prodam	POLÍTICA	GRUPO GCO	TIPO PO	NÚMERO 002

ASSUNTO GESTÃO DE RISCOS E CONTROLES INTERNOS		
REVISÃO 24/08/2023	DATA DE PUBLICAÇÃO 24/08/2021	VERSÃO 2.0

1. OBJETIVO

Estabelecer as diretrizes gerais e específicas a serem adotadas na PRODAM-SP ao regular desenvolvimento das atividades corporativas de Gestão de Riscos e Controles Internos, a fim de reduzir exposições aos riscos (incertezas), com o objetivo de assegurar que a identificação, análise, avaliação e gerenciamento dos riscos sejam realizados de acordo com as necessidades e as melhores práticas estabelecidas na Empresa, no intuito de aumentar a probabilidade de atingir as metas de curto, médio e longo prazo.

2. ABRANGÊNCIA

Esta Política se aplica a todos os Gestores e empregados da PRODAM-SP, incluindo seus Conselheiros, Diretores, e membros dos Comitês.

3. ÁREA RESPONSÁVEL

É de responsabilidade da Gerência de Gestão de Riscos e Controle Interno (GJR) a elaboração, manutenção e atualização desta política.

4. TERMOS E DEFINIÇÕES

Para fins desta Política, consideram-se os seguintes termos e conceitos:

***Accountability* (Prestação de Contas):** obrigação dos agentes ou organizações que gerenciam recursos públicos de assumir responsabilidades por suas decisões e pela prestação de contas de sua atuação de forma voluntária, assumindo integralmente a consequência de seus atos e omissões.

Ambiente de controle: é a base de todos os controles internos, sendo formado pelo conjunto de regras e estrutura que determinam a qualidade desses elementos. O ambiente de controle deve influenciar a forma pela qual se estabelecem as estratégias e os objetivose a forma como os procedimentos de controle interno são estruturados.

Alguns dos elementos desse ambiente são:

- integridade pessoal e profissional e valores éticos assumidos pelos colaboradores, administradores, membros dos demais órgãos estatutários e terceiros;
- comprometimento para reunir, desenvolver e manter profissionais competentes; e
- estrutura organizacional na qual estejam claramente atribuídas responsabilidades e delegação de autoridade, para que sejam alcançados os objetivos da organização ou das políticas públicas.

Apetite ao risco: nível de risco que a PRODAM-SP está disposta a aceitar (estratégico e operacional).

CGM: Controladoria Geral do Município de São Paulo.

Código de Conduta e Integridade: Guia orientador das condutas, princípios e valores que devem reger a atuação de colaboradores, administradores, membros dos demais órgãos estatutários e terceiros no exercício de suas atividades, nos negócios e relacionamentos da PRODAM-SP.

Componentes dos controles internos: é composto por ambiente de controle interno da empresa, avaliação de risco; atividades de controles internos; informação e comunicação; e monitoramento.

Controles internos: conjunto de regras, procedimentos, diretrizes, protocolos, rotinas de sistemas informatizados, conferências e trâmites de documentos e informações, entre outros, operacionalizados de forma integrada pela direção e pelos colaboradores da empresa, destinados a enfrentar os riscos e fornecer segurança razoável de que, na consecução da missão da empresa, os seguintes objetivos gerais serão alcançados: execução ordenada, ética, econômica, eficiente e eficaz das operações; cumprimento das obrigações de *accountability* (prestação de contas); cumprimento das leis e regulamentos aplicáveis; e salvaguarda dos recursos para evitar perdas, mau uso e danos.

Conformidade: estar em concordância com as leis e os regulamentos externos e internos.

Conselho de Administração (CA): órgão de natureza colegiada que visa estabelecer a orientação geral dos negócios da Empresa e a lastrear e decidir sobre questões estratégicas, cujo escopo visa garantir aos Acionistas e à Sociedade que a Empresa exerça suas atividades com a estrita observância das regras de governança, de transparência e que o conjunto dos procedimentos organizacionais adotados em seu âmbito de ação evidencie que as decisões tomadas preservem a integridade dos recursos públicos sob sua guarda, protejam o interesse coletivo e o patrimônio público.

Comitê de Auditoria Estatutário: Órgão auxiliar do Conselho de Administração, ao qual se reporta diretamente.

