

1. OBJETIVO

Estabelecer as diretrizes e práticas de Conformidade, Gestão Riscos e Controle Interno adotadas pela São Paulo Transporte S/A, a seguir denominada SPTrans, nos processos de negócio prioritários.

2. BASE LEGAL E NORMATIVA

- 2.1. Lei Federal nº 6.404, de 15.12.1976, que rege estatutariamente as empresas classificadas como “Sociedades Anônimas”;
- 2.2. Lei Municipal nº 13.241, de 12.12.2001, que dispõe sobre a organização dos serviços do Sistema de Transporte Coletivo Urbano de Passageiros na Cidade de São Paulo;
- 2.3. Decreto Municipal nº 58.200, de 19.04.2018, que confere nova regulamentação à Lei Municipal nº 13.241, de 12.12.2001;
- 2.4. Lei Federal nº 13.303, de 30.06.2016, que dispõe sobre o estatuto jurídico da empresa pública, da sociedade de economia mista e de suas subsidiárias, no âmbito da União, dos Estados, do Distrito Federal e dos Municípios;
- 2.5. Lei Federal nº 13.709, de 14 de agosto de 2018, que estabelece a Lei Geral de Proteção de Dados e Segurança da Informação;
- 2.6. Decreto Municipal nº 58.093, de 20.02.2018, que dispõe sobre princípios, normas de governança e de gestão a serem observados pelas empresas públicas, sociedades de economia mista, e respectivas subsidiárias das quais o Município de São Paulo detenha o controle, aplicando-se no que couber às autarquias, fundações públicas e serviços sociais autônomos;
- 2.7. Estatuto Social, disponível no site www.sptrans.com.br no link acesso à informação e no Portal Transparência São Paulo da Prefeitura;
- 2.8. Compromisso de Desempenho Institucional, disponível no Portal Transparência São Paulo da Prefeitura;
- 2.9. Missão e Visão, disponível no site www.sptrans.com.br no link acesso à informação e no Portal Transparência São Paulo da Prefeitura;
- 2.10. Comunicado da Presidência - CDP 028/18, de 22.05.2018, que constituiu o Comitê de Conformidade, Gestão de Riscos e Controle Interno, revogado pelo CDP 082/19, de 13.11.2019 e recomposto pelo CDP 017/21, de 24.02.2021;
- 2.11. Política de Segurança da Informação, vigente, que estabelece os princípios e diretrizes estratégicas de modelo de Gestão da Segurança da Informação;

APROVAÇÕES		DATA DE DIVULGAÇÃO
DIRETORIA EXECUTIVA	CONSELHO DE ADMINISTRAÇÃO	05/05/2025

- 2.12.** Código de Conduta e Integridade, disponível no site www.sptrans.com.br no link acesso à informação e no Portal Transparência São Paulo da Prefeitura;
- 2.13.** Manual de Procedimentos – MDP, contendo as Normas e Procedimentos relativos aos processos internos de trabalho, disponível na intranet;
- 2.14.** Norma ABNT NBR ISO 31000:2018, Gestão de riscos – Princípios e diretrizes;
- 2.15.** Guia de Orientação para Gerenciamento de Riscos Corporativos do Instituto Brasileiro de Governança Corporativa – IBGC.

3. AMPLITUDE

Aplica-se ao Conselho de Administração, às Diretorias, ao Conselho Fiscal, ao Comitê de Auditoria Estatutário, ao Comitê de Conformidade, Gestão de Riscos e Controle Interno e às Áreas responsáveis pelos processos de negócio prioritários na gestão de riscos.

