Prefeitura Municipal da Estância Turística de Holambra

PCTI - PLANO DE CONTINUIDADE DE TECNOLOGIA DA INFORMAÇÃO

Versão 1.0

SUMÁRIO

1. INTRODUÇÃO

Atualmente, as atividades da Prefeitura Municipal da Estância Turística de Holambra (PMETH) estão intrinsecamente ligadas ao bem-estar da sociedade. Buscamos realizar uma gestão transparente de contratos voltados para a tecnologia da informação, priorizando as melhores ferramentas e recursos tecnológicos em conjunto com a segurança da informação. Com equipes comprometidas em proporcionar um trabalho eficaz na prestação de serviços e na adoção das melhores tecnologias disponíveis, o plano de continuidade dos serviços de TI torna-se um documento crucial.

Considerando que a interrupção nos serviços de Tecnologia da Informação (TI) afeta a continuidade na prestação de serviços públicos, gerando prejuízos operacionais e financeiros. Este plano de continuidade de TI visa oferecer medidas ágeis e eficazes para a proteção e recuperação de processos críticos relacionados aos sistemas essenciais em situações de incidentes ou desastres, buscando sempre a ação mais eficiente diante das adversidades.

2. TERMOS E ABREVIAÇÕES

Sigla/Termo	Significado
CD	Comissão de Desastres
DCTI	Departamento de Comunicação e Tecnologia da Informação
DTI	Divisão de Tecnologia da Informação
GLPI	*Gestion Libre de Parc Informatique*
HD	*Hard Disk*
PAC	Plano de Administração de Crise
PCO	Plano de Continuidade Operacional
PDTIC	Plano Diretor de Tecnologia da Informação e Comunicação
PMETH	Prefeitura Municipal de Estância Turística de Holambra
PRD	Plano de Recuperação de Desastre
RAID	*Redundant Array of Independent Drives*
RPO	*Recovery Point Objective*
RTO	*Recovery Time Objective*
TI	Tecnologia da Informação
TIC	Tecnologia da informação e Comunicação

VoIP	Voz sobre IP

Tabela 01: Termos e abreviações.

3. OBJETIVOS

No Plano de Continuidade de TI (PCTI), são delineadas as estratégias cruciais para a continuidade dos serviços de Tecnologia da Informação e Comunicação (TIC), envolvendo os aspectos de contingência, continuidade e recuperação. O objetivo é assegurar a continuidade dos processos identificados como críticos para a Tecnologia da Informação e Comunicação da PMETH, fortalecendo a resiliência diante de potenciais adversidades.

4. SERVIÇOS ESSENCIAIS

A tabela 02 demonstra os serviços considerados essenciais, por ordem prioritária, em caso de acionamento deste PCTI.

Serviço	Criticidade	RPO[1]	RTO[2]	Impacto			
				Financeiro	Legal	Imagem	Operacional
Link Dedicado de Internet	ALTA	4 DIAS	4 HORAS	INDEFINIDO	ALTA	ALTA	ALTA
DataCenter - Servidores	ALTA	4 DIAS	8 HORAS	INDEFINIDO	ALTA	ALTA	ALTA
Portal/Site Municipal	MÉDIA	4 DIAS	24 HORAS	INDEFINIDO	MÉDIA	MÉDIA	MÉDIA
Sistema de Gestão Financeira e Orçamentária	ALTA	3 DIAS	8 HORAS	INDEFINIDO	ALTA	ALTA	ALTA
Sistema de Gestão De Recursos Humanos	ALTA	3 DIAS	8 HORAS	INDEFINIDO	ALTA	ALTA	ALTA
Sistema de Gestão de Compras e Licitações	ALTA	3 DIAS	8 HORAS	INDEFINIDO	ALTA	ALTA	ALTA
Portal da Transparência	MÉDIA	4 DIAS	24 HORAS	INDEFINIDO	MÉDIA	MÉDIA	MÉDIA
Serviços Online	MÉDIA	4 DIAS	24 HORAS	INDEFINIDO	MÉDIA	MÉDIA	MÉDIA
Monitoramento de vias Públicas	ALTA	4 DIAS	8 HORAS	INDEFINIDO	ALTA	ALTA	ALTA
Monitoramento de prédios Públicos	MÉDIA	6 DIAS	24 HORAS	INDEFINIDO	MÉDIA	MÉDIA	MÉDIA
Sistema da Ouvidoria Municipal - eSIC	MÉDIA	4 DIAS	24 HORAS	INDEFINIDO	MÉDIA	MÉDIA	MÉDIA
E-mail Institucional	ALTA	3 DIAS	8 HORAS	INDEFINIDO	ALTA	ALTA	ALTA
Telefonia VoiP	ALTA	3 DIAS	8 HORAS	INDEFINIDO	ALTA	ALTA	ALTA
Soluções de impressão e	MÉDIA	6 DIAS	48 HORAS	INDEFINIDO	MÉDIA	MÉDIA	MÉDIA

