



COMPANHIA PAULISTA DE TRENS METROPOLITANOS - CPTM



MANUAL: METODOLOGIA DE GESTÃO DE RISCOS

SÃO PAULO · MARÇO DE 2025

COMPANHIA PAULISTA DE TRENS METROPOLITANOS - CPTM

Rua Boa Vista, 162 - 13º andar - Sé - CEP: 01014-001

[e-mail: secretaria.executiva@cptm.sp.gov.br](mailto:secretaria.executiva@cptm.sp.gov.br)

MICHAEL SOTELO CERQUEIRA

Diretor – Presidente

CAROLINA VILELA SANTORO DE CASTRO VIANNA JACOB

Gerência de Governança, Controles Internos e Gestão de Riscos – GRI

RAFAEL BIEMMI ESPIRITO SANTO

Departamento de Gestão de Riscos e Controle Interno – DRIR

ELABORAÇÃO E REVISÃO

Rafael Biemmi Espírito Santo

Josana Lima Pimentel

Sumário

1. INTRODUÇÃO	4
2. OBJETIVOS	4
3. PRINCÍPIOS	5
4. RESPONSABILIDADES	6
5. PROCESSO DE GESTÃO DE RISCOS	8
5.1 Estabelecimento de Contexto	9
5.1.1. Definição do Escopo	9
5.2. Processo - Identificação, Análise e Avaliação de Riscos	10
5.2.1. Identificação de Riscos	10
5.2.2. Análise de Riscos	11
5.2.3. Avaliação de Riscos	12
5.2.3.1. Avaliação de Probabilidade	12
5.2.3.2. Avaliação de Impacto	13
5.2.3.3. Metodologias de Avaliação de Riscos	15
5.2.3.4. Nível do Risco	16
5.2.3.5. Avaliação do Nível de Risco com Análise dos Fatores de Risco	16
5.2.3.6. Matriz de Riscos	17
5.3. Tratamento de Riscos	18
5.3.1. Apetite a Risco	18
5.3.2. Opções de Tratamento aos Riscos	18
5.3.3. Plano de Ação	19
5.3.4. Plano de Contingência	20
5.4. Comunicação e Monitoramento	20
6. RISCOS NA CPTM	21
6.1. Categorias de Riscos	21
7. FERRAMENTAS DE APOIO	22
7.1. Estabelecimento de contexto - Matriz SWOT	22
7.2. Identificação e Análise dos Riscos: Brainstorming, Brainwriting, Entrevistas, Diagrama de Ishikawa	23
7.3. Avaliação de Riscos: Matriz de Riscos	25
7.4. Tratamento de Riscos: Plano de Ação e Plano de Contingência	26
8. REFERÊNCIAS BIBLIOGRÁFICAS	27

METODOLOGIA DE GESTÃO DE RISCOS

1. INTRODUÇÃO

A Companhia Paulista de Trens Metropolitanos – CPTM, adota uma abordagem estruturada para a gestão de riscos, com ênfase no planejamento estratégico e na estratégia de longo prazo, priorizando a gestão com foco na integridade por meio de um modelo matricial, em que é possível constituir mecanismos que geram valor aos processos, atuando de maneira coordenada para tratar as incertezas que podem impedir ou dificultar o alcance dos objetivos.

O Manual de Gestão Riscos apresenta conceitos, ferramentas e a metodologia utilizada na Companhia para condução adequada do processo de gerenciamento, com o propósito de servir como guia e dar suporte à concepção, implementação, monitoramento e melhoria contínua da gestão de riscos, com foco na previsibilidade dos processos.

A metodologia foi customizada de forma a ser aplicável a todas as áreas da Companhia. Reunindo as etapas necessárias para identificar, analisar, avaliar, tratar e monitorar os riscos, dentro de uma estrutura contextual e de comunicação a todos os envolvidos, se integrando aos demais processos organizacionais.

A base teórico-conceitual desta metodologia foi pautada em modelos amplamente utilizados internacionalmente para a boa condução da gestão de riscos, a saber:

- ABNT NBR ISO 31000:2018 Gestão de Riscos - Princípios e Diretrizes;
- ABNT NBR ISO/IEC 31010:2021 Gestão de Riscos - Técnicas para o processo de avaliação de riscos;
- COSO-ERM (Committee of Sponsoring Organizations - Enterprise Risk Management);
- The Institute of Internal Auditors - Modelo das Três Linhas de Defesa.

2. OBJETIVOS

- Contribuir para a consecução dos objetivos da Companhia, mitigando as incertezas;
- Promover a melhoria contínua;
- Melhorar o desempenho;

- Contribuir com a inovação;
- Criar e proteger valor para a Companhia;
- Dar Suporte à tomada de decisão;
- Alinhar a atuação gerencial ao apetite a riscos da Companhia;
- Melhorar o controle interno da gestão;
- Aperfeiçoar os mecanismos de governança e prestação de contas, contribuindo para o uso eficiente, eficaz e efetivo de recursos;
- Disseminar a cultura de gestão de riscos e controles internos;

3. PRINCÍPIOS

Em conformidade com a norma ABNT NBR ISO 31000: 2018, constituem princípios da gestão de riscos na CPTM:

- Ser integrada – ser parte integrante de todos os processos;
- Ser estruturada e abrangente – ser consistente e gerar dados para base comparativa futura, visando a melhoria contínua;
- Ser personalizada – ser adaptável aos contextos interno e externo, sendo 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 – adaptar-se às mudanças de cenário, decorrentes de 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 – dar atenção especial aos fatores humanos e culturais visto que estes influenciam a cadeia produtiva ou prestação de serviços de toda e qualquer empresa;
- Incentivar a melhoria contínua – promover o aprendizado através da experiência, bases comparativas com uso da melhor informação disponível, para a promoção da melhoria contínua.

4. RESPONSABILIDADES

O modelo das Três Linhas de Defesa é crucial para garantir uma estrutura de governança sólida, pois possibilita:

- Clarificar responsabilidades, evitando sobreposições ou lacunas;
- Promover a responsabilização, com cada linha exercendo funções complementares;
- Aumentar a resiliência organizacional, ao combinar ações operacionais, supervisão estratégica e auditoria independente;
- Fortalecer a cultura de riscos, criando uma abordagem integrada para identificar, tratar e monitorar riscos.

4.1. Modelo das Três Linhas do IIA - (The Institute of Internal Auditors)

4.1.1. 1ª Linha de Defesa – Gestão Operacional

Importância organizacional:

- Aumenta a eficiência operacional ao integrar os controles à rotina diária.

O que faz:

Responsável por identificar, analisar, avaliar, tratar e monitorar os riscos diretamente nas atividades diárias.

Quem faz:

Todas as áreas de resultado da Companhia. Realizando as atribuições presentes no normativo de estrutura organizacional – NG/002, aplicando controles internos com vistas à mitigação dos riscos que possam impactar a consecução dos objetivos.

