PLANO DE CONTINUIDADE DA TECNOLOGIA DA INFORMAÇÃO

Data:26/07/2024
Versão 1.0

Descrição	PLANO DE CONTINUIDADE DA TECNOLOGIA DA INFORMAÇÃO	
Objetivo	O plano de continuidade dos serviços de TIC é um documento que descreve as medidas e procedimentos que uma organização deve tomar para garantir a continuidade das operações para os casos de interrupção ou desastre. O plano de continuidade é de extrema importância para que possamos prover a disponibilidade, integridade e confidencialidade dos sistemas envolvidos na infraestrutura do município. O Plano de Continuidade de TIC (Tecnologia da Informação e Comunicação) tem como objetivo: abranger as estratégias necessárias à continuidade dos serviços de tecnologia contemplando a contingência, continuidade e recuperação. Está voltado a conceder continuidade aos processos definidos como críticos à infraestrutura tecnológica da Prefeitura Municipal de Mairiporã.	
Responsável	**Equipe do DTI**	**Criado em 26/07/2024**
Departamento	Tecnologia da Informação	

HISTÓRICO DE ALTERAÇÕES

Descrição		
Objetivo		
Responsável	**Equipe**	**Criado em**
Setor		

SUMÁRIO

PLANO DE CONTINUIDADE DE NEGÓCIO:

O Plano de Continuidade de Tecnologia da Informação (PCTI) fornece estratégias para garantir que serviços essenciais sejam identificados, para garantir sua preservação após a ocorrência de um desastre e até o retorno da situação normal de funcionamento do órgão ou instituição. Também provê quais planos de ação devem ser realizados em cada momento.

OBJETIVO

O PCTI deverá estabelecer cenários de situações inesperadas ou incidentes (quer sejam operacionais, desastres ou crises), além de formas de gerenciar os impactos imediatos de um incidente de interrupção, dando a devida atenção para:

1. bem-estar dos públicos internos e externos conforme a Política de Comunicação do do órgão;
2. alternativas estratégicas, táticas e operacionais para responder à interrupção;
3. prevenção de novas perdas ou indisponibilidade de atividades prioritárias;
4. detalhes sobre como e em que circunstâncias o órgão irá se comunicar com as partes interessadas e seus familiares ou contatos de emergência.

O PCTI fornece normas e padrões para que o órgão consiga recuperar, retomar e dar continuidade aos seus processos de negócios mais cruciais, evitando que eles sofram danos maiores.

Os planos aqui definidos seguirão o Modelo “Plan-Do-Check-Act” (PDCA) para planejar, estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar continuamente.

PAPÉIS E RESPONSABILIDADES

Papéis		Responsabilidades
Setor Responsável pela Segurança da Informação	Setor responsável pela normatização e atualização das normas de segurança da informação, em conjunto com as demais áreas competentes.	- Coordenar a elaboração do Plano de gestão de continuidade de negócio e cópias de segurança - Subsidiar a diretoria de TI com informações pertinentes à gestão de continuidade de negócio e cópias de segurança

CONTROLE DE EXECUÇÃO

Controle	Método de execução	Frequência
Setor Responsável pela Segurança da Informação	Realizar uma reunião com as equipes executoras do processo, para avaliar a aderência, os benefícios gerados e oportunidades de melhoria do processo. Essa revisão deve identificar se o processo necessita de revisão.	Anual

FERRAMENTAS

Indicadores de desempenho
Rotinas de validação do Plano
Metas de desempenho e testes

ANÁLISE DE IMPACTO NO NEGÓCIO:

Objetivo:

- Identificar os processos de negócios sensíveis ao tempo de indisponibilidade e os requisitos para recuperá-los em um prazo aceitável para a PMM de acordo com o nível de criticidade de cada um. Para tal, são identificados os eventos potenciais e os prováveis impactos, os processos afetados e os critérios que serão usados para quantificar e qualificar esses impactos.
- Esta atividade corresponde, basicamente, à realização de uma Análise de Impacto nos Negócios (AIN), também comumente conhecida como BIA (Business Impact Analisys), e utiliza os dados provenientes de análises de riscos realizadas anteriormente. É importante que representantes do negócio contribuam para a identificação dos impactos e prazos aceitáveis.

