PLANO DE CONTINUIDADE

Município de Santa Lúcia

2024

PREFEITURA MUNICIPAL
SANTA LÚCIA

Prefeitura Municipal de Santa Lúcia

PLANO DE CONTINUIDADE DE SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

Fevereiro

2024

RESUMO

A finalidade deste projeto é organizar um plano abrangente de continuidade de serviços de TI, visando assegurar a disponibilidade de maneira contínua dos sistemas e serviços críticos da organização perante as situações de emergência ou interrupções inesperadas. Uma equipe multidisciplinar será atribuída para fazer uma análise de riscos bem detalhada, identificando medidas de mitigação e desenvolver métodos de resposta a incidentes. O planejamento seguirá boas práticas de gestão de projetos e continuidade de negócios, com um cronograma definido e destinando recursos de forma adequada. A comunicação eficaz e a envoltura das partes interessadas serão prioritários ao decorrer do projeto em si. Contudo em seguida da implementação, serão feitos testes constantes para garantir a eficiência do plano e determinar oportunidades de aperfeiçoamento para o município de Santa lúcia.

Palavras – chave: Plano de Continuidade de Serviços de TI, boas práticas, sistemas e serviços críticos, disponibilidade contínua, emergência, análise de riscos, interrupções imprevistas, medidas de mitigação, procedimentos de resposta a incidentes, gestão de projetos, comunicação eficaz, envolvimento das partes interessadas, testes regulares, eficácia do plano, oportunidades de aprimoramento, município, Santa lúcia.

ABSTRACT

The purpose of this project is to organize a comprehensive IT service continuity plan, aiming to ensure the continuous availability of the organization's critical systems and services in the face of emergency situations or unexpected interruptions. A multidisciplinary team will be assigned to carry out a very detailed risk analysis, identifying mitigation measures and developing incident response methods. Planning will follow good project management and business continuity practices, with a defined schedule and allocating resources appropriately. Effective communication and engagement with interested parties will be priorities throughout the project itself. However, following implementation, constant testing will be carried out to ensure the efficiency of the plan and determine opportunities for improvement for the municipality of Santa Lúcia.

Keywords: IT Service Continuity Plan, good practices, critical systems and services, continuous availability, emergency, risk analysis, unforeseen interruptions, mitigation measures, incident response procedures, project management, effective communication, involvement stakeholders, regular testing, plan effectiveness, opportunities for improvement, municipality, Santa lúcia.

LISTA DE FIGURAS

LISTA DE TABELA

SUMÁRIO

CAPÍTULO 1

1.0 INTRODUÇÃO

A eventualidade de falhas nos serviços de Tecnologia da Informação resulta em abalos diretos na prestação dos serviços públicos referentes à população. Além do mais, provoca prejuízos tanto operacionais quanto financeiros, uma vez que as atividades desempenhadas pela Prefeitura, por meio de suas unidades administrativas distribuídas no município, necessitam significativamente dos recursos tecnológicos.

CAPÍTULO 2

2.0 FINALIDADE

O plano Continuidade de Tecnologia da Informação (TI) é um documento que define os processos fundamentais para assegurar uma continuidade dos serviços críticos de TI. Estes serviços são reconhecidos como cruciais para o funcionamento da organização e são integrados aos planos de contingência, continuidade e também de recuperação.

O objetivo principal é garantir a manutenção dos procedimentos, mesmo em situações de interrupção ou desastre.

CAPÍTULO 3

3.0 SERVIÇOS FUNDAMENTAIS

Os serviços a seguir, em ordem de prioridade, são considerados indispensáveis para a ativação e realização do atual plano de continuidade.

