INSTRUÇÃO NORMATIVA 03/2022

PLANO DE CONTINUIDADE SETOR DE TECNOLOGIA DA INFORMAÇÃO

Dispõe sobre a definição do Plano de Continuidade do Setor de Tecnologia da Informação (PCTI).

Através da Secretaria Municipal de Administração e Finanças, dispõe a criação do Plano de Continuidade do Setor de Tecnologia da Informação, que atua como resposta aos resultados de impacto e análise de riscos.

RESOLVE:

Art. 1º. Esta Instrução Normativa dispõe sobre a criação do Plano de Continuidade do Setor de Tecnologia da Informação, que atua como resposta aos resultados de impacto e análise de riscos.

Art. 2°. Esta Instrução Normativa entra em vigor na data da sua publicação.

Agudos, 11 de julho de 2022

Fernando Octaviani
Prefeito Municipal

Publicado em: **18 de julho de 2022**
Página: **29 a 38** do **Diário Oficial Eletrônico de Agudos.**

INSTRUÇÃO NORMATIVA 03/2022

PLANO DE CONTINUIDADE SETOR DE TECNOLOGIA DA INFORMAÇÃO

Anexo I

1. Apresentação

Uma vez que as falhas nos serviços de TIC impactam diretamente a continuidade da prestação dos serviços, almeja-se com este plano prover medidas de proteção rápidas e eficazes para os processos críticos de TI relacionados aos sistemas essenciais em casos de incidentes graves ou desastres. O plano de continuidade atuará como resposta aos resultados das análises.

2. Escopo

O Plano de Continuidade de TI (PCTI) abrange as estratégias necessáriasà continuidade dos serviços de TIC essenciais: contingência, continuidade e recuperação. Está voltado a conceder continuidade aos processos definidos como críticos para a TIC da Prefeitura Municipal de Agudos e serviços essenciais.

3. Serviços essenciais

São os seguintes serviços considerados essenciais, por ordem de priorização, para o acionamento e execução deste plano:

Serviço	Criticidade	RPO	Impacto			
			Financeiro	Legal	Imagem	Operacional
Sistemas Administrativos	Alta	Backup mais recente	Indefinido	Alto	Alto	Alto
Sistema de Saúde	Alta	Backup mais recente	Indefinido	Alto	Alto	Alto
Links de internet	Alta	Backup mais recente	Indefinido	Alto	Alto	Alto
Rede Interna	Média	Backup mais recente	Indefinido	Médio	Alto	Alto
Site institucional	Média	Backup mais recente	Indefinido	Baixo	Alto	Alto

4. Principais ameaças

Este plano deve ser acionado quando da ocorrência de cenários de desastre que apresentam risco à continuidade dos serviços essenciais.

EVENTO DE DESASTRE	POSSÍVEIS CAUSAS
01 - Interrupção de energia elétrica	* Causada por fator externo à rede elétrica do prédio ou de sua localidade com duração da interrupção superior a 12 horas. * Causada por fator interno que comprometa a rede elétrica do prédio com curto-circuitos, incêndio e infiltrações.
02 - Falha Climatização da sala servidor	Superaquecimento dos ativos devido a falha no dimensionamento de carga na sala servidor.
03 - Indisponibilidade de rede/circuitos	Rompimento de cabos de inter-conexão decorrente da execução de obras públicas, desastres ou acidentes.
04 - Falha humana	Acidente ao manusear equipamentos críticos.
05 - Ataques internos	Ataque aos ativos do DataCenter.
06 - Incêndio	Incêndios que comprometam os serviços de TIC.
07 - Desastres Naturais	Terremotos, tempestades, alagamentos e etc.
08 - Falha de hardware	Falha que necessite reposição de peça ou reparo, cujo reparo ou aquisição dependa de processo licitatório.
09 - Ataque cibernético	Ataque virtual que comprometa o desempenho, os dados ou configuração dos serviços essenciais.

5. Comitê de desastre/recuperação/comunicação (CDR)

Avaliar o plano periodicamente e decidir pelo seu acionamento quando houver a ocorrência de desastres, respondendo em nível institucional pela execução do plano e demais ocorrências relacionadas.

Inclui autoridades em nível institucional e tomadores de decisão da Prefeitura Municipal de Agudos.

Responsável por todas as comunicações durante um desastre. Especificamente, eles se comunicarão com os funcionários, clientes, autoridades, fornecedores e até mesmo com a mídia, se necessário:

- O líder desta equipe administrará e manterá o Plano de Administração de Crise.

- O Comitê CDR será composto pelos mesmos integrantes do Setor de Tecnologia da Informação.

