POLÍTICA DE GESTÃO DE RISCOS CORPORATIVOS

1. FINALIDADE

Estabelecer conceitos, diretrizes e reponsabilidades para realizar a Gestão dos Riscos, como forma de promover a melhoria contínua e garantir razoável certeza dos resultados esperados e do cumprimento dos objetivos estratégicos da Companhia.

2. ABRANGÊNCIA

Aplica-se a todos os empregados, diretoria e demais membros estatutários.

3. PRINCÍPIOS

A Gestão de Riscos na CPTM se pauta pelos princípios da Administração Pública tais como legalidade, impessoalidade, moralidade, publicidade, eficiência e transparência, pelos Códigos de Conduta e Integridade e está alinhada ao Planejamento Estratégico da Companhia.

Além dos princípios acima mencionados, a Gestão de Riscos deve se pautar pelos seguintes fundamentos:

- **Ser integrada** – ser parte integrante de todos os processos da CPTM.
- **Ser estruturada e abrangente** – ser consistente e gerar dados para base comparativa futura, visando à melhoria contínua.
- **Ser personalizada** – ser adaptável aos contextos interno e externo, e feita de forma personalizada de acordo com a realidade da CPTM.
- **Ser inclusiva** – considerar e envolver, conforme apropriado, todos aqueles que, de alguma forma, são ou possam ser afetados pelos processos da Companhia.
- **Ser dinâmica** – deve se adaptar às mudanças de cenário, devidas a fatores internos e externos à Companhia, apresentando uma resposta rápida de maneira oportuna, apropriada e tempestiva.
- **Considerar a melhor informação disponível** – utilizar dados e informações disponíveis, íntegros e atualizados.
- **Considerar fatores humanos e culturais** – considerar atenção especial aos fatores humanos e culturais visto que estes influenciam a cadeia produtiva ou prestação de serviços de toda e qualquer empresa.
- **Incentivar melhoria contínua** – promover o aprendizado através da experiência, bases comparativas com uso da melhor informação disponível para a promoção da melhoria contínua.

4. DEFINIÇÕES

- **Processo:** conjunto estruturado de atividades, ações e decisões que utilizam insumos e recursos para a obtenção de um resultado planejado.

- **Risco:** efeito da incerteza nos objetivos. Este efeito é a combinação de um evento (fonte de risco) com seu respectivo dano.
  Na CPTM, o termo risco será utilizado apenas para se referir àqueles eventos que podem afetar **negativamente** os objetivos propostos.

- **Riscos estratégicos:** riscos que, através de eventos indesejáveis, podem afetar a consecução dos objetivos estabelecidos no planejamento estratégico.

- **Riscos do negócio ou empresariais:** riscos que, através de eventos indesejáveis, podem afetar a prestação do serviço, a gestão empresarial, a gestão dos recursos e a gestão de implantação de projetos de expansão e modernização.

- **Riscos de processos:** riscos que, através de eventos indesejáveis, podem afetar o resultado esperado nos processos internos, realizados pelas áreas de resultado da Companhia.

- **Riscos de integridade:** riscos que, através de eventos indesejáveis, podem afetar o cumprimento das obrigações legais e regulatórias, com destaque ao comportamento ético, a transparência, a prestação de contas e a responsabilização.

- **Gestão de Riscos**: ações coordenadas com o objetivo de identificar, avaliar, tratar e monitorar os riscos de forma a proteger e criar valor à Companhia.

- **Probabilidade:** grau de possibilidade de um evento de risco ocorrer, ou seja, é a chance de algo acontecer.

- **Impacto:** grau de impacto do dano ou prejuízo potencial resultante da ocorrência de um evento de risco.

- **Criticidade dos riscos:** combinação entre a probabilidade de um evento ocorrer e o impacto potencial do possível dano resultante de sua ocorrência.

- **Área de Conformidade, Controles Internos e Gestão de Riscos:** Componente da organização responsável pela promoção da Conformidade, Controles Internos e Gestão de Riscos, no desempenho das suas atribuições.

- **Proprietário dos riscos:** gestor de um determinado processo, sendo o responsável pela identificação, análise, avaliação, tratamento e monitoramento dos riscos, no âmbito de suas atribuições na organização.

- **Matriz dos Riscos:** modelo padronizado utilizado na CPTM para a identificação dos eventos e danos que caracterizam os riscos de um determinado processo.

- **Mapa de Calor:** representação gráfica da criticidade dos riscos. Essa representação determina visualmente o nível de criticidade do risco, permitindo rápida avaliação para priorização de futuros tratamentos dos riscos mapeados.

