PLANO DE CONTINUIDADE DE SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

OBJETIVO

Identificar e mitigar falhas nos serviços de TI (Tecnologia da Informação) que impactam diretamente todos os setores administrativos e operacionais. Pretende-se com este plano definir procedimentos, ações e medidas rápidas para os processos críticos de TI. Este plano deve ser seguido para garantir os serviços essenciais em caso de emergências que possam ocorrer durante as atividades, visando aplicar as ações necessárias para correção e/ou eliminação do problema.

APLICAÇÃO

Este documento se aplica a todos os serviços e sistemas de Tecnologia da Informação que são providos no Município de Amparo.

DEFINIÇÕES

1. Áreas Sensíveis: Áreas que sofrem fortes efeitos negativos quando atingidas pelas consequências da emergência. Dentre elas encontram-se a data center, salas administrativas e demais locais que possuam equipamentos de informática.

2. Área Vulnerável: Área atingida pela extensão dos efeitos provocados por um evento de falha.

3. Contingência: Situação de risco com potencial de ocorrer, inerente as atividades, serviços e equipamentos, e que ocorrendo se transformará em uma emergência. Diz respeito a uma eventualidade; possibilidade de ocorrer.

4. Backup: Cópia de um sistema completo ou de um ou mais arquivos guardados em diferentes dispositivos de armazenamento.

5. Data Center: ou Centro de Processamento de Dados, é um ambiente projetado para concentrar servidores, equipamentos de processamento e armazenamento de dados, e sistemas de ativos de rede, como switches, roteadores e outros.

6. Incidente: É o evento inesperado ou situação que altera a ordem normal das coisas, capaz de causar danos leves ou graves aos sistemas e aos equipamentos de TI. Toda ocorrência anormal, que foge ao controle de um processo, sistema ou atividade, da qual possam resultar danos aos sistemas e/ou equipamentos de TI.

7. Intervenção: É a atividade de atuar durante a emergência, seguindo planos de ações para corrigir ou minimizar os possíveis danos aos equipamentos e sistemas de TI.

8. Firewall: É uma solução de segurança baseada em hardware ou software (mais comum) que, a partir de um conjunto de regras ou instruções, analisa o tráfego de rede para determinar quais operações de transmissão ou recepção de dados podem ser executadas.

9. Emergência: Situação gerada por evento em um sistema ou equipamento que resulte ou possa resultar em danos aos próprios sistemas ou equipamentos ou ao desempenho do trabalho de servidores.

PRINCIPAIS RISCOS

1. Desastres naturais: tempestades, alagamentos, caso fortuito etc.

2. Interrupção de energia elétrica: Causada por fator externo à rede elétrica do prédio ou de sua localidade com duração da interrupção superior a 60 (sessenta) minutos. Causada por fator interno que comprometa a rede elétrica do prédio com curto-circuito, incêndio e infiltrações;

3. Falha na climatização do Data Center: Superaquecimento dos ativos devido a falha no sistema de refrigeração;

4. Indisponibilidade de rede: Rompimento de cabos decorrente de execuções de obras internas, desastres ou acidentes;

5. Falha humana: Acidente ao manusear equipamentos;

6. Ataques internos: Ataque aos ativos do Data Center e equipamentos de TI;

7. Falha de hardware: falha que necessite reposição de peça ou reparo, cujo reparo ou aquisição dependa de processo licitatório;

8. Ataque externo: Ataque virtual que comprometa o desempenho, acesso aos dados ou configuração dos serviços essenciais.

AÇÕES EM CASO DE EMERGÊNCIA

1. Reunião: 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;

2. Contingência de Backup: devem ser adotadas as seguintes ações de contingência e continuidade por processo ou serviço essencial:

    a. Verificar status da aplicação de backup e estimar impacto de perda de dados;

    b. Identificar Jobs de backups cujos dados em questão foram afetados;

    c. Estimar volume de dados a serem recuperados, tempo de recuperação dos dados e possíveis perdas operacionais;

    d. Atestar retorno do funcionamento do ambiente principal;

    e. Testar a aplicação de backup após desastre;

    f. Validar políticas de backup implementadas;

    g. Documentar atividades e informar a todos o retorno das atividades.

3. Cenários de inoperância: seus respectivos procedimentos planejados, definindo as atividades prioritárias para restabelecer o nível de operação dos serviços no ambiente afetado, dentro de um prazo tolerável.

4. Identificação de ativos danificados ou comprometidos: A equipe técnica deverá identificar e listar todos os ativos danificados da ocorrência do desastre;

5. 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;

6. 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, storage, routers e switches, bem como respectivas configurações de proxy, DNS, rotas, VLANs etc.;

7. 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 e ao Patrimônio para os devidos procedimentos de baixa. Deverá ser mensurado o tempo a aquisição irá impactar o RTO de cada serviço, comunicando aos diretores 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;

8. 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.

ENCERRAMENTO DAS AÇÕES

Ao término das ações de recuperação, será gerado um relatório com as informações consolidadas em parecer específico, informando horário de restabelecimento de cada serviço, equipamentos adquiridos, procedimentos de recuperação realizados e fornecedores acionados.

Departamento de Tecnologia da Informação

Secretaria Municipal de Administração e Tecnologia da Informação