CETESB

COMPANHIA AMBIENTAL DO ESTADO DE SÃO PAULO

Referente ao Relatório à Diretoria Nº 027/2024/P, de 18/11/2024. (SEI 385.00001801/2024-18)

Relator: Thomaz Miazaki de Toledo.

DECISÃO DE DIRETORIA Nº 091/2024/P, de 21 de novembro de 2024.

Dispõe sobre a aprovação da "Política de Gestão de Riscos e Controles Internos" da CETESB – Companhia Ambiental do Estado de São Paulo.

A Diretoria Colegiada da CETESB - Companhia Ambiental do Estado de São Paulo, no uso de suas atribuições estatutárias e regulamentares, e considerando o contido no Relatório à Diretoria nº 027/2024/P, que acolhe, **DECIDE**:

Artigo 1º: Aprovar a *"Política de Gestão de Riscos e Controles Internos"*, constante do **ANEXO ÚNICO** que integra esta Decisão de Diretoria.

Artigo 2º: Esta Decisão de Diretoria entra em vigor após a necessária manifestação do CA – Conselho de Administração da CETESB, de acordo com as normas estatutárias.

Divulgue-se a todos os empregados da Companhia pelo sistema eletrônico e no Portal da CETESB na Internet.

Diretoria Colegiada da CETESB, em 21 de novembro de 2024.

ORIGINAL DEVIDAMENTE ASSINADO

THOMAZ MIAZAKI DE TOLEDO
Diretor-Presidente

ORIGINAL DEVIDAMENTE ASSINADO

THOMAZ MIAZAKI DE TOLEDO
Diretor de Gestão Corporativa e Sustentabilidade, em exercício

ORIGINAL DEVIDAMENTE ASSINADO

ADRIANO RAFAEL ARREPIA DE QUEIROZ
Diretor de Controle e Licenciamento Ambiental,

ORIGINAL DEVIDAMENTE ASSINADO

CAROLINA FIORILLO MARIANI
Diretora de Qualidade Ambiental

ORIGINAL DEVIDAMENTE ASSINADO

MAYLA MATSUZAKI FUKUSHIMA
Diretora de Avaliação de Impacto Ambiental

ANEXO ÚNICO

(a que se refere o artigo 1º da Decisão de Diretoria nº 091/2024/P, de 21/11/2024)

CETESB

COMPANHIA AMBIENTAL DO ESTADO DE SÃO PAULO

POLÍTICA DE GESTÃO DE RISCOS E CONTROLES INTERNOS

Aprovada na 607ª Reunião do Conselho de Administração, realizada em 26/11/2024.

Novembro/2024

POLÍTICA DE GESTÃO DE RISCOS E CONTROLE INTERNOS

1. OBJETIVO

Esta Política visa estabelecer princípios e diretrizes para a gestão de riscos e controles internos da CETESB – Companhia Ambiental do Estado de São Paulo em conformidade com a Lei nº 13.303/2016 e demais normativas aplicáveis.

2. ABRANGÊNCIA

A política se aplica de forma abrangente a toda a estrutura organizacional da CETESB, envolvendo uma ampla gama de indivíduos e funções, incluindo, mas não se limitando a: diretores e membros dos conselhos, membros dos comitês, ocupantes das funções de confiança e cargos comissionados "Ad nutum", empregados em geral, incluindo os cedidos pela e para a Companhia e os licenciados por qualquer motivo, colaboradores, estagiários, aprendizes e demais partes interessadas.

3. CONCEITOS

Para fins da presente Política, devem ser observados os seguintes conceitos:

Alta administração: composta pelo Conselho de Administração e pela Diretoria Colegiada. O Conselho de Administração é órgão colegiado de deliberação, responsável por fixar a orientação geral dos negócios da companhia, e fiscalizar a gestão, incluindo a gestão de riscos e controles. Já a Diretoria Colegiada é o órgão colegiado, incumbido de administrar e representar a Companhia.

Ação mitigatória: medida, adotada pela CETESB, para redução da exposição organizacional ao risco e que busca atenuar a respectiva possibilidade de materialização.