- **Planos de Ação:** resposta que o proprietário dos riscos, em conjunto com a equipe envolvida no(s) processo(s), deverá apresentar para estabelecer, organizar e controlar as atividades necessárias para a mitigação do risco identificado, determinando responsáveis, recursos e prazos para realização dessas atividades.

- **Planos de Contingência:** conjunto de atividades previamente planejadas para o enfrentamento da ocorrência de um evento indesejável e seus possíveis danos, com o objetivo de conter ou reduzir suas consequências, visando trazer a situação à normalidade com a maior brevidade possível, evitando assim, grandes impactos nos objetivos da CPTM.

5. DIRETRIZES

5.1. Gerais

- Manter a área responsável por verificar o cumprimento de obrigações da gestão de riscos, com atuação independente, dotando da estrutura e recursos compatíveis para o desempenho de suas funções.
- Disseminar e fortalecer a cultura da Gestão de Riscos na CPTM.
- Promover a prática da Gestão de Riscos como parte integrante dos processos de gestão, de forma integrada, estruturada e abrangente.
- Aprimorar gradualmente a metodologia e a aplicação da Gestão de Riscos.
- Estabelecer conceitos e melhores práticas.
- Tornar a Gestão de Riscos orgânica e contínua em toda a estrutura da Companhia passando pelas áreas de resultado, Diretoria Executiva e atividades do planejamento estratégico.
- Contribuir para o atingimento dos objetivos estratégicos e melhoria contínua da eficiência da gestão empresarial.

5.2. Gestão de Riscos

O processo de Gestão de Riscos deve ser contínuo e é de responsabilidade dos proprietários dos riscos.

Os proprietários dos riscos são os gestores dos processos no âmbito de suas atribuições, sendo os responsáveis pela identificação, análise, avaliação, tratamento e monitoramento de seus riscos.

Essa responsabilidade não exime as equipes envolvidas nos processos, da participação e interação com a Gestão de Riscos.

O mapeamento dos riscos irá se basear sempre na melhor informação disponível, seja ela de forma quantitativa, ou seja, sustentada por indicadores e dados históricos, seja ela de forma qualitativa dos processos, baseada na experiência individual e coletiva, na maturidade das rotinas e no histórico das ocorrências.

Os membros do Conselho de Administração, do Comitê de Auditoria Estatutário e da Diretoria devem dar todo o apoio e demonstrar comprometimento com a promoção da cultura da gestão de riscos em toda a Companhia, inclusive provendo os meios necessários para a conscientização, sensibilização, capacitação e mobilização, conforme apropriado.

Recomenda-se que se pratique a Gestão de Riscos em todos os processos principais da CPTM.

5.2.1. Detalhamento do Processo

O gestor deverá, em conjunto com sua equipe, efetuar o detalhamento dos processos sob sua responsabilidade, em subprocessos e atividades, a fim de identificar os eventos que podem de alguma forma prejudicar o atingimento dos objetivos, conforme fora planejado.

Para tanto, é importante considerar os insumos, recursos, ferramentas, procedimentos e as entregas esperadas, visando a mitigação de riscos que eventualmente possam afetar os resultados da área e os objetivos da Companhia.

5.2.2. Identificação dos Riscos

O proprietário dos riscos deverá, em conjunto com sua equipe, efetuar o levantamento dos eventos (fontes de risco) que possam afetar negativamente uma atividade e os danos que estes eventos podem ocasionar na obtenção do resultado esperado. Cabe nessa fase, fazer uso da melhor informação disponível, considerar os processos principais da área e as entregas esperadas.

É importante ressaltar que um mesmo evento de risco poderá ocasionar diversos danos.

5.2.3. Análise dos Riscos

O proprietário dos riscos e sua equipe deverão analisar as causas e as consequências para cada risco identificado.

Com base na experiência acumulada, no histórico de ocorrências, nos controles existentes e nos cenários interno e externo, deverá ser atribuído o grau de probabilidade do evento ocorrer e o grau do impacto dos danos decorrentes.

5.2.4. Avaliação dos Riscos

O proprietário dos riscos e sua equipe, após mapeamento realizado, deverão priorizar os riscos a serem tratados. A priorização será norteada pelo mapa de calor (representação gráfica da criticidade), estabelecido após atribuição de probabilidade dos possíveis eventos (fontes de risco) e impacto dos danos decorrentes.

A partir da priorização deverá ser estabelecido o tratamento a ser dado para sua mitigação, reduzindo a probabilidade do evento ocorrer ou o impacto do dano.

5.2.5. Tratamento do Risco

O proprietário dos riscos deverá propor o tratamento a ser dado para cada risco identificado, considerando o cenário atual e os recursos disponíveis.