Contribuição para o gerenciamento de riscos:

- Identificar potenciais riscos;
- Implementar controles internos relacionados às atividades;
- Garantir a execução de procedimentos de acordo com políticas e diretrizes institucionais;
- Atuar como a base para a gestão de riscos, garantindo que os riscos sejam tratados de forma proativa e no momento em que surgem.

4.1.2. 2ª Linha de Defesa – Supervisão e Monitoramento

Importância organizacional:

- Proporciona uma visão mais estratégica sobre os riscos organizacionais;
- Garante alinhamento com regulamentações externas e as metas de governança;

- Reduz conflitos de interesse ao separar a operação da supervisão.

O que faz:

Responsável por implementar os processos e cultura de gestão de riscos e controles internos na Companhia; Consolidar os mapeamentos de risco e de controles; Acompanhar a identificação, avaliação, tratamento e monitoramento dos riscos e controles internos pela gestão; Zelar para que os riscos e os controles internos mapeados estejam alinhados ao apetite a risco definidos pela gestão; Reportar os resultados do departamento sobre a situação dos riscos e a eficácia dos controles internos.

Quem faz:

A Gerência de Governança, Controles Internos e Gestão de Riscos é a área da Companhia que apoia tecnicamente todas as áreas, atua como principal interface com a Alta Administração sendo a responsável pela Cultura de Gestão de Riscos.

Contribuição para o gerenciamento de riscos:

- Aplicar metodologias e ferramentas para gerenciar riscos;
- Monitorar a eficácia dos controles da primeira linha;
- Facilitar treinamentos para promover a cultura de riscos.

4.1.3. 3ª Linha de Defesa – Auditoria Interna

Importância organizacional:

- Proporciona confiança e credibilidade à governança corporativa;
- Oferece inspirações isentas e independentes à alta administração;
- Apoia a tomada de decisão estratégica com base em relatórios robustos e imparciais.

O que faz:

Realiza auditorias independentes da eficácia das atividades da primeira e segunda linhas, reportando diretamente ao Conselho de Administração.

Quem faz:

A equipe de Auditoria interna da CPTM.

Contribuição para o gerenciamento de riscos:

- Avaliar a eficácia dos controles e dos processos de gerenciamento de riscos;
- Identificar lacunas e propor melhorias nos controles internos;
- Garantir que as políticas e regulamentações estejam sendo seguidas.

TRÊS LINHAS DE DEFESA NA CPTM



Figura 1 – Modelo das 3 Linhas de defesa aplicado na Companhia Paulista de Trens Metropolitanos - CPTM

Fonte: Metodologia de Gestão de Riscos - Controladoria Geral do Estado de São Paulo (adaptado)

5. PROCESSO DE GESTÃO DE RISCOS

O gerenciamento de riscos corporativos é um processo conduzido pela organização e aplicado no estabelecimento de estratégias, formuladas para identificar eventos em potencial, capazes de afetá-la, e administrar riscos de modo a mantê-los compatíveis com o apetite a risco da organização e possibilitar a garantia do cumprimento dos seus objetivos.

As definições a seguir proporcionam um melhor entendimento dos conceitos adotados para a gestão de riscos:

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

Eventos positivos serão tratados como oportunidades, sendo conduzidos diretamente pelos gestores dos processos onde sejam identificados esses riscos.

- **Risco Inerente:** É o risco natural das atividades, negócios ou processos, os riscos que existem antes de qualquer aplicação de medida mitigatória.

- **Risco Residual:** É o risco que persiste mesmo após a aplicação de medidas de mitigação.

- **Fonte de Risco:** origem ou causa potencial de um risco. Refere-se ao evento, condição ou circunstância que pode levar a uma situação de risco. É onde o plano de ação deve ser estruturado.

- **Fator de Risco:** é uma condição ou variável que intensifica a chance de um risco ocorrer ou agravar

seu impacto. A análise do fator de risco, levará a causa raiz do risco.

Visando facilitar a compreensão e categorizar os fatores de risco, a CPTM optou por utilizar um modelo internacionalmente reconhecido, o modelo dos 6M's (ver item 7.2.4.).

PROCESSO DE GESTÃO DE RISCOS DA CPTM

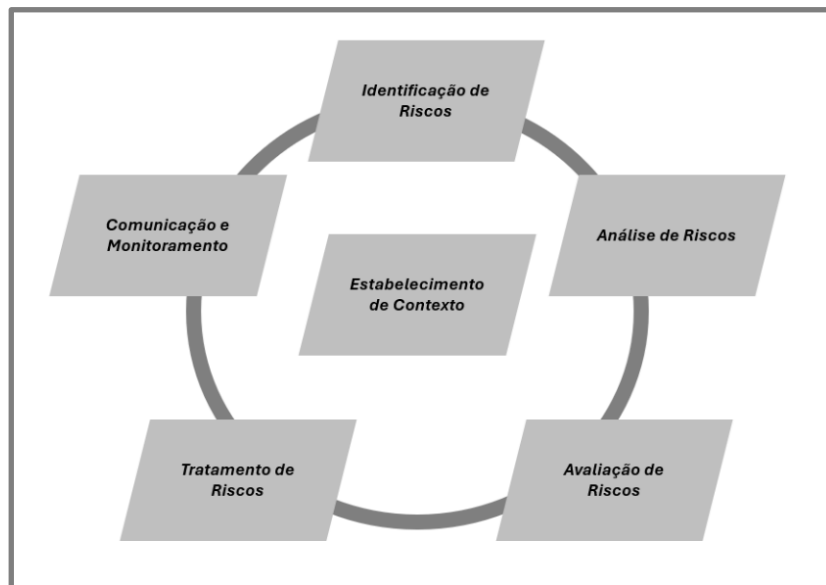


Figura 2 – Macroprocesso de Gestão de Riscos na Companhia Pauslita de Trens Metropolitanos - CPTM

Fonte: Metodologia de Gestão de Riscos - Controladoria Geral do Estado de São Paulo (adaptado)

5.1. Estabelecimento do Contexto

Conhecer os objetivos organizacionais e os processos a eles relacionados, bem como definir os contextos internos e externos a serem levados em consideração ao prever e gerenciar os riscos é determinante para estruturar uma gestão de riscos sólida, eficiente e eficaz para a Companhia.

Como o processo de gestão de riscos pode ser aplicado em diferentes níveis, é importante identificar claramente o escopo e os objetivos a serem considerados, assegurando o alinhamento aos objetivos organizacionais. Do ponto de vista institucional, os riscos serão avaliados de acordo com a Matriz SWOT da Companhia e sua Abordagem Estratégica 2025-2029, publicada no *site*.

