Plano de Continuidade de T.I.

SECRETARIA MUNICIPAL DE CIÊNCIA, TECNOLOGIA, DESENVOLVIMENTO ECONÔMICO E URBANO

2022

Plano de Continuidade de T.I.

SUMÁRIO

APRESENTAÇÃO

Falhas e erros nos serviços de tecnologia trazem impactos diretos na gestão pública e podem trazer prejuízos operacionais e financeiros. Atrapalham a boa prestação de serviços públicos, o objetivo desse plano é elaborar e fornecer medidas de proteção e recuperação rápidas e eficientes para processos críticos de TI relacionados aos sistemas essenciais em casos de incidentes e ou desastres. O plano de continuidade atuará como resposta aos resultados da Análise de impacto e na análise de risco, buscando sempre a melhor e mais ágil ação a ser tomada.

OBJETIVO

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

Este Plano pode ser executado no âmbito Municipal de maneira isolada ou como parte de um plano de continuidade de negócio (PCN) da Prefeitura Municipal

SERVIÇOS ESSENCIAIS

SERVIÇO	**CRITICIDADE** [1]	**RPO** [2]	**RTO** [3]	**IMPACTO** [4]			
				FINANCEIRO	**LEGAL**	**IMAGEM**	**OPERACIONAL**
CONTABIL	MEDIA	BACKUP MAIS RECENTE	2 DIAS	MÉDIO	ALTO	MÉDIO	ALTO
TRIBUTÁRIO	ALTA	BACKUP MAIS RECENTE	2 DIAS	ALTO	ALTO	MÉDIO	ALTO
FOLHA DE PGTO	MEDIA	BACKUP MAIS RECENTE	2 DIAS	MÉDIO	ALTO	ALTO	ALTO
PROTOCOLO	ALTA	BACKUP MAIS RECENTE	2 DIAS	MÉDIO	ALTO	ALTO	ALTO
ALMOXARIFADO	MEDIA	BACKUP MAIS RECENTE	2 DIAS	MÉDIO	MÉDIO	MÉDIO	ALTO

COMPRAS	MEDIA	BACKUP MAIS RECENTE	2 DIAS	MÉDIO	ALTO	MÉDIO	ALTO
OUVIDORIA	ALTA	BACKUP MAIS RECENTE	2 DIAS	BAIXO	ALTO	ALTO	ALTO
PATRIMONIO	BAIXA	BACKUP MAIS RECENTE	2 DIAS	BAIXO	MÉDIO	MÉDIO	MÉDIO
EXEC. FISCAL	MEDIA	BACKUP MAIS RECENTE	2 DIAS	MÉDIO	ALTO	ALTO	ALTO
TRANSPARENCIA	ALTA	BACKUP MAIS RECENTE	2 DIAS	BAIXO	ALTO	ALTO	ALTO
AD	ALTA	AD SECUNDÁRIO	8 HRS	ALTO	MÉDIO	MÉDIO	MÉDIO
SITE	ALTA	BACKUP MAIS RECENTE	2 DIAS	MÉDIO	MÉDIO	MÉDIO	MÉDIO
DIARIO OFICIAL	ALTA	BACKUP MAIS RECENTE	1 DIA	BAIXO	ALTO	ALTO	ALTO
E-MAIL	MEDIA	SLA DA EMPRESA	12 HRS	MÉDIO	MÉDIO	MÉDIO	MÉDIO
SERVIÇO DE LINK	ALTA	SLA DA EMPRESA	8 HRS	ALTO	ALTO	ALTO	ALTO
VIDEO MONITORAMENTO	MEDIA	BACKUP MAIS RECENTE	2 DIAS	BAIXO	MÉDIO	ALTO	MÉDIO
INFOVIA	MEDIA	SLA INFOVIA	2 DIAS	MÉDIO	MÉDIO	ALTO	ALTO
DIVIDA ATIVA	MEDIA	BACKUP MAIS RECENTE	2 DIAS	ALTO	ALTO	ALTO	ALTO
SAÚDE	ALTA	BACKUP MAIS RECENTE	1 DIA	MÉDIO	ALTO	ALTO	ALTO
LICITAÇÕES E CONTRATOS	ALTA	BACKUP MAIS RECENTE	2 DIA	MÉDIO	ALTO	ALTO	ALTO
PROCESSO DIGITAL	ALTA	BACKUP MAIS RECENTE	1 DIA	ALTO	ALTO	ALTO	ALTO