4. DEFINIÇÕES

- 4.1. Accountability:** é a obrigação que têm as pessoas, públicas ou privadas, às quais se tenha confiado recursos públicos, de assumir as responsabilidades de ordem fiscal, gerencial e programática que lhes foram conferidas, e de informar a sociedade e a quem lhes delegou essas responsabilidades sobre o cumprimento de objetivos, metas e o desempenho alcançado na gestão dos recursos públicos.
- 4.2. Alta Administração:** São os membros da Diretoria Executiva e do Conselho de Administração.
- 4.3. Conformidade:** é o cumprimento aos normativos internos e externos reguladores da Empresa, principalmente os inerentes ao controle interno.
- 4.4. Controle Interno:** é o conjunto de ações estruturadas e coordenadas que têm como objetivo a gestão dos riscos e o fornecimento de razoável segurança na consecução da missão da Empresa.
- 4.5. Evento:** é a ocorrência gerada com base em fontes internas e externas que pode causar impacto negativo ou positivo.
- 4.6. Gestão de riscos:** é o processo contínuo e integrado de planejar, organizar, dirigir e controlar os recursos da organização, por meio da adoção de medidas e políticas que busquem o equilíbrio entre riscos e custos.

APROVAÇÕES		DATA DE DIVULGAÇÃO
DIRETORIA EXECUTIVA	CONSELHO DE ADMINISTRAÇÃO	05/05/2025

- 4.7. Governança:** é a combinação de processos e estruturas implantadas pela Alta Administração, para informar, dirigir, administrar e monitorar as atividades da organização, com o intuito de alcançar os seus objetivos.
- 4.8. Integridade Pública:** é o alinhamento consistente e aderência a valores éticos, princípios e normas para garantir e priorizar os interesses públicos sobre os interesses privados no setor público.
- 4.9. Matriz de riscos:** é uma ferramenta utilizada para avaliação de risco.
- 4.10. Mapa de Riscos:** é uma ferramenta de visualização de informações, utilizada com o objetivo de comunicar os riscos e seus respectivos níveis, enfrentados nas diversas áreas da Empresa.
- 4.11. Mitigar:** é a ação no sentido de minimizar a probabilidade de ocorrência de riscos e o seu impacto aos objetivos da Empresa.
- 4.12. Monitoramento:** é o acompanhamento da qualidade do controle interno, visando assegurar a sua adequação aos objetivos, ao ambiente, aos recursos e aos riscos.
- 4.13. Nível do risco:** é a magnitude decorrente da ocorrência de um risco, levando em conta a combinação de seu impacto e a probabilidade de ocorrência.
- 4.14. Ocorrência:** é o acontecimento, fato sucedido ou circunstância, que origina uma mobilização.
- 4.15. Parte interessada (Stakeholder):** é a pessoa ou organização que pode afetar, ser afetada ou perceber-se afetada por uma decisão ou atividade.
- 4.16. Risco:** é a possibilidade de que um evento ocorra e afete os objetivos estratégicos da organização, por meio dos seus processos de trabalho ou projetos desenvolvidos.
- 4.17. Risco crítico:** é aquele que após o processo de Avaliação, por meio da Matriz de Riscos, apresenta um Nível de Risco alto, resultante da combinação dos graus de impacto e possibilidade – que evidencia um potencial de impacto significativo ou catastrófico sobre os objetivos e operações da Empresa, notadamente aqueles vinculados à missão e valores da Empresa.
- 4.18. Riscos de interesse:** é aquele que após o processo de Avaliação, por meio da Matriz de Riscos, apresenta um Nível de Risco médio ou inferior, porém, sua materialização pode resultar em consequências expressivas e, dessa forma, deve ser monitorado continuamente.
- 4.19. Risco residual:** é aquele ao qual a Empresa está exposta após a implementação de ações gerenciais para tratamento de um ou mais riscos previamente identificados.

APROVAÇÕES		DATA DE DIVULGAÇÃO
DIRETORIA EXECUTIVA	CONSELHO DE ADMINISTRAÇÃO	05/05/2025

5. DIRETRIZES E CRITÉRIOS

5.1. Principais Pilares

Constituem os principais norteadores desta Política:

- Comprometimento da Alta Administração com as iniciativas e mecanismos propostos com os temas correlacionados a este instrumento;
- Análise de eventos que impactem os principais processo de negócio da Empresa;
- Aderência à integridade, aos valores éticos e às melhores práticas;
- Fomento de mecanismos que minimizem riscos negativos e assegurem processos com razoável nível de segurança;
- Fomento aos comportamentos e comprometimento que criam e sustentam a conformidade, de modo a garantir a imparcialidade em todas as suas operações;
- Garantir comunicação e treinamentos internos necessários;
- Dispor de um canal para que possam ser realizadas denúncias, assim como os procedimentos e boas práticas para averiguações necessárias sobre comportamentos ilícitos ou antiéticos; e
- Processos, periódicos, para identificar a efetividade dos pilares da Política e Programa correlatos.

