TERESÓPOLIS
acima de tudo!

Ciência e Tecnologia

PLANO DE RECUPERAÇÃO DE DESASTRES DE SISTEMAS

Parte do Plano Operacional de Segurança da Informação

Versão 1.0

Junho / 2025

TERÊGOV DIGITAL

Prefeitura Municipal de Teresópolis

Secretaria Municipal de Ciência e Tecnologia

GESTÃO

José Leonardo Vasconcellos de Andrade
Prefeito

André Muniz Pinto
Secretário Municipal de Ciência e Tecnologia

Anderson Marques Duarte
Subsecretário Municipal de Ciência e Tecnologia

Cleiton Evandro Corrêa Pimentel
Diretor de Governança e Dados

Douglas Brian Neves da Penha
Chefe da Divisão de Programação

André Washington Garcia Suarez
Gestor de Infraestrutura / Rede
Encarregado de Proteção de Dados (DPO)

Carlos Augusto Vargas
Gestão de Sistemas

Ezequiel Pacheco dos Santos Machado
Analista Técnico
Ciência da Computação

Gabriel da Costa Garcia
Analista Técnico
Engenharia de Software

Matheus de Oliveira da Conceição
Analista Técnico

INTRODUÇÃO

Em um cenário cada vez mais marcado pela transformação digital e pela crescente dependência de sistemas eletrônicos para a prestação de serviços públicos, a resiliência tecnológica tornou-se um pilar essencial para a gestão municipal. Interrupções inesperadas — seja por falhas técnicas, ataques cibernéticos ou desastres naturais — podem comprometer a continuidade dos serviços e expor dados sensíveis, impactando diretamente a confiança da população e o cumprimento das obrigações legais.

Neste contexto, o Plano de Recuperação de Desastres (PRD) da Prefeitura de Teresópolis visa garantir que, mesmo diante de adversidades, os sistemas críticos da administração sejam restaurados com agilidade, segurança e transparência. O PRD é parte integrante da estratégia de governança digital e está alinhado às exigências da Lei Geral de Proteção de Dados (LGPD), às boas práticas da norma ISO/IEC 27001 e às diretrizes do Decreto Municipal nº 6018/2023.

Mais que um documento técnico, o PRD representa um compromisso institucional com a proteção da informação, a continuidade do serviço público e a mitigação de riscos operacionais — assegurando que a tecnologia continue a servir o cidadão mesmo em momentos de crise.

PLANO DE RECUPERAÇÃO DE DESASTRES (PRD)

1. Objetivos do PRD

- Garantir a continuidade dos sistemas digitais críticos após incidentes.
- Minimizar impactos à integridade, disponibilidade e confidencialidade das informações institucionais.
- Estar em conformidade com a LGPD, ISO/IEC 27001 e com o Decreto Municipal nº 6018/2023.

2. Escopo

- Abrange todos os sistemas digitais da Prefeitura: gestão de dados, redes, servidores, correio eletrônico, portais oficiais públicos, ambientes de TIC e dispositivos móveis.
- Aplica-se a todos os colaboradores e prestadores de serviço, conforme definido na PSI.

3. Classificação de Sistemas Críticos

Recovery Time Objective: RTO

Recovery Point Objective: RPO

Sistema	Prioridade	Tempo Máximo de Perda de Dados **(RPO)**	Tempo Máximo de Recuperação **(RTO)**
Gestão Administrativa RH/Fazenda/Contábil/Processos Eletrônicos)	Alta	1 hora	4 horas
Correio Eletrônico (E-mail)	Média	4 horas	8 horas
Portais Institucionais Principal/Educação/Licitação/Turismo	Alta	1 hora	4 horas
Servidor de Arquivos	Alta	1 hora	6 horas
Sistema de Backup	Crítica	0 hora	4 horas
Portal da Transparência	Média	2 horas	4 horas
Portal de Dados Abertos	Baixa	1 hora	6 horas
Portal dos Conselhos	Baixa	1 hora	6 horas
Gestão da Saúde	Alta	1 hora	2 horas
Gestão da Educação	Alta	1 hora	4 horas
Gestão da Assistência Social	Alta	1 hora	4 horas

PROCEDIMENTO DE SIMULAÇÃO DE DESASTRE

a) Realização de testes práticos (ex: simulações de perda de dados, ataque cibernético, queda de rede).

b) Avaliação da eficácia do plano e tempo de resposta.

c) Registro de lições aprendidas para melhorias contínuas.

