DECRETO Nº 5.598, DE 23 DE JANEIRO DE 2024.
Institui o Plano de Continuidade de Serviços de TI no âmbito do Poder Executivo Municipal.

Art. 1º. – Fica instituído o Plano de Continuidade de Serviços de TI, parte integrante deste Decreto, instrumento estratégico de avaliação de riscos, recuperação de dados e comunicação de processos, visando à continuidade dos serviços de Tecnologia da Informação – TI, no âmbito do Poder Executivo do Município de Matão.

Art. 2º. – Para efeito deste Decreto, ficam estabelecidas as diretrizes e normas constantes no **Anexo Único**.

Art. 3º – Este Decreto entra em vigor na data de sua publicação.

Palácio da Independência, aos 23 de janeiro de 2024

APARECIDO FERRARI
Prefeito Municipal

ANEXO ÚNICO

PLANO DE CONTINUIDADE DE SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO

PREFEITURA MUNICIPAL DE MATÃO

SUMÁRIO

1 – APRESENTAÇÃO

A Tecnologia da Informação nos órgãos governamentais desempenha um papel crítico na prestação de serviços essenciais à sociedade. A operação eficaz e contínua desse serviço é vital para o bem-estar dos cidadãos e o funcionamento dos órgãos públicos. Nesse sentido, a garantia da continuidade das operações de Tecnologia da Informação tornou-se uma responsabilidade crucial.

Ocorrências como desastres naturais, incidentes cibernéticos, interrupções de infraestrutura e outras ameaças podem afetar gravemente a capacidade de um órgão governamental de cumprir suas obrigações para com os cidadãos. Essas situações demandam ação pró-ativa e planejamento estratégico para minimizar o impacto negativo e garantir que os serviços essenciais possam ser mantidos, mesmo em situações de adversidade.

O Plano de Continuidade de Serviços de Tecnologia da Informação abrange as estratégias necessárias à continuidade dos serviços, determinados como essenciais, para contingência, continuidade e recuperação de dados e informações quando da ocorrência de desastres.

2 – OBJETIVO

Identificar e mitigar falhas nos serviços de 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 Tecnologia da Informação.

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 a correção do problema.

3 – APLICAÇÃO

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

4 – PRINCIPAIS RISCOS

- 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.
  - Rompimento de cabos de interconexão decorrente da execução de obras públicas, desastres ou acidentes.
- Falha na climatização do Data Center:
  - Superaquecimento dos ativos devido a falha no sistema de refrigeração do ambiente, falha na redundância e/ou automatização dos aparelhos de climatização.
- Indisponibilidade de rede:
  - Rompimento de cabos decorrente de execuções de obras internas, desastres ou acidentes.
- Falha humana:
  - Incidentes relacionados a falhas humanas ao lidar com equipamentos críticos que representam riscos para a saúde, tais como manuseio inadequado de circuitos elétricos, erros na operação de sistemas de processamento de dados, manipulação inadequada de servidores e serviços críticos, entre outros.
- Falha de hardware:
  - Falhas de hardware podem incluir problemas em servidores, dispositivos de armazenamento, redes e outros componentes essenciais. O objetivo é minimizar o tempo de inatividade e garantir a recuperação rápida dos serviços críticos.
- Ataques internos:
  - Ataque aos ativos do Data Center e equipamentos de Tecnologia da Informação.
- Ataque externo:
  - Ataque virtual que comprometa o desempenho, acesso aos os dados ou configuração dos serviços essenciais locais e/ou em nuvem e rede de dados.

- Incêndio:
  - Incêndios que comprometam parcialmente ou completamente a continuidade dos serviços de tecnologia do município.
- Desastres Naturais:
  - Estabelece medidas a serem tomadas para garantir a continuidade das operações em caso de desastres naturais, como: inundações, incêndios florestais e outros eventos climáticos extremos.

5 – PAPÉIS E RESPONSABILIDADES

COMITÊ DE DESASTRE:

- Avaliar o plano periodicamente e decidir pelo seu acionamento quando da ocorrência de desastres, respondendo em nível institucional pela execução do plano e demais ocorrências relacionadas.
- Inclui autoridades em nível institucional e tomadores de decisão.