5.2. Natureza de Riscos

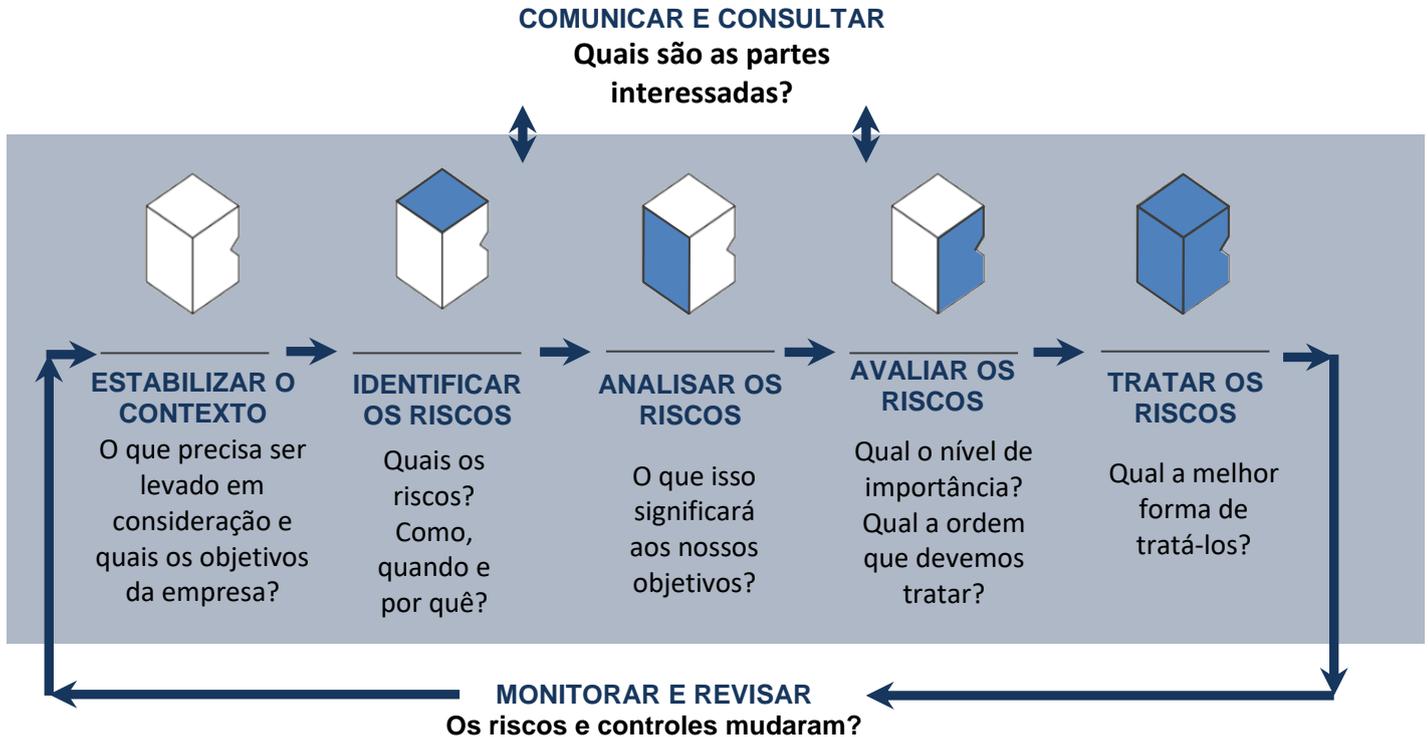
No processo de gestão de riscos a SPTrans adota os seguintes grupos:

Tipo de Natureza	Características
Estratégicos	Decorrentes na execução do plano de negócios e da estratégia da SPTrans, sejam eles: tomada de decisões ruins de negócios, ineficácia e ineficiência na implantação de novas decisões de negócios, alocação inadequada de recursos ou falha em responder adequadamente as mudanças no ambiente de negócios.
Financeiros	Decorrentes das operações financeiras da SPTrans, riscos de crédito e riscos de liquidez, incluindo a confiabilidade das informações constantes nos relatórios financeiros divulgados.
Operacionais	Relacionados às falhas e inadequações nos processos de trabalho, pessoas e sistemas.
Conformidade	Não cumprimento da legislação, normas técnicas, acordos, regulamentos, código de conduta e integridade.

