

PLANO DE GESTÃO DE RISCOS PARA INTEGRIDADE



PREFEITURA DE
SÃO PAULO
SUBPREFEITURA
PIRITUBA E JARAGUÁ

Subprefeitura Pirituba/Jaraguá

2025 - 2028

Rua Dr. Carlos da Cunha Matos, 67

São Paulo - SP

CEP 05140-040

pirituba@smsub.prefeitura.sp.gov.br

Subprefeita

Luciana Torralles Ferreira

Equipe de Integridade

Tatiane Aparecida Vicente

Responsável pelo Controle Interno

Isabella Romagnoli Guedes

Jeferson Neres dos Santos Pereira

Lucileila do Rosário Queiroz

Renata Duarte Monteiro

Permitida a reprodução desta obra, de forma parcial ou total, sem fins lucrativos, desde que citada a fonte ou endereço da internet no qual possa ser acessada integralmente em sua versão digital.

Sumário

1	Objetivo.....	4
2	Fundamentação.....	4
3	Escopo.....	4
4	Princípios de Gestão de Riscos	4
5	Governança do Processo	5
5.1	Estrutura.....	5
5.2	Atribuições	5
6	Metodologia.....	5
	Fases segundo o Manual CGM-SP:.....	5
7	Matriz de Riscos de Integridade	5
7.1	Riscos Finalísticos	5
	Risco 1 – Interferência externa ou favorecimento indevido em ações fiscalizatórias.....	5
	Risco 2 – Concessão irregular de licenças, alvarás e documentos autorizativos	6
7.2	Riscos de Apoio	6
	Risco 3 – Irregularidades em contratos, pagamentos e medições	6
	Risco 4 – Atendimento inadequado ao público e falhas de transparência	6
	Risco 5 – Fragilidades em processos internos (documentação, SEI, arquivos).....	7
	Risco 6 – Acesso não autorizado a dados pessoais	7
	Risco 7 – Retenção indevida de documentos e arquivos contendo dados pessoais.....	7
	Risco 8 – Tratamento inadequado de dados pessoais sensíveis.....	7
8	Tratamento dos Riscos – Plano de Ação Consolidado	8
9	Monitoramento e Avaliação	8
10	Comunicação e Cultura De Integridade.....	9
11	Revisão.....	9
12	Apetite ao risco.....	9
12.1	Conceito de Appetite ao risco	9
12.2	Relação com a Integridade.....	10
12.3	Apetite ao risco aplicado à Subprefeitura Pirituba	10

1 Objetivo

O Plano de Gestão de Riscos para Integridade tem por objetivo, estabelecer processos, responsabilidades e instrumentos para a identificação, avaliação, tratamento e monitoramento de riscos que possam comprometer a integridade administrativa, a legalidade dos atos, a continuidade das atividades e a confiança da sociedade nas ações da Subprefeitura Pirituba.

2 Fundamentação

O presente plano segue as diretrizes do Manual de Gestão de Riscos da CGM-SP, bem como princípios previstos em:

- Decreto Municipal de Integridade Pública e Gestão de Riscos;
- Normas internas do Município de São Paulo;
- Boas práticas de gestão pública (COSO, ISO 31000).

3 Escopo

O plano abrange os processos finalísticos e de apoio da Subprefeitura Pirituba, especialmente:

- Fiscalização de Posturas e Atividades Urbanas
- Zeladoria Urbana
- Atendimento ao Público / Praças de Atendimento
- Gestão de Contratos
- Licenciamento Urbanístico
- Administração Interna (RH, compras, contratos, frota)

4 Princípios de Gestão de Riscos

Conforme o manual da CGM-SP:

1. Transparência
2. Responsabilidade
3. Melhoria contínua
4. Foco em integridade
5. Proporcionalidade
6. Participação das áreas envolvidas

