Política de Continuidade de TI e Mapeamento de Riscos

Política de Continuidade de TI (PCTI) e Mapeamento de Riscos

Setor de TI

Prefeitura Municipal de Santa Adélia/SP

Alexandre Whitacker Boschin
Gestor de TI

Sumário

1- Apresentação 1

2- Fatores críticos para a Execução do PCTI 1

3- Revisão do PCTI 1

4- Serviços Essenciais 3

5- Principais Riscos e Ameaças 4

6- Equipe Técnica 4

7- Processos do PCTI 5

8- Encerramento do Plano 6

9- Modelo de Relatório de PCTI 7

1- Apresentação

A área de TI (Tecnologia da Informação) assumiu um papel imprescindível nos últimos anos, tanto no setor privado como nas organizações públicas. O principal foco da área de TI é a sua efetiva utilização como suporte às práticas e objetivos organizacionais.

Falhas nos serviços de TI trazem impactos diretos na prestação de serviços públicos à população, além de prejuízos operacionais e financeiros. Portanto, devido à importância da Tecnologia da Informação dentro da organização, este documento (PCTI) surge como uma importante ferramenta a fim de auxiliar a administração pública a tomar as devidas medidas preventivas da área, assim como, mitigar os efeitos de falhas que podem ocorrer no dia-a-dia na área da Tecnologia da Informação, descrevendo planos de contingência, recuperação e continuidade dos serviços essenciais de TI.

2- Fatores críticos para a Execução do PCTI

São considerados fatores críticos para as atividades previstas neste documento:

- Capacitação dos profissionais de TI;
- Capacitação de todos os usuários de sistemas e ativos de TI em geral;
- Disponibilidade orçamentaria;
- Alinhamento de todos os departamentos desta organização;
- Envolvimento total dos responsáveis para a sustentação das decisões necessárias para atingir os objetivos deste PCTI;

3- Revisão do PCTI

Este Plano de Continuidade de Tecnologia da Informação deverá ser revisado periodicamente.

A revisão se faz necessária a fim de acompanhar os fatores de risco, acrescentar possíveis novos serviços e evoluções dos recursos tecnológicos, assim como, melhorar os processos de execução deste plano.

4- Serviços Essenciais

Os serviços abaixo são considerados essenciais dentro desta organização:

Serviço	Criticidade	RPO*	RTO**
Servidor Local	Alta	12 horas	6 horas
Servidor em nuvem	Alta	12 horas	6 horas
Link (Internet)	Alta	8 horas	4 horas
Sistema de Saúde (PEC)	Alta	12 horas	6 horas
Sistema Contábil	Alta	12 horas	6 horas
Sistema Compras	Alta	12 horas	6 horas
Sistema RH	Alta	12 horas	6 horas
Sistema Protocolo	Alta	12 horas	6 horas
Sistema Tributos	Alta	12 horas	6 horas
Sistema Água	Alta	12 horas	6 horas
Sistema Geoprocessamento	Média	24 horas	12 horas
Sistema Social	Alta	24 horas	12 horas
Ouvidoria	Alta	12 horas	6 horas
Site	Alta	12 horas	6 horas
Portal da Transparência	Alta	12 horas	6 horas
E-mails Institucionais	Média	12 horas	6 horas
Telefonia Voip	Média	24 horas	12 horas
Monitoramento de Câmeras	Média	24 horas	12 horas

***RPO**: *Recovery Point Objective* é a métrica que determina a quantidade máxima de dados que uma organização pode perder em caso de falha do sistema. Esse indicador define o intervalo máximo de tempo para a perda de trabalho desde o último backup, seja em uma aplicação, serviço ou ambiente.

****RTO**: *Recovery Time Objective* é o tempo estimado por uma organização para que seus sistemas voltem ao normal a partir do momento em que ocorre uma interrupção.

5- Principais Riscos e Ameaças

Na tabela abaixo estão listadas os riscos e ameaças que podem ocasionar a interrupção dos serviços de TI:

Riscos/Ameaças	Descrição
Interrupção de energia elétrica	Ocasionada por fator externo ou interno, onde é comprometida a rede elétrica do prédio.
Interrupção de internet	Rompimento de cabos e/ou inconsistência no link de internet.
Falha humana	Falha humana ao manusear equipamentos críticos.
Falha de hardware	Falha que necessite reparo e/ou troca de peças, ou até mesmo a substituição do equipamento.
Ataque cibernético	Tentativa criminosa de acessar ilegalmente a rede de computadores da organização.
Desastres naturais	Terremotos, tempestades, alagamentos...
Incêndio	Incêndios nas instalações que comprometam os serviços

6- Equipe Técnica

A equipe técnica é a responsável por toda a infraestrutura de TI. Em caso de riscos, ameaças ou desastres, cabe a esta equipe mapear e avaliar os danos, e assim, executar as operações e os processos necessários, a fim de que, as aplicações voltem a funcionar o mais rápido possível.