Committee of Sponsoring Organizations of the Treadway Commission (COSO): entidade sem fins lucrativos, dedicada à melhoria dos relatórios financeiros através da ética, efetividade dos controles internos e governança corporativa,

para prevenir e evitar fraudes nas demonstrações contábeis das empresas, que desenvolveu a metodologia ERM - Enterprise Risk Management Framework para o mapeamento e gerenciamento de riscos corporativos;

Empresa: refere-se à Empresa de Tecnologia da Informação e Comunicação do Município de São Paulo - PRODAM / SP S.A., inscrita no CNPJ/MF Nº 43.076.702/0001-61.

Estatuto Social: Aprovado em conformidade com a Lei Federal 6.404 de 15/12/1976 e a Lei Federal nº 13.303 de 30/06/2016 e publicado em 10/03/2018.

Fraude: quaisquer atos ilegais caracterizados por desonestidade, dissimulação ou quebra de confiança. Estes atos não implicam o uso de ameaça de violência ou de força física.

GJO: Gerência de Conformidade, nomenclatura definida pela IA 016/2021.

GJR: Gerência de Gestão de Riscos e Controles Internos, criada pela IA 016/2021 e alterada pela IA022/2021.

Gestão de riscos: conjunto de ações estratégicas focadas em planejamento estratégico, e baseadas na identificação, administração, condução e prevenção dos riscos, ligadas a uma determinada atividade da empresa. Pode atuar de forma preventiva, erradicando possíveis perdas, sejam elas, institucionais, humanas ou materiais, e criando um ambiente de mitigação e prevenção.

Governança: combinação de processos e estruturas implantadas pela administração, para informar, dirigir, administrar e monitorar as atividades da organização, com o intuito de alcançar os seus objetivos.

Governança no setor público: compreende essencialmente os mecanismos de liderança, estratégia e controle postos em prática para avaliar, direcionar e monitorar a atuação da gestão, com vistas à condução de políticas públicas e à prestação de serviços de interesse da sociedade.

Incerteza: incapacidade de saber com antecedência a real probabilidade ou impacto de eventos futuros.

Mensuração de risco: significa estimar a importância de um risco e calcular a probabilidade e o impacto de sua ocorrência.

Plano de Ação (PA): instrumento de caráter corporativo que consolida uma visão de dois anos das estratégias e resultados pretendidos pela Empresa. Anualmente seu conteúdo é revisado, através do ciclo de Planejamento Empresarial, que é aprovado pelo Conselho de Administração da Empresa.

Política de gestão de riscos: declaração das intenções e diretrizes gerais de uma organização relacionadas à gestão de riscos.

Procedimento Operacional Padrão (POP): documento interno da PRODAM-SP, elaborado pela área técnica e aprovado pela sua respectiva Diretoria, que descreve a forma de execução, fluxos e competências para o desenvolvimento de tarefas e/ou processos.

Programa de Integridade e Boas Práticas – PIBP: consistente no conjunto de mecanismos e procedimentos internos destinados a detectar e prevenir fraudes, atos de corrupção, irregularidades e desvios de conduta, bem como a avaliar processos objetivando melhoria da gestão de recursos, para garantir a transparência, a lisura e a eficiência

Processo de gestão de riscos: aplicação sistemática de políticas, procedimentos e práticas de gestão para as atividades de identificação, avaliação, tratamento e monitoramento de riscos, bem como de comunicação com partes interessadas em assuntos relacionados a risco.

Probabilidade: possibilidade de ocorrer um evento.

Responsável pelo Controle Interno: colaborador formalmente indicado à CGM como responsável pelo respectivo controle interno da PRODAM-SP, a quem caberá a articulação necessária à efetivação do planejamento e desenvolvimento das atividades pertinentes ao controle interno, bem como a interlocução com a Controladoria Geral do Município para o recebimento de diretrizes e orientações relativas ao planejamento e desenvolvimento das atividades de controle interno

Resposta a risco: qualquer ação adotada para lidar com risco, podendo consistir em aceitar, compartilhar ou transferir, reduzir ou evitar.

Risco: possibilidade de ocorrência de um evento que venha a ter impacto no cumprimento dos objetivos.

Tipologia de Riscos: forma de classificação dos riscos, de acordo com tipos específicos, para facilitar seu agrupamento e avaliação pela Organização.