5.1.1. Definição do Escopo

A definição do escopo consiste em levantar informações detalhadas visando à compreensão do objeto da gestão de riscos. É importante ter clareza quanto ao objetivo que se pretende atingir. Quanto mais completa a compreensão, melhor o desenvolvimento do trabalho. Na CPTM, deve-se portanto considerar:

- Missão: Prestar serviços de transporte propiciando mobilidade com excelência, sustentabilidade e acesso a serviços associados, que tornem a experiência de optar pela CPTM única;
- Visão: Ser, de modo sustentável, o elo fundamental na cadeia intermodal de transporte de passageiros no Estado de São Paulo e a referência em projetos ferroviários aprimorando experiências em mobilidade humana;
- Valores: Comprometimento com transparência e integridade; Valorização do capital humano; Respeito ao meio ambiente e aos valores das comunidades; Zelo inegociável pela melhor técnica; Foco na inovação e empreendedorismo.

5.2. Processo - Identificação, Análise e Avaliação de Riscos (ISO 31000:2018)

Nessa etapa do processo de gestão de riscos, a ênfase é na avaliação dos riscos que compõem as fases: identificação, análise e avaliação, a figura abaixo ilustra esse estágio.

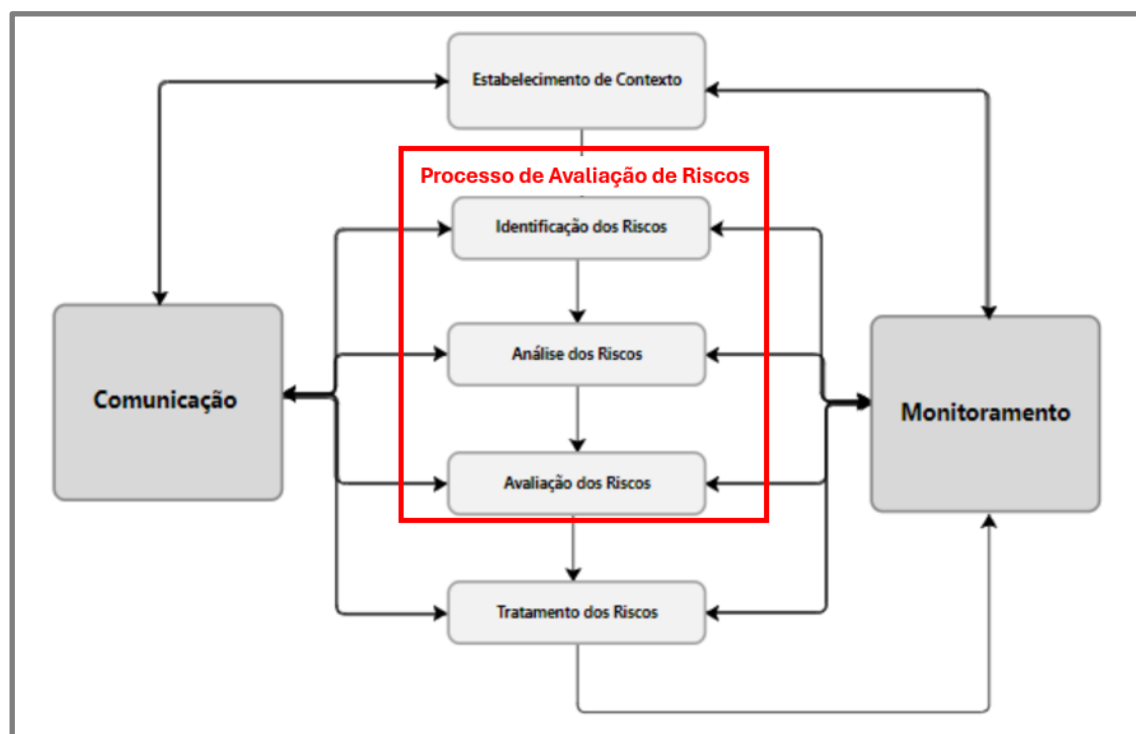


Figura 3 – Processo de Avaliação de Riscos - ISO 31000:2018

Fonte: ISO 31000:2018 (adaptado)

5.2.1. Identificação de Riscos

O objetivo do mapeamento é identificar riscos associados aos objetivos organizacionais e aos processos a que estão relacionados. Os proprietários dos riscos, junto com suas equipes, identificam eventos de risco (fontes

de incertezas) que possam impactar negativamente as atividades e os resultados esperados.

Para isso, podem ser utilizadas técnicas como o *Brainstorming*, *Brainwriting*, Entrevistas, Diagrama de Ishikawa, exemplificados no item 7.2.

5.2.1.1. Impacto nos Objetivos:

- Basear o levantamento na fidedignidade da informação, considerando os objetivos e processos.
- Com a identificação clara dos resultados esperados, é possível mapear riscos que possam comprometer o(s) objetivo (s);
- É importante destacar que um único evento de risco pode gerar múltiplos impactos em diferentes processos ou áreas;

5.2.2. Análise de Riscos

A análise de riscos consiste em compreender e reconhecer os eventos que podem impactar o alcance dos objetivos organizacionais. Após a identificação dos riscos, é necessário analisar as causas e as consequências. Esse processo deve considerar a experiência acumulada, o histórico de ocorrências, os controles existentes e os cenários internos e externos para atribuir:

- O grau de probabilidade de ocorrência do evento de risco;
- O grau de impacto dos danos que podem decorrer desse evento.

A análise de risco está inserida na etapa de "Avaliação de Riscos" do processo de gestão de riscos da ISO 31000, item 5.2. – figura 3, em que os riscos são enquadrados em níveis de criticidade. Essa análise é fundamental para:

- Identificar as causas que podem desencadear os eventos de risco;
- Avaliar as consequências que esses eventos podem gerar.

Descrever como cada risco impacta os objetivos associados, permite maior clareza sobre às vulnerabilidades da Companhia. É importante lembrar que um único evento de risco pode ter múltiplas causas e consequências, podendo afetar diversos objetivos simultaneamente. A profundidade da análise pode variar de acordo com:

- O propósito da análise;
- A disponibilidade e confiabilidade das informações;
- Os recursos disponíveis para conduzir o processo.

Esse processo torna a organização mais consciente e preparada para lidar com potenciais eventos de risco, contribuindo para decisões mais assertivas e a implementação de controles eficazes.

Após a análise, avaliação e verificação de controles existentes dos riscos mapeados é necessário reavaliar a criticidade com foco nos riscos residuais e na reclassificação.

As principais características dos riscos residuais são que não podem ser totalmente eliminados, apenas reduzidos ou controlados; dependem da eficácia das respostas ao risco, se os controles forem fracos, os riscos residuais serão maiores; podem ser aceitáveis ou não, a depender do apetite ao risco da Companhia; devem ser monitorados continuamente para garantir que não ultrapassem os limites aceitáveis.