Responsável:

- Setor Responsável pela Segurança da Informação
- Diretoria de TI

Entradas:

- Análise de riscos realizadas

Descrição das Atividades:

- Avaliar impacto de indisponibilidade do serviço - De acordo com o nível do risco envolvido, deve-se avaliar qual o impacto (financeiro, operacional, imagem, etc) que a indisponibilidade do serviço traria.
- Determinar prazos - Com base no valor do impacto obtido, estabelecer os prazos de RTO (Recovery Time Objective) e RPO (Recovery Point Objective) para cada serviço crítico analisado.
- Documentar resultados - Elaborar relatório com os serviços críticos, seus prazos de recuperação e recursos mínimos necessários para recuperação de funções essenciais do serviço.
- Encaminhar relatório para a Comissão Gestora de TI.
- Caso a Comissão Gestora de TI não esteja de acordo com os dados contidos no relatório, refazer a análise e adequar.

- **Saídas:**
- Relatório de serviços críticos

DEFINIR ESTRATÉGIAS DE CONTINUIDADE DE NEGÓCIO:

Objetivo:

- Identificar, com base nas avaliações realizadas na atividade anterior, as estratégias de continuidade e de recuperação disponíveis para os serviços mais críticos. Tais estratégias norteiam as tarefas e procedimentos a serem executados na ocorrência de um desastre e a identificação dos recursos humanos, tecnológicos, financeiros, etc necessários para sua implementação.
- Nesta fase avaliam-se quais as possíveis ações adotadas para implementar a gestão de continuidade, levando-se em conta a viabilidade de adoção da solução técnica.

Responsável:

- Setor Responsável pela Segurança da Informação
- Comissão Gestora de TI

Entradas:

- Relatório de serviços críticos, aprovado pela comissão

Descrição das Atividades:

- Definir estratégia de continuidade - Para cada serviço crítico, avalia-se as possíveis ações para manter o serviço a um nível minimamente operável, de acordo com os prazos estabelecidos nas fases anteriores, a quantidade de recursos necessária, etc.

Saídas:

- Estratégia de continuidade para os serviços críticos

ELABORAR E REVISAR ESTRATÉGIAS DE ADMINISTRAÇÃO DE CRISE:

Objetivo:

- Elaboração de proposta de Estratégias de Administração de Crise com o objetivo de definir as atividades das equipes envolvidas e gerenciar as ações de contingência e comunicação durante e após a ocorrência de um desastre, com intuito de minimizar impactos, até a superação da crise.

  São objetivos específicos do PAC:
- Garantir a segurança à vida das pessoas;
- Minimizar transtornos sobre os desdobramentos do 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 e com esclarecimentos condizentes com o ocorrido.

Responsável:

- Diretoria de TI

Entradas:

- Modelos dos Planos

Descrição das Atividades:

- Área responsável coleta informações para identificar principais cenários de falha e sobre a forma de atuação em cada cenário de falha identificado;
- Área preenche os planos, descrevendo os procedimentos a serem executados para cada cenário de falha levantado.

Saídas:

- Estratégias de Administração de Crise

ELABORAR E REVISAR ESTRATÉGIAS DE CONTINUIDADE OPERACIONAL:

Objetivo:

- Elaboração de proposta de Estratégias de Continuidade Operacional com o objetivo de elencar as atividades e procedimentos necessários para garantir a operacionalidade da atividade/serviço a um nível mínimo aceitável frente aos cenários de falhas descritos.
- A área responsável preenche os planos, elencando as atividades necessárias para a manutenção de um mínimo de operacionalidade do serviço/atividade. São definidos/revisados os procedimentos, atividades e os responsáveis pela execução das atividades.

Responsável:

- Diretoria de TI

Entradas:

- Modelos dos Planos

Descrição das Atividades:

- Área responsável coleta informações para identificar principais cenários de falha e sobre a forma de atuação em cada cenário de falha identificado.
- Área preenche os planos, descrevendo os procedimentos a serem executados para cada cenário de falha levantado

Saídas:

- Estratégias de Continuidade Operacional

ELABORAR E REVISAR ESTRATÉGIAS DE RECUPERAÇÃO DE DESASTRES:

Objetivo:

- Elaboração de proposta de Estratégias de Recuperação de Desastres com o intuito de descrever as atividades e procedimentos necessários para retornar as operações dos serviços críticos à normalidade frente à ocorrência de eventos adversos.
- A área responsável preenche os planos, elencando as atividades necessárias para a manutenção de um mínimo de operacionalidade do serviço/atividade. São definidos/revisados os procedimentos, atividades e os responsáveis pela execução das atividades.