APROVAÇÕES		DATA DE DIVULGAÇÃO
DIRETORIA EXECUTIVA	CONSELHO DE ADMINISTRAÇÃO	05/05/2025

5.3. Ciclo da Gestão de Riscos

Na SPTrans o Ciclo de Gestão de Riscos está representado, esquematicamente, da seguinte forma:



5.4. Linhas de Defesa

Estão diretamente relacionadas à prática de controles internos e servem de auxílio na identificação de estruturas e processos que atuam no atingimento dos objetivos.

5.4.1. Primeira Linha

Funções que gerenciam e têm propriedade de riscos: gestão operacional e procedimentos rotineiros de riscos e controles internos da Gestão de Riscos. É o nível no qual se identificam, avaliam e mitigam riscos mediante o desenvolvimento e a implementação de políticas e procedimentos internos que ofereçam garantia razoável de que as atividades estejam em conformidade com as metas e os objetivos institucionais.

APROVAÇÕES		DATA DE DIVULGAÇÃO
DIRETORIA EXECUTIVA	CONSELHO DE ADMINISTRAÇÃO	05/05/2025

5.4.2. Segunda Linha

Funções que supervisionam riscos: constituída por unidades, comitês ou outras estruturas organizacionais que garantam o funcionamento da primeira linha quanto à gestão de riscos e controles. São, por natureza, funções de gestão, e possuem o papel de coordenar as atividades de gestão de riscos; orientar e fornecer ferramentas e metodologia aos gestores operacionais (primeira linha) para a identificação e avaliação dos riscos; apoiar a definição de metas de exposição a risco; monitorar riscos específicos; auxiliar na definição de ações adotadas pela primeira linha; facilitar, apoiar e monitorar as atividades de gestão de riscos; apoiar as atividades da auditoria interna (terceira linha) no acompanhamento e auxílio na gestão de riscos e controle interno em todos os níveis da estrutura organizacional da entidade; e alertar a gestão operacional para questões em desenvolvimento e para mudanças no cenário dos riscos.

5.4.3. Terceira Linha

Funções que fornecem avaliações independentes: papel exercido pela auditoria interna, que fornece avaliações (asseguração) independentes e objetivas sobre os processos de gerenciamento de riscos, controles internos e governança aos órgãos de governança e à alta administração, abrangendo uma grande variedade de objetivos (incluindo eficiência e eficácia das operações; salvaguarda de ativos; confiabilidade e integridade dos processos de reporte; conformidade com leis e regulamentos) e elementos da estrutura de gestão de riscos e controle interno em todos os níveis da estrutura organizacional da entidade.

6. COMPETÊNCIAS

6.1. Conselho de Administração

Compete ao Conselho de Administração as seguintes atribuições:

- a. Aprovar a Política de Conformidade e Gerenciamento de Riscos, encaminhada pela Diretoria Executiva;
- b. Implementar e supervisionar o sistema de Gestão de Riscos e de Controle Interno estabelecido para prevenção e mitigação dos principais riscos, em especial os relacionados à integridade das informações contábeis e financeiras e os relacionados à ocorrência de corrupção e fraude.

APROVAÇÕES		DATA DE DIVULGAÇÃO
DIRETORIA EXECUTIVA	CONSELHO DE ADMINISTRAÇÃO	05/05/2025

6.2. Diretoria Executiva

Compete à Diretoria Executiva as seguintes atribuições:

- a. Aprovar a Política de Conformidade e Gerenciamento de Riscos proposta pelo Comitê.
- b. Deliberar sobre a implantação do Sistema de Gestão de Riscos e de Controle Interno da SPTrans para posterior aprovação do Conselho de Administração;
- c. Aprovar os relatórios periódicos elaborados pelo Comitê, para posterior aprovação do Conselho de Administração.