Tolerância ao risco: nível de risco que uma organização está disposta a aceitar.

Unidade Organizacional: são as Gerências que compõem cada uma das Diretorias.

5. DIRETRIZES GERAIS

5.1. A Gestão de Riscos e Controles Internos no âmbito da Empresa de Tecnologia da Informação e Comunicação do Município de São Paulo – PRODAM-SP observará o disposto nesta Política.

5.2. A Política de Gestão de Riscos e Controles Internos visará o desenvolvimento, disseminação e implementação de metodologias de gerenciamento de riscos corporativos e controles internos, com vistas a apoiar melhorias

contínuas nos processos organizacionais, projetos e iniciativas estratégicas da PRODAM-SP, contribuindo para o alcance dos objetivos estratégicos e cumprimento do propósito institucional.

6. PREMISSAS

6.1. Gestão de riscos e os controles internos são mecanismos de suporte à PRODAM-SP que visam auxiliar as tomadas de decisão, de forma a facilitar o alcance dos objetivos organizacionais, aumentando a probabilidade e o impacto dos eventos positivos (oportunidades) e reduzindo a probabilidade e o impacto dos eventos negativos (ameaças), por meio da identificação, priorização, avaliação e mitigação de riscos.

6.2. O comprometimento da alta direção, evidenciado pelo apoio explícito, é garantia da independência na execução dos mecanismos previstos nesta política.

6.3. A gestão de riscos e os controles internos são parte integrante de todos os processos organizacionais.

6.4. Todos os gestores e empregados são responsáveis pela gestão de riscos e controles internos em seus processos de atuação.

6.5. A organização da gestão de riscos e dos controles internos é estabelecida e mantida em ciclos de melhoria, para permitir ajustes e sua adaptação às mudanças organizacionais.

6.6. A organização deve prover recursos necessários para a implementação da política de gestão de riscos e controle interno.

6.7. Esta política abrange:

- **Riscos operacionais**: os riscos operacionais referem-se às possíveis perdas de eficiência e eficácia das operações da organização e correspondem a eventos internos e externos que podem comprometer as atividades da empresa, normalmente associados a falhas, deficiência ou inadequação de processos internos, pessoas, infraestrutura e sistemas de informação.
- **Riscos estratégicos:** riscos associados às decisões estratégicas da alta administração da Empresa que visam **atingir** seus objetivos de negócios, assegurando a capacidade ou habilidade da PRODAM-SP em proteger-se ou adaptar-se às mudanças do ambiente que ela esteja inserida.;
- **Riscos Financeiros:** eventos que podem comprometer a capacidade do órgão ou entidade de contar com os recursos **orçamentários** e financeiros necessários à realização de suas atividades, ou eventos que possam comprometer a própria execução orçamentária, como atrasos no cronograma de licitações;
- **Riscos de Integridade:** são os atributos, características ou exposições de caráter externo, organizacional

ou **individual** que possibilitam a ocorrência de comportamentos caracterizados como quebra da integridade institucional (ex.: corrupção, fraude), com efeitos negativos nos objetivos, atribuições ou missão de uma instituição pública;

- **Riscos de Conformidade**: riscos de sanções legais ou regulatórias, de perda financeira ou de reputação que a **PRODAM-SP** pode sofrer como resultados de falhas no cumprimento da aplicação de leis, acordos, regulamentos, Código de Contuta e Integridade, dentre outros;
- **Risco de fraude e corrupção:** possibilidade de qualquer ato ou omissão intencional concebido para enganar terceiros, **resultando** em a vítima sofrer uma perda e/ou o autor alcançar um ganho. Ainda assim, o mau uso de poder (político ou financeiro) confiado o determinado agente (público ou privado) para fins ilegítimos;
- **Risco de segurança da informação:** possibilidade de desproteção dos principais ativos da Organização – a **informação** – assim como a reputação e a marca da Empresa;
- **Risco de projeto**: evento com uma probabilidade de ocorrer no futuro, impactando oprojeto de forma negativa (ameaça) ou positiva (oportunidade);
- **Risco inerente**: risco a que uma organização está exposta sem considerar quaisquerações gerenciais que possam reduzir a probabilidade de sua ocorrência ou seu impacto;
- **Risco residual**: risco a que uma organização está exposta após a implementação de ações gerenciais para o tratamento do risco;
- **Riscos de imagem/reputação da empresa**: eventos que podem comprometer a confiança da sociedade, de parceiros, de clientes ou de fornecedores em relação à capacidade da Empresa em cumprir sua missão institucional;
- **Riscos legais:** eventos derivados de alterações legislativas ou normativas que podemcomprometer as atividades da Empresa.