digitalização							
Sistema de Gestão de Saúde	ALTA	3 DIAS	8 HORAS	INDEFINIDO	ALTA	ALTA	ALTA
Sistema de Gestão de Educação	ALTA	3 DIAS	8 HORAS	INDEFINIDO	ALTA	ALTA	ALTA
Diário Oficial	ALTA	2 DIAS	8 HORAS	INDEFINIDO	ALTA	ALTA	ALTA
Sistema de Controle Interno	MÉDIA	3 DIAS	8 HORAS	INDEFINIDO	MÉDIA	MÉDIA	MÉDIA

Tabela 02: Serviços essenciais.

[1]RPO - *Recovery Point Objective*: Método de gestão empregado na área de tecnologia da informação para calcular e/ou estimar a quantidade máxima de dados que uma organização estaria disposta a perder em situações de incidentes, sendo preferível que o limite calculado nunca seja alcançado.

[2]RTO - *Recovery Time Objective*: Este indicador guarda relação direta com o tempo máximo que o setor de tecnologia necessitará para restabelecer os serviços após uma parada crítica. Isso abrange considerações sobre o tempo de recuperação, testes, reparos, atualizações, e instalações, entre outros.

5. PRINCIPAIS RISCOS E AMEAÇAS

Este plano é ativado em casos de desastres que colocam em risco a continuidade dos serviços essenciais. Seguindo as normas ABNT NBR ISO 31000/2009 e ABNT NBR ISO 27005, foram identificadas as principais fontes de riscos e ameaças, juntamente com suas possíveis causas, conforme apresentado na Tabela 03.

Desastres / Riscos	Possíveis Causas / Fontes
Ataques Internos	Ataque aos recursos dos servidores
Ataques Cibernéticos	Ataque virtual a rede da PMETH que comprometa o desempenho, dados ou configuração dos serviços críticos.
Desastres Naturais	Terremotos, tempestades, alagamentos, rompimento de barragens, furacões , entre outros eventos naturais
Defeito de Hardware	Falha que exige substituição de peça, reparo ou aquisição sujeita a processo licitatório ou orçamentos.

Falha Humana	Acidentes durante o manuseio de equipamentos e erros em configurações, incluindo situações críticas que representam riscos à saúde, como falhas em circuitos elétricos, manipulação inadequada de processamento de dados, servidores e serviços de missão crítica.
Falha na climatização da sala dos Servidores	Aquecimento excessivo dos ativos devido a falha do ar condicionado
Incêndio	Incêndios que afetem parcial ou totalmente a continuidade dos serviços de Tecnologia da Informação do município.
Interrupção no fornecimento de energia elétrica	Elementos externos à rede elétrica da prefeitura ou à sua localização, como rompimento de cabos de interconexão, com uma duração que ultrapasse 12 horas. Ou originada por fatores internos que comprometem a rede elétrica do prédio, como curto-circuito, infiltrações ou incêndio.

Tabela 03: Desastres/Riscos.

6. PAPÉIS E RESPONSABILIDADES

6.1 Comissão de Desastres

Realiza avaliações periódicas dos planos e toma decisões para sua ativação em situações de emergência, sendo responsável a nível institucional pela elaboração de estratégias de implementação e coordenação de eventos correlatos. Em casos de desastres, serão realizadas comunicações abrangentes dirigidas aos servidores, munícipes, autoridades, fornecedores e, quando necessário, à mídia.

O líder da equipe será encarregado de gerenciar e atualizar o Plano de Administração de Crises (PAC). A Comissão será constituída pelos mesmos membros que compõem a Divisão de Tecnologia da Informação – DTI, além do Diretor de Comunicação e Tecnologia da Informação.

6.2 Equipe de TI

A divisão de tecnologia da informação (DTI) desempenha um papel crucial na gestão das instalações físicas que abrigam os sistemas de TIC, garantindo a adequada manutenção das instalações alternativas. Seu escopo inclui a avaliação de danos, supervisão de reparos e a avaliação específica de danos em qualquer infraestrutura

de rede. Além disso, fornecerá dados e conectividade de rede, abrangendo WAN, LAN e infraestrutura externa em colaboração com os prestadores de serviço.