Tabela 1 – Serviços de prioridade ao plano

Serviço	Análise de Criticidade	RPO (Recovery point objective)	RTO (Recovery Time Objective)	IMPACTO 4			
				FINANCEIRO	LEGAL	IMAGEM	OPERACIONAL
Armazenamento local de dados	Média	18h	10 h	Indefinido	Alto	Médio	Médio
Gestão de Sistemas em Nuvem	Média	10h	4h	Indefinido	Alto	Alto	Alto
Conexão Principal	Baixa	6h	5h	Indefinido	Alto	Alto	Alto
Gestão Tributário	Média	10h	4h	Indefinido	Alto	Alto	Alto
Emissão Nota Fiscal Eletrônica	Média	10h	4h	Indefinido	Alto	Alto	Alto
Sistema Contábil	Alta	10h	5h	Indefinido	Alto	Médio	Alto
Sistema folha	Baixa	10h	3h	Indefinido	Alto	Médio	Alto
Gestão de compras	Média	10h	4h	Indefinido	Alto	Médio	Médio
Regulamentação	Média	11h	5h	Indefinido	Alto	Médio	Médio
Gestão de Saúde	Alta	14h	5h	Indefinido	Alto	Alto	Alto
Gestão de Obras	Média	18h	10 h	Indefinido	Médio	Médio	Médio
Website Corporativo	Média	14h	7h	Indefinido	Médio	Alto	Médio

Portal Transparência	Média	21h	10 h	Indefinido	Médio	Alto	Médio
E-mail Institucional	Média	10h	4h	Indefinido	Médio	Médio	Médio
Gestão de Cemitério	Baixa	18h	10 h	Indefinido	Baixo	Baixo	Baixo
Conexão à Internet Própria	Média	10h	4h	Indefinido	Médio	Alto	Médio
Servidor Arquivos	Média	18h	10 h	Indefinido	Médio	Médio	Médio
Backup	Média	19h	10 h	Indefinido	Alto	Médio	Alto
Rede Privada Virtual (VPN)	Média	18h	10 h	Indefinido	Médio	Médio	Médio
Geoprocessamento	Baixa	18h	10 h	Indefinido	Médio	Médio	Médio
Plataforma de Serviços Online	Baixa	11h	5h	Indefinido	Alto	Alto	Médio
Boletim Oficial	Médio	19h	10 h	Indefinido	Médio	Médio	Médio

Objetivo de Tempo de Recuperação (Recovery Time Objective - RTO):

Este parâmetro está diretamente associado ao período máximo de tempo que o setor de tecnologia levará para restabelecer os serviços após uma interrupção crítica. Esse período deve considerar o tempo necessário para recuperação, testes, reparos, atualizações, reinstalações, entre outros processos.

Objetivo de de Ponto de Recuperação (Recovery Point Objective - RPO):

Concerne de um método importante de verificação empregado na área de tecnologia da informação para avaliar ou estimar a quantidade máxima de dados que a organização poderia tolerar perder em algum caso de incidentes.

CAPÍTULO 4

4.0 PRINCIPAIS ADVERSIDADES

Deverá colocar o plano em prática diante da ocorrência de uma situação de desastre que na qual represente uma ameaça à continuidade dos serviços fundamentais.

Tabela 2 - Situação de ameaças a continuidade

Desastres	Possíveis Causas
01 – Incidente de operação	- Acidentes no decorrer da manipulação de equipamentos críticos, como processamento de dados ou servidores.
02 – Defeito de hardware	- Falha onde requer uma substituição de componentes, ajustes ou até mesmo a substituição do equipamento, dependendo assim um processo licitatório.
03 – Interrupção no fornecimento de energia elétrica	- Provocado por agentes externos à rede elétrica da Prefeitura ou até mesmo devido a imprevistos municipais, com duração superior a 1 hora. - Determinada por fatores internos em que afetem a rede elétrica municipal, como incêndios, curtos-circuitos, entre outros incidentes elétricos.
04 – Interrupção na rede ou nos circuitos	- Ocorrência de Rompimento de cabos de interconexão respectivo a obras públicas, acidentes ou até mesmo desastres.

05 – Eventualidade de Incêndio	- Incêndios que na qual danifiquem parcialmente ou total a continuidade dos serviços de Tecnologia da Informação no município.
06 – Incidente de segurança cibernética	- Ataques diretamente à rede pública municipal com a finalidade de comprometer tanto servidores locais quanto em nuvem, computadores, e rede de dados.
07 – Ataque de acesso interno	-Visam ataques aos ativos dos servidores.
08 – Ocorrências de calamidades naturais	-Tempestades, inundações, incidentes imprevistos, entre outros.
09 - Deficiência na condição ambiental da sala de servidores	- Sobreaquecimento dos recursos, devido aos Problemas no sistema de resfriamento do ambiente, ausência de redundância ou até mesmo automatização dos dispositivos de controle de temperatura, entre vários outros fatores.

