Seção de Tecnologia da Informação

Plano de Continuidade de TI

Plano de Continuidade de TI

Sumário

1. APRESENTAÇÃO 3

2. OBJETIVO 3

3. PRINCIPAIS AMEAÇAS 4

4. RESPONSABILIDADES 5

5. SOLUÇÃO DE PROBLEMAS 6

6. MACROPROCESSOS DO PCTI 7

7. PLANEJAMENTO COMUNICATIVO EM CASOS DE URGÊNCIA 8

8. EXECUÇÃO DO PLANO 9

Plano de Continuidade de TI

1. APRESENTAÇÃO

Atualmente, grande parte dos serviços públicos prestados à população dependem da automatização oferecidas pela informática, falhas nos serviços de TI podem trazer impactos nesses serviços, portanto o objetivo do plano é estabelecer medidas de proteção para nortear os procedimentos a serem tomados em eventuais desastres e incidentes que possam afetar o funcionamento do sistema, eventos que podem ocorrer como queda de energia e outros fatores externos. O plano de continuidade será uma reflexão dos possíveis riscos e impactos que podem ocorrer em qualquer setor pertencente à Prefeitura.

2. OBJETIVO

O Plano de Continuidade de TI (PCTI) abrange as medidas necessárias à continuidade dos diversos serviços de TI, seja nos módulos do sistema de gestão de dados, seja nos demais serviços de informatização da Prefeitura Municipal de Jacupiranga os quais dependem da troca de dados pela Internet como: sistema de comunicação e gestão documental, sistema de dados, serviço de e-mail institucional, serviço de intranet, serviço de telefonia, e-SUS, ponto eletrônico, entre outros.

3. PRINCIPAIS AMEAÇAS

O plano deve ser ativado quando ocorrer um cenário de desastre que coloque em risco a continuidade dos serviços essenciais.

DESASTRES	POSSÍVEIS CAUSAS
01- Interrupção de energia	- Fator externo à rede elétrica da prefeitura como rompimento ou manutenção realizadas por parte prestadora de serviço de energia estadual. - Fator interno à rede elétrica da prefeitura como curto-circuito, infiltrações ou incêndio.
02- Indisponibilidade de rede	- Rompimento de cabos de interconexão devido à execução de obras, acidentes ou outros fatores. - Uso prolongado de cabeamento e conectores os quais oxidam e deterioram ao longo do tempo.
03 - Ataques internos	Ataque físico aos ativos do DataCenter como furtos e depredação.
04 - Falha humana	Acidente ao manusear equipamentos críticos como cabos de alimentação e internet.
05 - Falha de hardware	Falha que necessite reposição de peça ou reparo, cujo reparo ou aquisição dependa de processo licitatório.
06 - Desastres Naturais	Tempestades, alagamentos, etc.
07 – Incêndio	Incêndios que comprometam os serviços de TI.
08 - Ataque cibernético	Ataque virtual que comprometa o desempenho, os dados ou configuração dos serviços essenciais.

4. RESPONSABILIDADES

INTRODUÇÃO À EQUIPE DE TI

Atualmente, a equipe de TI composta pelo servidor municipal juntamente à equipe terceirizada avaliam regularmente o estado geral do funcionamento de TI e promovem soluções tecnológicas para as diversas pendências, que surgem conforme a necessidade, que surgem ao longo do tempo. Pelo fato da Tecnologia da Informação ser um ramo muito amplo, a equipe divide a análise em diferentes fatores.

COMUNICAÇÃO PREVENTIVA E EXPLICATIVA:

A equipe promove uma solução para esclarecer determinadas manutenções e orientar determinados riscos tecnológicos, sendo em casos mais graves a necessidade de comunicados internos e externos que orientam e previnem possíveis brechas tecnológicas em determinadas situações.

ANÁLISE DE INFRAESTRUTURA DE REDE:

A equipe avalia, repara e supervisiona eventuais problemas que surgem nas diversas instalações físicas que abrigam os sistemas de TI e garantem que as instalações de substituição sejam mantidas adequadamente, por meio de um processo interno entre a equipe de TI que faz o levantamento dos itens necessários que posteriormente são solicitados por meio de processo licitatório e instalados nos locais necessitados.

ANÁLISE DE REDES:

Avalia danos específicos da infraestrutura de rede para fornecer dados e conectividade de rede, incluindo WAN, LAN ou infraestrutura externa junto às empresas prestadoras de serviço.