Os riscos residuais são uma parte fundamental da gestão de riscos, pois representam os riscos que permanecem mesmo após a implementação de tratamento para mitigá-los. Eles precisam ser monitorados continuamente para garantir que estejam dentro dos limites aceitáveis para a Companhia.

5.2.3. Avaliação de Riscos

A avaliação do risco envolve a comparação do seu nível com o limite de exposição a riscos, a fim de determinar se o risco pode ser aceitável, se deve ser mitigado, se pode ser compartilhado ou se deve ser evitado. De modo a priorizar a construção de planos de ação para cada um.

5.2.3.1. Avaliação de Probabilidade

A probabilidade está diretamente relacionada as fontes de risco, e ao grau de possibilidade de um evento de risco ocorrer, ou seja, é a chance de algo acontecer dentro do prazo previsto para se alcançar o objetivo/resultado. Por exemplo, se o objeto da gestão de riscos é um projeto, estima-se a probabilidade da ocorrência do risco durante o prazo previsto para entrega do produto.

Na CPTM a escala de probabilidade possui 5 níveis, rara, baixa, moderada, alta e muito alta, com pesos de 1 a 5 respectivamente, conforme demonstrado a seguir:

Escala de Probabilidade		Frequência esperada	Descrição
Muito Alta	5	Ocorre na maioria das vezes	O evento risco se materializa na maior parte das situações
Alta	4	Alta frequência	O evento risco ocorre frequentemente
Moderada	3	Média frequência	O evento risco ocorre ocasionalmente
Baixa	2	Baixa frequência	O evento risco pode ocorrer, mas é improvável
Rara	1	Evento raro	O evento risco quase nunca ocorre

Tabela 1 – Escala de Probabilidade

Fonte: Elaboração Própria

5.2.3.2. Avaliação de Impacto

A avaliação do impacto está diretamente relacionada às consequências do evento de risco e deve levar em conta:

- Objetivos organizacionais: relacionar as consequências do risco com os objetivos estabelecidos;
- Impactos imediatos e futuros: considerar tanto as consequências diretas quanto aquelas que podem surgir ao longo do tempo, conforme o escopo da avaliação;

Na CPTM a escala de impacto possui 5 níveis, leve, baixo, moderado, alto e muito alto com pesos de 1 a 5 respectivamente.

Na avaliação de impacto deve ser considerado o risco preponderante para a classificação, conforme tabela de impacto a seguir.

Tabela de Impacto para os Riscos: Operacional; Imagem e Reputação; Cibernético; Meio Ambiente; Integridade; Capital Humano e Continuidade.

Escala de Impacto		Descrição do Impacto	Categoria Principal do Risco
Muito Alto	5	Impacto crítico, ameaça severamente a continuidade do negócio.	Escolher a categoria preponderante em relação ao impacto, caso o evento de risco se concretize.
Alto	4	Impacto alto, afeta significativamente a Companhia.	
Moderado	3	Impacto moderado, pode causar atrasos ou prejuízos pontuais.	
Baixo	2	Impacto baixo, pequeno efeito sobre a operação.	
Leve	1	Impacto mínimo, sem efeitos relevantes.	

Tabela 2 – Escala de Impacto

Fonte: Elaboração Própria

Para os riscos Financeiros, deve-se utilizar a tabela a seguir, que tem a mesma escala de 1 a 5, porém com o descritivo adequado para a realidade do orçamento da Companhia e seus objetivos estratégicos.

Tabela de Impacto para os Riscos: Financeiros

Escala de Impacto		Financeiro
		Perdas ou danos causados por fatores financeiros
Muito Alto	5	Queda na arrecadação e aumento em despesas fora da previsão orçamentária
Alto	4	Aumento em despesas não previstas em orçamento sem impacto na arrecadação
Moderado	3	Queda na arrecadação não previstas em orçamento sem impacto em despesas
Baixo	2	Aumento em despesas previstas em orçamento sem impacto na arrecadação
Leve	1	Queda na arrecadação previstas em orçamento sem impacto em despesas

Tabela 3 – Escala de Impacto – Riscos Financeiros

Fonte: Metodologia de Gestão de Riscos - Controladoria Geral do Município de São Paulo (adaptado)

5.2.3.3. Metodologias de Avaliação de Riscos

A avaliação de riscos combina técnicas quantitativas e qualitativas, escolhidas conforme a complexidade da análise, que irá variar de acordo com a disponibilidade dos dados a serem analisados.

1. Técnicas Quantitativas

- Proporcionam maior precisão e são indicadas para atividades mais complexas;
- Utilizam modelos matemáticos, exigindo dados confiáveis e premissas bem definidas;
- São úteis em casos com histórico conhecido e variabilidade previsível;
- Demandam mais esforço, recursos e rigor analítico.

2. Técnicas Qualitativas

Aplicadas quando os riscos não podem ser quantificados, por falta de dados históricos.

Utilizam escalas descritivas ou numéricas para indicar a probabilidade e o impacto, como:

- Probabilidade: rara, baixa, moderada, alta, muito alta;
- Impacto: muito alto, alto, moderado, baixo, leve;
- Podem ser personalizadas para atender às necessidades específicas da organização;
- Processo de avaliação com técnicas qualitativas.

Para obter consenso sobre probabilidade e impacto, é recomendável:

- Realizar entrevistas, seminários ou oficinas de trabalho, envolvendo especialistas que conheçam bem o objeto de gestão de riscos;
- Utilizar escalas e critérios claros, ajustados às particularidades da organização;
- Recomendações para avaliação.

De acordo com a ABNT NBR ISO 31000:2018, a avaliação de riscos pode ser influenciada por:

- Divergências de opinião, vieses, percepções de risco e julgamentos;
- Qualidade das informações utilizadas e limitações das técnicas.

Essas influências devem ser documentadas e comunicadas aos tomadores de decisão para garantir a transparência.

5.2.3.4. Nível de Risco

O nível do risco é definido com base na matriz de risco: probabilidade x impacto, que define a criticidade a partir da multiplicação do cruzamento dos valores estabelecidos, conforme pontuações definidas no quadro abaixo.

NÍVEL DE RISCO	
CLASSIFICAÇÃO DO RISCO	
Nível de Risco	Faixa
Risco Baixo	01 - 04
Risco Médio	05 - 09
Risco Alto	10 - 16
Risco Extremo	17 - 25

Tabela 4 – Nível de Criticidade dos Riscos

Fonte: Metodologia de Gestão de Riscos - Controladoria Geral do Estado de São Paulo (adaptado)

5.2.3.5. Avaliação do Nível do Risco com Análise dos Fatores de Risco

O processo de avaliação dos riscos deve levar em consideração a identificação, descrição, categoria principal em que se enquadra, o impacto e a probabilidade do evento, caso se concretize, além da abordagem aos fatores de risco que podem ser classificados como principais e secundários.