BACKUP SERVER	ALTA	DIARIO	1 DIA	ALTO	ALTO	ALTO	ALTO
SERVER FILE	ALTA	BACKUP MAIS RECENTE	1 DIA	ALTO	ALTO	ALTO	ALTO
FIREWALL	ALTA	BACKUP MAIS RECENTE	1 DIA	ALTO	ALTO	ALTO	ALTO
CONTROLE INTERNO	MÉDIA	BACKUP MAIS RECENTE	2 DIAS	ALTO	ALTO	MÉDIO	ALTO

1 - CRITICIDADE: NIVEIS CRITICOS PRÉ DEFINIDOS PELA GESTÃO.

2 – RPO – PONTO EM UMA LINHA DO TEMPO EM QUE OS DADOS DEVEM SER RECUPERADOS APÓS A OCORRÊNCIA DE UMA INTERUPÇÃO.

3 – RTO – PERIODO DE TEMPO DENTRO DO QUAL OS NÍVEIS MINIMOS DOS SERVIÇOS DEVEM SER RECUPERADOS APÓS A OCORRÊNCIA DA INTERRUPÇÃO.

4 – NIVEIS DE IMPACTO PRÉ DEFINIDOS PELA GESTÃO.

PRINCIPAIS RISCOS E AMEAÇAS

DESASTRES	POSSIVEIS CAUSAS
01 – Interrupção de energia elétrica	- Ocasionada por um fator externo à rede elétrica da prefeitura ou de sua localização com duração superior a 12 horas. - Ocasionada por fator interno onde é comprometida a rede elétrica do prédio com curto-circuito, Infiltrações ou incêndio.
02 – Falha de climatização da sala cofre	Superaquecimento dos ativos devido a falha no dimensionamento de carga na sala cofre.
03 – Indisponibilidade de rede/circuitos	Rompimento de cabos de interconexão devido à execução de obras, acidentes ou outros fatores
04 – Ataques internos	Ataque aos ativos do Data Center.
05 – Falha humana	Acidente ao manusear equipamentos, erros em configurações.
06 - Incêndio	Incêndios que comprometam os serviços de TI
07 – Desastres Naturais	Terremotos, tempestades, alagamentos, rompimento de barragens etc.

08 – Falha de hardware	Falha que necessite reposição de peça ou reparo ou aquisição que dependa de processo licitatório.
09 – Ataques Cibernéticos	Ataque virtual que comprometa o desempenho, os dados ou configuração dos serviços essenciais.

PAPEIS E RESPONSABILIDADES

CONSELHO DE DESASTRES (CD):

Avalia regularmente os planos e decide ativá-los em caso de desastre e responde a nível institucional para planejar a implementação e outros eventos relacionados. Serão comunicados os servidores, munícipes, autoridades, fornecedores e até a mídia quando necessário em caso de desastres.

O líder da equipe gerenciará e manterá o Plano de Administração de Crises (PAC).

O Conselho será composto pelos mesmos membros do Departamento de informática Infovia – CPD e pelo Secretário Municipal de Ciência e Tecnologia.

EQUIPE DE INSTALAÇÕES/AMBIENTE:

Responsável pelas instalações físicas que abrigam os sistemas de TI e garante que as instalações de substituição sejam mantidas adequadamente. Avalia os danos e supervisiona os reparos.

O líder desta equipe é responsável pela administração do Plano de Recuperação de Desastre (PRD).

EQUIPE 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

EQUIPE DE SERVIDORES E APLICAÇÕES:

Fornece a infraestrutura de servidor físico e virtual que a TI execute suas operações e processos necessários durante um desastre. Garante que cruciais aplicações funcionem conforme estabelecido para atingir os objetivos de negócios durante eventuais desastres. Eles serão os principais responsáveis por garantir e validar o desempenho de aplicações cruciais, se necessário auxiliam a equipe do Departamento de informática Infovia – CPD.