ANÁLISE DE DA INFRAESTRUTURA DE SERVIDORES:

A equipe opera e supervisiona na infraestrutura dos servidores físicos e virtuais do município, o qual estuda formas de agir em meio à ocorrência de um eventual desastre, garantindo o desempenho de aplicações essenciais ao serviço municipal.

MÉTODO OPERACIONAL:

A equipe faz o levantamento e realiza pedidos de equipamentos necessários para desenvolverem suas funções com eficiência, equipamentos esses que são específicos à sua área de atuação que exige a solução de problemas.

ANÁLISE DE BACKUP:

Além de programar as rotinas automáticas de backup e realizar backups manuais, a equipe verifica possíveis perdas e mapeia a quantidade de dados perdidos, analisando a melhor forma da recuperação dos dados quando necessário em eventuais acidentes.

SEGURANÇA DA INFORMAÇÃO:

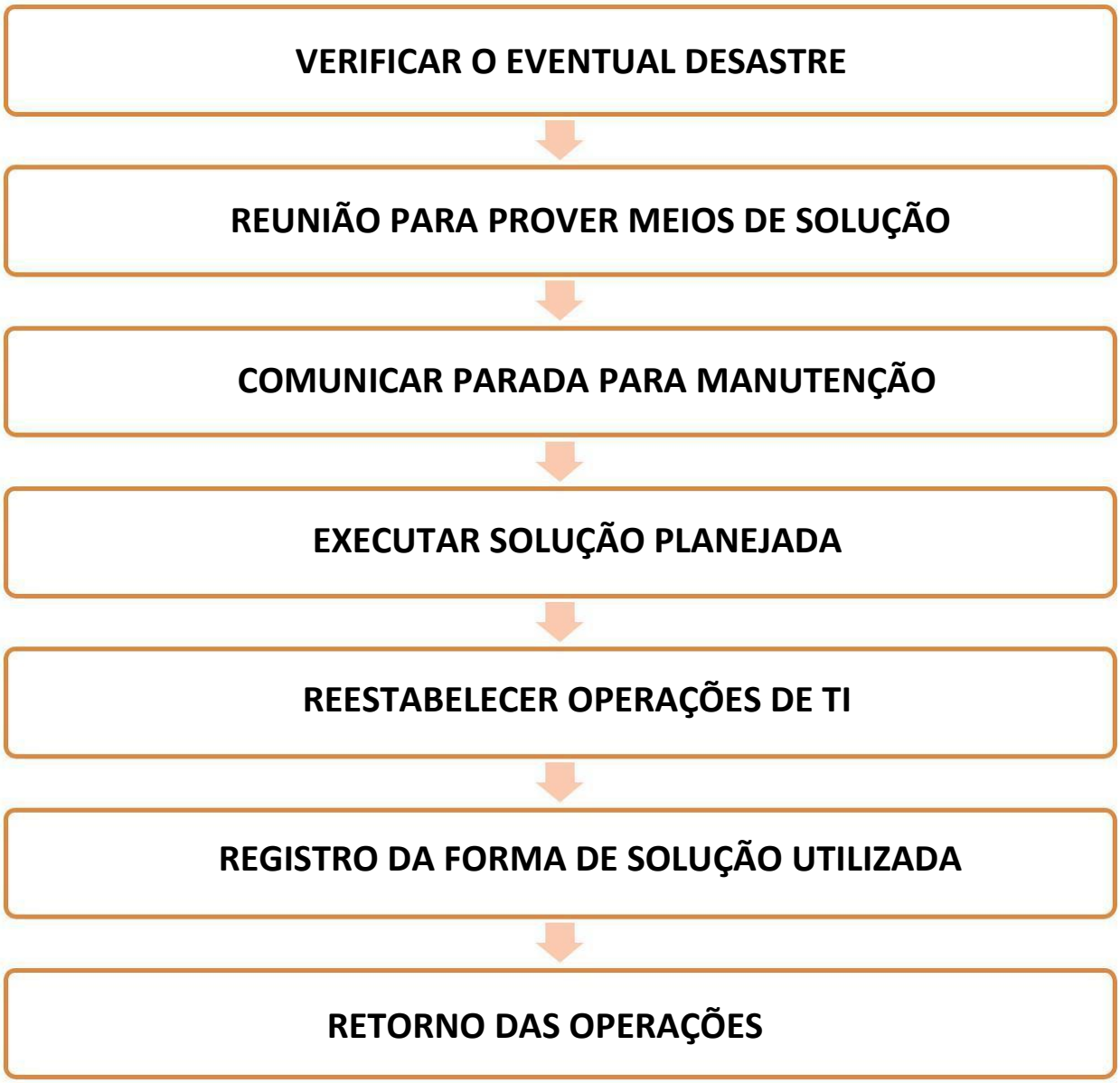
A equipe analisa e aplica mecanismos de segurança em ambientes primários e secundários, seja por meio de chaves, gavetas, softwares, criptografia, entre outros procedimentos, os quais evitam que desdobramentos de segurança afetem o acionamento da continuidade resguardando aplicações e dados.

