PLANO DE RESPOSTA A INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

Município de São Francisco de Assis/RS

1. OBJETIVO

Estabelecer procedimentos para identificar, conter, corrigir e comunicar incidentes de segurança da informação, garantindo a proteção de dados, continuidade dos serviços e mitigação de impactos, conforme boas práticas de segurança da informação e, quando aplicável, a Lei nº 13.709/2018 (LGPD).

2. ABRANGÊNCIA

Aplica-se a todos os órgãos, servidores, estagiários, terceirizados e fornecedores que lidem com sistemas, informações digitais ou documentos físicos da Prefeitura.

3. DEFINIÇÃO DE INCIDENTE DE SEGURANÇA

Incidente de segurança é qualquer evento que comprometa autenticidade, confidencialidade, integridade, irretratabilidade e disponibilidade das informaçõe**s**, incluindo:

- Vazamento, perda ou acesso não autorizado a dados;
- Alteração indevida de informações;
- Falhas em sistemas ou equipamentos;
- Ataques cibernéticos, malware, ransomware ou phishing;
- Extravio de documentos físicos contendo informações sensíveis ou pessoais.

4. DIRETRIZES DE RESPOSTA

4.1 Identificação e Registro

- Todos os incidentes devem ser imediatamente reportados ao departamento de tecnologia da informação ou à autoridade responsável pela segurança da informação.

- Registrar: data, hora, responsável, descrição do incidente, sistemas ou informações afetadas e possíveis impactos.

4.2 Classificação e Avaliação

- Avaliar a gravidade do incidente: baixo, médio ou alto impacto.

- Identificar se há envolvimento de dados pessoais ou sensíveis.

4.3 Contenção e Mitigação

- Isolar sistemas comprometidos.

- Revogar acessos não autorizados.

- Corrigir vulnerabilidades e aplicar medidas de segurança emergenciais.

4.4 Comunicação e Notificação

- Para incidentes envolvendo dados pessoais:

    - Comunicar os titulares afetados, quando houver risco relevante;

    - Notificar a **Agência Nacional de Proteção de Dados (ANPD)**, se exigido por lei;

- Para incidentes internos: informar gestores e autoridades responsáveis.

4.5 Análise Pós-Incidente

- Avaliar a causa raiz e impacto do incidente.

- Implementar medidas corretivas e preventivas para evitar recorrência.

- Documentar lições aprendidas e atualizar procedimentos.

5. RESPONSABILIDADES

- **Departamento de Tecnologia da Informação:** coordenar resposta, registrar incidentes e monitorar sistemas.

- **Gestores de área:** assegurar que incidentes sejam comunicados e que medidas corretivas sejam aplicadas.

- **Servidores e colaboradores:** reportar incidentes imediatamente e colaborar nas investigações.

6. TREINAMENTO E CONSCIENTIZAÇÃO

- Todos os servidores devem receber treinamento periódico sobre prevenção, identificação e reporte de incidentes.

7. REVISÃO E ATUALIZAÇÃO

- O plano será revisado periodicamente ou sempre que houver mudanças legais, normativas ou de infraestrutura de TI.

- Versões atualizadas serão publicadas e divulgadas a todos os órgãos e colaboradores.

8. DISPOSIÇÕES FINAIS

- O descumprimento das diretrizes do plano poderá gerar sanções administrativas, civis e penais, conforme legislação aplicável.

- Este plano entra em vigor na data de sua publicação.

São Francisco de Assis/RS, de outubro de 2025

Rubemar Paulinho Salbego
Prefeito Municipal de São Francisco de Assis