6. Invocação do PCTI.

Este plano será acionado quando da ocorrência de algum dos cenários de desastres, a insurgência ou ocorrência de um risco desconhecido ou caso uma vulnerabilidade tenha grande possibilidade de ser explorada. O plano também poderá ser invocado em casos de testes ou por determinação do Setor de Tecnologia da Informação em conjunto com a alta administração da Prefeitura Municipal de Agudos.

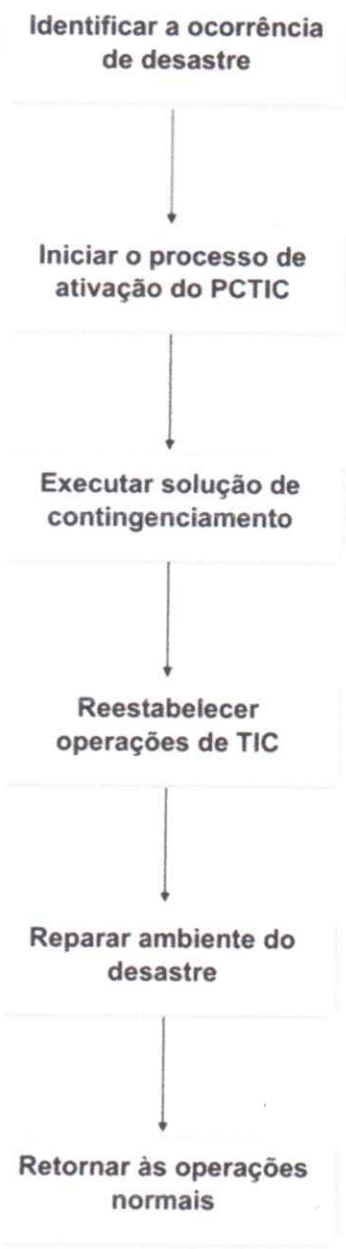
Os integrantes do comitê CDR serão responsáveis por acionar os contatos e partes interessadas, prioritariamente por telefone, ou pessoalmente caso seja possível.

LISTA DE ACIONAMENTO DE CONTATOS

EQUIPE	RESPONSÁVEL	TELEFONE	CONTATO
TECNOLOGIA DA INFORMAÇÃO	Setor de Tecnologia da Informação	+55 (14) 3262-0900	ti@agudos.sp.gov.br

7. Macroprocessos

Este plano 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.



O plano do PCTIC consiste em:

- Plano de Continuidade Operacional (PCO):

Garantir a continuidade dos serviços essenciais de TIC críticos na ocorrência de um desastre, enquanto recupera-se o ambiente principal.

- Plano de Administração de Crise (PAC):

Definir atividades das equipes envolvidas e orquestrar as ações de contingência e comunicação durante e após a ocorrência de umdesastre, com intuito de minimizar impactos até a superação da crise.

- Plano de Recuperação de Desastre (PRD):

Planejar e agir para que, uma vez controlada a contingência e passada a crise, a TIC retome seus níveis originais de operação no ambiente principal.

8. Estratégia de continuidade

A estratégia de continuidade para o cenário atual da TIC e serviços essenciais, está estabelecida da seguinte forma:

TIPO: WarmSite;

DESCRIÇÃO: Cópias de backup dos sistemas essenciais armazenadas em local alternativo.

A Prefeitura Municipal de Agudos mantém um backup em diferentes locais e servidores, mantendo a redundância caso haja problemas.

9. Plano de Continuidade operacional (PCO)

Este plano descreve os cenários de inoperância e seus respectivos procedimentos alternativos planejados, definindo as atividades prioritárias para garantir a continuidade dos serviços essenciais.

9.1. 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:

- Prover meios para manter o funcionamento dos principais serviços de TIC e a continuidade das operações de TI dos sistemas essenciais;

- Estabelecer procedimentos, controles e regras alternativas que possibilitem na continuidade das operações de TI durante uma crise ou cenário de desastre;

- Definir os formulários, checklists e relatórios a serem entregues pelas equipes ao executar a contingência.

9.2. Gestão

O Setor de Tecnologia da Informação é a unidade responsável por implementar, manter e melhorar o PCO e toda documentação inerente.

9.3. 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.

9.4. Encerramento do PCO

Uma vez validado o retorno dos sistemas essenciais e estabilidade do datacenter, deverá ser emitido um parecer relatando as atividades realizadas neste PCO.

Informar à equipe de CDR o retorno das atividades.

10. Plano de Administração de Crises (PAC)

Este plano especifica as ações ante os cenários de desastres. As ações incluem gerir, administrar, eliminar ou neutralizar os impactos inerentes ao relacionamento entre os agentes envolvidos e/ou afetados, até a superação da crise, através da orquestração das ações e de uma comunicação eficaz.