- **ID do Risco:** Identificação única do risco.
- **Descrição do Risco:** Explica de forma clara o risco identificado.
- **Categoria Principal:** Classifica o risco dentro da estrutura com enfoque na categoria principal de acordo com as categorias estabelecidas no item 6.1.
- **Fator Principal (6M's):** Identifica a principal causa do risco (Mão de Obra, Máquinas, Materiais, Métodos, Meio Ambiente, Medidas).
- **Fator Secundário (6M's):** Permite um segundo fator de risco relevante para melhor análise e tabulação de dados.
- **Impacto (Escala 1 a 5):** Determina a severidade do impacto.
- **Probabilidade (Escala 1 a 5):** Define a chance de ocorrência do risco usando como referência - um valor granular de 1 a 5 na matriz de risco.
- **Nível de Risco:** criticidade do risco definido por meio da multiplicação da probabilidade x impacto.

Exemplo de Avaliação do Nível dos Riscos com Análise dos Fatores de Risco

ID do Risco	Descrição do Risco	Categoria Principal	Fator Principal (6M's)	Fator Secundário (6M's)	Probabilidade (Escala 1 a 5)	Impacto (Escala 1 a 5)	Nível de Risco
001	Falha no sistema de bilhetagem eletrônica, impedindo a compra de bilhetes digitais.	Cibernético	Máquinas	Métodos	5	5	25
002	Atraso na manutenção de trens, reduzindo a frota operacional.	Operacional	Mão de Obra	Materiais	5	3	15
003	Escândalo de corrupção envolvendo fornecedores.	Integridade	Métodos	Meio Ambiente	3	5	15
004	Greve de funcionários, paralisando as operações por mais de 24h.	Capital Humano	Mão de Obra	Métodos	1	4	4
005	Crise financeira reduz repasses do governo para investimentos.	Financeiro	Métodos	Materiais	2	2	4
006	Notícia falsa sobre suposta falha nos trilhos gera pânico entre passageiros.	Imagem & Reputação	Meio Ambiente	Métodos	1	2	3
007	Rompimento de duto de óleo diesel na estação central.	Meio Ambiente	Materiais	Meio Ambiente	2	5	10
008	Publicação em redes sociais de conteúdo inadequado	Imagem & Reputação	Mão de Obra	Métodos	2	5	10

Tabela 5 – Exemplo de Avaliação do Nível dos Riscos com Análise dos Fatores de Risco

Fonte: Elaboração Própria

** Dados meramente ilustrativos.

5.2.3.6. Matriz de Risco

A Matriz de Risco, com os possíveis resultados da combinação das escalas de probabilidade e impacto, resulta em um valor que indica o nível de risco.

MATRIZ DE RISCO

MATRIZ DE RISCO		PROBABILIDADE				
		RARA	BAIXA	MODERADA	ALTA	MUITO ALTA
		1	2	3	4	5
IMPACTO	MUITO ALTO 5	5	10	15	20	25
	ALTO 4	4	8	12	16	20
	MODERADO 3	3	6	9	12	15
	BAIXO 2	2	4	6	8	10
	LEVE 1	1	2	3	4	5

Figura 4 – Matriz de Risco utilizada na Companhia Paulista de Trens Metropolitanos

Fonte: Metodologia de Gestão de Riscos - Controladoria Geral do Estado de São Paulo

A priorização será norteada pela matriz de riscos (representação gráfica da criticidade), estabelecida

após atribuição de probabilidade dos possíveis eventos (fontes de risco) e impacto dos danos decorrentes. A partir da classificação deverá ser definido o tratamento a ser dado para sua mitigação, reduzindo a probabilidade do evento ocorrer ou o impacto do dano.

Por fim, são identificados os controles já existentes, relacionados a cada um dos eventos de risco, assim como são listadas as ações de controle complementares, que serão úteis para o acompanhamento dos impactos.

Após a realização do processo de avaliação de riscos (identificação, análise e avaliação) e implementação do tratamento dos riscos é importante o mapeamento/implementação dos controles internos quando se faz necessário avaliar o risco residual e reclassificar o impacto dos riscos.

5.3. Tratamento de Riscos

Compreende o planejamento e a realização de ações para modificar o nível do risco. O nível do risco pode ser modificado por meio de medidas de resposta que mitiguem, transfiram, evitem ou aceitem o(s) risco(s).

Durante o tratamento do risco é importante monitorar a implementação das ações propostas para verificar se atende ao previsto no plano de tratamento ou se é necessário ajustes para alcançar a redução a um nível aceitável dos riscos eleitos para tratamento.

O tratamento de riscos envolve os seguintes passos:

- Eleger quais riscos terão suas respostas priorizadas;
- Escolher as medidas de tratamento a serem implementadas;
- Definir e detalhar as respostas aos riscos, de forma a adequar os níveis ao apetite estabelecido.

5.3.1. Apetite a Risco

Apetite a risco é o nível de risco que a Companhia está disposta a aceitar. Deve ser aprovada pela Alta Administração e servir como uma referência, a fim de estabelecer uma linha de corte para os riscos passíveis de serem aceitos e aqueles que necessariamente precisarão de planos de ação e/ou contingência.

5.3.2. Opções de Tratamento aos Riscos

Priorizados os riscos, o próximo passo é definir quais opções de tratamento serão adotadas. Cada risco deve ser relacionado a uma ou mais opções de tratamento, que incluem: mitigar, transferir, evitar ou aceitar.

Ao analisar a própria resposta, o gestor avalia o efeito sobre a probabilidade de ocorrência e o impacto do risco, assim como os custos e benefícios, selecionando, dessa forma, uma resposta que mantenha os parâmetros

dentro das tolerâncias a risco desejadas, a seguir tabela com opções de tratamento.

OPÇÕES DE TRATAMENTO DE RISCOS	
Opções	Descrição
Mitigar	Diminuir a probabilidade, o impacto ou ambos, a fim de tornar a criticidade da ocorrência do risco aceitável para a Companhia.
Transferir	Decisão da autoridade competente de compartilhar os riscos com outras entidades, mitigar através do compartilhamento que possa conferir à outra parte o tratamento do risco através de cláusulas contratuais, garantias, seguros e outros meios.
Evitar	Decisão da autoridade competente de não realizar a atividade, ou alterar o processo em questão, a fim de não se envolver ou agir de forma a se retirar de uma situação de riscos. As mudanças realizadas para a eliminação de um risco normalmente alteram o nível dos riscos que precisam ser analisados.
Aceitar	Decisão da autoridade competente por apenas efetuar o monitoramento com os mecanismos de controle existentes para riscos de baixa criticidade ou de relação desfavorável entre o custo de redução da exposição em comparação com o custo dos danos prováveis.