EQUIPE DE OPERAÇÕES:

Fornece aos servidores os equipamentos necessários para desenvolverem suas funções com agilidade e eficiência. Provisionarão todos os servidores da Prefeitura de Pedreira na resolução de problemas nos seus equipamentos específicos à sua atuação.
O líder da equipe administrará e manterá o Plano de Continuidade Operacional.

EQUIPE DE BACKUP:

Verifica possíveis perdas e mapeia a quantidade de dados perdidos, tempo para recuperar esses dados e estabelece as estratégias necessárias de recuperação.

EQUIPE DE SEGURANÇA DA INFORMAÇÃO:

Fornece mecanismos de segurança em ambientes primários e secundários. Evita que desdobramentos de segurança afetem o acionamento da continuidade resguardando aplicações e dados.

EQUIPE DE COMUNIÇÃO:

Responsável por todas as comunicações durante um desastre.
Essencialmente eles se comunicarão com funcionários, clientes, autoridades, fornecedores e com a mídia se necessário.
O líder dessa equipe administrará e manterá o Plano Operacional.

INVOCAÇÃO DO PLANO

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 CD em conjunto com a SCTDEU

EQUIPE	RESPONSÁVEL	TELEFONE	CONTATO	SETOR
INFRAESTRUTURA	Líder da equipe de infraestrutura	(19) 3893-1845	redes.ti@pedreira.sp.gov.br	DI
REDES	Líder da equipe de redes	(19) 3893-1845	redes.ti@pedreira.sp.gov.br	DI
INFRA/APLICAÇÔES	Líder da equipe de Aplicações	(19) 3893-1845	redes.ti@pedreira.sp.gov.br	DI

SEGURANÇA DA INFORMAÇÃO	Líder da equipe de SI	(19) 3893-1845	redes.ti@pedreira.sp.gov.br	DI
OPERAÇÕES	Líder da equipe de Suporte Técnico	(19) 3893-1845	redes.ti@pedreira.sp.gov.br	DI
BACKUP	Líder da equipe de infraestrutura	(19) 3893-1845	suporte@pedreira.sp.gov.br	DI
VALIDAÇÃOAMBIENTE	Gerentes de Sistema e Desenvolvimento	(19) 3893-1845	sandro@pedreira.sp.gov.br	DI
EQUIPE DE COMUNICAÇÃO	LÍDER DA EQUIPE DE COMUNICAÇÃO	(19) 38931845	Cienciaetecnologia@pedreira.sp.gov.br	SCTDEU

MACROPROCESSOS

O plano possui macroprocessos definidos conforme as atividades a seguir e são subdivididos em planos específicos para cada área de atuação quando ocorrer um desastre.

Os sub-plano do PCTI consistem em:

Plano de Continuidade Operacional (PCO):
Garantir a continuidade dos serviços essenciais de TI críticos na ocorrência de um desastre, enquanto recupera-se o ambiente principal.

Plano de Administração de Crise (PAC):

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.

Plano de Recuperação de Desastre (PRD):

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

ESTRATÉGIAS DE CONTINUIDADE

A estratégia de continuidade para o cenário atual de TI e serviços públicos essenciais, fica estabelecida da seguinte forma:

TIPO – WARM SITE TI

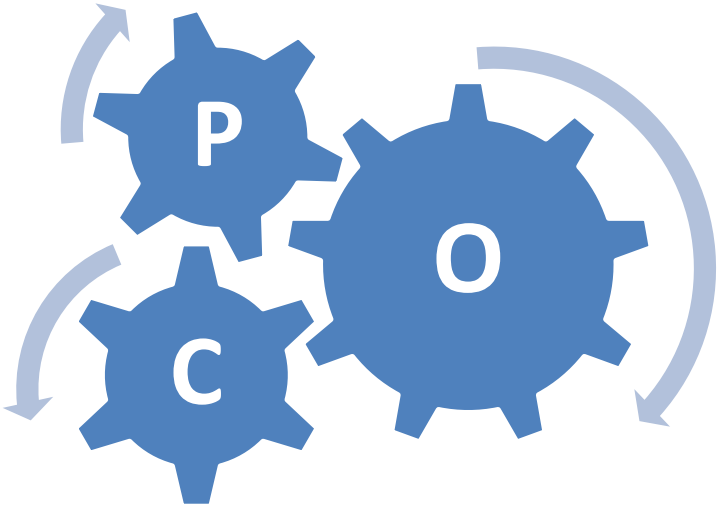
DESCRIÇÃO:

1. **CÓPIAS DE BACKUP DOS SISTEMAS ARMAZENADAS EM LOCAL ALTERNATIVO – SEDE DA INFOVIA-CPD E/OU NUVEM.**
2. **CONEXÃO REDUNDANTE.**
3. **ANEL ÓTICO QUE GARANTA A REDUNDÂNCIA.**

AÇÕES DE CONTIGÊNCIA E RECUPERAÇÃO:

MAPEAR PERDA DE DADOS E ATIVOS, REESTABELECER A ESTRUTURA AFETADA APÓS O AMBIENTE ESTAR OPERACIONAL, PROVER A RECUPERAÇÃO DOS DADOS EM BACKUP.

AS AÇÕES DE CONTINGÊNCIA E RECUPERAÇÃO SERÃO DETALHADAS NOS SUBPLANOS A SEGUIR:



PLANO DE CONTINUIDADE OPERACIONAL

PLANO DE CONTINUIDADE OPERACIONAL

Este plano descreve os cenários de inoperância e seus respectivos procedimentos alternativos planejados, prescreve ações diante de um cenário de desastre. As ações incluem gerenciar, administrar, eliminar ou paralizar os efeitos, inerentes ao relacionamento entre os agentes envolvidos e/ou afetados por meio de ação coordenada e comunicação efetiva até a superação da crise.

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:

A. Prover meios para manter o funcionamento dos principais serviços de TI e a continuidade das operações de TI, dos sistemas essenciais.

B. Estabelecer procedimentos, controles e regras alternativas que possibilitem a continuidade das operações de TI durante uma crise ou cenário de desastre.

C. Estabelecer uma equipe para cada plano PCO PRD e PAC.

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

E. Minimizar transtornos sobre os desdobramentos de incidente e estimular o esforço em conjunto para superação da crise.

F. Informar a população em tempo e com esclarecimentos condizentes com o ocorrido.

G. Orientar os servidores e demais colaboradores com informações e procedimentos de conduta.

GESTÃO

A SECRETARIA MUNICIPAL DE CIÊNCIA, TECNOLOGIA, DESENVOLVIMENTO ECONOMICO E URBANO E O DEPARTAMENTO DE TECNOLOGIA INFOVIA-CPD são as unidades responsáveis por implementar, manter e melhorar o PCO e toda documentação inerente.

EXECUÇÃO DO PLANO

Avaliação de Impacto de Desastre Identificada a ocorrência de um incidente ou crise o Líder da Equipe de Operação e Backup deve verificar a dimensão do impacto, extensão e possíveis desdobramentos do ocorrido.

ACIONAMENTO DO PLANO

Com o aval do CD ao acionamento ao plano, a EQUIPE DE OPERAÇÕES convocará reunião de emergência com os líderes responsáveis pele PRD e PAC com o intuito de:

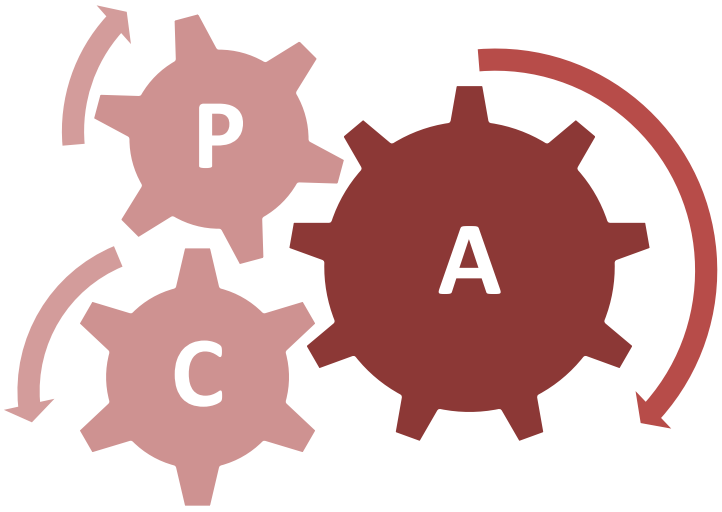
- Coordenar os prazos e organizar as ações de contingência.
- Informar as equipes as ações de contingência, os serviços essenciais deverão ser priorizados.