6.8. A gestão de riscos e os controles internos serão integrados ao planejamento estratégico, aos processos e às políticas estabelecidas pela PRODAM-SP.

6.9. A integração da gestão de riscos ao planejamento estratégico, processos e políticas organizacionais será implementada por meio de aplicação da metodologia de gestão de riscos e controles internos.

6.10. A metodologia de gestão de riscos e controles internos contempla a sistemática e artefatos utilizados para identificar, avaliar, tratar e monitorar os riscos corporativos, com a finalidade de garantir a continuidade do negócio.

6.11. A gestão de riscos deve priorizar o tratamento dos processos que concentrem os riscos corporativos críticos. Este tratamento será conduzido pela GJR em conjunto com o gestor do processo.

6.12. Para os processos que não concentrem riscos corporativos críticos, o tratamento dos riscos será realizado pelos responsáveis das respectivas unidades organizacionais por meio da autoaplicação da metodologia.

6.13. Planos de capacitação devem estar estruturados, desenvolvidos e aplicados continuamente para todos os colaboradores e gestores, para fortalecer a cultura organizacional nas áreas de atuação desta política.

6.14. Os relatórios com os Planos de Ação para mitigação dos riscos serão submetidos anualmente à Diretoria Executiva e ao Conselho de Administração e farão parte integrante do Plano de Integridade e Boas Práticas – PIBP da PRODAM-SP, a ser encaminhado à CGM.

6.15. O processo de gestão de riscos deve prever mecanismos de comunicação contínua, incluindo relatórios sobre o desempenho da gestão de riscos, como parte do processo de governança.

6.16. A gestão dos riscos referentes à fraude e corrupção será realizada pela Gerência de Conformidade (GJO) em conjunto com as unidades organizacionais da Empresa.

6.17. A PRODAM-SP deve definir e comunicar formalmente os papéis e responsabilidades de cada um dos colaboradores envolvidos no processo de gestão de riscos.

6.18. Esta política será complementada pelo Procedimento Operacional Padrão (POP), de Gestão de Riscos e Controle Interno.

7. DISPOSIÇÕES GERAIS

7.1. DEFINIÇÃO DO CONTEXTO

Com base nas metas, no planejamento estratégico, resultados esperados, influências dos ambientes internos e externos, além do apetite ao risco, definidos e/ou aprovados pelo Conselho de Administração e pela Diretoria Executiva da PRODAM-SP, serão definidas as prioridades, o escopo do trabalho e os critérios a serem considerados na Gestão de Riscos Empresariais.

7.2. MAPEAMENTO DOS RISCOS

A GJR fará a análise das fontes dos riscos, áreas afetadas, causas e consequências potenciais que podem influenciar adversamente as metas e/ou os objetivos estratégicos da PRODAM-SP.

7.3. CLASSIFICAÇÃO DOS RISCOS

Após a análise de cada incerteza, a GJR classificará os riscos utilizando a metodologia adotada pela PRODAM-SP e descrita no respectivo POP.

7.4. TRATAMENTO DOS RISCOS

7.4.1. Com base na classificação dos riscos a respectiva Diretoria deverá definir o tratamento a ser dado ao risco: (i) evitar; (ii) transferir; (iii) reduzir; ou, (iv) aceitar.

7.4.2. Caso a opção seja aceitar o risco, devem ser estabelecidas métricas de monitoramento.

7.4.3. Nos casos em que a definição por reduzir, evitar e/ou compartilhar a exposição ao risco, planos de ação/mitigação devem ser definidos - contendo o detalhamento do risco, os controles internos de mitigação adotados, responsáveis e prazo de conclusão -, e monitorados através de indicadores.

7.5. MONITORAMENTO DOS RISCOS

7.5.1. Para que o gerenciamento de riscos empresariais seja efetivo, a área responsável pela Gestão de Riscos deve acompanhar os riscos identificados e priorizados, com base nas melhores práticas de Gestão de Riscos.