EQUIPE DE INSTALAÇÕES / AMBIENTE:

- Responsável pelas instalações físicas que abrigam sistemas de Tecnologia da Informação e pela garantia de que as instalações alternativas sejam mantidas adequadamente. Avalia danos e supervisiona os reparos no local principal no caso de a localização primária sofrer destruição ou danos.
- O líder desta equipe administrará e manterá o Plano de Recuperação de Desastre.

EQUIPE DE REDE:

- Avaliar os danos específicos de qualquer infraestrutura de rede e fornecer dados e conectividade de rede de voz, incluindo WAN, LAN e quaisquer conexões de telefonia internamente dentro da Prefeitura Municipal de Matão ou de infraestrutura externa junto aos prestadores de serviço.

EQUIPE DE SERVIDORES / APLICAÇÕES:

- Fornecer a infraestrutura necessária para servidores físicos e virtuais, assim os serviços essenciais continuarão suas operações e processos durante um desastre.
- Garantir que as aplicações essenciais funcionem como exigido para atender aos objetivos de negócios em caso de desastres. Estas equipes serão os principais responsáveis por assegurar e validar o desempenho das aplicações essenciais.

EQUIPE DE OPERAÇÕES:

- Fornecer aos funcionários as ferramentas de que necessitam para desempenhar suas funções da forma mais rápida e eficiente possível. Eles precisarão provisionar todos os funcionários da Prefeitura Municipal de Matão na solução de contingência com as ferramentas específicas à sua atuação.
- O líder desta equipe administrará e manterá o Plano de Continuidade Operacional.

EQUIPE DE COMUNICAÇÃO:

- Responsável por todas as comunicações durante um desastre, eles se comunicarão especificamente com os funcionários, clientes, autoridades, fornecedores e até mesmo com a mídia, caso necessário
- O líder desta equipe administrará e manterá o Plano de Administração de Crise.

EQUIPE DE BACKUP:

- Analisar as perdas e mapear a quantidade de dados perdidos, tempo de recuperação desses dados e formular a estratégia de recuperação de dados de acordo com as políticas preestabelecidas.

EQUIPE DE SEGURANÇA DA INFORMAÇÃO:

- Prover mecanismos de segurança no ambiente principal e alternativo. Resguardar aplicações e dados, evitando que desdobramentos de segurança afetem a continuidade, cuja proteção estará contida na política de segurança.

O Departamento de Tecnologia da Prefeitura Municipal de Matão e seu corpo de funcionários se encarregarão das atividades de quaisquer equipes acima, caso ainda não estejam formalmente definidas.

6 – INVOCAÇÃO DO PLANO

O Plano de Continuidade será acionado quando da ocorrência de algum dos cenários de desastres, a insurgência ou ocorrência de um risco desconhecido ou uma vulnerabilidade tenha grande possibilidade de ser explorada.

Os integrantes da equipe de comunicação serão responsáveis por acionar os contatos e partes interessadas, prioritariamente por telefone, ou pessoalmente caso seja possível.

CONTATOS

EQUIPES	RAMAL	TELEFONE
COMITÊ DE DESASTRE	4075	(16)3383-4075
EQUIPE DE INSTALAÇÕES/AMBIENTE	4065	(16)3383-4065
EQUIPE DE REDES	3122	(16)3383-3122
EQUIPE DE SERVIDORES/APLICAÇÕES	3123	(16)3383-3123
EQUIPE DE OPERAÇÕES	3083	(16)3383-3083
EQUIPE DE COMUNICAÇÕES	4042	(16)3383-4042
EQUIPE DE BACKUP	3119	(16)3383-3119
EQUIPE DE SEGURANÇA DA INFORMAÇÃO	3090	(16)3383-3090

Ao acionar os contatos informar qual ponto de encontro mais próximo, local e detalhes para reunir as equipes.