A alçada de decisão sobre o tratamento a ser dado para cada risco será definida em norma apropriada para a Gestão dos Riscos da CPTM.

Os tratamentos possíveis são:

- **Evitar:** decisão que deve ser tomada por alçada competente de encerrar ou não iniciar determinada atividade, processo ou empreendimento, em face aos riscos identificados.
- **Reduzir:** atuar por meio da implantação de controles internos (normas, procedimentos, sistemas, verificações) e outras medidas capazes de atuar nas causas, na probabilidade de ocorrência ou na redução dos impactos do evento de risco, alterando sua criticidade para níveis inferiores aos previamente identificados. A definição e acompanhamento da implantação deverá ser registrada em Plano de Ação.
- **Transferir**: mitigar o risco, através do compartilhamento de responsabilidades, conferindo à terceira parte o tratamento do risco, através de cláusulas contratuais, garantias, seguros e outros meios.
- **Aceitar**: por decisão de alçada competente, estabelecer mecanismos de controle para riscos de baixa criticidade ou de relação desfavorável entre o custo de redução da exposição em comparação com o custo dos danos prováveis.

5.2.6. Treinamento

A CPTM proverá treinamento aos gestores e suas equipes na metodologia a ser aplicada para a Gestão de Riscos, bem como efetuará as medidas para promover a cultura da gestão de riscos, em toda a Companhia, por meio de ações de divulgação, comunicação periódica sobre o tema.

5.2.7. Comunicação

Serão relatados os riscos corporativos, tempestivamente e conforme apropriado, à Diretoria Executiva, ao Comitê de Auditoria Estatutário e ao Conselho de Administração.

5.2.8. Monitoramento

Cabe aos proprietários dos riscos, o monitoramento contínuo dos seus processos e dos riscos identificados, principalmente com foco nos planos de ação para mitigação a fim de promover a melhoria contínua.

As diversas etapas da gestão de riscos deverão ser monitoradas pelas áreas de resultados da Companhia, apoiadas pela área de Conformidade, Controles Internos e Gestão de Riscos que efetuará regularmente o relato do monitoramento dos riscos à Diretoria Executiva, ao Comitê de Auditoria Estatutário, minimamente, através de relatórios trimestrais e ao Conselho de Administração, quando solicitado.

6. RESPONSABILIDADES

6.1. Conselho de Administração

- Supervisionar os sistemas de gestão de riscos e de controle interno estabelecidos para a prevenção e mitigação dos principais riscos;
- Aprovar a Política de Gestão de Riscos Corporativos, assim como suas revisões.

6.2. Comitê de Auditoria Estatutário

- Analisar a Política de Gestão de Riscos Corporativos, assim como quaisquer revisões, subsidiando o Conselho de Administração;
- Acompanhar de forma sistemática a gestão de riscos;
- Supervisionar as atividades da área de Conformidade, Controles Internos e Gestão de Riscos;
- Avaliar a efetividade e a suficiência dos sistemas de controle e de gerenciamento de riscos.

6.3. Diretoria Colegiada

- Fornecer à área de Conformidade, Controles Internos e Gestão de Riscos, a estrutura e recursos necessários compatíveis para o desempenho de suas funções;
- Respeitar as diretrizes de governança corporativa e políticas, assim como monitorar sua observância em toda a CPTM, sendo para tanto subsidiada pela área de Conformidade, Controles Internos e Gestão de Riscos;
- Apoiar e incentivar as práticas de gestão de riscos;
- Validar os relatórios de riscos corporativos;
- Aprovar a aceitação dos riscos, conforme a alçada estabelecida em norma de gestão de riscos.

6.4. Diretor de Área

- Apoiar a gestão de riscos pelas áreas de resultado sob sua responsabilidade, bem como as medidas de tratamento necessárias e oportunas;
- Participar da gestão de riscos, no âmbito de suas atribuições, especialmente nos riscos relacionados ao negócio, para os quais os diretores são os proprietários;
- Aprovar a aceitação dos riscos conforme a alçada estabelecida em norma de gestão de riscos;
- Apoiar a implementação do sistema de gestão de riscos incluindo políticas e normas;
- Validar o mapeamento dos riscos no âmbito das áreas de resultados sob sua responsabilidade;
- Contribuir para elaboração do relatório de riscos corporativos.