7.5.2. Indicadores de riscos serão estabelecidos e monitorados respeitando o ciclo dos processos, servindo de base para tomada de decisão.

7.5.3. O monitoramento de riscos será realizado de forma contínua, permitindo identificar situações adversas e adotar as ações corretivas ou de contorno, minimizando impactos nos processos da organização.

7.5.4. Eventuais perdas aferidas por meio dos indicadores de monitoramento dos riscos deverão ser consolidadas para definição de ações e metas de contenção.

8. OPERACIONALIZAÇÃO

8.1. A operacionalização da gestão de riscos será definida através de Procedimento Operacional Padrão (POP) específico ao tema e seguirá as recomendações do COSO, o manual da Controladoria Geral do Município de São Paulo e as melhores práticas adotados pelo mercado para Gestão de Riscos e Controles Internos.

9. RESPONSABILIDADES

9.1. CONSELHO DE ADMINISTRAÇÃO

- implementar e supervisionar os sistemas de gestão de riscos e controle interno estabelecidos para a prevenção e mitigação dos principais riscos a que está exposta a Empresa, inclusive os riscos relacionados à integridade das informações contábeis e financeiras e os relacionados à ocorrência de corrupção e fraude;
- aprovar o planejamento estratégico da Empresa, apresentado pela Diretoria, que conterá a estratégia de longo prazo atualizada com análise de riscos e oportunidades para, no mínimo, os próximos 05 (cinco) anos.

9.2. COMITÊ DE AUDITORIA ESTATUTÁRIO

- supervisionar as atividades desenvolvidas nas áreas de controle interno;
- monitorar a qualidade e a integridade dos mecanismos de controle interno;
- avaliar e monitorar exposições de risco da empresa.

9.3. DIRETOR-PRESIDENTE

- Efetuar recomendações a esta Política, se entender necessário;
- acompanhar a implementação desta Política, a fim de garantir sua função.

9.4. GERÊNCIA DE AUDITORIA INTERNA (GPA)

- aferir a adequação do controle interno, a efetividade do gerenciamento dos riscos e a adequação dos controles internos.

9.5. DIRETORIA EXECUTIVA

- Aprovar em Reunião de Diretoria a Política de Gestão de Riscos e Controles Internos;
- cumprir e fazer cumprir a presente Política e normativos relacionados à gestão de riscos e controles internos.

9.6. DIRETORES

- definir e monitorar, junto com a sua equipe, os planos de ação para mitigação dos riscos respectivos à sua área e/ou processos sob sua subordinação;
- garantir que o plano de ação/mitigação seja implementado dentro do prazo estipulado e de forma satisfatória;
- comunicar à área responsável pela gestão de riscos e controles internos sobre a identificação de novos riscos ou eventos que sejam relevantes e suas respectivas evoluções;
- implementar os controles internos, de acordo com a classificação dos riscos e o tratamento definido, de forma

efetiva e compatível com a natureza, complexidade, grau de importância e riscos dos processos;

- definir e operacionalizar os controles internos considerando os riscos internos e externos que se pretende gerenciar, tendo em vista a mitigação da ocorrência de riscos ou impactos sobre os objetivos da PRODAM-SP;
- definir controles internos baseados no modelo de gerenciamento de riscos.

9.7. DIRETORIA JURÍDICA E DE GOVERNANÇA CORPORATIVA (DJU)

- Revisar a Política de Gestão de Riscos e Controles Internos no que tange às questões jurídicas.

9.8. GERÊNCIA DE GESTÃO DE RISCOS E CONTROLES INTERNOS (GJR)

- gerir e garantir a manutenção desta política na PRODAM-SP;
- identificar de Riscos em conjunto com as Unidades Organizacionais;
- elaborar e revisar o Procedimento Operacional Padrão (POP), referente à gestão de riscos e controle interno;
- definir as responsabilidades relacionadas às atividades de gestão de riscos;
- elaborar os relatórios anuais de consolidação dos Riscos da PRODAM-SP;
- apoiar os gestores de processo na definição dos Planos de Ação/mitigação necessários para tratamento dos Riscos;
- monitorar a implementação dos Planos de Ação;
- reportar, de modo transparente, as informações relacionadas às suas atividades de gerenciamento de Riscos;
- liderar os trabalhos para detecção de Riscos a fim de garantir a eficácia dos Controles internos de mitigação dos riscos.