5 Governança do Processo

5.1 Estrutura

- **Patrocinador institucional:** Subprefeito(a)
- **Unidade de Controle Interno e Gestão de Riscos:** Supervisores das áreas + representantes da Unidade de Controle Interno
- **Gestores de Riscos:** Supervisores das áreas e Coordenadores
- **Equipes responsáveis:** Equipes executoras das atividades

5.2 Atribuições

- **Unidade de Controle Interno:** validações, priorização de riscos, aprovação do plano
- **Gestor de Riscos:** coordenação, consolidação de matrizes, relatórios
- **Pontos focais:** identificação, registro e atualização das informações

6 Metodologia

Fases segundo o Manual CGM-SP:

1. Contextualização
2. Identificação dos riscos
3. Análise dos riscos (probabilidade × impacto)
4. Avaliação e priorização
5. Tratamento dos riscos
6. Implementação dos controles
7. Monitoramento e comunicação

7 Matriz de Riscos de Integridade

A matriz abaixo segue parâmetros usuais da CGM-SP (escala de 1 a 5).

7.1 Riscos Finalísticos

Risco 1 – Interferência externa ou favorecimento indevido em ações fiscalizatórias

- **Causa:** Pressão política; influência econômica; falhas de rastreabilidade.
- **Impacto:** Desvio de finalidade, responsabilização, perda de confiança social.
- **Probabilidade:** Média

- **Impacto:** Alto
- **Nível de risco:** Alto
- **Controles existentes:** Ordem de serviço; sistemas de registros; supervisão.
- **Ações de tratamento:**
 - Auditorias internas semestrais
 - Treinamento sobre integridade

Risco 2 – Concessão irregular de licenças, alvarás e documentos autorizativos

- **Causa:** Falhas procedimentais; documentação incompleta; interpretação divergente da legislação; pressão externa.
- **Probabilidade:** Média
- **Impacto:** Alto
- **Nível:** Alto
- **Ações de tratamento:**
 - Checklists padronizados
 - Procedimentos revisados e publicados
 - Dupla checagem em casos sensíveis
 - Capacitação permanente

7.2 Riscos de Apoio

Risco 3 – Irregularidades em contratos, pagamentos e medições

- **Probabilidade:** Média
- **Impacto:** Alto
- **Ações de tratamento:**
 - Checklists de fiscalização contratual
 - Publicação de POPs
 - Separação de funções (quem solicita ≠ quem fiscaliza)
 - Cadastro de riscos por contrato

Risco 4 – Atendimento inadequado ao público e falhas de transparência

- **Probabilidade:** Baixa
- **Impacto:** Médio
- **Tratamento:**
 - Padronização dos roteiros de atendimento (Instruções de Trabalho – LGPD)
 - Relatórios mensais de reclamações

Risco 5 – Fragilidades em processos internos (documentação, SEI, arquivos)

- **Probabilidade:** Média
- **Impacto:** Médio
- **Ações de Tratamento:**
 - Padronização de processos (Instruções de Trabalho – LGPD)
 - Auditorias internas semestrais

Risco 6 – Acesso não autorizado a dados pessoais

- **Causa:** Compartilhamento inadequado de credenciais; ausência de controle de acesso por perfil; consulta indevida a processos e prontuários; falhas no gerenciamento de permissões.
- **Impacto:** Violação da LGPD; quebra de sigilo; responsabilização administrativa; danos à imagem institucional.
- **Probabilidade:** Média
- **Impacto:** Alto
- **Nível de risco:** Alto
- **Controles existentes:** controle de acesso mediante login e senha; restrição de acesso nos processos SEI; Instruções de Trabalho com definição de responsáveis.
- **Ações de Tratamento:**
 - Auditorias de acesso aos sistemas corporativos;
 - Capacitação anual em LGPD.