Apetite ao risco: quantidade e tipo de riscos que a CETESB está disposta a buscar ou aceitar.

Controle: política ou um procedimento que integra o controle interno.

Controle interno: é integrado ao processo de gestão, em todas as áreas e níveis da organização, sendo desenvolvido para proporcionar segurança razoável com respeito à realização dos objetivos relacionados às operações, à divulgação e à conformidade.

POLÍTICA DE GESTÃO DE RISCOS E CONTROLE INTERNOS

Estrutura de governança: regulada pela Lei nº 13.303/2016, é composta por órgãos colegiados e independentes que têm a função de orientar, administrar e fiscalizar a gestão da CETESB, garantindo a transparência, a eficiência e a responsabilidade na condução dos negócios.

Gestão de riscos: atividades coordenadas para dirigir e controlar uma organização com uma abordagem para riscos.

Gerenciamento de riscos: atividades de identificar, analisar, avaliar, tratar e monitorar os riscos.

Indicador de risco: métrica utilizada para monitorar e analisar a variação dos riscos corporativos, os quais são mapeados a partir de dados obtidos no ambiente interno e externo à Companhia.

Impacto: consequência sobre os objetivos, resultante da ocorrência do evento.

Integridade: a qualidade ou o estado de possuir princípios morais elevados, incluindo retidão, honestidade e sinceridade, bem como o desejo de fazer aquilo que é certo, professando e vivendo de acordo com um conjunto de valores e expectativas.

Matriz de riscos: representação gráfica da exposição organizacional aos riscos corporativos identificados pela CETESB, de acordo com a criticidade correspondente, estabelecida pela multiplicação do impacto pela probabilidade.

Política de Gestão de Riscos: declaração de intenções e diretrizes gerais de uma organização sobre gestão de riscos.

Risco: são eventos futuros e incertos que têm o potencial de impactar negativamente seus resultados, sua reputação perante o público interno/externo ou sua segurança.

Risco inerente: risco a que uma organização está exposta sem considerar quaisquer medidas de controle que possam reduzir a probabilidade de sua ocorrência ou seu impacto.

Risco residual: o risco à realização dos objetivos que permanece após as medidas de controle terem sido desenhadas e implementadas.

Tolerância ao risco: é o nível de variação aceitável para alcançar um objetivo.

POLÍTICA DE GESTÃO DE RISCOS E CONTROLE INTERNOS

4. PRINCÍPIOS

A gestão de riscos e controles internos da Companhia deve observar os seguintes princípios:

I. Comprometimento da alta administração com a Gestão de Riscos e Controles Internos da Companhia;
II. Independência da estrutura de governança em relação aos seus membros para supervisão do desenvolvimento e desempenho da gestão de riscos e dos controles internos.
III. Adoção da abordagem por linhas de defesa, que contempla a atuação integrada entre: gestão dos processos, controles internos, gestão de riscos e conformidade e a Auditoria Interna;
IV. Compromisso de todos os colaboradores com a gestão de riscos e com os controles internos;
V. Linguagem comum sobre Gestão de Riscos e Controles Internos em toda a CETESB;
VI. Gestão integrada de riscos em todos os processos organizacionais;
VII. Garantia do cumprimento das normas e regulamentos, bem como a aderência às políticas e procedimentos internos, com a integridade e valores éticos;
VIII. Transparência e Integridade das informações;
IX. Prestação de Contas e Responsabilidade pelas decisões tomadas *(Accountability)*; e
X. Diversidade, inclusão e direitos humanos.

5. DIRETRIZES

I. A estrutura de gerenciamento de risco da CETESB é organizada e estruturada de acordo com os princípios e metodologias estabelecidos pelo COSO (Committee of Sponsoring Organizations of the Treadway Commission) e pela ABNT NBR ISO (International Organization for Standardization). Essas abordagens garantem que os processos de gerenciamento de risco sejam abrangentes e alinhados com as melhores práticas, facilitando a identificação, análise, avaliação e mitigação de riscos associados às operações da CETESB.
II. Ao aderir à estrutura COSO, a Companhia visa aprimorar seus controles internos e governança geral, enquanto os padrões ISO fornecem um método sistemático para gerenciar riscos de forma eficaz. Essa estrutura dupla não apenas fortalece a sustentabilidade da

CETESB, mas também promove transparência e responsabilidade em suas práticas de gerenciamento de risco.

