PREFEITURA DE
ARRAIAL DO CABO

Plano de Recuperação de Desastres (PRD) para Sistemas de TI

VERSÃO 1.0

Ficha Técnica

Prefeito Municipal de Arraial do Cabo
Marcelo Magno Felix dos Santos

Vice-Prefeito Municipal de Arraial do Cabo
Diego Silveira

Gabinete do Prefeito
Suellen Rodrigues Cardoso

Secretaria de Governo
Thiago Félix dos Santos

Procuradoria Geral do Município
Milena Alcântara da Silva

Controladoria Geral do Município
Jose Carlos Moura de Carvalho

Secretaria Municipal de Finanças e Orçamento
Denise Mendonça de Macedo Barreto

Secretaria Municipal de Administração Tributária
Oscar Victorino Barreto Neto

Secretaria Municipal de Educação, Cultura, Ciência, Tecnologia, Esporte e Lazer
Bernardo Martins de Alcântara Veiga da Silva

Secretaria Municipal De Administração
Carolina Fraser Lima de Oliveira

Secretaria Municipal De Saúde
Jorge Luiz Diniz Moura Filho

Secretaria Municipal De Segurança Pública
Magda Fraga Martins

Secretaria Municipal De Ordem Pública, Posturas e Fiscalização
Carlos Victor Simões Pereira

Fundação Instituto de Pesca de Arraial do Cabo - FIPAC
Rodrigo de Jesus Felix

Secretaria Municipal De Compras e Licitação
Diogo dos Santos de Morais

Instituto de Desenvolvimento de Arraial do Cabo - IDAC
Rafael Grego de Carvalho

Secretaria Municipal De Obras e Urbanismo
Pedro Reis Cajueiro de Andrade

Ficha Técnica

Secretaria Municipal de Habitação e Regularização Fundiária
Ayron Pinto Freixo

Instituto de Previdência Cabista - IPC
Shanna Barros de Andrade

Secretaria Municipal de Desenvolvimento Social, Trabalho, Renda e Direitos Humanos
Ramon Loureiro Plácido

Secretaria Municipal De Turismo
Genival Alves Pacheco Junior

Secretaria Municipal De Serviços Públicos
Carlos Henrique de Matos Vieira

Secretaria Municipal de Mobilidade Urbana
Maycon Victorino Cardoso

Secretaria Municipal de Ambiente e Saneamento
Pedro Henrique de Mello Correa

Secretaria Municipal de Defesa do Consumidor - PROCON
Silvia Carla de Oliveira

Fundação de Meio Ambiente, Pesquisa, Ciência e Tecnologia - FUNTEC
Ronnie Placido Neves

Equipe Responsável pela elaboração do Plano de Recuperação de Desastres

Subsecretário de Ciência e Tecnologia
Victor Hugo Ferreira Fontes

Coordenador de Modernização e Gestão Digital
Francisco Carlos Lourenço de Mattos

Diretor de Dados e Estatística
Luis Carlos Vieira Granja

Coordenadora de Dados e Estatística
Rayane Ferreira Dias

Assessor de Coleta e Capacitação de Dados Estatísticos
Roberto Rodrigues Felix Ferreira

Sumário

1.OBJETIVO 05

2. ESCOPO 05

Inventário de Hardware 05

Licenciamento de Software 05

Conectividade 05

Interdependências 05

3. Tipos de Desastres Considerados 06

4. Estratégia de Continuidade e Recuperação 06

4.1 Classificação de Sistemas Críticos 06

5. Procedimentos de Recuperação 07

5.1 Antes do Desastre (Prevenção) 07

5.2 Durante o Desastre 07

5.3 Após o Desastre 07

5.4 Comitê de Recuperação de Desastres 08

6. Cadeia de comando e contatos de contingência detalhados abaixo 08

6.1 Contingência 08

6.2 Testes e Atualizações 08

7. Documentação (armazenada física e digitalmente) 08

8. Conformidade 09

1. OBJETIVO

Estabelecer diretrizes e procedimentos para garantir a continuidade dos serviços públicos essenciais e a recuperação rápida dos sistemas de tecnologia da informação (TI) em caso de desastres naturais, falhas técnicas, ataques cibernéticos ou outros eventos críticos

2. ESCOPO

Este plano abrange os sistemas e infraestrutura de TI sob a responsabilidade da Prefeitura Municipal de

Arraial do Cabo, incluindo:

- ✓ Sistemas de gestão municipal (administrativo, financeiro, tributário);
- ✓ Sistemas de saúde e educação;
- ✓ Serviços públicos online;
- ✓ Infraestrutura de rede e data center;
- ✓ E-mails e servidores municipais;
- ✓ Banco de dados e arquivos digitais;
- ✓ Conectividade (links de internet e redes locais);
- ✓ Interdependências entre sistemas.

Inventário de Hardware: - Servidores físicos e virtuais - Storages - Equipamentos de rede (switches, roteadores, firewalls) - Estações de trabalho críticas;

Licenciamento de Software: - Sistemas operacionais - Bancos de dados - Aplicações críticas;

Conectividade: - Provedores com redundância contratada - Links dedicados;

Interdependências: - Mapeamento com diagrama de dependência sistêmica.