CAPÍTULO 5

5.0 AÇÕES E COMPROMISSOS

De suma responsabilidade o município de Santa lúcia é encarregado por revisar periodicamente seu plano de continuidade de tecnologia da informação e de tomar decisões sobre avivar o processo em casos de desastres, assumindo a responsabilidade institucional pela sua implementação e outras ocorrências relacionadas. Será responsável também aos processos tecnológicos perante aos serviços necessitados.

5.1 FORMAÇÃO ESTRATÉGICA

Será encarregada a equipe técnica para realizarem instalações físicas que abrigam o sistema de tecnologia da informação e comunicação (TIC) cujo garantirá que as instalações alternativas sejam mantidas adequadamente. Caberá também à equipe técnica avaliar danos específicos à infraestrutura de rede e fornecimento de dados e conectividade de rede, incluindo LAN, WAN, ou infraestrutura externa com fornecedores de serviços.

Além de tudo, fornecerão infraestrutura de servidores físicos e virtuais para garantia que as operações e processos fundamentais sejam executados durante um desastre, garantindo de forma segura o funcionamento adequado das aplicações essenciais para um atendimento aos objetivos de negócios. Será responsável por assegurar a validação do desempenho das aplicações essenciais, fornecendo ferramentas aos funcionários para executar suas funções de maneira eficiente, provisionando trabalhos na solução de contingência e garantindo a recuperação de dados de acordo com as políticas estabelecidas; Toda a equipe técnica.

5.2 CHAMADO DO PROJETO

O plano será colocado em vigor em caso de qualquer ocorrência de desastres, riscos desconhecidos ou até mesmo vulnerabilidades exploráveis. Além

do mais, o plano poderá ser usado para testes de validação dos processos envolvidos. Contudo os funcionários da equipe técnica serão responsáveis por mobilizar os contatos e partes interessadas, de preferência por telefone ou pessoalmente, quando possível.

5.3 TRANSFORMAÇÃO

Este plano tem macroprocessos acentuados nas atividades mencionadas onde se desdobra em planos que são específicos para cada área de atuação em caso de desastre, finalizando com a recuperação das operações.

Figura 1 – Processos de atividades

CAPÍTULO 6

6.0 DIRETRIZES DE CONTINUIDADE DO PLANO

Toda execução do Plano de Continuidade dos Serviços de TI será realizada através das atividades descritas no plano destacado abaixo.

6.1 DIFUSÃO

A implementação de difusão abrange os links de internet e os servidores físicos, visando garantir uma continuidade do serviço se caso houver falhas.

6.2 BACKUP

Estabelecimento da política de backup do município, em que compreende, no mínimo: backups completos (full) de forma organizada, além do desenvolvimento de snapshots para emergências específicas, como a recuperação de sistemas de banco de dados.

6.3 MEDIDAS DE RECUPERAÇÃO

Identificação de perdas referente a dados e ativos, seguida pelo restabelecimento de toda a estrutura prejudicada e, posteriormente, pela recuperação de dados a partir dos backups. As ações de contingência e recuperação são detalhadas logo a seguir.

6.4 PLANO DE ADMINISTRAÇÃO DE DESASTRES - PAD

O plano descreve detalhadamente as medidas a serem tomadas diante dos cenários de desastre. As ações abrangem o gerenciamento, eliminação ou neutralização dos impactos inerentes, administração, coordenando as ações e mantendo uma comunicação diligente entre os agentes envolvidos ou afetados até a solução da crise. Contudo na execução do plano ocorre a comunicação durante

um desastre onde nesse caso, é primordial estabelecer um contato com diversas áreas, em especial com as afetadas, para informá-las sobre o impacto na continuidade dos serviços e o tempo necessário para recuperação.

A Prioridade será na notificação aos responsáveis pelas áreas afetadas, fornecendo detalhes sobre os impactos e os serviços afetados, bem como estimativas de recuperação. Se caso os serviços afetados envolverem usuários de forma externa, a área de comunicação deverá ser informada para emissão de comunicados sobre a indisponibilidade, e garantir um meio de contato específico para manter as unidades administrativas atualizadas devem ser essenciais, sobre o desastre e a inatividade dos serviços de TI, além das regulares de contingência em andamento.