9.9. GERÊNCIA DE CONFORMIDADE (GJO)

- revisar a Política de Gestão de Riscos e Controles Internos;
- realizar, em conjunto com as unidades organizacionais da Empresa, a gestão de riscos referentes à conformidade, integridade, em especial à fraude e corrupção.

9.10. GERÊNCIA DE COMUNICAÇÃO INSTITUCIONAL (GPC)

- Operacionalizar a publicação e a divulgação desta Política conforme orientações da Gerência de Conformidade (GJO).

9.11. UNIDADES ORGANIZACIONAIS

- os Gerentes das unidades organizacionais são responsáveis por adotar medidas de gestão de riscos e controles internos e verificar continuamente sua eficácia, para garantir o alcance dos objetivos empresariais,

privilegiando: a identificação, avaliação, tratamento e monitoramento;

- assegurar a implementação dos Planos de Ação definidos para tratamento dos Riscos nos prazos estabelecidos;
- reportar à GJR as informações relacionadas às suas atividades no gerenciamento de Riscos;
- comunicar à GJR tempestivamente sobre eventuais riscos ainda não identificados, sejam eles novos ou não;
- aprovar os procedimentos que direcionem as ações individuais na implementação dos conceitos de gerenciamento de Riscos na sua área de atuação, a fim de assegurar que as Respostas aos Riscos sejam executadas;
- detalhar e alinhar com a GJR a implementação do Plano de Ação/mitigação, segundo a prioridade nele definida.

9.12. RESPONSÁVEL PELO CONTROLE INTERNO

- efetuar a interlocução com a Controladoria Geral do Município de São Paulo para o recebimento de diretrizes e orientações relativas ao planejamento e desenvolvimento das atividades de controle interno;
- efetuar o planejamento e o desenvolvimento das atividades pertinentes ao controle interno, considerando as diretrizes e orientações da Controladoria Geral do Município;
- analisar as principais situações administrativas, contratuais e orçamentárias;
- verificar os fluxos, trâmites e prazos processuais;
- acompanhar o atendimento das demandas da Controladoria Geral do Município, do Tribunal de Contas do Município, do Ministério Público, bem como eventuais respostas a outros Órgãos de Controle Externo, seja do Poder Judiciário, ou Legislativo;
- monitorar os principais programas do órgão ou entidade, apontando eventual falta de condição para atingimento de metas;
- verificar a qualidade do atendimento prestado pelo órgão ou entidade em suas diversas modalidades;
- acompanhar e avaliar os atos de gestão, com vistas à mitigação dos pontos de fragilidade e suscetibilidade à corrupção;
- incentivar as boas práticas voltadas ao aprimoramento do controle interno;
- apresentar o relatório periódico ao titular do órgão ou entidade, com os devidos apontamentos de correções e sugestões de melhoria; e,
- encaminhar à CGM, até o último dia útil de dezembro do ano corrente, o Relatório anual com as atividades desenvolvidas pelo controle interno.

10. APROVAÇÃO

Esta Política deverá ser aprovada pela Diretoria-Executiva em Reunião de Diretoria (RD).

11. VIGÊNCIA E ATUALIZAÇÃO

Esta Política será válida pelo período de até 2 (dois) anos, devendo ser atualizada neste período ou em prazo inferior, nas hipóteses de alteração da legislação ou regulamentação, ou no caso de mudança do direcionamento estratégico da Empresa.

