2026

Política de Privacidade e Proteção de Dados Pessoais Institucional da SMIT

PREFEITURA RIO | Integridade e Transparência

Política de Privacidade e Proteção de Dados Pessoais Institucional da SMIT

1. Introdução e Objetivo

A Secretaria Municipal de Integridade e Transparência (SMIT) reafirma seu compromisso com a cultura da ética, integridade e proteção dos dados pessoais. Esta Política tem como **objetivo** estabelecer as diretrizes para o tratamento de dados pessoais na SMIT, garantindo que a transparência pública caminhe lado a lado com a proteção dos direitos fundamentais de liberdade e privacidade dos cidadãos e colaboradores.

2. Aplicabilidade

Esta política aplica-se a:

- Todos os agentes públicos (estatutários, comissionados, requisitados) da SMIT;
- Estagiários e prestadores de serviço;
- Terceiros ou entidades parceiras que processem dados em nome da SMIT.

3. Finalidade

O tratamento de dados pessoais pela SMIT ocorre para o estrito cumprimento de suas competências legais, que incluem:

- Combate à corrupção e promoção da integridade pública;
- Gestão dos canais de transparência passiva e ativa;
- Realização de avaliação da integridade de agentes públicos e fornecedores;
- Gestão administrativa e de recursos humanos interna;
- Gestão de contratos e de prestação de serviços;
- Fornecimento de capacitações, palestras e oficinas;
- Organização de eventos;
- Atendimento ao cidadão através da Ouvidoria e da Central Anticorrupção.

4. Princípios da LGPD

A SMIT observa rigorosamente os pilares da LGPD:

- **Finalidade:** uso dos dados para propósitos específicos e legítimos vinculados às atribuições da Secretaria.

- **Adequação:** O tratamento é compatível com as finalidades informadas.
- **Necessidade:** Coletamos apenas o mínimo de dados necessários para atingir o objetivo público (princípio da minimização).
- **Livre acesso**: garantir aos titulares o direito de acesso facilitado às suas informações.
- **Qualidade:** Garantimos aos titulares que seus dados sejam exatos e atualizados, conforme a necessidade do serviço.
- **Segurança:** adotar medidas técnicas administrativas para proteger os dados contra acessos não autorizados, vazamentos ou outras formas de tratamento inadequado.
- **Transparência:** informar de forma clara e acessível sobre o tratamento de dados realizado.
- **Prevenção**: antecipar e evitar a ocorrência de danos aos titulares dos dados.
- **Não discriminação**: vedar o tratamento que vise fins discriminatórios ilícitos ou abusivos.

5. Direitos do Titular de Dados

A SMIT assegura ao cidadão e aos seus colaboradores o exercício de seus direitos, incluindo:

1. **Confirmação e Acesso:** Saber se existe tratamento e acessar seus dados.
2. **Correção:** Retificar dados incompletos ou inexatos.
3. **Eliminação/Bloqueio:** Quando os dados forem desnecessários ou tratados em desconformidade com a lei.
4. **Informação:** Saber com quais entidades públicas ou privadas a SMIT compartilhou dados.

6. Ciclo de Vida dos Dados Pessoais

O tratamento de dados na SMIT segue as etapas:

- **Coleta:** Realizada de forma transparente (ex: formulários inscrição nas capacitações, atendimento a chamados pelo 1746).
- **Processamento e Armazenamento:** Em ambiente seguro, seguindo as diretrizes de segurança da informação da Prefeitura.
- **Eliminação:** Após cumprida a finalidade pública e os prazos legais de guarda, os dados serão descartados ou anonimizados

7. Gestão de Acesso

O acesso aos dados pessoais dentro da SMIT deve ser feito em estrito cumprimento ao exercício de funções públicas, e deve respeitar:

- **Necessidade de Saber:** O acesso é concedido apenas a servidores cujas funções exijam o conhecimento de tais dados.
- **Credenciais Únicas:** É proibido o compartilhamento de senhas e logins.
- **Rastreabilidade:** As operações de tratamento deixam logs para fins de auditoria.
- **Vedação de acesso a terceiros**: terceiros que não servidores públicos da SMIT não devem acessar os dados - incluindo ex-funcionários que não pertençam mais aos quadros da Secretaria