Quanto ao encerramento do plano após a verificação, a estabilidade dos servidores e o funcionamento dos sistemas essenciais, os departamentos relevantes vão ser contatados para informar sobre a retomada das operações e serviços. O departamento de tecnologia da informação também deverá organizar um relatório sobre as atividades pós-desastre, como a abertura de chamados correlatos e remanejamento de canais de informação.

6.5 PLANO DE CONTINUIDADE OPERACIONAL - PCO

O plano de Continuidade Operacional (PCO) descreve os cenários de inoperância e também os procedimentos alternativos para garantia da continuidade dos serviços cruciais durante e após um desastre ou crise.

Em relação aos objetivos pode-se incluir; O estabelecimento de procedimentos alternativos durante crises, manter o funcionamento dos serviços principais, minimizar transtornos, definir formulários e relatórios para execução da contingência e orientar os envolvidos. Contudo na execução do plano ocorre a avaliação de Impacto de desastre, visando a Identificação da dimensão de algum impacto ocorrido e possíveis desdobramentos do incidente ou crise cujo responsável deverá verificar e ficar atualizado ao assunto; Quanto ao acionamento do plano é de organizar uma reunião de emergência para coordenação de ações contingenciais e priorizar os serviços essenciais; E por fim a contingência de backup que na qual devem ser adotadas as seguintes ações de contingência e continuidade por

processo ou serviço essencial, descritas na tabela logo abaixo, sendo assim o encerramento do processo de PCO deve evidenciar as atividades:

Tabela 3 – Ação de contingência e continuidade

INSTRUÇÃO
Checar a situação da aplicação de backup e avaliar o impacto da perda de dados.
Localizar os procedimentos de backup nos quais os dados em questão foram comprometidos.
Calcular a quantidade de dados a serem recuperados, o período necessário para a recuperação dos dados e potenciais prejuízos operacionais.
Verificação da retomada da operação do ambiente principal.
Realizar testes na aplicação do backup pós-incidente.
Verificação da eficácia de diretrizes de backup executadas.

6.6 PLANEJAMENTO DE RECUPERAÇÃO DE CRISES

Este plano é responsável pela definição dos procedimentos para restabelecer os serviços na qual foram afetados dentro de um prazo aceitável, abrangendo a recuperação de dados do backup, avaliação de danos e reconfiguração de ativos.

Quanto ao processo de execução do plano e processo de finalização do plano de recuperação de desastres para a execução pode-se apontar a identificação de ativos que foram danificados; Interrupções de conexões e de serviços descontinuados; A elaboração de cronograma de recuperação considerando prioridades; RTO e disponibilidade de recursos; A substituição e reconfiguração de ativos; Criação de ambiente de testes e enfim a recuperação de dados do backup.

Portanto ao término de todo o procedimento de recuperação, as informações serão consolidadas em parecer específico informando o horário de restabelecimento de cada serviço, equipamentos adquiridos, procedimentos de recuperação realizados e fornecedores acionados.

CAPÍTULO 7

7.0 ANÁLISE DO PLANO DE TECNOLOGIA DA INFORMAÇÃO

O Plano de Continuidade dos Serviços de Tecnologia da Informação e Comunicação no município será sujeito a revisões periódicas pela diretoria de tecnologia da informação, em que é responsável por sua idealização.

Essa revisão é necessária para auxiliar adequadamente os fatores de risco e demandas identificadas, além de aceitar a implementação de forma contínua de avanços nas estratégias deste plano. Essa ação é realizada de acordo com as atualizações e avanços nos recursos de tecnologia disponíveis na Prefeitura.

.

CAPÍTULO 8

8.0 PRINCIPAIS REQUISITOS PARA EXECUÇÃO DO PLANO DE CONTINUIDADE

São considerados elementos essenciais para fins de execução das atividades traçadas neste plano:

O monitoramento contínuo tanto de riscos quanto de necessidades pela diretoria de tecnologia da Informação; O envolvimento de responsáveis para respaldo das decisões necessárias objetivando alcançar os objetivos do plano; Alinhamento adequado entre os departamentos técnicos e também de administrativos envolvidos perante ao planejamento; O treinamento dos profissionais de TI e dos usuários dos ativos de TI de forma geral; A disponibilidade de recursos orçamentários.