Devem ser adotadas as seguintes ações de contingência e continuidade por processo ou serviço essencial:

ID	INSTRUÇÃO	DURAÇÃO	OBSERVAÇÃO	RESULTADO
1	Verificar status da aplicação de backup e estimar impacto de perda dados (janela)			
2	Identificar as rotinas de backup cujos dados em questão foram afetados			
3	Estimar volume de dados a serem recuperados, tempo de recuperação dos dados e possíveis perdas operacionais			
4	Atestar retorno do funcionamento do ambiente principal com Líder do PRD			
5	Teste de aplicação de backup após desastre			
6	Validar políticas de backup implementadas			

ENCERRAMENTO DO PCO

Uma vez que o funcionamento do retorno dos sistemas essenciais e estabilidade do datacenter forem validados, deverá ser emitido um parecer relatando as atividades realizadas neste PCO. Informar à equipe de CD o retorno das atividades.



PLANO DE ADMINISTRAÇÃO DE CRISE

PLANO DE ADMINISTRAÇÃO DE CRISES (PAC)

O plano prescreve ações diante de um cenário de desastre. As ações incluem gerenciar, administrar, eliminar ou paralisar os efeitos, inerentes ao relacionamento entre os agentes envolvidos e/ou afetados por meio de ação coordenada e comunicação efetiva até a superação da crise.

O objetivo do programa é garantir que todos os envolvidos se comuniquem antes, durante e depois de um desastre, gerenciem a crise e alcancem uma compreensão linear das ações.

Os objetivos específicos do PAC são:

1- Garantir a segurança à vida das pessoas;
2- Minimizar transtornos sobre os desdobramentos de incidente e estimular o esforço em conjunto para superação da crise.
3- Orientar os servidores e demais colaboradores com informações e procedimentos de conduta.
4- Informar a população em tempo e com esclarecimentos condizentes com o ocorrido.

EXECUÇÃO DO PLANO

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:

1 - 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

2 - Comunicação após um Desastre

A equipe de comunicação, após reunião com líderes do PRD e PCO, 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 restabelecer os serviços inativos.

3 – 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.

Contatos a serem disponibilizados:

Telefones:

19 38931845
19 999830025

E-mail:

cienciaetecnologia@pedreira.sp.gov.br
diretorgeral.ti@pedreira.sp.gov.br
mateus@pedreira.sp.gov.br
suporte@pedreira.sp.gov.br
sandro@pedreira.sp.gov.br

4 - Comunicar instalações públicas municipais:

Acionar diretamente 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.

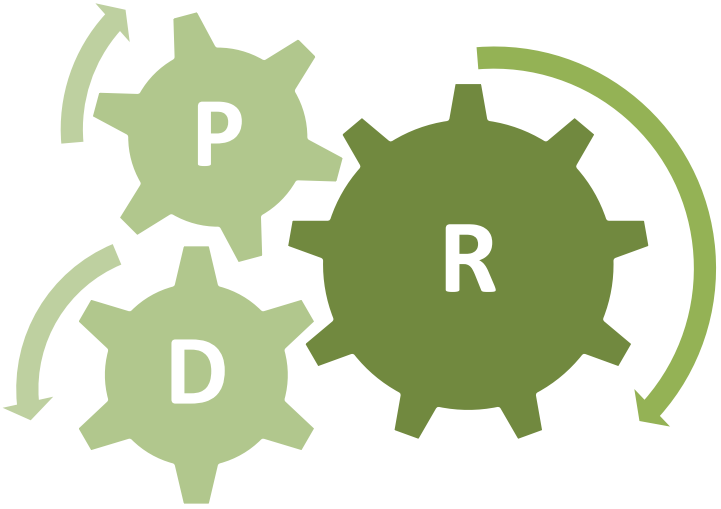
5 - Comunicar retorno das operações:

Deverá comunicar a todas as partes acima mencionadas quando ocorrer o retorno das operações à normalidade.