Inventário de Ativos

a) Lista detalhada de todos os ativos de TIC (hardware, software, infraestrutura).

b) Identificação de responsáveis por cada ativo.

c) Classificação de criticidade e dependência entre sistemas.

Plano de Continuidade de Negócios (PCN) Integrado

a) Estratégias para manter serviços essenciais enquanto ocorre recuperação técnica.

b) Possibilidade de trabalho remoto ou alternativo, se aplicável.

c) Inclusão das áreas não-TI impactadas por incidentes digitais (ex: atendimento ao cidadão de forma presencial e on-line).

Plano de Capacitação dos Colaboradores

a) Treinamentos periódicos sobre resposta a incidentes.

b) Campanhas de conscientização sobre segurança da informação.

c) Inclusão de orientações específicas para estagiários e colaboradores temporários, conforme previsto na PSI.

Infraestrutura Redundante

a) Uso de servidores espelhados ou em nuvem.

b) Configuração de Failover automático.

c) Linha de internet secundária ou contingência de comunicação.

Registro Formal de Incidentes

a) Sistema para catalogar cada ocorrência com data, impacto, tempo de resolução.

b) Avaliação de recorrência e priorização de prevenção.

c) Interface com o Comitê Gestor de Proteção de Dados e o DPO.

Métricas e Indicadores de Recuperação

a) Percentual de restauração de dados em tempo alvo (RPO/RTO).

b) Tempo médio de indisponibilidade por tipo de incidente.

c) Índice de falhas em testes de backup/restore.

Plano de Atualizações do PRD

a) Cronograma de revisão do PRD (trimestral, semestral ou anual).

b) Inclusão de novas tecnologias, riscos emergentes e mudanças legais.

c) Integração com revisões da PSI versão 3.0.

Etapas para Implementar uma Simulação de Desastre Digital

Definir Objetivos do Simulado

a) Testar tempo de resposta da equipe de TI e SI.

b) Avaliar a eficácia dos backups e restauração.

c) Verificar comunicação entre setores e com o DPO.

d) Identificar falhas nos procedimentos e controles.

Escolher o Cenário de Desastre

Exemplos:

a) Ataque de ransomware em servidores institucionais.

b) Queda de energia que afeta o Data Center.

c) Vazamento de dados pessoais de cidadãos.

d) Falha no sistema de correio eletrônico institucional.

Planejar o Simulado

a) Criar uma narrativa realista do incidente.

b) Definir os sistemas afetados e os impactos esperados.

c) Estabelecer tempo de início e fim do exercício.

d) Designar observadores para registrar ações e decisões.

Mobilizar a Equipe

a) Envolver os gestores de SI, TIC, DPO, Governança de Dados e representantes da Secretaria de Ciência e Tecnologia.

b) Informar previamente os participantes sobre o simulado (sem revelar o cenário).

c) Garantir que todos conheçam seus papéis e responsabilidades.

Executar o Simulado

a) Iniciar o cenário conforme planejado.

b) Monitorar as ações tomadas: isolamento de sistemas, acionamento de backups, comunicação com stakeholders.

c) Registrar tempos de resposta, decisões e dificuldades.

Avaliar e Documentar

a) Realizar uma reunião de avaliação com todos os envolvidos.

b) Elaborar um relatório com pontos fortes, falhas e sugestões de melhoria.

c) Atualizar o PRD e a PSI com base nos aprendizados.