Responsável:

- Setor Responsável pela Segurança da Informação e outras áreas da TI

Entradas:

- Modelos dos Planos

Descrição das Atividades:

- A área responsável coleta informações para identificar os principais cenários de falha e sobre a forma de atuação em cada cenário identificado.
- A área preenche os planos, descrevendo os procedimentos a serem executados para cada cenário de falha levantado.

Saídas:

- Estratégias de Recuperação de Desastres

DEFINIR CRONOGRAMA DE ESTRATÉGIAS DE TESTES E VALIDAÇÃO:

Objetivo:

- Definir juntamente com as áreas técnicas quais planos serão testados bem como definição das datas em que os testes serão executados.
- Os testes têm como finalidade validar os planos elaborados, executando os procedimentos descritos, analisando se os passos estão corretos, se o tempo de execução está estimado corretamente e se o fluxo de atividades está corretamente ordenado, além de também servirem como entrada para a próxima revisão do plano. Novos planos deverão ser testados.

Responsável:

- Setor Responsável pela Segurança da Informação

Entradas:

- Estratégias de Continuidade Operacional, Estratégias de Recuperação de Desastres

Descrição das Atividades:

- Na definição dos testes deve ser avaliado o impacto nos serviços (se é aceitável a indisponibilidade, ainda que parcial, ou se devem ser realizados em um ambientes simulado ou de homologação, de forma a evitar a indisponibilidade), quais cenários serão testados, datas e respectivas aprovações.

Saídas:

- Estratégias de testes e validação que serão realizados

EXECUTAR E DOCUMENTAR TESTES:

Objetivo:

- As equipes técnicas executam os testes planejados. Os testes e os resultados são documentados para fins de análise crítica.
- O teste deve ser executado exatamente conforme descrito nos Planos, de forma a validar sua eficácia. Caso seja detectada a necessidade de alteração dos procedimentos descritos, isso deve ser documentado nos resultados dos testes, para que seja encaminhada para a revisão do respectivo plano.

Responsável:

- Setor Responsável pela Segurança da Informação

Entradas:

- Estratégias de Continuidade Operacional, Estratégias de Recuperação de Desastres.

Descrição das Atividades:

- Executar os testes agendados.
- Documentar o resultado

Saídas:

- Resultado dos testes

AVALIAR E ARMAZENAR OS RESULTADOS DOS TESTES:

Objetivo:

- Nesta atividade, os resultados obtidos nos testes são analisados criticamente para definição das ações necessárias e armazenados, para servirem como evidências de análise crítica do processo e da documentação.
- As evidências podem ser utilizadas para eventuais auditorias realizadas na PMM para demonstrar que os planos são efetivamente testados e validados, além de servirem como entrada para futura revisão dos planos.

Responsável:

- Setor Responsável pela Segurança da Informação

Entradas:

- Resultados dos testes.

Descrição das Atividades:

- Analisar criticamente os resultados obtidos.

Saídas:

- Relatório de testes

IDENTIFICAR E REGISTRAR OPORTUNIDADES DE MELHORIA:

Objetivo:

- Identificar e registrar oportunidades de melhoria tanto no que diz respeito ao processo de Gestão de Continuidade, quanto aos documentos em vigor, para serem implementadas no próximo ciclo.
- Para esta atividade devem ser analisados o resultado dos testes e da avaliação dos incidentes críticos.

Responsável:

- Setor Responsável pela Segurança da Informação
- Gestores

Entradas:

- Resultados dos testes, análise histórica de incidentes.

Descrição das Atividades:

- Identificar oportunidades de melhoria.

Saídas:

- Documento com oportunidades de melhoria

Anexo I- MODELO DE PLANO DE CONTINUIDADE DE NEGÓCIO PARA SERVIÇOS DE TIC

- **Justificativa e Objetivo**

Uma vez que falhas nos serviços de Tecnologia da Informação e Comunicação (TIC) impactam diretamente a continuidade da prestação da PMM 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.