A responsabilidade da DTI também se estende à garantia da infraestrutura de servidores físicos e virtuais, essenciais para a continuidade das operações de TIC durante desastres. A DTI garantirá o funcionamento adequado de aplicações essenciais, assegurando que atendam aos objetivos de negócios durante e após um desastre.

A divisão de TI será fundamental na validação do desempenho das aplicações essenciais e fornecerá ferramentas necessárias para os funcionários desempenharem suas funções de maneira rápida e eficiente.

Por fim, a divisão de TI analisará perdas, mapeará a quantidade de dados perdidos e o tempo de recuperação, formulando estratégias de recuperação de dados em conformidade com as políticas pré-estabelecidas.

7. INVOCAÇÃO DO PLANO

O Plano de Continuidade de Tecnologia da Informação (PCTI) será ativado diante da ocorrência de qualquer cenário de desastre, insurgência, identificação de um risco desconhecido ou se uma vulnerabilidade apresentar uma elevada probabilidade de exploração. Além disso, o plano pode ser acionado para situações de teste ou por determinação do Departamento de Comunicação e Tecnologia da Informação (DCTI).

Contatos:

- Divisão de Tecnologia da Informação:
    - Telefone: (19) 3802-8000 – Ramal: 210
    - E-mail: ti@holambra.sp.gov.br

8. MACROPROCESSOS

O PCTI tem macroprocessos conforme a figura 01, divididos em planos específicos para cada área, em caso de desastre.

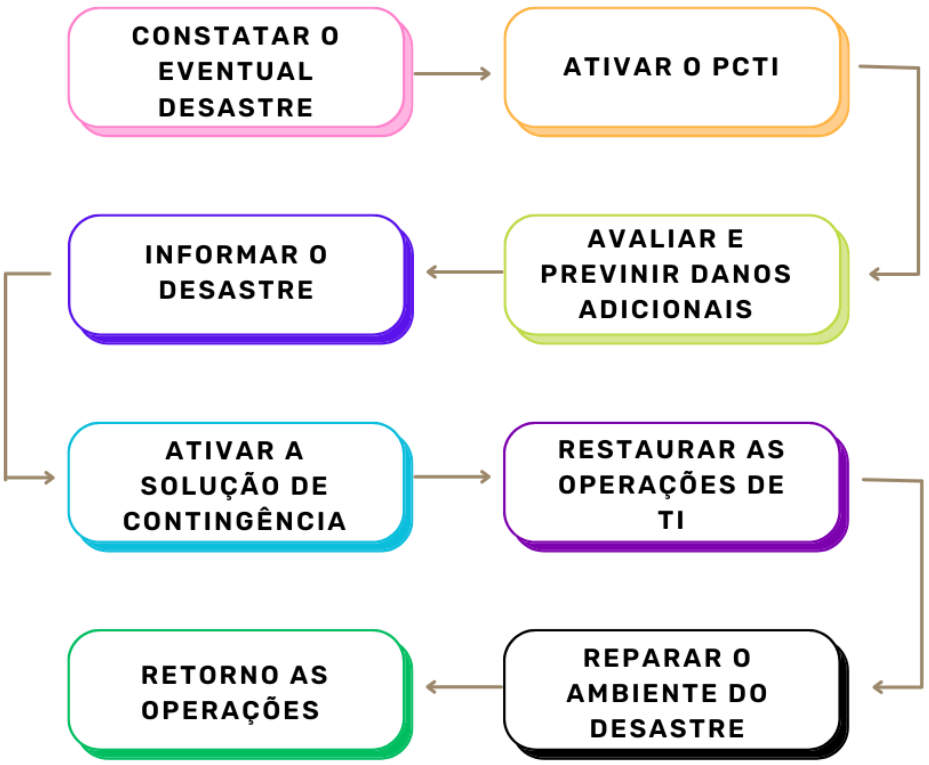

Figura 01: Plano de Continuidade

Além dos macroprocessos descritos, o PCTI também se fragmenta em subplanos que abrangem:

8.1 Plano de Continuidade Operacional (PCO):

Assegurar a continuidade dos serviços críticos de TI durante um desastre, enquanto restaura-se o ambiente principal.

8.2 Plano de Administração de Crise (PAC):

Definir as atividades das equipes e coordenar ações de contingência e comunicação durante e após um desastre, visando minimizar impactos até a recuperação total.

8.3 Plano de Recuperação de Desastre (PRD):

Planejar e implementar ações para que, após controlar a contingência e superar a crise, a STI retome suas operações normais no ambiente principal.