6.3. Conselho Fiscal

Compete ao Conselho Fiscal as seguintes atribuições:

- a. Fiscalizar, por qualquer de seus membros, os atos dos administradores e verificar o cumprimento dos seus deveres legais e estatutários;
- b. Acompanhar os relatórios de atividades da Auditoria Interna e da área de conformidade, gestão de riscos e controle interno;
- c. Reunir-se periodicamente com a auditoria interna e com a área de conformidade, gestão de risco e controle interno.

6.4. Comitê de Auditoria Estatutário

Compete ao Comitê de Auditoria Estatutária as seguintes atribuições:

- a. Assessorar o Conselho de Administração auxiliando no monitoramento das ações desenvolvidas nos temas desta política;
- b. Supervisionar as atividades dos auditores independentes, avaliando sua independência, a qualidade dos serviços prestados e a adequação de tais serviços às necessidades da Sociedade;
- c. Supervisionar as atividades desenvolvidas nas áreas de controle interno, de auditoria interna e de elaboração das demonstrações financeiras da Sociedade;
- d. Receber da Ouvidoria denúncias, inclusive sigilosas, internas e externas à Sociedade, em matérias relacionadas ao escopo de suas atividades;
- e. Monitorar a qualidade e a integridade dos mecanismos de controle interno, das demonstrações financeiras e das informações e medições divulgadas pela Sociedade;
- f. Avaliar e monitorar exposições de risco da Companhia, podendo requerer, entre outras, informações detalhadas sobre políticas e procedimentos;
- g. Avaliar e monitorar, em conjunto com a administração e a área de auditoria interna, a adequação das transações com partes relacionadas.

APROVAÇÕES		DATA DE DIVULGAÇÃO
DIRETORIA EXECUTIVA	CONSELHO DE ADMINISTRAÇÃO	05/05/2025

6.5. Área de Conformidade, Gestão de Riscos e Controle Interno

Compete à Área de Conformidade, Gestão de Riscos e Controle Interno as seguintes atribuições:

- a. Propor políticas de Conformidade e Gerenciamento de Riscos e comunicá-las a todo o corpo funcional da organização;
- b. Verificar a aderência da estrutura organizacional e dos processos, produtos e serviços da empresa às leis, normativos, políticas e diretrizes internas e demais regulamentos aplicáveis;
- c. Comunicar à Diretoria, aos Conselhos de Administração e Fiscal e ao Comitê de Auditoria Estatutário a ocorrência de ato ou conduta em desacordo com as normas aplicáveis à empresa;
- d. Verificar a aplicação adequada do princípio da segregação de funções, de forma que seja evitada a ocorrência de conflitos de interesse e fraudes;
- e. Elaborar, divulgar e verificar o cumprimento do Código de Conduta e Integridade;
- f. Estabelecer mecanismos destinados à proteção de denunciante de boa-fé;
- g. Propor procedimentos que assegurem a pronta interrupção de irregularidades ou infrações detectadas e a tempestiva remediação dos danos gerados;
- h. Coordenar os processos de identificação, classificação e avaliação dos riscos a que está sujeita a Sociedade;
- i. Coordenar a elaboração e monitorar os planos de ação para mitigação dos riscos identificados, verificando continuamente a adequação e a eficácia da gestão de riscos;
- j. Estabelecer planos de contingência para os principais processos de trabalho da organização;
- k. Elaborar relatórios periódicos de suas atividades, submetendo-os à Diretoria, aos Conselhos de Administração e Fiscal e ao Comitê de Auditoria;
- l. Garantir a transparência da pessoa jurídica;
- m. Garantir a confiabilidade dos indicadores de desempenho da entidade;
- n. Outras atividades correlatas definidas pelo Diretor Estatutário.

6.6. Auditoria Interna

Compete à Auditoria Interna as seguintes atribuições:

- a. Avaliar a conformidade dos trabalhos, processos e resultados da Sociedade com as normas, regulamentos internos e legislação específica;

APROVAÇÕES		DATA DE DIVULGAÇÃO
DIRETORIA EXECUTIVA	CONSELHO DE ADMINISTRAÇÃO	05/05/2025

- b. Aferir a adequação do controle interno, a efetividade do gerenciamento dos riscos e dos processos de governança e a confiabilidade do processo de coleta, mensuração, classificação, acumulação, registro e divulgação de eventos e transações, visando ao preparo de demonstrações financeiras.

