PLANO DE CONTINUIDADE DE SERVIÇOS TECNOLOGIA DA INFORMAÇÃO

PREFEITURA MUNICIPAL DE SANTA RITA DO PASSA QUATRO - SP

HISTÓRICO DE VERSÕES

VERSÃO	DATA	DESCRIÇÃO
1.0	**20/12/2023**	Publicação Inicial

SUMÁRIO

1. INTRODUÇÃO

A Prefeitura de Santa Rita do Passa Quatro está em constante expansão e evolução, visando melhorias nos processos e melhor atendimento ao munícipe, tornando-se assim cada vez mais dependente dos recursos tecnológicos para atender essas expectativas maneira eficiente e eficaz.

Nesse contexto é importante considerar que todo ambiente de tecnologia da informação é suscetível a falhas e diante de uma ocorrência de falha as ações para se mitigar os impactos causados pela mesma é de fundamental importância para reduzir seus efeitos, por isso este plano tem como objetivo básico estabelecer ações de proteção rápidas e eficazes para os processos críticos de TI relacionados aos sistemas essenciais em casos de incidentes graves ou desastres. A identificação das principais ameaças e dos processos críticos serão fundamentais para que se possa efetuar a gestão de riscos do ambiente tecnológico da Prefeitura e dessa forma reduzir o impacto em eventuais situações de desastre.

2. ESCOPO

Este plano terá como abrangência a definição de ações estratégicas que visam a continuidade de todos os serviços de Tecnologia da Informação classificados como essenciais de todas as Coordenadorias da Prefeitura Municipal de Santa Rita do Passa Quatro, contemplando a contingência, recuperação e continuidade das atividades de Prefeitura.

3. SERVIÇOS ESSENCIAIS

Os serviços essenciais de TI podem ser definidos como todo o serviço que participa dos processos administrativos executados para a resposta da demanda ao munícipe. De certa forma são os serviços que em situação de

indisponibilidade afetarão a prestação dos serviços requisitados à Prefeitura Municipal, gerando impactos que podem ser de ordem financeira, legal, na imagem da Prefeitura ou de ordem operacional.

Listamos abaixo, após análise do Centro de Processamento de Dados, os serviços considerados essenciais para a execução dos trabalhos e serviços da administração municipal.

SERVIÇOS / AÇÕES				IMPACTO			
SERVIÇO	CRITICIDADE	RPO	RTO	FINANCEIRO	LEGAL	IMAGEM	OPERACIONAL
Datacenter Municipal	Alto	24h	24h	Alto	Alto	Alto	Alto
Sistema de Saúde	Alto	24h	6h	Alto	Médio	Alto	Alto
Nota Fiscal Eletrônica	Alto	24h	24h	Alto	Alto	Alto	Alto
Sistemas Administrativos	Alto	24h	24h	Alto	Alto	Alto	Alto
Internet - Link Principal*	Alto	3h	1h	Baixo	Baixo	Baixo	Alto
Servidor de Arquivos	Alto	24h	12h	Baixo	Alto	Baixo	Alto
Portal Oficial Municipal (Site Institucional)	Médio	24h	8h	Baixo	Alto	Médio	Médio
E-mail Institucional	Médio	24h	24h	Baixo	Médio	Médio	Médio
Monitoramento Urbano (Sistema de Câmeras)	Baixo	3d	24h	Baixo	Baixo	Baixo	Baixo
Sistemas de Backup	Baixo	24h	12h	Baixo	Baixo	Baixo	Baixo

RPO - Recovery Point Objective: *Método de controle utilizado em tecnologia de informação para calcular e/ou estimar a quantidade limite de dados que uma organização toleraria perder em casos de incidentes e que, de preferência o limiar calculado nunca seja atingido.*

RTO - Recovery Time Objective: *Este indicador está diretamente relacionado ao tempo máximo que o setor de tecnologia levará para restabelecer os serviços após a parada crítica, devendo ser levado em consideração o tempo de recuperação, testes e reparos.*

** Serviços de alta criticidade, porém já possuem redundância, ou seja, um link secundário para assumir os serviços no caso de falhas nos links*

principais, justificando o pouco tempo de RTO e RPO para solucionar eventuais falhas, essa é uma das formas de antecipar a indisponibilidade de serviços essenciais utilizadas pela Prefeitura.

4. PRINCIPAIS AMEAÇAS

Todos os ambientes de Tecnologia da Informação e Comunicação são suscetíveis a ameaças que podem impactar na indisponibilidade dos serviços essenciais, sendo as principais mapeadas e descritas neste tópico.

4.1 Interrupção de Energia Elétrica

Evento causado por fator externo, ou seja, na rede da concessionaria que interrompa o fornecimento de energia;

Rompimento de cabos decorrente da execução de obras públicas, desastres ou acidentes;

Evento causado por fator interno, ou seja, na rede elétrica interna da Prefeitura ocasionado por padrão elétrico insuficiente, curto-circuito, infiltrações ou avaria em equipamentos da rede elétrica interna.