7 – FERRAMENTAS DO PLANO DE CONTINUIDADE

Com base nos ativos atuais à disposição do Departamento de Tecnologia da Informação, serão utilizadas estratégias de redundância e recuperação variadas, conforme apresentado a seguir. A redundância é a duplicação de elementos que constituem uma infraestrutura, ou seja, tem a finalidade de manter cópias/acessos que podem ser ativados como reservas, quando ocorrer danos ou falhas, tanto nos componentes físicos quanto nos virtuais de um sistema/infraestrutura.

7.1 – Redundância de Links

Atualmente, a Prefeitura dispõe de redundância de links de Internet em seu data center, ou seja, links de provedores distintos que chegam ao local com dupla abordagem.

7.2 – 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.

7.3 – 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 uma recuperação imediata de um cenário para análise em caso de desastre.

7.4 – Redundância de Backups

Atualmente, a Prefeitura dispõe de ferramenta profissional e corporativa 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.

8 – PROCESSOS

Este plano tem seus macroprocessos definidos nas atividades a seguir e se desmembra em planos específicos para cada área de atuação na ocorrência de um desastre.

8.1 – PLANO DE CONTINUIDADE OPERACIONAL (PCO):

Deve garantir a continuidade dos serviços essenciais de TI críticos na ocorrência de um desastre, enquanto se recupera o ambiente principal.

OBJETIVO E ESCOPO

É escopo deste plano 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 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;
- Estabelecer uma equipe para cada plano PCO, PRD e PAC;
- Definir os formulários, checklists e relatórios a serem entregues pelas equipes ao executar a contingência.

EXECUÇÃO DO PLANO

Avaliação de Impacto de Desastre:

- Identificada a ocorrência de um incidente ou crise, o Líder da Equipe de Operação deve verificar a dimensão do impacto, extensão e possíveis desdobramentos do ocorrido.
- Divulgar a informação a todas as equipes envolvidas.

Acionamento do plano:

- Dado o aval pelo Comitê, a equipe de operações convocará uma reunião de emergência com os líderes responsáveis pela PRD e PAC para o acionamento do plano com o intuito

de:

- Coordenar prazos e orquestrar as ações de contingência;
- Informar as equipes das ações de contingência com a priorização dos serviços essenciais.

Contingência de Warm Site:

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 dados (janela);
- Identificar jobs de backup 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 com Líder do PRD;
- Teste de aplicação de backup após desastre;
- Validar políticas de backup implementadas.

ENCERRAMENTO DO PCO

Uma vez validado o funcionamento do retorno dos sistemas essenciais e a estabilidade do data center, deverá ser emitido um parecer relatando as atividades realizadas neste plano de continuidade e informar a todos o retorno das atividades.

8.2 – PLANO DE ADMINISTRAÇÃO DE CRISE (PAC):

Deve definir atividade das equipes envolvidas e orquestrar as ações de contingência e comunicação durante e após a ocorrência de um desastre, com intuito de minimizar impactos até a superação da crise, através de ações e de uma comunicação eficaz.

OBJETIVO

São objetivos específicos do PAC:

- Garantir a segurança à vida das pessoas;
- Minimizar transtornos sobre os desdobramentos de incidente e estimular o esforço em

conjunto para superação da crise;

- Orientar os funcionários e demais colaboradores com informações e procedimentos de conduta;
- Informar a sociedade em tempo hábil e transmitir esclarecimentos condizentes com o ocorrido.

EXECUÇÃO DO PLANO

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 equipe de comunicação será responsável por contatar estas unidades e passar as informações pertinentes a cada grupo, setor ou seguimento;
- A prioridade da equipe de comunicação será assegurar que as autoridades competentes tenham sido notificadas da catástrofe, principalmente se envolver risco às pessoas, fornecer informações de localização, natureza, magnitude e impacto do desastre;
- A equipe de comunicação elaborará um breve programa de comunicação para acionar as partes envolvidas e afetadas de modo a manter todos bem informados e passar a perspectiva dos esforços necessários para o restabelecimento dos serviços inativos.