III. A Gestão de Riscos deve ser integrada em todos os processos da organização, inclusive para basear as tomadas de decisões em todos os níveis, para garantir a identificação, análise, avaliação, mitigação e monitoramento de riscos, que impactem no alcance dos objetivos estratégicos da Companhia, assegurando a sua integridade, a transparência e a eficiência dos processos internos.

IV. O processo de Gestão de Riscos e Controles Internos da CETESB é projetado para ser abrangente, sistemático e fundamentado por metodologia definida que será efetivamente comunicada e disseminada por toda a organização.

V. O ciclo de gestão de riscos terá uma periodicidade de execução anual. Essa regularidade garante que as práticas de gestão de riscos permaneçam atualizadas e responsivas ao ambiente em implementação.

VI. A CETESB implementará treinamentos e recursos para promover a conscientização e o entendimento da metodologia estabelecida. O compromisso em estabelecer uma estrutura de gestão de riscos coesa é essencial para promover uma cultura de responsabilidade e gestão de riscos proativa.

5.1. PROCESSO DE GESTÃO DE RISCOS

Figura 1 - Processo de Gestão de Riscos ABNT NBR ISO 31000 (Adaptado).

O processo de gestão de riscos da CETESB, é projetado para ser abrangente e sistemático, considerando as etapas essenciais para garantir a mitigação eficaz de riscos. O processo inclui os seguintes estágios principais:

I. **Entendimento do contexto** - etapa inicial que envolve a identificação dos objetivos relevantes para os processos organizacionais e a definição dos contextos externos e internos que influenciam o gerenciamento de risco. Entender o contexto é crucial para adaptar estratégias de gerenciamento de risco que se alinhem com as metas da CETESB.

II. **Identificação de riscos** - nesta fase, os eventos de riscos potenciais que podem impactar os objetivos da CETESB são sistematicamente identificados. Os riscos são categorizados em vários tipos, incluindo riscos estratégicos, operacionais, financeiros,

de reputação, relacionados à conformidade, relacionados à integridade e riscos de segurança e privacidade da informação. Esta categorização auxilia no foco adequado dos esforços de gerenciamento de risco.

III. **Análise de riscos** - envolve um exame completo dos riscos identificados, incluindo as causas subjacentes e as consequências potenciais de cada um deles. Ao analisar os riscos em detalhes, a CETESB pode entender melhor suas implicações e se preparar para respostas eficazes.

IV. **Avaliação de riscos** – nessa etapa, os riscos identificados são avaliados com base na probabilidade de ocorrência e no impacto potencial na organização. Esta avaliação ajuda a determinar a gravidade de cada risco e a urgência necessária para lidar com eles.

V. **Tratamento de riscos** - após avaliar os riscos, os gestores do risco, desenvolvem e implementam estratégias para gerenciá-los de forma eficaz. As opções para tratamento de risco incluem mitigar o risco, compartilhá-lo com outras partes, aceitá-lo ou evitá-lo completamente, dependendo da natureza do processo organizacional e gravidade do risco.

VI. **Priorização de riscos** - esta etapa envolve definir quais riscos exigem atenção imediata com base nos níveis de risco calculados (produto da probabilidade e impacto), priorizando especificamente aqueles categorizados como "Alto" e "Muito Alto". No entanto, outros riscos podem ser priorizados conforme o entendimento de sua relevância, permitindo que recursos sejam alocados de forma eficaz para lidar com problemas críticos

VII. **Monitoramento e revisão** – este estágio inclui, o envolvimento contínuo com todas as partes interessadas para o monitoramento contínuo dos riscos identificados, a revisão da eficácia dos controles existentes e o ajuste das estratégias de tratamento de risco conforme necessário para promover a melhoria contínua. Além de revisões regulares para assegurar que a estrutura de gerenciamento de riscos permaneça dinâmica e responsiva a mudanças.