- **Escopo**

O Plano de Continuidade de TIC abrange as estratégias necessárias à continuidade dos serviços de TIC essenciais: contingência, continuidade e recuperação. Está voltado a conceder continuidade aos processos definidos como críticos para a TI e serviços essenciais da [...].

Em decorrência da baixa maturidade da organização nos processos da Gestão da Continuidade de Negócios, da falta de comitês ou equipes multidisciplinares com a responsabilidade definidas para essa atividade, a não formalização de Metodologia de Análise de Riscos e Análise de Impacto nos Negócios, este plano tratará apenas do risco mais evidente da [...].

- **Área**

O PCTIC será administrado, avaliado e acionado no âmbito da Comissão de Tecnologia da Informação, tendo sua manutenção, organização e melhoria revistas e atualizadas anualmente pelo Comitê de Gestão de Tecnologia da Informação e Comunicação.

- **Principais Riscos**

O PCTIC foi desenvolvido para ser acionado quando da ocorrência de cenários de desastres que apresentam risco à continuidade dos serviços essenciais. O quadro abaixo define alguns riscos e suas causas:

EVENTO DE DESASTRE	POSSÍVEIS CAUSAS
Interrupção de energia elétrica	- Causada por fator externo à rede elétrica do prédio ou de sua localidade com duração da interrupção superior a 24 horas. - Causada por fator interno que comprometa a rede elétrica do prédio com curto-circuitos, incêndio e infiltrações. - Impossibilidade de acionar o Grupo gerador no

	momento de uma queda de energia
Indisponibilidade de Backup	- Cópia de segurança dos dados não disponíveis ou sem integridade
Indisponibilidade de rede/circuitos	- Rompimento de fibra óptica decorrente de execução obras públicas, desastres ou acidentes. - Mal funcionamento de switch gerenciador de segmento de rede - Interrupção dos serviços de conectividade com as operadoras de telecomunicação por mais de 12 horas
Ataque cibernético	- Ataque virtual que comprometa o desempenho, os dados ou a configuração dos serviços essenciais.

- **Papéis e Responsabilidades**

DEPARTAMENTO DA TECNOLOGIA DA INFORMAÇÃO:

- Avaliar o plano de Continuidade de Serviços Essenciais de forma periódica e decidir pelo seu acionamento quando da ocorrência de desastres, respondendo em nível institucional pela execução do plano e demais ocorrências relacionadas.
- Responsável por informar sobre a evolução das providências em andamento visando restaurar o serviço inoperante junto a servidores, autoridades e Assessoria de comunicação, que se encarregará de prestar informações à Mídia, se for o caso.
- Inclui autoridades em nível institucional e tomadores de decisão
- O Diretor administrará e manterá o Plano de Administração de Crise

EQUIPE DE CONECTIVIDADE:

- Avaliar os danos específicos de qualquer infraestrutura de rede no fornecimento de dados.
- Fornecer a infraestrutura de servidores físicos e virtuais necessária para a execução das operações e processos essenciais durante um desastre.
- Prover mecanismos de segurança no ambiente principal e alternativo.
- Monitoramento e Análise do datacenter
- Responsável pela infraestrutura que abriga os sistemas de TIC e pela garantia

que as estruturas alternativas (lógicas ou físicas) são mantidas adequadamente.

- Avaliar os danos e supervisionar a execução das estratégias de recuperação de desastres.
- Formular estratégia de recuperação de dados de acordo com as políticas pré-estabelecidas.
- O líder desta equipe administrará e manterá as estratégias de recuperação de desastres.

EQUIPE DE ENGENHARIA:

- Monitorar e recuperar as instalações elétricas do Datacenter: Estabilizadores, No-Breaks e Geradores;

- **Invocação do Plano**

O PCTIC 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 DTI em conjunto com a alta administração da PMM. O acionamento das demais equipes será realizado pelos integrantes da Equipe de Conectividade, de acordo com as características de cada ocorrência, havendo o registro do evento através de sistema de chamado onde serão consignadas as informações como data do incidente, descrição sucinta do ocorrido e quais as equipes acionadas.