Tabela 6 – Tratamento de Riscos

Fonte: Metodologia de Gestão de Riscos - Controladoria Geral do Estado de São Paulo (adaptado)

5.3.3. Plano de Ação

A escolha das medidas de resposta ao risco pode ser realizada em oficinas de trabalho com a participação de pessoas que conheçam bem o objeto de gestão de riscos. Recomenda-se a utilização de técnicas que permitam a identificação da maior quantidade de medidas de resposta ao risco, tais como *brainstorming*, *brainwriting*, entrevistas, visitas técnicas, pesquisas etc.

São dicas que ajudam a identificação de medidas de resposta ao risco, responder às seguintes perguntas-chave:

- Que medidas poderiam ser adotadas para reduzir a probabilidade de ocorrência do risco?
- É possível adotar medidas para transferir o risco?
- Qual é a causa raiz dessa fonte de risco?

Essas medidas devem atacar as causas do risco, de modo a reduzir a probabilidade de ocorrência. Os planos de ação necessariamente trabalharão na mitigação do evento risco se concretizar, portanto, atuarão na redução da probabilidade de ocorrência do risco.

Na decisão quanto à implantação das medidas de resposta ao risco, considerar a quantidade e o nível dos riscos mitigados por cada medida, bem como o grau de redução do nível gerado pela medida, bem como, verificar a viabilidade da implantação das medidas (custo-benefício, viabilidade técnica, tempestividade, efeitos colaterais do tratamento etc.).

Após decidir sobre as respostas, o gestor precisa desenvolver um plano de tratamento e assegurar-se de que a resposta ao risco seja conduzida. Ressaltando que sempre existirá algum nível de risco, não somente porque os recursos são limitados, mas também em decorrência da incerteza e das limitações inerentes a todas as atividades, segue modelo de Plano de Tratamento de Riscos:

PLANO DE TRATAMENTO DE RISCOS					
Prioridade	Opções de Tratamento	Responsável	Ações	Status/Observações	Prazo
1	Mitigar	Áreas de TIC e Educação Continuada	1- Elaboração de um calendário de ações em segurança da informação e comunicação. 2- Prover capacitação em temas de segurança da informação e comunicação. 3- Elaboração do Termo de Responsabilidade de TI.	Em andamento	2º semestre de 2025

Tabela 7 - Exemplo de Plano de Tratamento de Riscos

Fonte: Metodologia de Gestão de Riscos - Controladoria Geral do Estado de São Paulo

É importante que, na elaboração do plano de tratamento, se avalie também a necessidade de melhorar ou extinguir controles ineficientes. Somente depois dessa avaliação, e se ainda for identificada a necessidade de redução do nível do risco, podem ser propostos novos controles, para tratamento dos riscos residuais, observados sempre critérios de eficiência e eficácia da sua implementação.

Importante destacar que cabe aos gestores proprietários dos riscos, primeira linha, a elaboração de planos de ação, exemplo no item 7.4., para o tratamento dos riscos, considerando a declaração de apetite a riscos da Companhia.

5.3.4. Plano de Contingência

Para situações em que ocorrem a concretização do evento de risco, o plano de contingência é uma medida que deve ser tomada, na qual é estabelecido, dentre outras medidas ordenadas, procedimentos de reação, protocolos de comunicação e subordinação, avaliação do impacto, estabelecimento de prioridades.

5.4. Comunicação e Monitoramento

De acordo com a norma ABNT NBR ISO 31000:2018, durante todas as etapas do processo de gerenciamento de riscos, é importante haver comunicação com as partes interessadas, a fim de assegurar que as informações pertinentes sejam coletadas, consolidadas, sintetizadas e compartilhadas.

É necessário monitorar e adaptar continuamente a estrutura de gestão de riscos para abordar mudanças

nos contextos externos e internos, incluindo alterações nos critérios de risco e no próprio risco, que podem requerer revisão dos tratamentos adotados, assim como identificação de novos riscos. Dessa forma, a Companhia pode monitorar e aprimorar continuamente a adequação, a solidez e a eficácia da estrutura de gestão de riscos

Os riscos devem ser relatados, tempestivamente e conforme apropriado, à Diretoria Executiva, ao Comitê de Auditoria Estatutário e ao Conselho de Administração.

A comunicação e o monitoramento envolvem os seguintes passos:

- Identificar os canais de comunicação da Companhia, para elaboração de um Plano de Comunicação. Na CPTM os canais de comunicação são e-mail, intranet e as redes sociais.

- A frequência do monitoramento dos riscos e apresentação à Alta Administração é trimestral, apresentado em relatórios pertinentes para Diretoria Colegiada e Conselhos.

Visam assegurar que todos os envolvidos estejam cientes de seus papéis e responsabilidades, de modo a promover a conscientização e a compreensão do risco. Fornecendo a base para a tomada de decisões.

6. RISCOS NA CPTM

6.1. Categorias de Risco

Utilizam-se categorias para agrupar os riscos classificando-os por temas, o que pode direcionar as responsabilidades após definido o tratamento necessário para sua mitigação. Na CPTM os riscos são categorizados conforme tabela a seguir e deve ser considerado em sua análise o risco em que o impacto é preponderante.

Categoria de Risco	Descrição
Financeiro	Riscos relacionados a perdas financeiras, orçamento, inadimplência, fluxo de caixa.
Operacional	Riscos que impactam a operação e qualidade dos serviços, incluindo falhas técnicas, atrasos, infraestrutura e processos.
Imagem e Reputação	Riscos relacionados à percepção pública, mídia, credibilidade e confiança da população.

Cibernético	Riscos ligados à segurança da informação, ataques hackers, vazamento de dados e falhas em sistemas.
Meio Ambiente	Riscos associados a impactos ambientais, conformidade com leis ambientais e mudanças climáticas.
Integridade	Riscos relacionados a fraudes, corrupção, conflitos de interesse, nepotismo, desvios de conduta, não conformidades e problemas relacionados à Governança Corporativa.
Capital Humano	Riscos ligados à gestão de pessoas, cultura organizacional, rotatividade, capacitação e engajamento.
Continuidade	Riscos externos, motivados por crises sanitárias, mudanças regulatórias, instabilidade socioeconômica e impactos globais que afetam a capacidade de manter as atividades essenciais.

Tabela 8 – Categorias de Riscos

Fonte: Elaboração Própria

7. FERRAMENTAS DE APOIO – ABNT NBR ISO/IEC 31010:2021 - Gestão de Riscos - Técnicas para o processo de avaliação de riscos.

7.1. Estabelecimento de contexto: Matriz SWOT.

A Matriz SWOT (do Inglês Strengths, Weaknesses, Opportunities and Threats) é uma ferramenta que auxilia na análise dos elementos do contexto interno e externo à Companhia identificando forças, fraquezas, oportunidades e ameaças que podem afetar diretamente o objeto de gestão de riscos e, consequentemente, o atingimento dos resultados almejados.