VIII. **Comunicação e consulta** – a transparência é vital para gerenciar riscos de forma eficaz e, por isso, nesse momento, a CETESB enfatiza a comunicação clara de riscos

e as ações tomadas para mitigá-los com todas as partes interessadas em todas as etapas do processo de gerenciamento de riscos. Essa comunicação é conduzida de forma aberta e objetiva, promovendo uma cultura de confiança e colaboração.

Em resumo, a abordagem estruturada para gerenciamento de riscos na CETESB não apenas aprimora a capacidade da Companhia de abordar desafios potenciais, mas também promove uma cultura proativa de conscientização de riscos e responsabilidade entre todos os envolvidos.

5.2. CONTROLES INTERNOS

O sistema de controles internos da CETESB compreende um conjunto abrangente de procedimentos e medidas projetados para mitigar riscos, proteger ativos, garantir a precisão e confiabilidade das informações financeiras e aumentar a eficiência e eficácia das operações.

A gestão desses controles internos deve aderir às seguintes diretrizes:

I. **Integração de recursos** - a estrutura de controle interno deve integrar perfeitamente políticas, planos, ações, atividades, sistemas e recursos institucionais para criar uma abordagem coesa à gestão de riscos.
II. **Adoção de metodologia de gestão** - o processo de controle interno deve ser definido e sistematizado com apoio de metodologia e boas práticas. Essa metodologia deve incorporar a gestão de riscos estabelecida pela CETESB e estar em conformidade com todas as leis, padrões e estruturas aplicáveis para garantir o alinhamento legal e operacional.
III. **Estabelecimento de controles preventivos e corretivos** - é essencial institucionalizar a aplicabilidade do processo de controle interno implementando controles preventivos, que abordam os riscos antes que eles se materializem, e controles corretivos, que são aplicados após a ocorrência de um risco.
IV. **Natureza Preventiva dos Controles** - o processo de controle interno deve focar principalmente em medidas preventivas, ser exercido continuamente e ter como

objetivo corrigir quaisquer desvios dos parâmetros estabelecidos. Essa abordagem posiciona os controles internos como instrumentos vitais de gestão.

V. **Condições Efetivas de Implementação** - é necessário criar as condições apropriadas para a implementação bem-sucedida de procedimentos de controle interno que integrem efetivamente as práticas de gerenciamento de risco. Isso garante que os controles internos não sejam apenas operacionais, mas também responsivos ao cenário de risco da organização.

Ao aderir a essas diretrizes, a CETESB aprimora seu ambiente de controle interno, promovendo uma cultura de responsabilização e garantindo que a organização gerencie riscos de forma eficaz ao atingir seus objetivos operacionais.

6. ESTRUTURA PARA GESTÃO DE RISCOS E CONTROLES INTERNOS

A gestão de riscos é um aspecto fundamental da governança eficaz. Sendo assim, a estrutura para gestão de riscos e controles internos na CETESB é fundamentada no modelo de três linhas de defesa[1], ilustrado a seguir:

Figura 2 - Modelo das três linhas do The IIA

[1] IIA. Declaração de Posicionamento do IIA: As três linhas de defesa no gerenciamento eficaz de riscos e controles. TCU. 2013

I. **Primeira linha de defesa (Gerenciamento operacional)** – gestores operacionais que detêm a propriedade dos riscos e controles dentro de seus processos. Eles são responsáveis pelo gerenciamento abrangente dos riscos do processo, o que inclui identificar, analisar, avaliar, tratar e monitorar esses riscos. Seu envolvimento direto garante que o gerenciamento de riscos seja parte integrante das atividades operacionais, aumentando a resiliência geral da organização.