Risco 7 – Retenção indevida de documentos e arquivos contendo dados pessoais

- **Causa:** Manutenção de cópias em computadores locais; armazenamento em pastas compartilhadas; falha na exclusão de arquivos temporários, e-mails ou documentos digitalizados.
- **Impacto:** Exposição indevida de dados pessoais; descumprimento da LGPD; aumento da superfície de risco.
- **Probabilidade:** Média
- **Impacto:** Médio
- **Nível de risco:** Médio
- **Controles existentes:** orientação para exclusão de arquivos temporários; utilização do SEI como repositório oficial.
- **Ações de Tratamento:**
 - Verificações periódicas de conformidade.

Risco 8 – Tratamento inadequado de dados pessoais sensíveis

- **Causa:** Falhas na proteção de prontuários funcionais; manuseio inadequado de laudos médicos; compartilhamento indevido de informações de saúde.

- **Impacto:** Grave violação à privacidade; responsabilização institucional; danos ao titular.
- **Probabilidade:** Baixa
- **Impacto:** Muito Alto
- **Nível de risco:** Alto
- **Controles existentes:** arquivamento físico controlado; restrição de acesso aos prontuários.
- **Ações de Tratamento:**
 - Controle formal de consulta aos prontuários com registro de acessos;
 - Revisão anual dos procedimentos da SUGESP.

8 Tratamento dos Riscos – Plano de Ação Consolidado

Nº	Ação	Área Responsável	Prazo	Indicador	Status
1	Instituir Unidade de Controle Interno	Gabinete	-	Portaria publicada	Feito
2	Criar checklists padronizados para licenciamento	Supervisão de Planejamento / CPDU	45 dias	Checklists elaborados	Feito
3	Revisar POPs da fiscalização contratual	Sup. Adm. / Unidades que fiscalizam contratos	90 dias	POP revisado	Feito
4	Treinamento de integridade para servidores	SUGESP	180 dias	% treinados	Feito
5	Atualizar a matriz de riscos	Gestores de Riscos	30 dias	Matriz publicada	Feito
6	Realizar auditoria interna na fiscalização	Unidade de Controle Interno	180 dias	Relatório de Auditoria emitido	Pendente
7	Realizar auditoria de conformidade LGPD nos processos com tratamento de dados pessoais	Unidade de Controle Interno + Núcleo LGPD	180 dias	Relatório de auditoria emitido	Pendente
8	Capacitar servidores sobre LGPD, privacidade e proteção de dados	SUGESP + Controle Interno + Núcleo LGPD	anual	Percentual de servidores capacitados	Pendente
9	Revisar as Instruções de Trabalho relacionadas ao tratamento de dados pessoais	Núcleo LGPD + Unidades Responsáveis	anual	Quantidade de ITs revisadas	Pendente

9 Monitoramento e Avaliação

- Reuniões semestrais da Unidade de Controle Interno e Gestores de Riscos
- Atualização anual da matriz de riscos
- Indicadores:
 - Número de riscos tratados
 - Controles implementados
 - Percentual de capacitação
 - Relatório anual enviado ao Gabinete e, quando aplicável, à CGM-SP
 - Número de incidentes de privacidade e integridade registrados

- Percentual de processos com restrição de acesso corretamente aplicada
- Percentual de servidores capacitados em LGPD
- Quantidade de auditorias de conformidade realizadas em LGPD
- Quantidade de não conformidades identificadas e corrigidas em LGPD
- Percentual de unidades com revisão anual das Instruções de Trabalho

10 Comunicação e Cultura De Integridade

- Divulgação interna do plano de gestão de riscos e da matriz de riscos
- Canal interno para comunicação de irregularidades
- Treinamentos regulares, incluindo temas de assédio, comportamento ético, conflitos de interesse
- Inserção de conteúdo de integridade e LGPD na integração de novos servidores

11 Revisão

O plano deve ser revisado sempre que houver:

- Alterações estruturais na Subprefeitura
- Mudanças relevantes na legislação
- Ocorrências críticas ou auditorias da CGM
- Pelo menos 1 vez ao ano

12 Appetite ao risco

12.1 Conceito de Appetite ao risco

Appetite ao risco é o nível de risco que uma organização está disposta a aceitar no alcance de seus objetivos — sem comprometer sua integridade, legalidade ou imagem institucional. Em outras palavras, é o limite entre o risco aceitável e o risco inaceitável.

