prodam	POLÍTICA	GRUPO GCO	TIPO PO	NÚMERO 002

ASSUNTO GESTÃO DE RISCOS E CONTROLES INTERNOS		
REVISÃO Conforme Política de Governança de Normativos Internos - GCO-PG-003	DATA DE PUBLICAÇÃO 24/01/2024	VERSÃO 3.0

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 Conformidade, Gestão de Riscos e Controles Internos (GJO) 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.

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

Comitê de Gestão de Riscos e Controles Internos (CGRCI): constituído por meio de Instrução Normativa, é um órgão de caráter consultivo e permanente para questões relativas à Gestão de Riscos e Controles Internos, tendo como objetivos principais a avaliação, coordenação e o monitoramento das atividades de gestão de riscos corporativos da PRODAM-SP.

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.

Dono do Risco (ou Proprietário do Risco): responsável pela identificação e gerenciamento dos riscos do processo sob sua gestão. Essa responsabilidade, normalmente, será atribuída aos titulares das Unidades Organizacionais.

Fraude: ato intencional, de má fé, praticado por um ou mais indivíduos da Empresa, entre gestores, responsáveis pela governança, colaboradores ou terceiros, envolvendo o uso propositado de falsidade para obter uma vantagem injusta ou ilegal.

Gestão de Riscos: aplicação sistemática de políticas, procedimentos e práticas de gestão 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.

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

Plano de Ação: estratégia composta por diferentes atividades, com o propósito de controlar eventos no ciclo de vida do risco. Define qual será o objetivo, quanto tempo levará, quais recursos precisarão ser implementados e os responsáveis por executá-lo.

Programa de Integridade e Boas Práticas (PIBP): consiste 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 uma atuação transparente, ética, eficiente e em conformidade com a legislação vigente.

Resposta ao 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 da Empresa.

Risco Inerente: risco ao qual a Empesa está exposta, sem considerar quaisquer ações gerenciais que possam reduzir a probabilidade de sua ocorrência ou seu impacto.

Risco Residual: risco ao qual a Empresa está exposta, após a implementação de ações gerenciais para o tratamento do risco.

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

5. DIRETRIZES

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 visa o desenvolvimento, disseminação e implementação de metodologias de gerenciamento de riscos corporativos, com vistas a apoiar a melhoria contínua nos processos organizacionais, projetos e iniciativas estratégicas da PRODAM-SP, contribuindo para o alcance dos objetivos estratégicos e cumprimento do propósito institucional.

5.3. A alta administração da Empresa evidenciará seu comprometimento, por meio de apoio explícito, garantindo a independência na execução dos mecanismos previstos nesta política.

5.4. A gestão de riscos e os controles internos integrarão os processos organizacionais.

5.5. O dono do risco será responsável pela identificação e gerenciamento dos riscos do processo sob sua gestão, porém todos os envolvidos no processo compartilham dessa responsabilidade.

5.6. A gestão de riscos deve priorizar o tratamento dos processos que concentrem os riscos corporativos críticos. Este tratamento será realizado pelos responsáveis pelo processo, sob a coordenação do Comitê de Gestão de Riscos e Controles Internos (CGRCI) e apoiado pela Gerência de Conformidade, Gestão de Riscos e Controles Internos (GJO).

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

5.8. Planos de capacitação devem estar estruturados, desenvolvidos e aplicados continuamente para todos os colaboradores e gestores, para fortalecer a cultura organizacional de riscos.

5.9. Os relatórios com os Planos de Ação para mitigação dos riscos serão submetidos anualmente à Diretoria Executiva e ao Conselho de Administração.

5.10. 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.

5.11. A gestão dos riscos referentes a fraude e corrupção será realizada pela Gerência de Conformidade, Gestão de Riscos e Controles Internos (GJO), em conjunto com as unidades organizacionais da Empresa.

6. DISPOSIÇÕES GERAIS

6.1. Processo de Gestão de Riscos Corporativos

Processo conduzido pela Gerência de Conformidade, Gestão de Riscos e Controles Internos (GJO), em conjunto com a Unidades Organizacionais donas dos riscos, sob a supervisão do Conselho de Administração e do Comitê de Auditoria Estatutário.