6.5. Áreas de resultado

- Estabelecer, manter e avaliar práticas de negócio eficientes, considerando a gestão de seus riscos;
- Validar seus apontamentos de risco, junto à área de Conformidade, Controles Internos e Gestão de Riscos;
- Descrever plano de ação detalhado com identificação do responsável e da data de implantação;
- Assegurar a implantação do plano de ação conforme descrição e prazo definidos;
- Propor planos de contingência, conforme apropriado;
- Aprovar a aceitação dos riscos conforme a alçada estabelecida em norma de gestão de riscos;
- Propor ao Diretor de área a aceitação de riscos fora da alçada de aceitação do proprietário;

- Elaborar a matriz de riscos para os contratos formalizados nos termos da Lei Federal nº 13.303/2016, Capítulo II – Dos Contratos, respeitado o disposto no Regulamento de Licitações e Contratos da CPTM.

6.6. Área de Conformidade, Controles Internos e Gestão de Riscos

- Elaborar e propor a Política de Gestão de Riscos Corporativos, assim como quaisquer revisões, submetendo-a ao Comitê de Auditoria Estatutário, à Diretoria Colegiada e à aprovação do Conselho de Administração;
- Estabelecer as metodologias a serem utilizadas na gestão de riscos;
- Elaborar e propor a norma aplicável e apropriada de Gestão de Riscos, definindo a metodologia a ser utilizada para condução do processo de gestão dos riscos corporativos;
- Monitorar de forma sistemática a gestão de riscos e o cumprimento de seus objetivos;
- Reavaliar periodicamente a adequação da estratégia de gestão de risco da CPTM;
- Elaborar os relatórios de riscos;
- Promover a cultura de gestão de riscos na CPTM;
- Identificar e analisar os tipos de risco relevantes que comprometam o atendimento aos objetivos da CPTM;
- Propor a escala de probabilidade e impacto utilizada para avaliação da criticidade dos riscos;
- Propor elenco de indicadores de riscos;
- Atuar pró ativamente na identificação de novos tipos de risco para a CPTM;
- Prover o Conselho de Administração, o Comitê de Auditoria Estatutário e a Diretoria Colegiada com avaliações tempestivas sobre a efetividade da gestão de riscos e dos processos de governança, da adequação dos controles e do cumprimento das normas e regulamentos associados às atividades da CPTM;
- Coordenar e definir os padrões a serem seguidos relativos aos processos de gestão de riscos e os sistemas de suporte;
- Consolidar a avaliação de riscos, por meio da elaboração de relatórios, e reportá-los à Diretoria Colegiada, ao Comitê de Auditoria Estatutário e ao Conselho de Administração, conforme apropriado;
- Conscientizar os gestores sobre a importância da gestão de riscos e a responsabilidade inerente aos empregados, gestores e membros do Conselho de Administração, do Comitê de Auditoria Estatutário e da Diretoria.

6.7. Área Jurídica

- Opinar previamente sobre a legalidade dos atos e documentos da CPTM apoiando a Gerência de Conformidade, Controles Internos e Gestão de Riscos, nos termos e limites definidos em normativos internos.

6.8. Auditoria Interna

- Atuar como apoio operacional para a área de Conformidade, Controles Internos e Gestão de Riscos no desenvolvimento e desempenho de suas atribuições quanto à Gestão de Riscos;
- Aferir a efetividade do gerenciamento dos riscos.

6.9. Área Responsável

- A Presidência – PR e a Gerência de Conformidade, Controles Internos e Gestão de Riscos – GRI são responsáveis por esta Política.

6.10. Atualizações

- A CPTM revisitará a presente Política periodicamente e promoverá modificações que atualizem suas disposições de modo a reforçar o compromisso permanente com a transparência, sendo comunicadas as ocorrências de atualizações pelo site e outros canais de comunicação.

7. DISPOSIÇÕES FINAIS

- O disposto acima se aplica, imediatamente, para toda a CPTM, a partir da publicação do presente Política.

8. REFERÊNCIA

- Lei Federal nº 13.303/2016;
- Estatuto Social;
- Norma de Diretrizes do Programa de Integridade;
- Código de Conduta e Integridade da CPTM;
- Código de Conduta e Integridade – Fornecedores, Prestadores de Serviços e Parceiros da CPTM;
- Outras políticas corporativas;
- COSO – Gerenciamento de Riscos Corporativos – Estrutura Integrada;
- Norma ABNT NBR ISO 31000:2018 – Gestão de Riscos – Diretrizes.

9. CONTROLE DE VERSÕES

Versão	Data	Pág.	Motivo
01	14/12/2020	Todas	RD 15520 de 20/11/2020 RCA 019 de 14/12/2020 Em cumprimento à Lei 13303/2016 e Estatuto Social da CPTM. A PR é responsável por esta Política
02	31/01/2022	Todas	Atualização da Política. Parecer jurídico 641/2021. RD 16160 de 20/01/2022. RCA 052 de 31/01/2022.

10. ÍNDICE