6.7. Ouvidoria

Compete à Ouvidoria as seguintes atribuições:

- a. Atender, acompanhar e responder às reclamações, solicitações, denúncias, sugestões e elogios relativos a serviços prestados pela SPTrans, atuando como canal de segunda instância;
- b. Gerir o canal de denúncias que possibilite o recebimento de denúncias internas e externas relativas ao descumprimento do Código de Conduta e Integridade e das demais normas internas de ética e obrigacionais;
- c. Apoiar na elaboração do Código de Conduta e Integridade;
- d. Remeter ao Comitê de Auditoria Estatutário denúncias, inclusive sigilosas, internas e externas à sociedade, em matérias relacionadas ao escopo de suas atividades;
- e. Apoiar no estabelecimento de mecanismos destinados à proteção de denunciante de boa-fé;
- f. Padronizar e manter atualizados os procedimentos para atendimento e tratamento das manifestações;
- g. Manter estatísticas das manifestações registradas, com divulgação interna e externa das informações, visando proporcionar a avaliação dos serviços pela Administração e a transparência pública.

6.8. Comitê de Conformidade, Gestão de Riscos e Controle Interno

O Comitê de Conformidade, Gestão de Riscos e Controle Interno, vinculado à Diretoria da Presidência, sob liderança do Diretor de Planejamento de Transporte, têm as seguintes atribuições:

- a. Zelar pelo cumprimento das políticas de conformidade e gestão de riscos estabelecidas na SPTrans;
- b. Auxiliar a Área de *Compliance* no monitoramento da adequação e efetividade dos processos de conformidade e gestão de riscos no âmbito da organização;
- c. Manifestar-se sobre metodologias de gerenciamento de riscos adotadas e relatórios de gestão de risco;
- d. Manifestar-se sobre políticas e diretrizes inerentes à conformidade, gestão de riscos e controle interno;

APROVAÇÕES		DATA DE DIVULGAÇÃO
DIRETORIA EXECUTIVA	CONSELHO DE ADMINISTRAÇÃO	05/05/2025

- e. Monitorar ações visando o enquadramento, a adequação e a mitigação dos riscos que apresentam níveis acima do tolerado;
- f. Prestar apoio à Área de *Compliance* em assuntos de conformidade, gestão de riscos e controle interno;
- g. Elaborar relatórios e pareceres sobre matérias submetidas ao Comitê;
- h. Propor treinamentos e atividades voltadas ao desenvolvimento e capacitação dos membros do Comitê e dos Grupos de Trabalho para exercício de suas atribuições;
- i. Manter atas das reuniões, de relatórios e pareceres sobre demandas específicas para o Comitê registradas e disponibilizadas.

7. DISPOSIÇÕES FINAIS

7.1. No cumprimento da presente Política devem ser considerados o conjunto de Normas e Procedimentos da Empresa, e o Código de Conduta e Integridade.

7.2. Casos omissos e demais dúvidas correlacionadas devem ser submetidas à Diretoria Executiva para deliberação e aprovação.

8. APROVAÇÕES

Esta Política de Conformidade, Gestão de Riscos e Controle Interno foi aprovada pela Diretoria Executiva em 27 de março de 2025 e pelo Conselho de Administração em 29 de abril de 2025.

9. REVISÕES

HISTÓRICO DE REVISÕES		
REVISÃO	DATA	ALTERAÇÃO
0	18.06.2018	Emissão inicial.
1	29.04.2025	Atualização da Base Legal, da Amplitude e de Definições, inclusão dos principais pilares da Política, do Ciclo do Processo de Gestão de Riscos e das Linhas de Defesa, detalhamento das características da Natureza de Riscos e inclusão de Competências do CAE, Conselho Fiscal e das Áreas prioritárias na gestão de risco.

APROVAÇÕES		DATA DE DIVULGAÇÃO
DIRETORIA EXECUTIVA	CONSELHO DE ADMINISTRAÇÃO	05/05/2025