Os integrantes das equipes, após acionados, iniciarão a avaliação e investigação do ocorrido, podendo acionar outras equipes caso necessário.

- **Árvore de Acionamento de Contatos**

Equipe de Conectividade

Nome do Servidor	Ramal	E-mail	Papel
Valdeir Aparecido de Almeida	949	sa.cpd@mairipora.sp.gov.br	Responsável

Equipe de Infrarede

Nome do Servidor	Ramal	E-mail	Papel
Alexandre Chimura sakemi	959	sa.cpdseguranca@mairipora.sp.gov.br	Responsável

- **Protocolo de Tratamento do PCTIC**

O protocolo de tratamento dos eventos definidos neste Plano de continuidade de Serviços Essenciais (PCTIC) é composto de fases ou macroprocessos que se encontram definidos e desmembrados em subplanos específicos para cada área de atuação, quando da ocorrência de um desastre. A sequência das atividades está representada abaixo, de forma genérica, a saber:

1) Identificação e declaração de desastres;

2). Comunicar o desastre a Chefia superior;

3) Ativação do processo de DR (disaster recovery);

4) Avaliação da corrente e prevenção de mais danos;

5) Ativação da solução de Contingência;

6). Estabelecer operações de TI;

7) Reparação e reconstrução da instalação principal;

8) Retorno das operações para o Ambiente principal.

As Estratégias do PCTIC juntamente com seus objetivos estão assim organizados:

- Estratégias de Administração de Crise:
  - Definição das atividades das equipes envolvidas e gerenciar as ações de contingência e comunicação durante e após a ocorrência de um desastre, com intuito de minimizar impactos, até a superação da crise.
- Estratégias de Continuidade Operacional:
  - Seu objetivo é garantir a continuidade dos serviços críticos de TIC na ocorrência de um desastre, enquanto recupera-se o ambiente principal. Essas estratégias são fortemente orientadas aos processos(sistemas) e serviços.
  - Cada Serviço Identificado como crítico pelo documento “Análise de Impacto no Negócio” terá suas Estratégias de Continuidade Operacional:

- Estratégias de Recuperação de Desastre:
  - Planejar e agir para que, uma vez controlada a contingência e passada a crise, a TI da PMM retome seus níveis originais de operação no ambiente principal.
  - Cada Serviço Identificado como crítico pelo documento “Análise de Impacto no Negócio” terá suas Estratégias de Recuperação de Desastres.
- Estratégias de Testes e Validação (PTV):
  - Um plano de Continuidade de Negócios só está apto a funcionar após ser testado e exercitado. Essas estratégias definem a periodicidade e tipos de teste que serão realizados.

- **Estratégias de Continuidade**

A estratégia de continuidade para o cenário atual de TIC e serviços essenciais está formulada em site alternativo do tipo “cold site”.

- Cold site – Site Redundância em Local diferente
  - Backup dos sistemas essenciais armazenados em local alternativo localizado no [...], realizado semanalmente, com poder computacional igual ao Datacenter principal.

As ações de contingência e recuperação são detalhadas nas estratégias a seguir.

Anexo II MODELO ESTRATÉGIAS DE ADMINISTRAÇÃO DE CRISES

Essas estratégias especificam 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.

- **Objetivo e Escopo**

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

São objetivos específicos das Estratégias de Administração de Crise:

- Garantir a segurança à vida das pessoas;
- Minimizar transtornos sobre os desdobramentos do 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 e com esclarecimentos condizentes com o ocorrido.

- **Execução das estratégias**

Na ocorrência de um desastre será necessário entrar em contato com todas as 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 setor.

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	Telefone	Data/Hora Registro
Corpo de Bombeiros	193	

SAMU	192	
Polícia Militar	190	
Defesa Civil	4419-0015	
Polícia Federal	(11) 3538-5000	

Tabela de Autoridades

Fornecedor	Contato	Data/Hora Registro
Idea Solutions	(11) 2122-2465	
ASA SEGURANCA	(11) 94003-2201	
USNET	(11) 3090-9327	

Tabela de Prestadores de Serviço de Energia Elétrica e Infraestrutura

Fornecedor	Contato	Data/Hora Registro
Elektro	08007010102	
TELEFONICA	08007751212	

Tabela de Prestadores de Serviço de Telecomunicações e Data Center

- **Comunicação após um Desastre**

Após reunião com líderes do PRD e PCO, 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.