4.2 Ataques cibernéticos

Ataques cibernéticos a rede pública municipal, que possam comprometer os computadores, servidores locais e em nuvem e/ou rede de dados.

4.3 Falha na climatização da sala de servidores de rede

Superaquecimento dos ativos causado devido a falha no sistema de refrigeração do ambiente, composta por dois aparelhos de ar-condicionado (redundância).

4.4 Falha Humana

Acidente ao manusear equipamentos críticos que envolvam risco a saúde como circuitos-elétricos, falhas humanas no manuseio inadequado

de processamento de dados, manuseio inadequado em servidores ou em serviços de missão crítica dentre outros.

4.5 Ataques internos

Ataque aos ativos tangíveis e intangíveis da Prefeitura tais como do Data Center, computadores ou servidores de arquivos, sistemas e rede de dados e Internet, causados por próprios funcionários.

4.6 Incêndios

Incêndios que comprometam parcialmente ou completamente a continuidade dos serviços de Tecnologia da Informação da Prefeitura.

4.7 Desastres naturais

Tempestades, alagamentos, dentre outros.

4.8 Falha de Hardware

Falha de equipamento que necessite reposição de peças, reparos, ou até mesmo a substituição integral do pela qual demande processo licitatório.

5. APLICAÇÃO DO PLANO

O plano será acionado quando houver qualquer ocorrência de algum dos cenários de desastres ou no caso da identificação de uma vulnerabilidade tenha grande possibilidade de ser explorada.

O plano também poderá ser acionado em casos de testes para validação dos processos envolvidos.

Os integrantes do Centro de Processamento de Dados serão responsáveis por acionar os contatos e partes interessadas, prioritariamente por telefone, ou pessoalmente caso seja possível.

5.1 Macroprocessos do Plano

A execução do plano de continuidade é baseada nas seguintes etapas, sendo o mesmo desmembrado em planos específicos por área de atuação:

- Identificação da Ocorrência de Desastre;
- Início do Plano de Continuidade de Serviços;
- Acionamento de Soluções de Contingência;
- Reestabelecimento dos Serviços;
- Reparo no Ambiente;
- Reestabelecimento da Operação.

6. FERRAMENTAS

Com base nos ativos atuais à disposição do Centro de Processamento de Dados serão utilizadas as estratégias de redundância e recuperação variadas conforme apresentado a seguir:

6.1 Redundância de Links

Atualmente a Prefeitura dispõe de redundância de links de Internet em seu Datacenter, ou seja, links de segmentos de rede distintos que chegam ao local por caminhos separados de modo a evitar o rompimento acidental de cabos que eventualmente possa ocorrer.

6.2 Redundância de Discos

Atualmente a Prefeitura dispõe de servidores que possuem redundância de discos através da tecnologia RAID de modo a prover cópia em tempo real em discos de dados distintos, ou seja, no caso de falha de um disco não há perda de dados e/ou paralisação dos serviços.

6.3 Snapshots

Os Snapshots são cópias rápidas realizadas localmente nos servidores de arquivos e sistemas, esse tipo de tecnologia permite a restauração de todo um sistema/conjunto de arquivos de forma

praticamente instantânea, de modo a prover recuperação imediata de um cenário para análise em caso de desastre.

6.4 Redundância de Backups

Atualmente a Prefeitura dispõe de ferramenta profissional para realização de backups, permitindo o armazenamento de cópias no ambiente local e em nuvem, garantindo maior segurança no caso de eventual desastre no ambiente físico da Prefeitura.

6.5 Warm Site

A utilização de um Warm Site consiste em um ambiente provisório para disponibilizar as cópias de segurança (backups) mais atuais dos serviços classificados como essenciais, ou seja, os serviços com maior impacto na prestação de serviços até que se restabeleça o ambiente normal que foi objeto de desastre. Esta estratégia seria usada para os sistemas on-premisse, ou seja, hospedados no Datacenter da Prefeitura de Santa Rita do Passa Quatro.

6.6 Hot Site

Um hot site é um local externo para a retomada de serviços essenciais em um processo de recuperação de desastre e possui toda infraestrutura necessária para a retomada das atividades regulares da Prefeitura, considerando os sistemas da Prefeitura que sua hospedagem e armazenamento já se encontram em nuvens corporativas com estruturas redundantes.

7. ESTRATÉGIA

A execução do Plano de Continuidade dos Serviços de TI será realizada através das atividades descritas nos planos a seguir:

7.1 Plano de Continuidade Operacional - PCO

Este plano descreve os cenários de inoperância e seus respectivos procedimentos alternativos planejados, definindo as atividades prioritárias para garantir a continuidade dos serviços essenciais.