10.1. Objetivo Geral

O objetivo deste plano é garantir a comunicação, gerenciar as crises e viabilizar uma compreensão linear a todos os envolvidos das ações antes, durantee após a ocorrência de uma catástrofe.

10.1.1 Objetivos específicos

- Garantir a segurança à vida das pessoas;

- Minimizar transtornos sobre os desdobramentos de incidente e estimular esforço em conjunto para superação da crise;

- Orientar os funcionários e demais colaboradores com informações e procedimentos de conduta:

- Informar a sociedade em tempo e com esclarecimentos condizentes com o ocorrido.

10.2. Execução do Plano

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 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.

Autoridade	b. Número	Data / Hora do registro	Num. Ocorrência
Polícia	190		
Bombeiros	193		
SAMU	192		

10.3. Comunicação após um desastre

Após reunião, 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 todos a perspectiva dos esforços necessários para o restabelecimento dos serviços inativos.

10.4. Comunicação com os funcionários

A equipe de comunicação deverá prover um meio de contato específico para este fim, com intuito de que os setores da Prefeitura Municipal de Agudos mantenham-se informados da ocorrência de um desastre e da inatividade dos serviços essenciais de TI.

10.5. Encerramento do PAC

Uma vez validado o funcionamento do retorno dos sistemas essenciais e estabilidade do datacenter, as equipes entrarão em contato com as partes descritas neste plano provendo as informações de retorno das operações com as informações de status dos serviços essenciais.

Compor o relatório com relação das atividades necessárias após a ocorrência dos desastres como remanejamento dos canais de informação, abertura e acompanhamento de chamados correlatos ao ocorrido.

11. Plano de Recuperação de Desastres (PRD)

Este plano descreve os cenários de inoperância e seus respectivos procedimentos planejados, definindo as atividades prioritárias para restabelecer o nível de operação dos serviços no ambiente afetado dentro de um prazo tolerável.

11.1. Objetivo e escopo

É escopo deste plano garantir o retorno das operações do ambiente principal depois da ocorrência de uma crise ou cenário de desastre, tratando-se apenas dos ativos, conexões e configurações deste ambiente:

- Avaliar danos aos ativos e conexões do datacenter e prover meios para sua recuperação.

- Evitar desdobramentos de outros incidentes na facilidade principal;

- Restabelecer o datacenter dentro do prazo tolerável.

11.2. Execução do plano

11.2.1. Identificar ativos danificados

As equipes deverão identificar e listar todos os ativos danificados da ocorrência do desastre.

11.2.2. Identificar acessos interrompidos

A equipe deverá identificar as interrupções de conexões e acessos gerados após o desastre, informando se a abrangência está na rede local, rede WAN ou com o provedor de serviços.

11.2.3. Listar serviços descontinuados

A equipe do PRD deverá mapear quais serviços foram descontinuados contendo as informações de perda de ativo e de conexão com intuito de levar ao conhecimento do comitê. 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.

11.2.4. Elaborar cronograma de recuperação

O líder do PRD após o mapeamento das perdas e impactos elaborará um breve cronograma de recuperação das aplicações levando em consideração:

- A priorização dos serviços essenciais, ou determinação de nívelinstitucional;
- O RTO definido para cada serviço essencial;
- A força de trabalho disponível.

11.2.5. Substituição de ativos e equipamentos

Em caso de perda de ativos, deverá ser imediatamente informado ao comitê de DR a necessidade de reposição de ativos perdidos que não puderem ser recuperados. A equipe irá mensurar quanto tempo a aquisição irá impactar o RTO de cada serviço, comunicando ao CDR se há alguma solução alternativa a ser tomada enquanto é realizada a aquisição.

A equipe de instalação deve verificar se os ativos que foram danificados estão cobertos por garantia e se poderá ser acionada neste caso, através dos fornecedores.

As informações pertinentes à alteração do tempo de recuperação dos serviços serão passadas às equipes do PCO e PAC.

11.2.6. Reconfiguração de ativos e equipamento

A equipe de instalação deverá verificar se as configurações dos ativos reparados ou substituídos estão em pleno funcionamento. Caso não estejam, prover cronograma estimado para configurar estes ativos informando as equipes competentes.

12. Teste de ambiente

O ambiente principal do datacenter antes do recovery dos dados do backup deverá ser testado a fim de garantir que o processo de recuperação ocorra conforme o planejado.

Os testes visam garantir os mesmos níveis de capacidade e disponibilidade dos serviços essenciais antes do desastre.

13. Recuperar dados do backup

Proceder a recuperação dos dados para as aplicações, seja do storage ou debackup:

- Validar as configurações e funcionalidades dos sistemas;
- A validação pode ser realizada pelos testes automatizadose de monitoramento;
- Por equipe designada pela equipe de configuração dos sistemas (GESIS).

13.1. Encerramento do PRD

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