A análise do ambiente interno se concentra nas forças e fraquezas da Companhia, abrangendo os fatores sobre os quais ela tem controle ou pode intervir, como: visão, missão, valores, objetivos estratégicos, estrutura organizacional, governança, pessoas, sistemas, políticas, processos, cultura organizacional, entre outros.

Já a análise do ambiente externo identifica as oportunidades e ameaças, sendo representadas por um contexto favorável ou desfavorável sobre os quais a Companhia não tem poder de decisão ou influência. Reúne elementos como: fatores sociais, culturais, políticos, jurídicos, regulatórios, financeiros, tecnológicos, econômicos e ambientais.

Assim, observando as forças e oportunidades da matriz, tem-se os fatores positivos a serem aproveitados. Por outro lado, as fraquezas e ameaças identificadas, trazem os fatores negativos a serem observados e evitados.

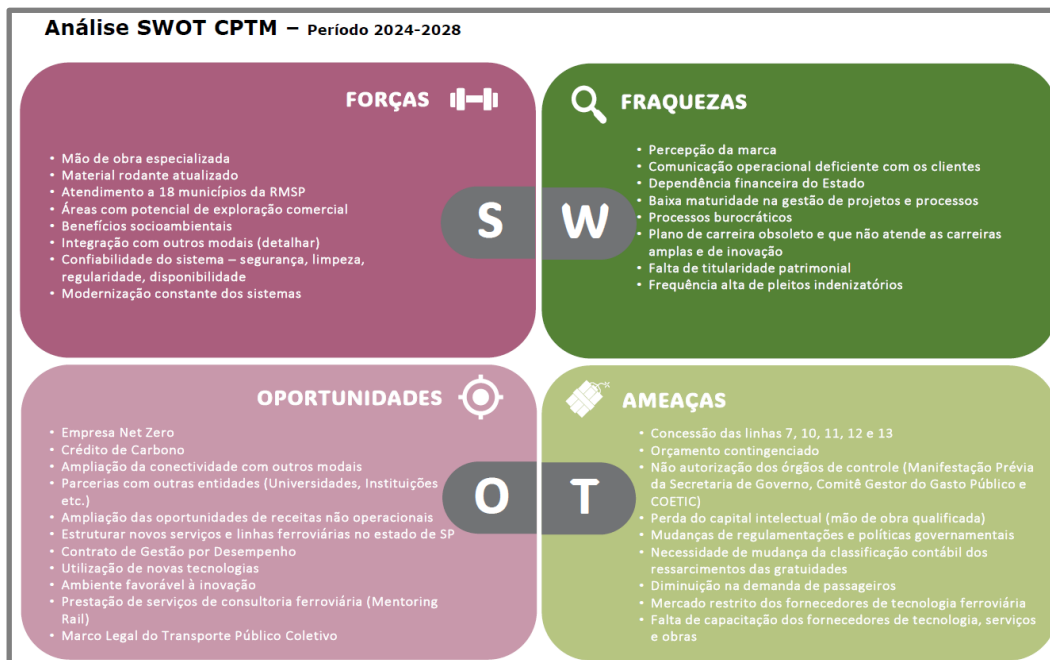


Figura 5 – Matriz SWOT utilizada no Planejamento Estratégico da Companhia Paulista de Trens Metropolitanos - CPTM

Fonte: Elaboração própria

7.2. Identificação e Análise dos Riscos: *Brainstorming*, *Brainwriting*, Entrevistas, Diagrama de Ishikawa.

A identificação e análise de riscos podem ser conduzidas com o auxílio de diversas ferramentas que facilitam a coleta e organização de informações. Entre as principais técnicas utilizadas, destacam-se:

7.2.1. *Brainstorming*

O *Brainstorming* é uma técnica colaborativa para geração de ideias, amplamente utilizada na identificação de riscos. Durante o encontro, os participantes se reúnem para, de forma livre e direcionada, compartilhar percepções, apontar possíveis problemas e propor soluções. O objetivo principal dessa técnica, no contexto do gerenciamento de riscos, é identificar os possíveis riscos que podem impactar o alcance dos objetivos organizacionais.

Regras para Conduzir um *Brainstorming* Eficiente:

1. **Ambiente descontraído:** crie um espaço aberto e confortável, onde todos se sintam à vontade para contribuir.
2. **Priorize quantidade:** incentive a geração de muitas ideias, sem filtros iniciais.
3. **Evite críticas:** durante a sessão, não se deve julgar ou rejeitar nenhuma ideia apresentada.
4. **Estimule criatividade:** incentive propostas fora do comum ou inovadoras, mesmo que pareçam pouco convencionais.
5. **Combine e melhore ideias:** explore a possibilidade de unir ideias ou aprimorá-las com base em contribuições adicionais.

O *Brainstorming* é uma ferramenta poderosa para explorar uma ampla gama de riscos e, quando bem conduzido, promove a colaboração e o engajamento das partes interessadas, aumentando a eficácia do processo de gestão de riscos.

7.2.2. *Brainwriting*

O *Brainwriting* é um método alternativo ao *Brainstorming* com o mesmo objetivo, a diferença é que a manifestação das ideias no *Brainstorming* ocorre verbalmente e com a técnica do *Brainwriting* ocorre por meio da escrita.

7.2.3. Entrevistas

A ferramenta de Entrevistas em gestão de riscos auxilia na identificação dos riscos associados a determinadas áreas de responsabilidade.

As entrevistas podem ser realizadas junto aos principais interessados no projeto, lideranças e especialistas no assunto, buscando identificar os riscos possíveis de antever, com foco em elencar os riscos e o que pode ser feito para evitá-los. Dessa forma, essa ferramenta contribui para a tomada das melhores decisões.

A utilização do modelo de Entrevista Semiestruturada é mais apropriada por estabelecer um roteiro prévio e ao mesmo tempo permitir perguntas fora do roteiro, além de ser um método mais flexível que proporciona um diálogo mais espontâneo.

7.2.4. Diagrama de Causa e Efeito – Ishikawa - 6M's

O diagrama de causa e efeito é uma ferramenta que pode ser utilizada para contribuir na identificação de possíveis causas para um determinado efeito.

O diagrama mostra graficamente a relação das causas com o efeito e entre si mesmas, ajudando a identificar e analisar as causas de um problema, para tanto, são analisadas as possíveis causas: materiais (insumos, matéria-prima); mão de obra (envolvidos no processo); medidas (métricas, dados que servem para avaliação e melhoria contínua); máquinas (tudo relacionado a equipamentos); métodos (relacionado a como o trabalho é realizado) e meio ambiente (influências internas e externas que podem ser consideradas causas em uma análise de riscos) .

