Prefeitura Municipal de
Cândido Rodrigues
Estado de São Paulo

PLANO DE GESTÃO DE RISCOS DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO – TIC

Município de Cândido Rodrigues – SP

1. OBJETIVO

Estabelecer diretrizes para a **identificação, análise, avaliação e tratamento de riscos** relacionados à Tecnologia da Informação e Comunicação (TIC) no âmbito da Administração Pública Municipal de Cândido Rodrigues, visando reduzir impactos sobre a continuidade dos serviços públicos e a segurança da informação.

2. ABRANGÊNCIA

Este Plano aplica-se a todos os órgãos, secretarias, setores, unidades administrativas, educacionais, de saúde e assistência social do Município, abrangendo sistemas de informação, infraestrutura tecnológica, redes, equipamentos e serviços de TIC.

3. BASE NORMATIVA E REFERENCIAL

O presente Plano fundamenta-se em:

- Plano Diretor de Tecnologia da Informação e Comunicação – **PDTI 2025–2028**;
- Política de Segurança da Informação – **PSI**;
- Plano de Continuidade dos Serviços de TIC – **PCSTI**;
- Política de Backup e Recuperação de Dados;
- Portaria de criação do Setor de Tecnologia da Informação e do **CGSI**;
- Lei Federal nº 14.129/2021 – Lei de Governo Digital;
- Lei Federal nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD);
- Boas práticas de gestão de riscos (ISO 31000 / ISO 27005);
- Recomendações do Tribunal de Contas do Estado de São Paulo – **TCESP**.

4. CONCEITOS BÁSICOS

- **Risco:** possibilidade de ocorrência de evento que impacte negativamente a confidencialidade, integridade ou disponibilidade das informações e serviços de TIC.
- **Ameaça:** causa potencial de um incidente indesejado.

- **Vulnerabilidade:** fraqueza que pode ser explorada por uma ameaça.
- **Impacto:** consequência da materialização do risco.

5. METODOLOGIA DE GESTÃO DE RISCOS

A gestão de riscos de TIC no Município de Cândido Rodrigues será realizada de forma **simplificada e progressiva** , observando as seguintes etapas:

I – identificação dos riscos;
II – análise e avaliação dos riscos;
III – definição de estratégias de tratamento;
IV – acompanhamento e revisão periódica.

6. IDENTIFICAÇÃO DOS PRINCIPAIS RISCOS DE TIC

Sem prejuízo de outros riscos que venham a ser identificados, destacam-se:

- indisponibilidade de sistemas críticos;
- falhas de infraestrutura de rede e conectividade;
- perda ou corrupção de dados;
- incidentes de segurança da informação;
- falhas nos procedimentos de backup e recuperação;
- dependência de fornecedores e prestadores de serviços;
- indisponibilidade de suporte técnico especializado.

7. ANÁLISE E AVALIAÇÃO DOS RISCOS

Os riscos identificados serão avaliados considerando:

- **probabilidade de ocorrência** ;
- **impacto operacional e institucional** ;
- **criticidade dos serviços afetados** .

A avaliação poderá ser registrada de forma simplificada, utilizando escalas qualitativas (baixo, médio, alto), compatíveis com a realidade administrativa do Município.

8. TRATAMENTO DOS RISCOS

As estratégias de tratamento dos riscos poderão incluir:

I – adoção de medidas preventivas;
II – mitigação por meio de controles técnicos e administrativos;

III – aceitação do risco, quando tecnicamente justificável;
IV – transferência do risco, quando aplicável (ex.: contratos de suporte).

As ações de tratamento deverão observar as diretrizes da PSI, do PCSTI e da Política de Backup.

9. PAPÉIS E RESPONSABILIDADES

9.1 Administração Municipal

- apoiar a implementação da gestão de riscos de TIC.

9.2 Setor de Tecnologia da Informação

- coordenar a identificação e o acompanhamento dos riscos;
- propor medidas de tratamento;
- articular o apoio técnico da empresa prestadora de serviços de TIC.

9.3 Comitê Gestor de Segurança da Informação – CGSI

- acompanhar a gestão de riscos de TIC;
- apoiar a avaliação de riscos críticos;
- propor ajustes e melhorias no Plano.

9.4 Empresa Prestadora de Serviços de TIC

- apoiar tecnicamente a identificação e o tratamento dos riscos, quando contratada.

10. MONITORAMENTO E REVISÃO

A gestão de riscos de TIC deverá ser monitorada periodicamente, com revisão deste Plano sempre que houver mudanças relevantes na infraestrutura, nos sistemas ou no contexto institucional do Município.

11. DISPOSIÇÕES FINAIS

O presente Plano de Gestão de Riscos de Tecnologia da Informação e Comunicação integra o conjunto de instrumentos de governança, segurança da informação e continuidade dos serviços de TIC do Município de Cândido Rodrigues, entrando em vigor na data de sua aprovação.

Cândido Rodrigues – SP
Administração Pública Municipal