Repetir Periodicamente

a) Realizar simulados completos anualmente e parciais semestralmente.

b) Alternar cenários para cobrir diferentes tipos de riscos.

c) Integrar com treinamentos e campanhas de conscientização.

ESTRATÉGIA DE ADAPTAÇÃO DO SIMULADO

Mapeamento da Estrutura Organizacional

a) Identifique os setores envolvidos diretamente com TIC e Segurança da Informação.

b) Confirme os responsáveis por cada sistema crítico (ex: correio eletrônico, portais, backups).

c) Envolva os nomes citados no PSI: DPO, Diretor de Governança, Gestores de SI e TI.

Escolher Cenários Relevantes

a) Baseie-se em riscos reais enfrentados pela Prefeitura: falha de energia no Data Center, ataque de ransomware, perda de backups, etc.

b) Priorize sistemas com maior impacto na prestação de serviços ao cidadão.

Personalize os Papéis e Responsabilidades

a) Use os cargos e funções descritos no PSI para montar a equipe de simulação.

b) Exemplo: o Diretor de Governança pode ser o coordenador geral; o DPO, responsável pela comunicação com a ANPD.

Integre com o PSI e Normas Internas

a) Certifique-se de que o simulado respeita os princípios de integridade, confidencialidade, disponibilidade e autenticidade.

b) Use os procedimentos de backup, restore, controle de acesso e monitoramento descritos no PSI como base para o exercício.

Capacite os Participantes

a) Realize treinamentos prévios com os colaboradores envolvidos.

b) Crie materiais educativos (cartilhas, vídeos curtos) sobre o plano de recuperação e o simulado.

Documente e Avalie

a) Elabore fichas de avaliação para cada participante.

b) Registre tempos de resposta, decisões tomadas e dificuldades encontradas.

c) Atualize o PRD e o PSI com base nos aprendizados.

Envolva a Alta Gestão

a) Apresente o plano ao Prefeito e Secretários para garantir apoio institucional.

b) Use os resultados do simulado para reforçar a importância da segurança da informação como cultura organizacional.

CENÁRIOS CRÍTICOS REAIS PARA SIMULAÇÕES DE DESASTRE

Ataque Cibernético (Ransomware ou Vazamento de Dados)

a) Invasão de sistemas institucionais com criptografia de dados.

b) Exposição de dados pessoais de cidadãos, violando à LGPD.

c) Interrupção de serviços essenciais como e-mail, portais e sistemas administrativos e tributários;

d) Ataques DDOS para a derrubada de sistemas / sistemas fora do ar

Queda Prolongada de Energia no Data Center

a) Afeta servidores, backups e sistemas críticos;

b) Pode comprometer a integridade dos dados e a continuidade dos serviços.

c) Exige ativação de contingência e restauração rápida / redundância;

d) Exige a ativação rápida de geradores de energia.

Desastre Socioambiental (Enchente ou Deslizamento) / ausência de recursos mínimos de comunicação

a) Impacto físico em infraestrutura de TIC e prédios públicos.

b) Necessidade de evacuação e ativação de serviços remotos com planos específicos de segurança (VPN);

c) Risco de perda de equipamentos e mídias de backup.

Incêndio em Ambiente de Operação ou no Data Center

a) Danos irreversíveis a servidores e ativos de informação.

b) Necessidade de restauração via backups externos (em nuvem);

c) Ativação de plano de contingência com recursos alternativos.

Erro Humano ou Configuração Indevida

a) Exclusão acidental de dados ou logs.

b) Instalação de software não autorizado que compromete a segurança.

c) Violação de normas da PSI e necessidade de responsabilização.

Falha de Comunicação Institucional

a) Interrupção de internet ou rede interna.

b) Impossibilidade de acesso a sistemas e e-mails.

c) Necessidade de canais alternativos e comunicação emergencial.

Contaminação por Código Malicioso em Equipamentos Móveis

a) Propagação de vírus por pendrives ou notebooks.

b) Risco de comprometimento da rede institucional.

c) Necessidade de isolamento e verificação técnica urgente.