12. LEGISLAÇÕES E DOCUMENTOS RELACIONADOS

12.1. LEGISLAÇÕES EXTERNAS

- Lei Federal nº 13.303 de 30/06/2016 (Lei das Estatais): 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. A elaboração deste documento foi motivada por esta lei;
- Lei Federal 12.527/11 de 18/11/2011 (Lei de Acesso à Informação - LAI): regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. (Lei de Acesso à Informação - LAI);
- Lei Federal nº 6.404 de 15/12/1976 (Lei das Sociedades Anônimas): dispõe sobre as sociedades por ações;
- Lei Municipal nº 7.619, de 23/06/1971: dispõe sobre constituição da Companhia de Processamento de Dados do Município de São Paulo - PRODAM-SP, e dá outras providências;
- Decreto Municipal nº 59.496, de 08/06/2020: regulamenta o artigo 53 da Lei Orgânica do Município de São Paulo, bem como dispositivos das Leis nº 15.764, de 27 de maio de 2013, e nº 16.974, de 23 de agosto de 2018, dispondo sobre o sistema de controle interno municipal, a organização e o funcionamento da Controladoria Geral do Município, a adoção de medidas administrativas para transparência e controle, e o Programa de Integridade e Boas Práticas, para a prevenção da corrupção;
- Decreto Municipal nº 58.093/2018 de 20/02/2018: 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 Paulodetenha o controle, aplicando-se no que couber às autarquias, fundações públicas e serviços sociais autônomos, bem como revoga o Decreto nº 57.566, de 27 de dezembro de 2016 e os artigos 1º ao 11do Decreto nº 53.916, de 16 de maio de 2013, e introduz

alterações no Decreto 53.687, de 2 de janeiro de 2013

- Portaria Conjunta CGU e Ministério do Planejamento, Orçamento e Gestão Nº 1, de 10 /05/2016: dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo federal;
- Portaria CGM Nº 117 de 14/08/2020: fixa prazos e estabelece os procedimentos para estruturação, execução e monitoramento dos Planos de Integridade e Boas Práticas.
- Portaria CGM Nº 126 de 04/09/2020: disciplina a interlocução entre a Controladoria Geral do Município e os responsáveis pelo controle interno de órgãos e entidades da Administração Pública Municipal.
- Portaria CGM Nº 108 de 18/05/2021: altera a Portaria CGM Nº 126, de 4 de setembro de 2020.

12.2. NORMATIVOS EXTERNOS

- Normas ABNT (Associação Brasileira de Normas Técnicas):
  - ABNT NBR ISO 31000:2018, de 23/03/2018 (Gestão de Riscos – Diretrizes);
  - ABNT ISO/IEC 31010:2012, de 04/04/2012 (Gestão de Riscos – Técnicas para Avaliação de Riscos); e,
  - ABNT ISO GUIA 73:2009, de 31/11/2009 (Gestão de Riscos – Vocabulário).
- COSO (Committee of Sponsoring Organizations of the Treadway Commission) I e II.

12.3. NORMATIVOS INTERNOS

- Código de Conduta e Integridade da PRODAM-SP;
- Estatuto Social da PRODAM-SP;
- Regimento Interno da PRODAM-SP;
- Regimento Interno do Comitê de Auditoria Estatutário; e,
- GCO-NO-001 Norma de Auditoria Interna, versão 1 de 09/12/2019.

13. DOCUMENTOS INCORPORADOS E REVOGADOS

Esta Política revoga e substitui o seguinte documento normativo e demais disposições em contrário:

- P-002 - Política de Conformidade, Gestão de Riscos e Controle Interno, Versão 1 de 28/06/2018.

14. DISPOSIÇÕES FINAIS

14.1. Os casos omissos serão apreciados pela Diretoria Jurídica e de Governança Corporativa (DJU) da PRODAM-SP.

14.2. A PRODAM–SP poderá criar um Comitê de Gestão de Riscos e Controles Internos, que terá suas atribuições definidas na Instrução que o instituir e determinar a publicação de Regimento Interno.

15. REVISÕES E APROVAÇÕES

Responsabilidade	**Área**
Elaboração e Atualização	Gerência de Gestão de Riscos e Controles Internos (GJR)
Revisão	Gerência de Conformidade (GJO) e Diretoria Jurídica e de Governança Corporativa (DJU)
Aprovação	Diretoria Executiva

Esta política foi aprovada pela Diretoria-Executiva da Prodam-SP, na 2050ª Reunião de Diretoria ocorrida no dia 18/08/2021, conforme respectiva ata, anexa ao processo SEI nº 7010.2021/0008617-1.

HISTÓRICO DE VERSÕES E ALTERAÇÕES

Versão	**Data**	**Alteração**	**Origem da Alteração**
1.0	28/06/2018	Primeira versão	Atendimento à Lei 13.303/16
2.0	24/08/2021	Revisão e atualização do conteúdo	Mudança na estrutura da área (IA 016/21 e IA022/21) e atualização necessária pelo tempo decorrido desde a 1ª versão