



PREFEITURA MUNICIPAL DE PIRATININGA

Praça Dr. Mário Ribeiro da Silva, Nº. 14 – Caixa Postal 50

Fone: (14) 3265-9530 – Fax: (14) 3265-9531

CEP: 17490-090 – CNPJ 46.137.451/0001-76 – Piratininga – São Paulo

site: www.piratininga.sp.gov.br - e-mail: contato@piratininga.sp.gov.br

PLANO DE CONTINUIDADE DOS SERVIÇOS DE TIC – PCSTIC

1. IDENTIFICAÇÃO

Documento: Plano de Continuidade dos Serviços de TIC – PCSTIC

Órgão: Prefeitura Municipal de Piratininga

Unidade Responsável: Diretoria de Tecnologia da Informação – DTI

Versão: 1.1

Exercício: 2025

2. OBJETIVO

Estabelecer diretrizes e procedimentos para assegurar a continuidade, recuperação e restabelecimento dos serviços essenciais de Tecnologia da Informação e Comunicação (TIC), minimizando impactos à Administração Pública.

3. FUNDAMENTAÇÃO LEGAL E REFERENCIAL

- Lei nº 13.709/2018 – LGPD
- Lei nº 14.133/2021
- Decreto nº 10.540/2020 – SIAFIC

Referencial técnico (aplicação proporcional):

- ABNT NBR ISO/IEC 27005
- ABNT NBR ISO 31000

A presente política observa, de forma proporcional à estrutura do município, as diretrizes dessas normas, especialmente no que se refere à identificação, análise e tratamento de riscos, bem como à continuidade dos serviços de TIC.

4. ESCOPO

Abrange:

- Sistemas de informação
- Servidores e infraestrutura
- Rede e conectividade
- Serviços em nuvem (SaaS)
- Comunicação institucional
- Ambiente físico de TI

5. DEFINIÇÕES

- Continuidade de TIC: capacidade de manter ou restabelecer serviços
- Incidente: evento que cause indisponibilidade

- Incidente: evento que cause indisponibilidade
- RTO: tempo máximo de recuperação
- RPO: perda máxima de dados aceitável

6. SISTEMAS E MODELO OPERACIONAL

Os sistemas de TIC operam em modelo híbrido, contemplando soluções locais e em nuvem (SaaS).

Sistemas em operação

- SIAFIC – Fiorilli – Local
- Folha de Pagamento – Fiorilli – Local
- Arrecadação – Fiorilli – Local
- Sistema de Saúde – Governança Brasil – SaaS
- e-SUS – Local
- 1Doc – SaaS
- Aprova Digital – SaaS
- GeSUAS – SaaS
- Ponto – Secullum – SaaS
- E-mail e Portal – SaaS
- FortDesk / FortView – SaaS

Modelo de operação

Os sistemas em SaaS são hospedados em infraestrutura de fornecedores (como AWS e Microsoft), com alta disponibilidade, backup e recuperação sob responsabilidade contratual.

Os sistemas locais contam com suporte técnico contratado, incluindo rotinas de backup e recuperação gerenciadas pelos fornecedores.

7. CLASSIFICAÇÃO DE CRITICIDADE

- Alta: SIAFIC, Folha, Arrecadação, Saúde, Internet
- Média: Protocolo, Assistência Social, Ponto, E-mail
- Baixa: Portal institucional

8. INFRAESTRUTURA DE TIC

- Internet
- Rede LAN/Wi-Fi
- Servidores
- Firewall
- Energia (nobreak)

9. IDENTIFICAÇÃO DE RISCOS DE TIC

Os riscos são identificados com base na experiência operacional, histórico de ocorrências e criticidade dos serviços.

Principais riscos:

- Falhas de servidores
- Indisponibilidade de sistemas
- Falhas de conectividade
- Interrupções de energia
- Incidentes de segurança da informação
- Erros operacionais
- Falhas de fornecedores

- Indisponibilidade de serviços em nuvem

10. ESTRATÉGIAS DE CONTINUIDADE

Considerando o modelo híbrido:

I – Sistemas SaaS

Continuidade garantida pelos fornecedores (SLA, backup e redundância).

II – Sistemas Locais

Backup e recuperação gerenciados por fornecedores, com acompanhamento da TI.

III – Infraestrutura

Dependência de energia, rede e equipamentos, com uso de nobreak e suporte técnico.

IV – Política de Backup

As rotinas seguem a política institucional de backup do município.

11. PARÂMETROS DE RECUPERAÇÃO (RTO/RPO)

- Críticos: até 24h
- Administrativos: até 48h
- Apoio: até 72h

12. RESPONSABILIDADES

- DTI: coordenação
- Gestores: apoio
- Fornecedores: suporte e continuidade
- Administração: validação

13. TRATAMENTO DE INCIDENTES

Os incidentes são tratados conforme criticidade, com ações para restabelecimento, acionamento de fornecedores e comunicação à Administração.

Os incidentes relevantes são registrados.

14. AVALIAÇÃO DO PLANO

Baseada nos incidentes ocorridos e nas ações adotadas, visando melhoria contínua.

15. REVISÃO

Anual ou conforme necessidade.

16. INTEGRAÇÃO COM POLÍTICAS INSTITUCIONAIS

Este plano observa as diretrizes da Política de Segurança da Informação e da Política de Backup do Município de Piratininga, disponíveis no portal oficial: <https://www.piratininga.sp.gov.br/public/admin/globalarq/cria/documento-auxiliar/98cfaa2de12d549d4a1e052ceeae211.pdf>

17. DISPOSIÇÕES FINAIS

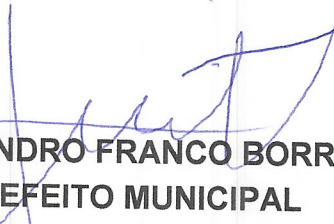
O plano integra a governança de TIC e está alinhado ao PDTIC vigente, sendo executado conforme capacidade operacional e recursos disponíveis.

18. APROVAÇÃO

Piratininga, 30 de maio de 2025



RENATO YOSHIAKI CORREIA HIMENO
DIRETOR DE TECNOLOGIA DA INFORMAÇÃO



CARLOS ALESSANDRO FRANCO BORRO DE MATOS
PREFEITO MUNICIPAL