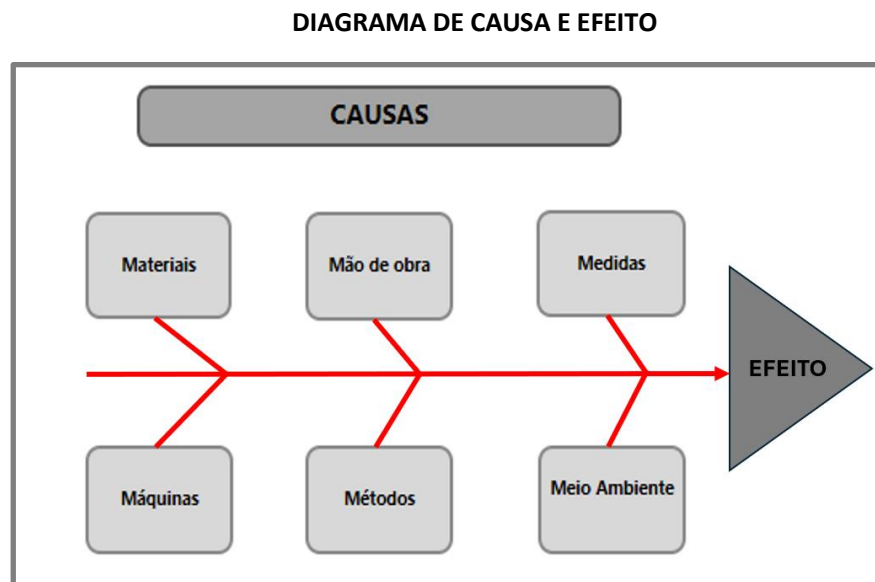


Figura 6 – Diagrama de Ishikawa

Fonte: Elaboração própria

7.3. Avaliação de Riscos: Matriz de Riscos

7.3.1. Matriz de Riscos preenchida com o Nível de Criticidade e dados da legenda

A Matriz é preenchida de acordo com o nível de criticidade (Avaliação do Nível do Risco com Análise dos Fatores de Risco) exemplificada no item 5.2.3.5., e a numeração dos riscos na legenda, para visualização do risco correspondente a criticidade apresentada na matriz.

MATRIZ DE RISCO – NÍVEL DE CRITICIDADE E DADOS DA LEGENDA

MATRIZ DE RISCO		PROBABILIDADE				
		RARA	BAIXA	MÉDIA	ALTA	MUITO ALTA
		1	2	3	4	5
IMPACTO	MUITO ALTO 5					3
	ALTO 4	4	2	1		
	MÉDIO 3	6 e 7	5 e 8	9		
	BAIXO 2					
	MUITO BAIXO 1					

Figura 7 – Matriz de Risco – Nível de Criticidade e Dados da Legenda

Exemplo: Riscos “Operacionais”

Fonte: Metodologia de Gestão de Riscos - Controladoria Geral do Estado de São Paulo (adaptado)

7.3.2. A legenda é preenchida com a finalidade de auxiliar na identificação numérica do risco disposto na Matriz de Risco.

NÚMERO	RISCO
1	Greve
2	Degradação ou paralisação do serviço
3	Descontinuidade da oferta do serviço 710
4	Descontinuidade ou redução do serviço contratado
5	Acidente
6	Perda de atratividade do serviço
7	Indisponibilidade de equipamentos de estações
8	Dano nas Instalações
9	Atraso na entrega de novas instalações

Tabela 9 – Exemplo de Legenda

Fonte: Elaboração própria

7.4. Tratamento dos Riscos: Plano de ação e Plano de Contingência

O Plano de Ação é um documento específico para prevenção e melhoria, orienta para as tomadas de decisão, é elaborado para garantir que determinado risco eleito para tratamento tenha um planejamento estruturado onde seja estabelecido foco em questões como: o quê, quando, onde, quem, por que, como e quanto custa (em inglês, *what, when, where, who, why, how* e *how much*) o tratamento proposto para determinado risco. Já o Plano de Contingência tem o enfoque em medidas emergenciais para resposta a crises com a finalidade de minimizar impactos e garantir uma resposta rápida e eficaz.

Com a utilização da ferramenta 5W e 2H é possível elaborar o plano com ênfase no risco mapeado a fim de realizar ações e prazos específicos para sua mitigação, identificação de responsáveis, mapeamento de custos e visibilidade do processo de construção da estratégia de tratamento.

8. REFERÊNCIAS BIBLIOGRÁFICAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS – ABNT. **NBR ISO/IEC 31000: Gestão de Riscos – Diretrizes**. Rio de Janeiro, 2018.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS – ABNT. **NBR ISO/IEC 31010: Gestão de Riscos - Técnicas para o Processo de Avaliação de Riscos**. Rio de Janeiro, 2021.

COSO. Committee of Sponsoring Organizations of the Treadway Commission. **Enterprise Risk Management - ERM** (Gerenciamento de Riscos Corporativos). 2017.

IIA. The Institute of Internal Auditors. **Modelo das 3 três linhas do IIA 2020 – Uma atualização das três linhas de defesa**.

BRASIL. Tribunal de Contas da União. **Referencial Básico de Gestão de Riscos**, DF, 2018.

BRASIL. Controladoria Geral da União. **Guia Prático de Gestão de Riscos para a Integridade**. Brasília, DF, 2018.

BRASIL. Controladoria Geral da União. **Manual para a Implementação de Programa de Integridade**. Brasília, DF, 2017.

BRASIL. Ministério do Desenvolvimento Regional. **Manual de Gestão de Riscos, Controles Internos e Integridade**. Brasília, DF, 2020.

Distrito Federal. Controladoria Geral do Distrito Federal. **Capacitação em Gestão de Riscos e Integridade**, 2022.

Minas Gerais. Controladoria Geral do Estado de Minas Gerais. **Guia Metodológico de Gestão de Riscos e Processos**, 2021.

São Paulo. Controladoria Geral do Estado de São Paulo. **Metodologia de Gestão de Riscos**, 2023.

São Paulo. Controladoria Geral do Estado de São Paulo. **Guia Prático de Gestão de Riscos à Integridade**, 2023.

São Paulo. Controladoria Geral do Município de São Paulo. **Manual de Gestão de Riscos**, 2023.

São Paulo. Companhia Paulista de Trens Metropolitanos. **Política de Gestão de Riscos**, 2023.

São Paulo. Companhia Paulista de Trens Metropolitanos. **Gestão de Riscos de Processo** NI 01/022, 2023.

São Paulo. Companhia Paulista de Trens Metropolitanos. **Declaração ao Apetite a Riscos**, 2022.

São Paulo. Companhia Paulista de Trens Metropolitanos. **Cartilha Gestão de Riscos de Processo**, 2024.