8. Segurança da Informação e Boas Práticas

A SMIT deve adotar medidas técnicas e administrativas para proteger dados contra acessos não autorizados e incidentes, entre as quais:

- **Criptografia e Backup:** Proteção de dados em trânsito e em repouso.
- **Cuidado com Documentos Físicos:** Mesas limpas e armários trancados ao final do expediente.
- **Comunicação Segura:** Uso de canais institucionais para o envio de dados pessoais.

> **Importante:** A segurança da informação é uma responsabilidade coletiva e é também uma questão organizacional! O uso ético e seguro dos dados é o pilar da nossa integridade!

9. Funções e Responsabilidades

A governança de dados na SMIT é dividida entre:

Ator	**Responsabilidades**
Encarregadas de Dados Setoriais da SMIT	Atuar como canal de comunicação entre SMIT, titulares de dados pessoais e a Autoridade Nacional (ANPD); orientar servidores sobre boas práticas.
Comitê de Privacidade (CPDP)	Definir diretrizes estratégicas, avaliar riscos, elaborar as documentações do Programa de Governança em Privacidade e deliberar sobre

	a ocorrência de incidentes de segurança de dados, cabendo eventualmente recomendar a comunicação para a ANPD e necessariamente realizar o registro.
Servidores Públicos da SMIT	- Tratar os dados dos chamados 1746 somente para a prestação do serviço solicitado. - Tratar os dados pessoais contidos em processos do PROCESSO.RIO e SEI.RIO somente para a prestação do serviço solicitado. - Garantir que planilhas e relatórios não tratem dados pessoais desnecessários. - Utilizar dados de cidadãos e servidores com zelo e sempre ter finalidade definida. ▪ Incluir cláusulas de proteção de dados em contratos e instrumentos jurídicos congêneres.

10. Treinamento e Conscientização

A SMIT promoverá ações contínuas de capacitação. Participar dos treinamentos sobre LGPD e integridade não é apenas uma norma, mas um requisito para o exercício da função pública moderna e segura.

11. Contato

Em caso de dúvidas sobre esta Política, solicitações de direitos ou reporte de incidentes, o titular deve entrar em contato com os membros do Comitê de Privacidade da SMIT:

- **Consultar:** Encarregadas de Dados Pessoais Setoriais da SMIT.
- **E-mail:** lgpd.smit@prefeitura.rio

12. Versão e Revisão

Versão	Data	Descrição	Responsável
1.0	06/2026	Aprovação da Política de Privacidade Institucional pelo Comitê (CPDP / SMIT)	CPDP / SMIT

Esta Política deve ser revisada anualmente pelo CPDP/SMIT, ou sempre que houver alteração relevante na legislação, na estrutura da SMIT ou nas operações de tratamento de dados, preferencialmente em alinhamento com o ciclo anual do Índice de Avaliação da Adequação à LGPD (IAALGPD).

Anexo I: o que pode ou que não pode

O perigo da exposição indevida

A LGPD também protege como os dados são exibidos, armazenados e compartilhados. Mesmo sem vazamento digital, a exposição física ou visual de informações pessoais já configura falha de segurança.

Exemplo: Uma planilha impressa com nomes, telefones e endereços deixada na impressora, que pode ser fotografada ou levada por alguém indevidamente.

Formas comuns de exposição indevida

Documentos impressos visíveis — planilhas, listas de presença, protocolos abertos sobre mesas ou deixados na impressora.

E-mails sem sigilo — com anexos contendo dados pessoais enviados para grupos ou destinatários errados.

Mensagens em aplicativos — compartilhamento de dados via WhatsApp ou grupos informais.

Capturas de tela e fotos de documentos — imagens de relatórios ou fotos da tela do computador circulando fora dos canais oficiais.

