OBJETIVO

Estabelecer as diretrizes para orientar as atividades corporativas de conformidade, gestão de riscos e controle interno.

1. ABRANGÊNCIA

Empresa de Tecnologia da Informação e Comunicação do Município de São Paulo – PRODAM-SP.

2. ÁREA RESPONSÁVEL

A elaboração e manutenção desta política é de responsabilidade da Gerência de Conformidade, Gestão de Riscos e Controle Interno (GPR).

3. CONCEITOS

3.1. ***Accountability*:** 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.

3.2. **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 objetivos e a forma como os procedimentos de controle interno são estruturados. Alguns dos elementos desse ambiente são:

a) integridade pessoal e profissional e valores éticos assumidos pelos colaboradores, administradores, membros dos demais órgãos estatutários e terceiros;

b) comprometimento para reunir, desenvolver e manter profissionais competentes; e

c) estrutura organizacional na qual estejam claramente atribuídas responsabilidades e delegação de autoridade, para que sejam alcançados os objetivos da organização ou das políticas públicas.

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

3.4. **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.

3.5. **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:

a) execução ordenada, ética, econômica, eficiente e eficaz das operações;

b) cumprimento das obrigações de *accountability (prestação de contas)*;

c) cumprimento das leis e regulamentos aplicáveis; e

d) salvaguarda dos recursos para evitar perdas, mau uso e danos.

3.6. **Conformidade:** agir de acordo com uma regra; estar em concordância com as leis e os regulamentos externos e internos.

3.7. **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.

3.8. **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.

3.9. **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.

3.10. **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.

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

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

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

3.14. **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.

3.15. **Probabilidade:** possibilidade de ocorrer um evento.

3.16. **Resposta a risco:** qualquer ação adotada para lidar com risco, podendo consistir em tratar, evitar, transferir ou aceitar.

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

3.18. **Tipologia de Riscos:** forma de classificação dos riscos, de acordo com tipos específicos, para facilitar seu agrupamento e avaliação pela Organização. Os principais tipos de risco incluem:

a. **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;

b. **Risco de segurança da informação:** possibilidade de desproteção dos principais ativos da Organização – a informação – assim como a reputação e a marca da Empresa;

c. **Risco de projeto:** evento com uma probabilidade de ocorrer no futuro, impactando o projeto de forma negativa (ameaça) ou positiva (oportunidade);

d. **Risco inerente:** risco a que uma organização está exposta sem considerar quaisquer ações gerenciais que possam reduzir a probabilidade de sua ocorrência ou seu impacto;

e. **Risco residual:** risco a que uma organização está exposta após a implementação de ações gerenciais para o tratamento do risco;

f. **Riscos financeiros / orçamentários:** 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;

g. **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;

h. **Riscos legais:** eventos derivados de alterações legislativas ou normativas que podem comprometer as atividades da Empresa;

i. **Riscos operacionais:** 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.

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

4. PREMISSAS

4.1. A conformidade, gestão de riscos e os controles internos são mecanismos de governança e de tomada de decisão, cuja finalidade é 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).

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

4.3. A conformidade, gestão de riscos e os controles internos são parte integrante de todos os processos organizacionais.

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

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

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

4.7. Esta política abrange:

a) **Riscos operacionais**: vinculados a processos internos, pessoas, infraestrutura e sistemas de informação - além dos riscos de imagem e legais; e

b) **Riscos estratégicos:** relacionados ao planejamento estratégico da organização.

4.8. Esta política é complementada pelas medidas e práticas do Programa de Integridade da PRODAM-SP voltadas ao combate dos desvios de fraude e corrupção.

5. DIRETRIZES

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

5.2. 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.

5.3. A metodologia de gestão de riscos e controles internos contempla a sistemática e artefatos utilizados para identificar, avaliar, tratar e monitorar os riscos corporativos.

5.4. A gestão de riscos deve priorizar o tratamento dos processos que concentrem os riscos corporativos críticos. Este tratamento será conduzido pela unidade responsável pela gestão de riscos, Gerência de Conformidade, Gestão de Riscos e Controle Interno (GPR), em conjunto com o gestor do processo.