3. TIPOS DE DESASTRES CONSIDERADOS

Tipo de Evento	Risco	Impacto Potencial
Desastres naturais	Alto	Operacional, Financeiro, Reputacional
Falhas elétricas ou de hardware	Médio	Operacional, Financeiro
Ataques cibernéticos	Alto	Operacional, Financeiro, Reputacional, Legal
Erros humanos	Médio	Operacional, Financeiro
Incêndios, explosões ou vandalismoBaixo	Baixo	Operacional, Financeiro, Reputacional
Perda de pessoal chave	Médio	Operacional

Tipo de Evento	Risco	Impacto Potencial
Falhas de provedores de serviço	Médio	Operacional, Financeiro
Emergências de saúde pública	Baixo	Operacional

4. ESTRATÉGIA DE CONTINUIDADE E RECUPERAÇÃO

4.1 Classificação de Sistemas Críticos

Sistema	Prioridade	RTO	RPO	Proprietário	Dependências
Sistemas de arrecadação	Alta	4h	1h	Sec. Fazenda	Banco de Dados principal, Rede interna
Sistema de Educação	Média	8h	4h	Sec. Educação	Servidor de Aplicação, Rede
E-mails institucionais	Média	6h	2h	Coord. TI	Servidor de E-mail, Conectividade

Portal de Transparência	Baixa	24h	12h	Coord. TI	Servidor Web, BD Secundário

Indicadores de desempenho: - % de RTO e RPO atendidos nos testes - Tempo médio de recuperação - Frequência de falhas por categoria

5. PROCEDIMENTOS DE RECUPERAÇÃO

5.1 Antes do Desastre (Prevenção)

✓ Backups incrementais a cada 4h e full diários;
✓ Armazenamento: local + nuvem (Provedor X - Região Y);
✓ Retenção: 30 dias (diários), 3 meses (semanais), 1 ano (mensais);
✓ Testes mensais de restauração (sistemas críticos), trimestrais para demais;
✓ Redundância em sistemas críticos com failover semestral testado;
✓ MFA, IPS/IDS, segmentação de rede, escaneamento de vulnerabilidades;
✓ Treinamento anual da equipe TI, bianual para usuários-chave;
✓ Inventário atualizado e contratos com cláusulas de continuidade;
✓ Simulações de desastre completas a cada 6 meses;

5.2 Durante o Desastre

✓ Acionamento imediato do Comitê via fluxograma;
✓ Isolamento técnico de sistemas afetados;
✓ Comunicação com gestores e população via site, rádio, redes sociais;
✓ Registro padronizado de impacto e ações tomadas.

5.3 Após o Desastre

✓ Avaliação do impacto com ferramentas e métricas;
✓ Ativação de backups conforme prioridade;
✓ Monitoramento de estabilidade pós-restauração;
✓ Relatório técnico e administrativo (prazo: 7 dias);
✓ Reversão para ambiente de produção com checklist validado;

5.4 Comitê de Recuperação de Desastres

✓ Coordenador de TI (líder técnico);
✓ Representante da Defesa Civil;
✓ Representantes das Secretarias (Administração, Saúde, Fazenda, Educação, Cultura, Ciência e Tecnologia, Esporte e Lazer, e Procuradoria Geral do Município);
✓ Consultores externos especializados (se necessário);

6. CADEIA DE COMANDO E CONTATOS DE CONTINGÊNCIA DETALHADOS ABAIXO

6.1. CONTINGÊNCIA

✓ Servidores na nuvem (modelo "warm") – AWS/Azure com RPO diário e RTO de 6h;
✓ Datacenter de contingência: Sala TI da Subsecretaria de Ciência e Tecnologia (infraestrutura verificada e climatizada);
✓ Procedimentos manuais (prontuário físico, formulários impressos) com treinamentos anuais e documentação protegida fisicamente;

6.2 TESTES E ATUALIZAÇÕES

✓ Testes semestrais completos (ambientes alternativos ativados);
✓ Indicadores: tempo de recuperação, perda de dados, falhas por etapa;
✓ Revisão anual obrigatória + após incidentes;
✓ Processo formal de inclusão de novos sistemas e ameaças.

7. DOCUMENTAÇÃO (ARMAZENADA FÍSICA E DIGITALMENTE)

✓ Inventário de ativos
✓ Lista de sistemas críticos
✓ Contatos emergenciais
✓ Relatórios de backup
✓ Diagramas de rede
✓ POPs de restauração e contingência
✓ Glossário de termos técnicos
✓ Histórico de revisões

8. CONFORMIDADE

Este plano segue as boas práticas do Guia de Continuidade de Serviços de TIC (SLTI/MGI) e as normas ABNT NBR ISO/IEC 27031 e ISO 22301.

Última revisão: Abril/2025

Próxima revisão obrigatória: Abril/2026 (ou imediatamente após incidentes).