- **Comunicação com os servidores**

A equipe de comunicação deverá prover um meio de contato específico para este fim, com intuito de que as unidades do órgão se mantenham informadas da ocorrência de um desastre e da inatividade dos serviços essenciais.

- **Comunicar colaboradores externos, cidadãos e mídia**

A equipe de comunicação, em consonância com a Comunicação do órgão, deverá fornecer informações pertinentes aos colaboradores externos: cidadãos e outros órgãos. Buscar publicar em meios oficiais e de ampla divulgação, com aval do comitê de continuidade e institucional, informações sobre o ocorrido.

- **Comunicar retorno das operações**

A equipe responsável pelo retorno deve emitir um parecer relatando as atividades

realizadas e comunicar a todas as partes acima supracitadas quando ocorrer o retorno das operações à normalidade.

Anexo III- MODELO ESTRATÉGIAS DE CONTINUIDADE OPERACIONAL

- **Estratégias de Continuidade Operacional**

As Estratégias de Continuidade Operacional descrevem os procedimentos de contingência em uma situação de falha ou interrupção nos ativos que sustentam esses processos.

Elas devem ser revisadas anualmente ou quando ocorrem mudanças significativas na organização, atualizado e gerenciado conjuntamente pelos líderes das equipes.

- **Aplicabilidade**

  É aplicável ao processo de negócio crítico: Funcionamento de um Sistema

- **Procedimentos**

Cenário:	**Indisponibilidade do ambiente físico / Indisponibilidade Total dos Equipamentos do Datacenter**
Área responsável pelo Plano:	Infrarede
Responsável Pelo Plano:	Alexandre Chimura Sakemi
Contato	(11)4604-0959
Objeto	Em caso de indisponibilidade do Datacenter Principal, a equipe de conectividade deverá ser realocada para o ambiente de contingência, com a finalidade de subir os serviços mínimos para o funcionamento dos sistemas.
CONTRAMEDIDAS/ PREMISSAS	
Contramedidas	**Premissas**
Contrato Vigente	O contrato com a empresa dos sistemas deve estar vigente e constar o serviço de gerenciamento de banco de dados e configuração de ambiente
Ambiente de Contingência:	Site Redundância
Prazo da Operação	até 24 horas
Posto de Comando	TI do Site Redundância
RESPONSÁVEIS PELA EXECUÇÃO	
Membros do Grupo	
Nome	Responsabilidade
Responsabilidades	
Antes do incidente	O Responsável pelo Plano deverá realizar um treinamento de parada de ambiente e locomoção até o ambiente de contingência com toda a equipe. Revisar e atualizar este Plano caso necessário.

Durante o incidente		O Responsável pela execução do Plano entrará em contato rapidamente com todos os gestores dos setores envolvidos e guiará a equipe para o data center de contingência
Após o Incidente		O responsável pela execução do Plano estará acompanhando os responsáveis dos setores envolvidos, realizará um relatório de ocorrência para conferir se todos os procedimentos foram realizados e deverá revisar e atualizar este Plano.
Fornecedores		
Nome		
Telefone		
Procedimento de Continuidade		
Procedimento	**001**	**Acionamento do responsável pelo PCO e transporte dos funcionários**
Responsável		Diretor TI
Tempo		Até 2 horas
Instruções		
1		O Diretor da TI acionará o responsável pelo PCO
2		O Diretor ligará para o setor de transporte com o objetivo de enviar os funcionários para o ambiente de contingência
3		O Diretor irá se encontrar com a equipe na sala do Site Redundância
Procedimento	**002**	
Responsável		Líder da Equipe de Conectividade
Tempo		Até 24 horas
1		Entrar em contato com o Fornecedor
2		Entrar em contato com o líder da equipe de sistemas para que o Banco de Dados de Contingência assuma o papel principal
3		Entrar em contato com o líder da equipe de infra para ligar e validar as máquinas virtuais de contingência.
4		Verificar a operabilidade do Sistema
5		Comunicar o responsável pela execução do Plano que o sistema está operacional
6		A equipe de conectividade começará a trabalhar no ambiente de contingência

Anexo IV – MODELO ESTRATÉGIAS DE RECUPERAÇÃO DE DESASTRES

- **Estratégias de Recuperação de Desastres**

Essas estratégias descrevem 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.