7.1.1 Objetivos:

O principal objetivo é garantir ações de continuidade durante e depois da ocorrência de uma crise ou cenário de desastre, tratando-se apenas das ações de contingência definidas na estratégia. São objetivos do PCO:

- Prover meios para manter o funcionamento dos principais serviços e a continuidade das operações, dos sistemas essenciais;
- Estabelecer procedimentos, controles e regras alternativas que possibilitem a continuidade das operações durante uma crise ou cenário de desastre.

7.1.2 Execução do plano:

- Avaliação de Impacto de Desastre: Identificada a ocorrência de um incidente ou crise, o responsável deverá verificar a dimensão do impacto, extensão e possíveis desdobramentos do ocorrido.
- Acionamento do Plano: Convocação de uma reunião de emergência, com o intuito de coordenar prazos e orquestrar as ações de contingência, informar aos envolvidos as ações de contingência com a priorização dos serviços essenciais.
- Contingência de Backup:
    - Devem ser adotadas as seguintes ações de contingência e continuidade por processo ou serviço essencial:
        - Verificar status da aplicação de backup e estimar impacto de perda de dados;
        - Identificar serviços de backups cujos dados em questão foram afetados;

- Estimar volume de dados a serem recuperados, tempo de recuperação dos dados e possíveis perdas operacionais;
- Atestar retorno do funcionamento do ambiente principal;
- Testar a aplicação de backup após desastre;
- Validar políticas de backup implementadas.

- Encerramento do PCO: documentar atividades e informar a todos o retorno das atividades.

7.2 Plano de Administração de Desastre - PAD

Este plano especifica as ações ante os cenários de desastres. As ações incluem gerir, administrar, eliminar ou neutralizar os impactos inerentes aos relacionamentos entre os agentes envolvidos e/ou afetados, até a superação da crise através da orquestração das ações e de uma comunicação eficaz.

7.2.1 Objetivos:

O objetivo deste plano é garantir a comunicação, gerenciar as crises e viabilizar uma compreensão linear a todos os envolvidos das ações antes, durante e após a ocorrência de uma situação de desastre.

São objetivos diretos do PAD:

- Garantir a segurança e integridade das pessoas e das informações;
- Minimizar transtornos sobre os desdobramentos de incidentes e estimular o esforço em conjunto para superação da crise;
- Orientar os funcionários e demais colaboradores com informações e procedimentos de conduta;
- Informar a todos os afetados pela indisponibilidade em tempo e com esclarecimentos condizentes com o ocorrido.

7.2.2 Execução do Plano:

7.2.2.1 Comunicação na ocorrência de um desastre:

Na ocorrência de um desastre será necessário entrar em contato com diversas áreas, principalmente as afetadas para informá-las de seu efeito na continuidade dos serviços e tempo de recuperação.

A prioridade será assegurar que os Coordenadores, Diretores e responsáveis pelas áreas afetadas sejam notificados sobre a situação de desastre com as informações dos impactos e serviços afetados e a previsão para o que eles sejam restabelecidos.

Quando o serviço impactado atingir usuários externos, deverá ser notificado ao Setor de Imprensa para que sejam tomadas as providencias quanto à divulgação de nota comunicando a indisponibilidade para o público em geral.

O Centro de Processamento de Dados deverá prover um meio de contato específico para este fim, com intuito de que as unidades da administração Municipal se mantenham informadas da ocorrência de um desastre e da inatividade dos serviços essenciais de TI, como também as ações de contingência em andamento para restauração das operações.

7.2.2.2 Encerramento do Plano:

Uma vez validado o funcionamento do retorno dos sistemas essenciais e estabilidade do Datacenter, o Centro de Processamento de Dados entrará em contato com os colaboradores internos e as demais partes descritas neste plano, provendo as informações de retorno das operações com as informações de status dos serviços essenciais.

O Centro de Processamento de Dados também deverá compor relatório com relação das atividades necessárias após a ocorrência do desastre como remanejamento dos canais de informação, abertura e acompanhamento de chamados correlatos ao ocorrido.

7.3 Plano de Recuperação de Desastres - PRD

Este plano descreve os cenários de inoperância e seus respectivos procedimentos planejados, definindo as atividades prioritárias para

restabelecer o nível de operação dos serviços no ambiente afetado, dentro de um prazo tolerável.

7.3.1 Objetivos:

O objetivo deste plano garantir o retorno das operações do ambiente principal após a ocorrência de incidente ou desastre, tratando-se apenas dos ativos, conexões e configurações deste ambiente.

São objetivos do PRD:

- Avaliar danos aos ativos e conexões do sistema afetado e prover meios para sua recuperação;
- Evitar desdobramentos de outros incidentes na infraestrutura principal;
- Restabelecer o sistema afetado dentro do prazo tolerável.