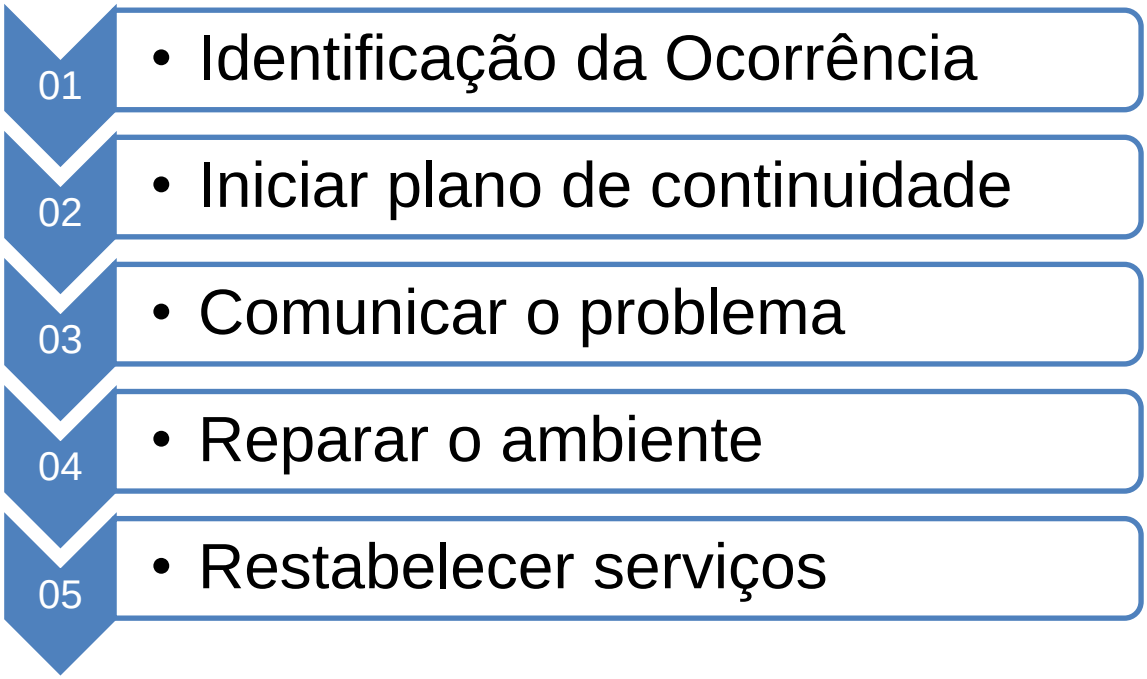
Profissional	Cargo
Alexandre Whitacker Boschin	Gestor da Tecnologia de Informação
Daniel Vinícius Maia Polizeli	Técnico de Informática

Contatos da equipe técnica:

- E-mail: ti@santaadelia.sp.gov.br
- Celular/Wapp: (17) 99752-2075
- Celular/Wapp: (17) 99724-1266

7- Processos do PCTI

Este PCTI tem os seguintes processos bem definidos:



1. O primeiro passo é a **identificação da ocorrência**. O responsável pela equipe de TI deverá identificar e verificar a dimensão do incidente, o impacto e os possíveis desdobramentos.
2. O segundo passo é o **acionamento do plano de continuidade**. O responsável deverá convocar uma reunião de emergência com o intuito de coordenar prazos e organizar ações de contingência. Se o incidente prejudicar mais de um setor, verificar e priorizar os serviços mais essenciais.
3. O terceiro passo é a **comunicação do problema**. Na ocorrência de um problema será necessário entrar em contato com diversas áreas, principalmente as áreas afetadas. É primordial que os responsáveis das

áreas afetadas sejam notificados sobre a situação do incidente, informações dos impactos e previsão para restabelecimento do serviço. Se o incidente impactar usuários externos, a área de comunicação da organização deverá ser notificada para que a mesma tome providências quanto à divulgação de uma nota comunicando a indisponibilidade para o público em geral.

4. O quarto passo é a **reparação do ambiente**. Em caso de incidentes que afetem o ambiente, como por exemplo o rompimento de cabos, será necessário fazer o reparo e os ajustes para que o serviço seja restabelecido.
5. O quinto passo é o **restabelecimento dos serviços**. Para o devido restabelecimento dos serviços, os seguintes passos devem ser respeitados:
    a. Substituição de equipamentos (caso necessário);
    b. Reconfiguração dos equipamentos;
    c. Reconfiguração dos acessos;
    d. Recuperação dos dados (Backup);
    e. Ambiente de testes;
    f. Validação dos testes

8- Encerramento do Plano

Após o restabelecimento dos serviços e dos ambientes devidamente testados e validados, a equipe de TI deverá comunicar todos os departamentos envolvidos, fornecendo informações sobre o retorno das operações e dos serviços.

O responsável deverá compor relatório sobre todas as atividades realizadas na ocorrência. Este relatório deverá conter informações como:

- Horário de restabelecimento de cada serviço;
- Equipamentos substituídos (caso houver);
- Procedimentos de recuperação realizados.

9- Modelo de Relatório de PCTI

Relatório PCTI

Local:_____

Data:_____

Descrição da Ocorrência:

Equipamentos substituídos:

Horário de Restabelecimento do Serviço	Procedimentos de recuperação realizados

Assinatura do Responsável:_____