Elas devem ser revisadas anualmente ou quando ocorrem mudanças significativas na organização, atualizado e gerenciado pelos líderes das equipes.

- **Objetivo e Escopo**

É escopo deste plano garantir o retorno das operações da PMM no ambiente principal depois da ocorrência de uma crise ou cenário de desastre tratando-se apenas dos ativos, conexões e configurações deste ambiente.

São objetivos:

I. Avaliar danos aos ativos, serviços essenciais e conexões do datacenter, provendo meios para sua recuperação.

II. Evitar desdobramentos de outros incidentes na instalação principal.

III. Restabelecer o serviço/sistema essencial no DC principal, dentro do prazo tolerável

- **Regras e Procedimentos**

PREFEITURA MUNICIPAL DE MAIRIPORÃ

DEPARTAMENTO DE TECNOLOGIA DA INFORMAÇÃO

Cenário		Indisponibilidade de Equipamentos do Datacenter
Área responsável pelo Plano:		Conectividade
Responsável Pelo Plano:		Valdeir Aparecido De Almeida
Contato:		(11)4604-0949
Objetivo:		Em caso de Indisponibilidade de Equipamento do Datacenter Principal, a equipe de conectividade deverá identificar os ativos danificados e contatar os fornecedores para realizar a substituição ou reparo.
Ambiente de Contingência:		-----
Prazo da Operação		Até 8 horas
Posto de Comando		TI – Redes
CONTRAMEDIDAS/ PREMISSAS		
Contramedidas		**Premissas**
Contrato Vigente		O contrato de manutenção com substituição de Peças com o Fornecedor deve estar vigente
RESPONSÁVEIS PELA EXECUÇÃO		
Membros do Grupo		
Nome		**Responsabilidade**
Responsabilidades		
Antes do incidente		O Responsável pelo Plano deverá verificar se o contrato de manutenção está válido e de acordo com o RTO.
Durante o incidente		Verificar qual foi a falha no ativo de informação. Entrar em contato com o fornecedor para reparo/e ou
Após o Incidente		Analisar como foi a atuação do fornecedor durante o tratamento do incidente. Revisar o contrato com o fornecedor se necessário, aplicar multa caso não obedeça ao SLA.
Fornecedores		
Nome		
Telefone		
Procedimento de Continuidade		
Procedimento	**001**	**Reparo de Equipamento**
Responsável		Conectividade
Tempo		Até 6 horas
Instruções		
1		Um membro da equipe de conectividade irá verificar a falha do equipamento
2		Entrar em contato com o Fornecedor. O fornecedor tem 6h para sistemas críticos.

3	Em até 6 horas o fornecedor deve prover novo equipamento ou conserto
4	Após a instalação de um novo equipamento o Líder da Equipe de Conectividade deve comunicar o Diretor da TI que o sistema está operante e encerrar o incidente

Anexo V – MODELO DE ESTRATÉGIAS DE TESTES E VALIDAÇÃO

- **Validação e Teste do PCTIC**

Cumprindo o propósito de reavaliar os procedimentos planejados visando a melhoria contínua, o PCTIC será testado e validado em reunião entre os líderes de cada subplano anualmente 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.

A execução dos passos planejados deve ser registrada no sistema de chamados indicando Data de execução, Tipo do teste, descrição de motivo e Status, respeitando os seguintes critérios a serem informados no registro:

- **Tipos de testes a serem realizados:**

  - Teste de mesa

    Teste de complexidade simples, no qual é realizada uma análise (crítica ensaios de execução), dos procedimentos e informações descritas, com o objetivo de atualizar e(ou) validar os procedimentos e as informações contidas no plano;

  - Simulação no ambiente: Simular uma situação real de interrupção

    Teste de complexidade média no qual uma situação “artificial” é criada, por exemplo, é realizada a parada de um processo em horários diferentes das operações diárias (finais de semana, após expediente, etc.) sendo o resultado utilizado para validar se os planos possuem as informações necessárias e suficientes, de forma a permitir recuperação de determinado arranjo de contingência ou processo com sucesso.