POLÍTICA DE SEGURANÇA DA INFORMAÇÃO (PSI)
MUNICÍPIO DE MERIDIANO – SP

1. Introdução

A informação é um ativo essencial do Município e precisa ser protegida contra acessos indevidos, falhas técnicas ou mau uso. Esta Política de Segurança da Informação (PSI) estabelece regras claras para garantir que os dados, sistemas e equipamentos sejam utilizados de forma segura, responsável e em conformidade com a legislação.

2. Objetivos

- ✓ Proteger a **confidencialidade, integridade e disponibilidade** das informações municipais.
- ✓ Reduzir riscos de falhas ou incidentes de segurança digital.
- ✓ Cumprir a **Lei Geral de Proteção de Dados (LGPD)** e demais normas legais.
- ✓ Promover **uso responsável da tecnologia** entre servidores e colaboradores.
- ✓ Estabelecer **procedimentos claros** para incidentes de segurança.

3. Abrangência

Esta política é obrigatória para todos que utilizam recursos de TI da Prefeitura: servidores efetivos, comissionados, contratados, estagiários e prestadores de serviços.

4. Diretrizes Principais

4.1 Responsabilidades

- ✓ **Responsável de TI:** coordena a aplicação da PSI, controla acessos e responde a incidentes.
- ✓ **Gestores de Secretarias:** garantem que suas equipes cumpram as regras.
- ✓ **Servidores e Colaboradores:** devem usar os recursos de forma adequada e comunicar falhas ou incidentes.

4.2 Controle de Acesso

- ✓ Cada usuário deve ter **login e senha individuais**.
- ✓ Senhas devem ser seguras e trocadas periodicamente.
- ✓ O acesso é concedido apenas conforme a função de cada servidor.
- ✓ Em desligamentos ou afastamentos, acessos devem ser cancelados de imediato.

4.3 Proteção de Dados

- ✓ Seguir a **LGPD** em todas as atividades que envolvam dados pessoais.
- ✓ Coletar e armazenar apenas informações necessárias e por tempo limitado.
- ✓ Backup diário (local) e semanal (nuvem), com testes periódicos de restauração.

- ✓ Descarte seguro de documentos e mídias contendo dados.

4.4 Uso Aceitável

- ✓ Os recursos de TI devem ser usados **exclusivamente para fins institucionais**.
- ✓ É proibido instalar softwares não autorizados, acessar conteúdos ilegais ou compartilhar senhas.
- ✓ O e-mail institucional é para uso de trabalho; não deve ser usado para spam, correntes ou fins pessoais.

4.5 Incidentes de Segurança

- ✓ Todo incidente (vírus, acesso indevido, perda de dados) deve ser comunicado imediatamente ao setor de TI.
- ✓ O setor de TI deve registrar, analisar e tratar os incidentes, tomando medidas de contenção e recuperação.
- ✓ Após cada incidente, deve ser feita uma avaliação para evitar repetições.

4.6 Conscientização

- ✓ Todos os servidores devem receber orientações simples sobre boas práticas de segurança digital.
- ✓ Capacitações básicas serão realizadas anualmente.

5. Segurança Física e Ambiental

- ✓ O acesso a equipamentos críticos (servidores, roteadores) deve ser restrito.
- ✓ Equipamentos devem ser protegidos contra quedas de energia (uso de nobreaks) e riscos ambientais (fogo, água).

6. Monitoramento e Auditoria

- ✓ O setor de TI deve acompanhar os acessos aos sistemas e verificar logs de atividades suspeitas.
- ✓ Auditorias simplificadas devem ser feitas anualmente.

7. Penalidades

O uso inadequado dos recursos de TI ou a violação desta política poderá gerar:

- ✓ Advertência;
- ✓ Suspensão de acesso;
- ✓ Processo administrativo;
- ✓ Responsabilização civil e criminal, conforme a gravidade.

8. Revisão da Política

A PSI será revisada anualmente ou sempre que houver mudanças relevantes na legislação, nos sistemas utilizados ou na infraestrutura de TI.

9. Disposições Finais

Esta Política entra em vigor na data de sua aprovação e deve ser cumprida por todos os servidores e colaboradores. Seu objetivo é garantir segurança digital, proteger dados e fortalecer a confiança da população na administração municipal.

Meridiano, 09 de dezembro de 2025.