Pastas de rede sem controle — arquivos compartilhados sem senha ou restrição de acesso. **Ponto de atenção:** o acesso às pastas compartilhadas deve ser removido assim que o funcionário for desligado da equipe! É atribuição da chefia imediata providenciar a remoção de acesso do servidor que não pertencer mais à Secretaria!

Compartilhamento das informações com terceiros não autorizados - servidores públicos que acessam dados no exercício de uma função pública não podem compartilhar tais informações com terceiros não autorizados.

Utilização das redes sociais - postar imagens em redes sociais que, voluntária ou involuntariamente, mostrem documentos da Secretaria que não sejam públicos, tais como: imagens que mostram a tela do computador ou documentos que estejam em cima das estações de trabalho.

Boas práticas para evitar exposição indevida

Mantenha o sigilo visual – evite documentos com dados pessoais expostos em mesas ou balcões.

Use senhas e permissões – em planilhas, sistemas e arquivos compartilhados.

Evite cópias desnecessárias – quanto menos duplicação, menor o risco.

Verifique antes de enviar – confirme destinatários de e-mails e mensagens.

Guarde e descarte corretamente – triture papéis e apague arquivos que não são mais necessários.

Evite compartilhamento indevido - não compartilhe dados pessoais com a imprensa, com empresas não identificadas, com terceiros não autorizados.

Anexo II: Checklist: Minha Mesa é Segura?

Guia Prático de Proteção de Dados para o Servidor

💻 Ao Sair da Mesa (Mesmo por 1 minuto!)

- [ ] **Bloqueei a tela?** (Atalho: Windows + L).
- [ ] **Mesa limpa?** Não deixei processos, listagens ou documentos com dados pessoais (CPF, nomes, endereços) expostos.
- [ ] **Gavetas trancadas?** Documentos sensíveis estão guardados e a chave está comigo.

📧 Ao Enviar E-mails e Mensagens

- [ ] **Destinatário correto?** Conferi duas vezes se o "João Silva" é o servidor certo ou um cidadão externo.
- [ ] **Cópia Oculta (Cco)?** Se o e-mail é para várias pessoas externas, escondi os endereços delas no campo Cco.
- [ ] **Anexo seguro?** Verifiquei se o arquivo anexado contém apenas o necessário (removi abas ocultas em Excel ou dados desnecessários).

📁 No Manuseio de Documentos

- [ ] **Impressão recolhida?** Não deixei documentos parados na bandeja da impressora comum.
- [ ] **Pendrives na impressora?** Ao terminar de usar a impressora, retire o pendrive.
- [ ] **Descarte correto?** Papéis com dados pessoais foram para a fragmentadora, nunca para o lixo comum.
- [ ] **Digitalização segura?** Após escanear um documento, apaguei o arquivo da memória da multifuncional ou da pasta pública.

📸 Nas Redes Sociais e Fotos

1. [ ] **Fundo da foto limpo?** Verifiquei se não aparecem monitores ligados ou papéis legíveis atrás de mim.
2. [ ] **Dados tarjados?** Se postar um documento oficial, cobri todos os dados que identifiquem pessoas físicas.
3. [ ] **Ambiente preservado?** Evitei expor o rosto de cidadãos em atendimento sem autorização.

🔐 Segurança Digital

- [ ] **Senhas protegidas?** Não tenho post-its com senha no monitor ou sob o teclado.
- [ ] **Rede oficial?** Estou usando a VPN ou a rede da Prefeitura (evite Wi-Fi público para tratar dados da SMIT).

- [ ] **Suspeita de Incidente?** Se vi algo errado ou perdi um token/documento, já avisei as Encarregadas de Dados.

Dúvidas ou Incidentes?

Entre em contato imediatamente com as **Encarregadas de Dados da SMIT**.

A proteção de dados começa com a nossa integridade!

Para saber mais acesse a Política de Privacidade Institucional da SMIT disponível em: https://smit.prefeitura.rio/lgpd/

PREFEITURA
RIO

Integridade e
Transparência

integridade_rio smit_rio

smit.prefeitura.rio