Consiste no estabelecimento de estratégias, formuladas para identificar em toda a Empresa, eventos em potencial, capazes de afetá-la, e administrar os riscos de modo a mantê-los compatíveis com a exposição de riscos da Empresa e possibilitar a garantia razoável do cumprimento dos seus objetivos. Os riscos corporativos envolvem as atividades do negócio da PRODAM-SP, que podem afetar os seus objetivos estratégicos, incluindo os de integridade e regulatórios.

A figura abaixo representa as etapas deste processo:

Fonte: Gestão de Riscos - Diretrizes (ABNT NBR ISO 31000:2018).

6.1.1. DEFINIÇÃO DO CONTEXTO, ESCOPO E CRITÉRIOS

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.

6.1.2. IDENTIFICAÇÃO/ANÁLISE DOS RISCOS

A GJO, em conjunto com os donos dos riscos, 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.

Nesta etapa, os riscos serão categorizados de acordo com a natureza das consequências da sua materialização.

Esta política abrange, dentre outras categorias:

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 Conduta e Integridade, dentre outros;

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 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 de Segurança da Informação: riscos de falhas e vulnerabilidades que podem expor dados e informações da Empresa a ameaças.

6.1.3. AVALIAÇÃO / CLASSIFICAÇÃO DOS RISCOS

Após a análise de cada incerteza, a GJO, em conjunto com os donos dos riscos, classificará os riscos em função da

probabilidade de ocorrência e do impacto da sua materialização, utilizando a metodologia adotada pela PRODAM-SP. Nesta etapa, o propósito é apoiar decisões, por meio da comparação dos resultados da análise de riscos com os critérios estabelecidos para determinar as ações necessárias, quando for o caso.

6.2. TRATAMENTO DOS RISCOS

6.2.1. 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.

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

6.2.3. Nos casos em que houver definição por reduzir, evitar e/ou compartilhar a exposição ao risco, devem ser definidos planos de ação/mitigação, contendo o detalhamento do risco, os controles internos de mitigação adotados, responsáveis e prazo de conclusão, bem como monitoramento por meio de indicadores.

6.3. MONITORAMENTO E ANÁLISE CRÍTICA

6.3.1. 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.

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

6.3.3. 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.

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

6.4. COMUNICAÇÃO E CONSULTA

A comunicação, para a conscientização e o entendimento do risco, e a consulta, para obtenção de retorno e informações auxiliares para a tomada de decisão, devem ocorrer em todas as etapas do processo, conforme estabelecido na metodologia adotada pela PRODAM-SP.

6.5. REGISTRO E RELATO

O processo de gestão de riscos e seus resultados deverão ser documentados e relatados por meio de mecanismos apropriados, conforme estabelecido na metodologia adotada pela PRODAM-SP.

7. RESPONSABILIDADES

7.1. CONSELHO DE ADMINISTRAÇÃO (CA)

- Implementar e supervisionar, com o auxílio da área de conformidade, os sistemas de gestão de riscos e controles internos 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.

7.2. COMITÊ DE AUDITORIA ESTATUTÁRIO (CAE)

- Avaliar e monitorar exposições a riscos da Empresa.

7.3. COMITÊ DE GESTÃO DE RISCOS E CONTROLES INTERNOS (CGRCI)

- Aprovar a metodologia a ser utilizada na condução do processo de gerenciamento de riscos;
- Coordenar o processo de gestão de riscos corporativos críticos;
- Acompanhar o mapeamento dos riscos da PRODAM-SP realizado pela Área de Gestão de Riscos e Controles Internos;
- Monitorar, de forma sistemática, o gerenciamento de riscos, assim como o estágio de evolução e realização das ações definidas para a prevenção e mitigação dos riscos;
- Avaliar, periodicamente, a eficácia das políticas e dos sistemas de gerenciamento de riscos e de controles internos, formalizando seu posicionamento e encaminhando esta avaliação para atuação da Área de Gestão de Riscos e Controles Internos;
- Submeter à Diretoria Executiva os Relatórios de Gestão de Riscos, contendo as recomendações que julgar apropriadas;
- Apreciar os relatórios emitidos pelos Órgãos Fiscalizadores, Auditorias Interna e Externa no tocante às deficiências dos controles internos e de conformidade e respectivas providências das áreas envolvidas;
- Recomendar ações para disseminar internamente a cultura e sensibilidade a riscos e controles na Empresa.

