.
Registrar	Documentar riscos, controles, avaliações e decisões no sistema de gestão.
Reportar	Comunicar riscos, níveis de exposição, incidentes e planos de ação às partes interessadas.
Revisar	Reavaliar riscos, controles e metodologias periodicamente para garantir aderência e eficácia.
Transferir	Delegar total ou parcialmente o risco a terceiros.
Tratar	Executar respostas ao risco (mitigar, aceitar, transferir, evitar).
Validar	Confirmar se avaliações, classificações, controles e dados estão corretos e consistentes.