Ele define até que ponto a Subprefeitura pode tolerar incertezas, considerando:

- sua missão institucional;
- o interesse público;
- as normas legais e éticas;
- a capacidade de controle e resposta.

12.2 Relação com a Integridade

No contexto de **integridade pública**, o apetite ao risco **não é o mesmo que assumir riscos ilegais ou antiéticos**.

Ele serve para diferenciar:

- **Riscos aceitáveis:** inerentes à atividade pública e controlados por boas práticas (ex.: decisões técnicas sujeitas a diferentes interpretações legais);
- **Riscos não aceitáveis:** aqueles que afetam princípios éticos, violam normas, causam dano à imagem da Administração ou configuram corrupção, fraude ou favorecimento.

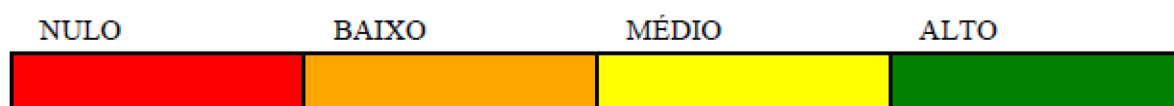
Assim, o **apetite ao risco para integridade** tende a ser **baixo ou nulo** em relação a:

- Corrupção ou fraude;
- Conflito de interesses;
- Desvio de finalidade;
- Quebra de sigilo;
- Discriminação ou assédio;
- Falta de transparência.

12.3 Apetite ao risco aplicado à Subprefeitura Pirituba

Área / Processo	Tipo de Risco	Apetite ao Risco	Justificativa
Fiscalização	Favorecimento indevido / interferência externa	Nulo	Fere princípios de impessoalidade e legalidade
Licenciamento	Erro procedimental sem dolo	Baixo	Deve ser evitado, mas pode ocorrer por falhas humanas passíveis de correção
Contratos	Atraso na execução de contrato	Médio	Pode ser tolerado se houver plano de mitigação e controle financeiro
Atendimento ao público	Reclamações por demora	Médio	Inerente à limitação de recursos, desde que haja transparência
Integridade / Ética	Assédio, corrupção, fraude	Nulo	Inaceitável sob qualquer circunstância
Administração interna	Falhas operacionais em sistemas	Médio	Tolerável, desde que rapidamente corrigido
Todas que manipulam dados pessoais	Acesso não autorizado a dados pessoais	Nulo	Viola a LGPD, a confidencialidade e a confiança institucional
Todas que manipulam dados pessoais	Compartilhamento indevido de dados pessoais	Nulo	Contraria os princípios da finalidade, necessidade e adequação
SUGESP	Exposição de dados pessoais sensíveis (saúde e prontuários)	Nulo	Pode causar danos significativos aos titulares e responsabilização institucional
Todas que manipulam dados pessoais	Falhas na exclusão de arquivos temporários e documentos digitais	Baixo	Tolerável apenas de forma excepcional e mediante ação corretiva imediata
Sistemas e Processos	Erros na aplicação de restrições de acesso no SEI	Baixo	Deve ser objeto de monitoramento contínuo e correção prioritária

Termômetro do Apetite ao Risco



A Subprefeitura Pirituba adota apetite ao risco baixo a nulo para todos os riscos relacionados à integridade pública, ética, transparência e legalidade. Riscos operacionais e administrativos de baixo impacto poderão ser tolerados, desde que acompanhados por controles mitigadores eficazes e plano de ação corretivo.

Como o PGRI já adota apetite baixo ou nulo para riscos relacionados à integridade, ética, transparência, quebra de sigilo e legalidade, os riscos de privacidade devem ser enquadrados predominantemente como apetite nulo, especialmente quando envolverem acesso indevido, compartilhamento indevido ou exposição de dados pessoais e dados pessoais sensíveis.