7.3.2 Execução do Plano:

- Identificação de ativos danificados ou comprometidos: A equipe técnica deverá identificar e listar todos os ativos danificados da ocorrência do desastre.
- Identificação de acessos comprometidos: A equipe deverá identificar as interrupções de conexões e acessos gerados após o desastre, relatando se trata de um problema interno ou externo ao ambiente municipal, bem como o fornecimento das informações quanto aos sistemas afetados em caso de terceiros.
- Listagem dos serviços descontinuados: A equipe técnica deverá mapear quais serviços foram descontinuados, contendo as informações de perda de ativo e de conexão, com intuito documentar e corrigir os serviços. O relatório deverá abranger todos os componentes necessários à plena operação da aplicação como servidores, máquinas virtuais, banco de dados, firewall, storages, roteadores e switches, bem como respectivas configurações de proxy, DNS, rotas de comunicação, dentre outras.

- Elaboração do cronograma de recuperação: Após o mapeamento das perdas e impactos, a equipe técnica elaborará um breve cronograma de recuperação das aplicações, levando em consideração:
    - A priorização dos serviços essenciais, ou determinação de nível institucional;
    - O RTO definido para cada serviço essencial;
    - A força de trabalho disponível.

- Substituição de ativos: Em caso de perda de ativos, deverá ser imediatamente informado ao Departamento de Compras a necessidade de aquisição de ativos perdidos que não puderem ser recuperados. Deverá ser mensurado como o tempo de aquisição irá impactar o RTO de cada serviço, comunicando aos Coordenadores se houver alguma solução alternativa a ser tomada enquanto é realizada a aquisição. Deverá ser analisado para os ativos danificados, as coberturas contratuais e/ou garantias.
- Reconfiguração de ativos: A equipe deverá verificar que as configurações dos ativos reparados ou substituídos estão em pleno funcionamento. Caso não estejam, deverá prover cronograma estimado para configurar estes ativos.
- Ambiente de testes: Deve ser elaborado um ambiente para testes de recuperação garantindo o pleno restabelecimento da aplicação/serviços afetados pelo incidente e/ou desastre ocorrido. Os testes incluem a garantia dos níveis de capacidade e disponibilidade dos serviços.
- Recuperação dos dados do backup: Proceder a recuperação dos dados para as aplicações afetadas. Validar as configurações e funcionalidades dos sistemas. A validação pode ser realizada pelos testes automatizados de monitoramento dos serviços ou por equipe designada.
- Encerramento do PRD: Ao término do procedimento de recuperação, as informações serão consolidadas em parecer específico informado o horário de restabelecimento de cada serviço, equipamentos adquiridos, procedimentos de recuperação realizados e fornecedores acionados.

8. REVISÃO DO PLANO

O Plano de Continuidade dos Serviços de Tecnologia da Informação será válido a partir de sua publicação, sendo revisado anualmente pela equipe do Centro de Processamento de Dados, responsável por sua elaboração.

A revisão anual se faz necessária para o devido acompanhamento dos fatores de risco e necessidades identificadas, assim como para acrescentar melhorias nas estratégias na execução do Plano de Continuidade, conforme eventuais atualizações e evolução dos recursos disponíveis na Prefeitura.

O critério de revisão proverá o acompanhamento e realinhamento estratégico do Plano, tornando uma ferramenta cada vez mais prática e completa para atender os objetivos da Prefeitura Municipal.

9. FATORES CRÍTICOS

São considerados fatores fundamentais para a execução das atividades previstas neste Plano:

- Acompanhamento dos riscos e necessidades pelo Centro de Processamento de Dados;
- O envolvimento dos Coordenadores e Diretores para sustentar as decisões necessárias para atingir os objetivos do plano;
- O correto alinhamento entre os departamentos técnicos e administrativos envolvidos no Plano;
- Capacitação dos profissionais de TI e dos usuários dos ativos de TI em geral;
- Disponibilidade orçamentária.

10. CONCLUSÃO

O Plano de Continuidade de Serviços de Tecnologia da Informação é uma ferramenta de suma importância que servirá de guia buscando reduzir ao máximo eventuais paralisações causadas por desastres ou fatores de risco apresentados neste plano, de forma a prover o reestabelecimento de serviços essenciais no menor tempo e com o menor impacto possível para a instituição e para os munícipes que usam de forma direta e indireta os serviços de tecnologia da informação e comunicação municipais.

É de fundamental importância o alinhamento deste Plano junto ao núcleo administrativo da Prefeitura, de modo a prover recursos necessários para a constante evolução nas ferramentas utilizadas na Prefeitura, a fim de reduzir os riscos e evitar eventuais desastres que possam ocorrer causando a necessidade do acionamento deste plano.