ENCERRAMENTO DO PAC

Uma vez que o funcionamento do retorno dos sistemas essenciais e estabilidade do datacenter forem validados, a EQUIPE DE COMUNICAÇÃO contatará as partes descritas neste plano disponibilizando 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 correlatos ao ocorrido.



PLANO DE RECUPERAÇÃO DE DESASTRE

PLANO DE RECUPERAÇÃO DE DESASTRES (PRD)

O plano descreve os cenários de interrupção e seus respectivos procedimentos, definindo atividades a serem priorizadas para restaurar os níveis de operação do serviço no ambiente afetado dentro de um prazo tolerável.

OBJETIVO E ESCOPO:

O escopo do plano é garantir que o ambiente primário volte a funcionar após uma situação de crise ou desastre, lidando apenas com os ativos, conexões e configurações desse ambiente.

O PRD visa:

1 - Avaliar os danos aos ativos e conexões do datacenter e fornecer métodos de recuperação;
2 - Evitar desdobramentos de outros incidentes na facilidade principal;
3 - Normalizar o datacenter dentro de um prazo tolerável;

EXECUÇÃO DO PLANO

1 - Identificar ativos danificados:

As equipes de INSTALAÇÃO/BACKUP/SERVIDORES/REDE devem identificar e listar todos os ativos danificados durante a ocorrência do desastre.

2 – Identificar acessos interrompidos:

A EQUIPE DE REDE 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.

3 - Listar serviços descontinuados:

Deverá ser mapeado pela equipe PRD quais foram os serviços descontinuados contendo as informações de perda de ativo e de conexão com a intenção de levar ao conhecimento do CD. Este relatório deverá abranger 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.

4 - Criar cronograma de recuperação:

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

- A priorização dos serviços essenciais, ou determinação de nível institucional.

- O RTO definido para cada serviço essencial.
- A força de trabalho disponível.

5 - Substituição de ativos e equipamentos:

Caso houver perda de ativos, imediatamente deverá ser informada ao CD a necessidade de aquisição de ativos perdidos que não puderem ser recuperados. A equipe irá mensurar quanto tempo o processo licitatório irá impactar o RTO de cada serviço comunicando ao CD se há alguma alternativa a ser tomada enquanto é realizado o processo licitatório.

A equipe de INSTALAÇÕES deverá verificar quais ativos 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.

6 - Reconfiguração de ativos e equipamento:

A equipe de INSTALAÇÕES verificará se as configurações dos ativos reparados ou substituídos estão em funcionamento pleno. Caso não estiverem, elaborará um cronograma estimado para configurar estes ativos informando à EQUIPE DE COMUNICAÇÃO e ao CD.

7 - 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 incluem:

Garantir os mesmos níveis de capacidade e disponibilidade dos serviços essenciais antes do desastre;

8 - Recuperar dados do backup:

Proceder a recuperação dos dados para as aplicações.

Validar as configurações e funcionalidades dos sistemas:

a) A validação pode ser realizada pelos testes automatizados de monitoramento dos serviços;

b) Por equipe designada pela equipe de configuração dos sistemas;

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

DOCUMENTO DE VALIDAÇÃO DE TESTE

O PCTI será testado e validado em reunião entre os líderes de cada sub-plano a cada semestre ou com a insurgência de novos fatores de risco, mudança na análise de impacto, ou com a inclusão de um novo serviço no plano de continuidade.

DATA	TIPO	MOTIVO	STATUS

VERSÃO 1.0 – DEZEMBRO DE 2022

CARLOS HENRIQUE DE ARAUJO
SECRETARIA MUNICIPAL DE CIÊNCIA, TECNOLOGIA, DESENVOLVIMENTO ECONÔMICO E URBANO