5. SOLUÇÃO DE PROBLEMAS

Após um eventual desastre, a equipe de TI é acionada para solucionar o problema, a solução consiste em: verificar a origem do problema, avaliar a melhor método de reparo e operar o reparo para o retorno do serviço, quando ocorre qualquer cenário de desastre, insurgência ou risco desconhecido, ou quando há uma alta probabilidade de que uma vulnerabilidade seja explorada, a equipe é solicitado por meio dos contatos.

6. MACROPROCESSOS DO PCTI

O PCTI tem seus macroprocessos definidos nas atividades a seguir e se desmembra em planos específicos para cada área de atuação quando da ocorrência de um desastre.



7. PLANEJAMENTO COMUNICATIVO EM CASOS DE URGÊNCIA

Comunicação na ocorrência de um Desastre

No caso 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 equipe de comunicação será responsável por contatar estas unidades e passar as informações pertinentes a cada grupo, setor ou seguimento.

A comunicação com cada parte ocorrerá da seguinte forma:

- **Comunicar às autoridades**

A prioridade da equipe de comunicação será assegurar que as autoridades competentes tenham sido notificadas da catástrofe, principalmente se envolver risco às pessoas, fornecendo as seguintes informações de localização, natureza, magnitude e impacto do desastre.

- **Comunicação após um Desastre**

Após reunião interna, a equipe vai elaborar um breve programa de comunicação para acionar as partes afetadas de modo a informar e passar a todos a perspectiva dos esforços necessários para reestabelecer os serviços inativos.

- **Comunicação com os servidores**

A equipe de comunicação disponibilizará um meio de contato para este fim, com intuito de que as instalações públicas municipais se mantenham informadas da ocorrência de um desastre e da inatividade dos serviços essenciais de TI, os contatos a serem disponibilizados para os funcionários serão os contatos de: e-mail institucional e telefone corporativo da equipe técnica.

- **Comunicação nas instalações públicas**

Contatar unidades afetadas pelo desastre e fornecer contato. Deverá ser informada a natureza, o impacto e a abrangência do desastre, como também as ações de contingência em andamento, essa operação é comumente intermediada entre a equipe técnica diretamente com a prestadora de serviços de telecomunicação. Assim como ocorre o contato notificando o retorno do devido funcionamento das operações.

8. EXECUÇÃO DO PLANO

Procedimentos pós-incidente

Ocorrido o incidente, são executados respectivamente:

- Verificação da origem do problema;
- Verificação das consequências do incidente;
- Atuação no incidente:
  - Interrupção elétrica: Ativação de nobreaks a fim de amenizar a parada brusca dos dispositivos, possibilitando o desligamento programado;
  - Indisponibilidade de rede: Realização de substituição/reconfiguração de aparelhagem de rede, bem como atuando no cabeamento com emendas ou lançamento de novo cabeamento em local rompido ou oxidado;
  - Ataques Internos: Acionamento da polícia militar de forma contenciosa;
  - Falha Humana: Circular de orientação contendo boas práticas para tratar de problemas comuns que causam desastras na rede;
  - Falha de Hardware: Parada programada do dispositivo para avaliação da causa da falha, bem como providência de peça necessária a ser substituída;
  - Desastres Naturais: Realização de desligamento e recolhimento dos aparelhos para não entrar em contato com curtos-circuitos e alagamentos;
  - Incêndio: Acionamento de Corpo de Bombeiros;
  - Ataque Cibernético: Ativação do monitoramento de tráfego de rede, bem como acionamento da Provedora de Internet a fim de identificar a origem do ataque, para assim reconfigurar a intranet e restauração dos backups seguros nos locais críticos.

_____

Wilson Pontes Junior
Chefe da Seção de T.I.

_____

Juliana Durau
Secretária de Administração