O plano deve ser ativado em caso da ocorrência de qualquer cenário de desastre identificado, insurgência, manifestação de um risco desconhecido ou quando uma vulnerabilidade tenha uma alta probabilidade de ser explorada. Qualquer problema identificado por qualquer servidor, deverá ser imediatamente comunicado ao Departamento de Tecnologia da Informação.

Contatos:

- **Telefone: (16) 3383-4075 - (16) 3383-3083 ou (16) 99732-2774 (whatsapp)**
- **E-mail: cpd@matao.sp.gov.br**

*Caso não haja conectividade ou linha telefônica disponível, ceder essas informações por meio de publicações, ou outra estratégia definida no momento.

As informações a serem dadas irão se referir a:

- Se é seguro para eles entrarem no ambiente afetado;
- Onde eles devem ir se não puderem ter acesso ao prédio;
- Que serviços ainda estão disponíveis para eles;
- Expectativas de trabalho durante o desastre.

ENCERRAMENTO DO PAC

Uma vez validado o funcionamento do retorno dos sistemas essenciais e estabilidade do data center, a equipe de comunicação entrará em contato com as partes descritas neste plano, provendo as informações de retorno das operações com as informações de status dos serviços essenciais.

Compor relatório com relação das atividades necessárias após a ocorrência do desastre, como remanejamento dos canais de informação, abertura e acompanhamento de chamados do ocorrido.

8.3 – PLANO DE RECUPERAÇÃO DE DESASTRE (PRD):

Deve planejar e agir para que, uma vez controlada a contingência e passada a crise, a Prefeitura Municipal de Matão retome seus níveis originais de operação no ambiente principal.

OBJETIVO E ESCOPO

O escopo deste plano é garantir a recuperação das operações do ambiente principal após um incidente ou desastre. Isso abrange ativos, conexões e configurações específicas deste ambiente.

São objetivos do PRD:

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

EXECUÇÃO DO PLANO

A equipe técnica deve identificar e listar todos os ativos danificados e interrupções de conexões após o desastre, especificando se são problemas internos ou externos ao ambiente, também devem relatar sistemas afetados por terceiros.

A equipe técnica deve mapear os serviços descontinuados, incluindo informações sobre perda de ativos e conexões. O relatório deve abranger todos os componentes necessários para a operação, como servidores, máquinas virtuais, bancos de dados, *firewall*, armazenamento, roteadores e *switches*, com configurações de *proxy*, DNS, rotas, VLANs, etc.

Após avaliar as perdas e impactos, a equipe técnica elaborará um cronograma de recuperação das aplicações, considerando:

- A priorização dos serviços essenciais ou definição de nível institucional;
- O tempo de indisponibilidade para cada serviço essencial;
- A disponibilidade da força de trabalho.

Se houver perda irreparável de ativos, o Comitê será notificado imediatamente sobre a necessidade de aquisição de substitutos. A equipe deve verificar quais ativos foram danificados e cobertos por garantia e se poderá ser acionada, neste caso, através da lista de fornecedores.

A equipe verificará se as configurações dos ativos reparados ou substituídos estão funcionando corretamente. Se necessário, será fornecido um cronograma estimado para configurar esses ativos.

Um ambiente de testes será criado para garantir a recuperação completa das aplicações e serviços afetados pelo incidente ou desastre. Os testes incluirão a verificação dos níveis de capacidade e disponibilidade dos serviços.

A recuperação dos dados para as aplicações afetadas será realizada. As configurações e funcionalidades dos sistemas serão validadas por meio de testes automatizados de monitoramento de serviços ou pela equipe designada.

ENCERRAMENTO DO PRD

Ao concluir o processo de recuperação, todas as informações serão consolidadas em um parecer específico. Este parecer incluirá o horário de restabelecimento de cada serviço, detalhes sobre os equipamentos adquiridos, procedimentos de recuperação executados e acionamento de fornecedores.

9 – REVISÃO

O Plano de Continuidade dos Serviços de Tecnologia da Informação será válido a partir de sua publicação, sendo revisado sempre que necessário, pelo Departamento de Tecnologia da Informação, que foi responsável por sua elaboração.

10 – VERSÃO

VERSÃO 1.0	**DEZEMBRO DE 2023**