IMPACTOS OPERACIONAIS

a) Interrupção de serviços essenciais, como sistemas administrativos, portais institucionais e e-mails.

b) Paralisação de processos internos, afetando atendimento ao cidadão e execução de políticas públicas.

c) Perda de produtividade dos colaboradores, especialmente se os sistemas forem comprometidos por malware ou ransomware.

Impactos na Segurança da Informação

a) Violação da confidencialidade de dados pessoais e institucionais, em desacordo com a LGPD.

b) Comprometimento da integridade de documentos e registros oficiais.

c) Exposição de credenciais e senhas, facilitando ataques futuros.

Impactos Legais e Regulatórios

a) Multas e sanções por descumprimento da LGPD e outras normas de proteção de dados.

b) Obrigatoriedade de notificação à ANPD e aos titulares dos dados.

c) Processos administrativos e judiciais, especialmente se houver negligência comprovada.

Impactos Financeiros

a) Custos com recuperação de sistemas, contratação de especialistas e aquisição de novas ferramentas.

b) Investimentos emergenciais em infraestrutura, como servidores, backups e segurança.

c) Perda de recursos públicos,

Impactos Reputacionais

a) Desconfiança da população quanto à capacidade da Prefeitura de proteger os seus dados.

b) Exposição negativa na mídia, como aconteceu com instituições financeiras afetadas por ataques recentes.

c) Danos à imagem institucional, que podem afetar parcerias e convênios.

Impactos Estratégicos

a) Necessidade de revisão urgente de políticas e procedimentos, como o PSI.

b) Reforço na capacitação dos colaboradores, especialmente sobre engenharia social e boas práticas.

c) Pressão para modernização da infraestrutura de TIC.

MATRIZ DE IMPACTO DE ATAQUE CIBERNÉTICO

Categoria	Descrição do Impacto	Nível de Severidade	Ação Imediata
Operacional	Interrupção de sistemas institucionais, portais e e-mails	Alto	Ativar plano de continuidade e contingência
Segurança da Informação	Vazamento de dados pessoais, quebra de confidencialidade e integridade dos registros	Crítico	Isolar sistemas, notificar DPO e ANPD
Legal/Regulatório	Violação da LGPD, risco de penalidades e processos administrativos	Crítico	Relatar incidente à ANPD, iniciar apuração legal
Financeiro	Custos com recuperação, contratação de serviços emergenciais, compra de infraestrutura	Alto	Acionar recursos de contingência orçamentária
Reputacional	Exposição negativa na mídia, queda de confiança da população	Alto	Estabelecer plano de comunicação com público
Estratégico	Pressão por revisão da PSI e reforço de infraestrutura e governança	Médio	Realizar reunião emergencial com gestores e comitês

Considerações Finais

O Plano de Recuperação de Desastres dos Sistemas foi desenvolvido com o objetivo de assegurar a continuidade dos serviços essenciais da estrutura digital da Prefeitura Municipal de Teresópolis diante de incidentes críticos que comprometam a infraestrutura tecnológica. Por meio da identificação de ativos, avaliação de riscos, definição de estratégias de recuperação e atribuição de responsabilidades, este plano estabelece uma abordagem proativa e estruturada para enfrentar adversidades com agilidade e eficácia.

A implementação e o aperfeiçoamento contínuo do PRD são responsabilidades compartilhadas entre as áreas envolvidas, exigindo comprometimento, capacitação e atualização periódica dos procedimentos aqui descritos. Nesse contexto, a prevenção e a pronta resposta representam pilares fundamentais para a redução dos impactos

operacionais, proteção de dados sensíveis e preservação da confiança de cidadãos, servidores, colaboradores e prestadores de serviços.

Concluímos que este plano não se configura apenas como uma medida técnica, mas como um reflexo do compromisso institucional com a segurança, a resiliência e a responsabilidade na gestão da informação. Essa cultura deve ser permanentemente fomentada e operacionalizada pela Secretaria de Ciência e Tecnologia, como guardiã desta política.