II. **Segunda linha de defesa (Gerenciamento de Riscos e Conformidade)** – a função na CETESB é incorporada pela Divisão de Conformidade e Gestão de Riscos, que é a responsável por fornecer a experiência e suporte essenciais para o gerenciamento operacional, oferecendo orientação sobre questões de risco e controle. Ela desempenha um papel crítico no monitoramento da primeira linha de defesa para garantir que as práticas de gerenciamento de riscos sejam executadas de forma eficiente e eficaz. Ao questionar e dar suporte à gestão operacional, a segunda linha ajuda a reforçar a estrutura de gestão de risco da organização; e

III. **Terceira linha de defesa (Auditoria Interna)** – a função de auditoria interna é oferecer avaliações independentes sobre o alcance de objetivos estratégicos e metas organizacionais. Eles fornecem avaliações abrangentes ao órgão de governança e à alta administração, garantindo um alto nível de independência e objetividade que não está presente na segunda linha de defesa. Seus *insights* são vitais para identificar áreas de melhoria e aprimorar a governança geral.

O modelo de três linhas de defesa, apoiado por uma estrutura de governança robusta e o envolvimento de auditores independentes, garante que a CETESB gerencie riscos de forma eficaz, alinhando-se aos seus objetivos estratégicos. Essa abordagem estruturada promove a responsabilização e apoia uma cultura de melhoria contínua dentro da organização:

I. **Estrutura de Governança –** inclui a alta administração e os órgãos de governança responsáveis por estabelecer os objetivos da organização. Eles definem estratégias para atingir esses objetivos e criam processos de governança que facilitam a gestão de

risco eficaz. Essa liderança é crucial para promover uma cultura de responsabilidade e gestão de risco proativa em toda a organização.

II. **Auditoria independente e órgãos externos –** auditores independentes e órgãos externos servem como linhas adicionais de defesa dentro da estrutura de gestão de risco. Eles fornecem avaliações objetivas às partes interessadas da organização, incluindo o órgão de governança e a alta gerência. Suas avaliações contribuem para uma compreensão mais abrangente do cenário de risco da organização e aumentam a transparência para as partes interessadas.

Diante disso, a divisão de responsabilidades específicas e a coordenação entre funções de gerenciamento de riscos na CETESB são imprescindíveis para que o papel inerente de cada grupo no processo de gerenciamento de riscos seja coordenado adequadamente, conforme tabela abaixo:

Primeira Linha de Defesa	Segunda Linha de Defesa	Terceira Linha de Defesa
Proprietários/ Gestores dos riscos	**Controle de Risco e Conformidade**	**Avaliação de Riscos e Controles**
• Gestão Operacional.	• Independência limitada; e • Reporte inicial a gestão.	• Auditoria Interna; • Independência; e • Reporte à governança.

Tabela 1 - Coordenar as três linhas. Fonte: IIA.

7. RESPONSABILIDADES

1.1. ESTRUTURA DE GOVERNANÇA

7.1.1. CONSELHO DE ADMINISTRAÇÃO

I. Aprovar, mediante proposta da Diretoria Colegiada, a Política de Gestão Riscos e Controles Internos;

II. Definir os limites de apetite a riscos; e

III. Supervisionar os sistemas de gestão de riscos e controles internos, mediante relatórios e reportes submetidos pela Divisão de Conformidade e Gestão de Riscos.

7.1.2. COMITÊ DE AUDITORIA

I. Assessorar o Conselho de Administração no que for pertinente ao processo de gestão de Riscos e Controles Internos da CETESB.

7.1.3. CONSELHO FISCAL

I. Contribuir com o processo de gestão de riscos, com o registro da matéria em ata, as informações que forem pertinentes ao Processo de Gestão de Riscos e Controles Internos da CETESB.

7.1.4. DIRETORIA COLEGIADA

I. Garantir o cumprimento da Política de Gestão de Riscos e Controles Internos da CETESB e os normativos relacionados à gestão de riscos e controles internos;
II. Avaliar e aprovar o escopo para início dos trabalhos de gerenciamento de riscos;
III. Tomar conhecimento e supervisionar os trabalhos pertinentes à gestão de riscos;
IV. Supervisionar a gestão de riscos e controles internos das áreas;
V. Avaliar a efetividade do Processo de Gestão de Riscos e Controles Internos, por meio de monitoramento dos resultados, anualmente;
VI. Submeter com apoio da Divisão de Conformidade e Gestão de Riscos (PMC) os resultados validados da Gestão de Riscos e Controles Internos para o Conselho de Administração; e
VII. Aprovar normas específicas de Riscos.