7.4. DIRETORIA EXECUTIVA

- Avaliar os planos de ação para mitigação dos riscos antes de submeter ao Conselho de Administração.

7.5. 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 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.

7.6. GERÊNCIA DE AUDITORIA INTERNA (GPA)

- Aferir a adequação dos controles internos e a efetividade do gerenciamento dos riscos.

7.7. GERÊNCIA DE CONFORMIDADE, GESTÃO DE RISCOS E CONTROLES INTERNOS (GJO)

- Identificar, analisar e avaliar riscos em conjunto com as Unidades Organizacionais;
- Apoiar as unidades organizacionais na definição dos Planos de Ação/mitigação necessários para tratamento dos riscos;
- Monitorar a implementação dos Planos de Ação;
- Reportar às instâncias da Estrutura de Governança, 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.
- Realizar, em conjunto com as unidades organizacionais da Empresa, a gestão dos riscos, em especial aqueles referentes à conformidade, integridade.

7.8. GERÊNCIA DE COMUNICAÇÃO INSTITUCIONAL (GPC)

- Operacionalizar a publicação e a divulgação desta Política conforme orientações da Gerência de Conformidade, Gestão de Riscos e Controles Internos (GJO).

7.9. UNIDADES ORGANIZACIONAIS

- Os titulares 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, análise, avaliação, tratamento e monitoramento;

- Assegurar a implementação dos Planos de Ação definidos para tratamento dos Riscos nos prazos estabelecidos;
- Reportar à GJO as informações relacionadas às suas atividades no gerenciamento de Riscos;
- Comunicar à GJO tempestivamente sobre eventuais riscos ainda não identificados, sejam eles novos ou não;
- Aprovar os procedimentos que direcionem as ações específicas 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 GJO a implementação do Plano de Ação/mitigação, segundo a prioridade nele definida.

8. APROVAÇÃO

Esta Política deverá ser validada pela Diretoria-Executiva em Reunião de Diretoria (RD) e submetida à aprovação do Conselho de Administração.

9. VIGÊNCIA E ATUALIZAÇÃO

Em conformidade com o disposto pela Política de Governança de Normativos Internos – GCO-PG-003.

10. LEGISLAÇÕES E DOCUMENTOS RELACIONADOS

10.1. 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 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 Paulo detenha 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 11 do 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.

10.2. NORMATIVOS EXTERNOS

- Normas ABNT (Associação Brasileira de Normas Técnicas):
  - ABNT NBR ISO 31000:2018, de 23/03/2018 (Gestão de Riscos – Diretrizes);
  - ABNT NBR IEC 31010:2021, de 30/08/2021 (Gestão de riscos - Técnicas para o processo de avaliação de riscos);
  - 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.

10.3. NORMATIVOS INTERNOS

- Código de Conduta e Integridade da PRODAM-SP;

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

11. DOCUMENTOS INCORPORADOS E REVOGADOS

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

- GCO-PO-002 - Política de Gestão de Riscos e Controles Internos, Versão 2.0 de 24/08/2021.

12. DISPOSIÇÕES FINAIS

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

12.2. Os casos omissos serão apreciados pelo Comitê de Gestão de Riscos e Controles Internos da PRODAM-SP.

13. REVISÕES E APROVAÇÕES

Responsabilidade	**Área**
Elaboração e Atualização	Gerência de Conformidade, Gestão de Riscos e Controles Internos (GJO)
Revisão	Comitê de Gestão de Riscos e Controles Internos (CGRCI)
Aprovação	Diretoria Executiva e Conselho de Administração

Esta política foi aprovada pela Diretoria-Executiva da PRODAM-SP, na 2236ª Reunião de Diretoria ocorrida no dia 21/12/2023, e pelo Conselho de Administração, na 1023ª Reunião do Conselho de Administração ocorrida em 04/01/2024, conforme informações contidas no processo SEI 7010.2023/0011902-2.

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
3.0	24/01/2024	Revisão e atualização do conteúdo	Mudança na estrutura da área (IN-E Nº 005/2023) e atualização necessária pelo tempo decorrido desde a 2ª versão