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

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

5.7. 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.

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

5.9. As eventuais perdas aferidas por meio dos indicadores de monitoramento dos riscos deverão ser consolidadas para definição de ações e metas de contenção.

5.10. Os relatórios com as ações de tratamento de riscos serão submetidos semestralmente à Diretoria e ao Conselho, contemplando o detalhamento dos riscos críticos, dos controles, os responsáveis e prazos para implementação do plano de ações para o tratamento dos riscos.

5.11. 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.

5.12. A gestão dos riscos relativos a desvios de fraude e corrupção será realizada pelas instâncias intervenientes do Programa de Integridade da PRODAM-SP:

a) Envolver os conselhos de administração, conselho fiscal e a diretoria executiva

A atuação dos conselhos de administração, conselho fiscal e diretoria executiva assume papel primordial para o sucesso do processo de gestão de riscos, uma vez que são estes os principais tomadores de decisão sobre questões estratégicas na empresa.

b) Estabelecer papéis e responsabilidades

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. RESPONSABILIDADES

6.1. O Conselho de Administração é responsável por supervisionar os sistemas de conformidade, gestão de riscos e controles internos;

6.2. A Auditoria Interna é responsável por aferir a efetividade do gerenciamento de riscos e a adequação dos controles internos;

6.3. A Diretoria é responsável por aprovar, cumprir e fazer cumprir a política e normativos relacionados à conformidade, gestão de riscos e controles internos;

6.4. Os Diretores são responsáveis pela execução dos planos de ação de tratamento de riscos das áreas e processos sob sua subordinação;

6.5. A Gerência de Conformidade, Gestão de Riscos e Controle Interno - GPR é a unidade organizacional responsável pela gestão e manutenção desta política na PRODAM-SP;

6.6. Os gestores das unidades organizacionais são responsáveis por adotar medidas de conformidade, gestão de riscos e controles internos e verificar continuamente sua eficácia, para garantir o alcance dos objetivos empresariais.

7. DISPOSIÇÕES FINAIS

Qualquer alteração ou revisão da presente Política deverá ser previamente submetida ao Conselho de Administração da PRODAM-SP.

Os casos omissos serão apreciados pela Diretoria Executiva da PRODAM-SP.

ROGERIO IGREJA BRECHA JUNIOR
Diretor-Presidente

MARCOANTONIO MARQUES DE OLIVEIRA
Presidente do Conselho de Administração

ANEXO
LEGISLAÇÃO E DOCUMENTOS RELACIONADOS

Esta política foi elaborada com base nos dispositivos legais, estatutários e regulamentos internos aplicáveis, abaixo listados:

LEIS

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 Regulamento 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 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 a constituição da PRODAM-SP.

DECRETOS

Decreto Municipal 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.

OUTROS DOCUMENTOS EXTERNOS

Instrução da CVM 358, de 03/01/2002 (Comissão de Valores Mobiliários)

Dispõe sobre a divulgação e uso de informações sobre ato ou fato relevante relativo às companhias abertas, disciplina a divulgação de informações na negociação de valores mobiliários e na aquisição de lote significativo de ações de emissão de companhia aberta, estabelece vedações e condições para a negociação de ações de companhia aberta na pendência de fato relevante não divulgado ao mercado;

Instrução Normativa Conjunta da CGU e Ministério do Planejamento nº 01 de 10/05/2016

Dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo federal;

Política Corporativa de Gestão de Riscos, Controle Interno e Conformidade do SERPRO

Normas ABNT (Associação Brasileira de Normas Técnicas);

ISO 31000:2009, 31010:2012 e GUIA 73:2009;

COSO (*Committee of Sponsoring Organizations of the Treadway Commission*) I e II.

OUTROS DOCUMENTOS INTERNOS

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.

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.

HISTÓRICO DE ALTERAÇÕES

Versão	Alteração	Origem da Alteração