7.1.5. SECRETARIA EXECUTIVA DA GOVERNANÇA:

I. Orientar os membros dos órgãos de governança sobre o processo de gestão de riscos;

II. Apoiar estrategicamente na gestão da informação sobre Gestão de Riscos e Controles Internos a Estrutura de Governança; e

III. Assessorar a Divisão de Conformidade e Gestão de Riscos (PMC) no que for pertinente às matérias que são submetidas à estrutura de governança.

7.2. ESTRUTURA DE GESTÃO

7.2.1. GESTÃO OPERACIONAL (GESTORES DONOS DO PROCESSO):

IV. Identificar, analisar e avaliar os riscos inerentes dos processos sob sua responsabilidade, visando adotar medidas de controle que previnam o comprometimento na prestação de serviço público;

V. Tratar os riscos em seus processos organizacionais bem como estabelecer ações de mitigação para os riscos considerados priorizados;

VI. Assegurar que o risco dos processos sob sua responsabilidade seja gerenciado conforme a Política de Gestão de Riscos e o Programa de Integridade da CETESB;

VII. Disseminar a cultura de riscos e controles internos no âmbito da CETESB;

VIII. Monitorar os riscos para garantir que as respostas adotadas mantenham os níveis de risco adequados, conforme a Política de Riscos e Controles Internos e o Programa de Integridade;

IX. Garantir que as informações sobre o gerenciamento de riscos sejam disponibilizadas às instâncias competentes; e

X. Realizar a gestão integrada dos riscos dos processos sob sua responsabilidade que envolvam mais de uma instância.

7.3. INSTÂNCIAS INTERNAS DE APOIO A GESTÃO DE RISCOS E CONTROLES INTERNOS

7.3.1. DIVISÃO DE CONFORMIDADE E GESTÃO DE RISCOS (PMC)

I. Atuar como segunda linha de defesa, no fornecimento da expertise, apoio, monitoramento e questionamento quanto ao gerenciamento de riscos realizado pela gestão operacional;
II. Estabelecer e revisar continuamente a Política de Gestão de Riscos e Controles Internos da CETESB;
III. Orientar e fornecer metodologia e procedimentos de gestão de riscos de integridade, de avaliação e de monitoramento do Programa de Integridade da Companhia;
IV. Coordenar o desenvolvimento e adequação do gerenciamento de riscos e controles internos na CETESB;
V. Propor o escopo para início dos trabalhos de gerenciamento de riscos e controles internos
VI. Facilitar a implementação de práticas eficazes de gerenciamento de riscos por parte da gerência operacional;
VII. Monitorar e avaliar criticamente as situações dos riscos dos processos corporativos;
VIII. Monitorar e comunicar as situações de riscos de integridade da CETESB;
IX. Monitorar e acompanhar os planos de ação mitigatória;
X. Consultar e comunicar os resultados dos trabalhos realizados, à Diretoria responsável pela área gestora do risco, por meio da Matriz de Riscos, contendo a classificação dos níveis de riscos como baixo, moderado, alto e muito alto;
XI. Disseminar a cultura de riscos e controles internos no âmbito da CETESB; e
XII. Elaborar relatórios das atividades, submetendo-os à Diretoria Colegiada, Conselho de Administração, Conselho Fiscal e Comitê de Auditoria.

7.4. AUDITORIA INTERNA

XIII. Atuar como terceira linha de defesa, na avaliação da efetividade do processo de gestão de riscos e controles internos e seus resultados;

XIV. Avaliar a efetividade dos controles implementados para mitigar riscos, apontando necessidades de melhorias para a gestão operacional;

XV. Assessorar e reportar a estrutura de governança na supervisão da gestão de riscos e controles vinculados a processos críticos; e

XVI. Apoiar a operacionalização da PMC, para o alcance de seus objetivos, mediante a abordagem sistemática e disciplinada para avaliar e melhorar a eficácia dos processos de gerenciamento de riscos, dos controles e da governança.

7.5. INSTÂNCIAS EXTERNAS DE APOIO A GESTÃO DE RISCOS E CONTROLES INTERNOS

7.6. AUDITORIA INDEPENDENTE E ÓRGÃOS EXTERNOS

Tais instâncias não compõe a estrutura da Companhia, entretanto desempenham um papel importante para a governança e controle organizacional.

XVII. A auditoria independente realiza a avaliação e auditaria dos registros e controles contábeis, visando redução do risco de não-conformidades, buscando que a informação contábil reportada represente com fidedignidade a situação patrimonial e financeira da Companhia.

XVIII. Os órgãos externos são instâncias autônomas e independentes, responsáveis por fiscalizar, pelo controle e pela regulação, na promoção da governança das organizações públicas. São Exemplos típicos: TCE/SP - Tribunal de Contas de São Paulo, CGE/SP – Corregedoria Geral do Estado de São Paulo, MPSP - Ministério Público de São Paulo e Poder Judiciário.

PRAZO DE REVISÃO

Elaborado por	*Aprovado por*	*Versão*	*Vigente desde*
	Conselho de Administração da CETESB XXX Reunião realizada em XX/XX/XXXX	XX	XX/XX/20XX

Divulgação: ☐ Público Interno ☐ Público Externo

Esta Política deve ser revisada no prazo máximo de 02 (dois) anos, ou sempre que necessário, de forma a manter o seu conteúdo atualizado.

8. ANEXOS

- Metodologia de Gestão de Riscos;
- Relatório de atividades da Divisão de Conformidade e Gestão de Riscos; e
- Matriz de Riscos e Controles Internos.

9. REFERÊNCIAS

- ABNT NBR ISO 31000:2018 – Diretrizes para a gestão de riscos;
- ABNT NBR ISO 31073:2022 – Gestão de Riscos - Vocabulário;
- COSO. CONTROLE INTERNO – estrutura integrada: sumário executivo. IIA Brasil. 2013.
- COSO. GERENCIAMENTO DE RISCOS CORPORATIVOS – estrutura integrada: sumário executivo. IIA Brasil. 2014.
- COSO. GERENCIAMENTO DE RISCOS CORPORATIVOS – Integrado com Estratégia e Performance: sumário executivo. IIA Brasil. 2017;
- DECRETO Nº 68.158, DE 9 DE DEZEMBRO DE 2023, institui a Política de Gestão de Riscos da Administração Pública do Estado de São Paulo;
- DECRETO Nº 67.683, DE 3 DE MAIO DE 2023, institui o Plano Estadual de Promoção de Integridade e dá providências correlatas;
- DECRETO Nº 62.349, DE 26 DE DEZEMBRO DE 2016. Dispõe sobre o programa de integridade e a área de conformidade a ser adotado por empresas controladas direta ou indiretamente pelo Estado de São Paulo, regulamentando a aplicação da Lei federal nº 13.303, de 30 de junho de 2016, e criando instâncias e procedimentos de fomento ao controle interna;
- IIA - THE INSTITUTE OF INTERNAL AUDITORS. Declaração de posicionamento: As três linhas de defesa no gerenciamento eficaz de riscos e controles. IIA Brasil. 2013;
- IIA - THE INSTITUTE OF INTERNAL AUDITORS. Modelo das três linhas de defesa. IIA Brasil. 2020;

- LEI Nº 13.303, DE 30 DE JUNHO DE 2016. 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;
- TCU - TRIBUNAL DE CONTAS DA UNIÃO. Referencial Básico de Gestão de Riscos. 2018;
- TCU - TRIBUNAL DE CONTAS DA UNIÃO. Manual de gestão de riscos do TCU. 2020;
- TCU - TRIBUNAL DE CONTAS DA UNIÃO. Referencial Básico de Governança Organizacional. 2020; e
- TCE/SP – TRIBUNAL DE CONTAS DO ESTADO DE SÃO PAULO. Manual de controles internos. 2022.

10. CONTROLE DE VERSÕES

Versão	Autor	Descrição	Data
00	Divisão de Conformidade e Gestão de Riscos - PMC	Criação	14/11/2024