9. ESTRATÉGIAS DE CONTINUIDADE

A abordagem de continuidade para o atual cenário de TIC e serviços críticos é delineada da seguinte maneira:

9.1 Backup

As medidas tomadas em relação aos backups foram estabelecidas de acordo com a política de backup do Município. No entanto, atualmente, a divisão de tecnologia da informação não dispõe de uma estrutura dedicada ao armazenamento externo. É importante observar que a implementação do armazenamento em nuvem, está no planejamento, inclusive é uma das metas do Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC). A necessidade de realizar backups remotamente é essencial para garantir a continuidade dos serviços em caso de desastre nas instalações ou no datacenter da PMETH.

9.2 Redundâncias

A redundância está diretamente associada aos links de internet e aos servidores físicos e/ou em nuvem, garantindo a continuidade do serviço em caso de falha. A inclusão de um segundo link de internet para redundância está planejada como parte das metas do PDTIC.

Os servidores utilizam a técnica de armazenamento denominada RAID (Redundant Array of Independent Drives) de espelhamento, que emprega um conjunto de HD (disco rígido) para aumentar a proteção dos dados. Essa abordagem cria um subsistema de armazenamento a partir de diversos discos individuais, tratando-os como uma única unidade para o sistema operacional. Os dados são replicados em vários discos do sistema, assegurando cópias idênticas dos arquivos originais. Em caso de falha em um HD, o outro mantém os dados, garantindo a integridade do sistema e dos dados.

Adicionalmente, os servidores apresentam redundância em suas fontes de alimentação, ambas conectadas a um único *nobreak*. O cenário planejado consiste em adquirir um segundo *nobreak*, permitindo que cada fonte seja conectada individualmente a um *nobreak* distinto. Isso proporcionará uma redundância mais eficaz em casos de falha em alguma fonte ou *nobreak*.

Outro elemento crucial de redundância é a presença de um segundo sistema de ar condicionado na sala dos servidores. Isso permite o uso do segundo sistema em caso de defeito ou necessidade de manutenção do primeiro, garantindo um ambiente estável para os servidores.

9.3 Ações de contingência e recuperação

Identificar a perda de informações e ativos, restaurar a estrutura afetada e, uma vez que o ambiente principal esteja em funcionamento, realizar a recuperação dos dados a partir dos backups.

10. PCO – PLANO DE CONTINUIDADE OPERACIONAL

Este plano apresenta os cenários de inoperância e os procedimentos alternativos planejados, destacando as atividades prioritárias que visam assegurar a continuidade dos serviços essenciais.

10.1 Objetivo e escopo

O principal propósito é assegurar a continuidade das ações durante e após a ocorrência de uma crise ou desastre, concentrando-se exclusivamente nas estratégias de contingência previamente delineadas. Os objetivos do Plano de Continuidade Operacional (PCO) compreendem:

- Implementar medidas para preservar o funcionamento dos serviços essenciais e garantir a continuidade das operações, especialmente nos sistemas fundamentais.
- Estabelecer procedimentos, controles e diretrizes alternativas que possibilitem a manutenção das operações ao longo de uma crise ou cenário de desastre.

10.2 Execução do plano

- Avaliação de impacto de desastre: diante da identificação de um incidente ou crise, é incumbência do responsável examinar a magnitude do impacto, a extensão e possíveis consequências do ocorrido.
- Início do plano dado: após a aprovação da Comissão de Desastres para a ativação do plano, a equipe convocará uma reunião de emergência com o objetivo de coordenar prazos e ações de contingência. Nesse contexto, serão

informadas às partes envolvidas as ações de contingência, priorizando os serviços críticos e essenciais.

Devem ser adotadas as medidas de contingência e continuidade, ilustradas na tabela 04, para cada processo ou serviço essencial. Após a restauração dos sistemas essenciais e a confirmação da estabilização dos servidores, deverá ser elaborado um relatório descrevendo as atividades executadas neste Plano de Continuidade Operacional (PCO) e preenchendo a tabela 04.

Instrução	Duração	Observação	Resultado
Avaliar o status da aplicação de backup e estimar o impacto da perda de dados (janela de backup).			
Identificar as rotinas de backup que foram afetadas pelos dados em questão			
Estimar o volume de dados a ser recuperado, o tempo de recuperação dos dados e possíveis perdas operacionais			
Verificar o retorno do funcionamento dos servidores			
Realizar teste de aplicação de backup após desastre.			
Validar a eficácia das políticas de backup implementadas.			

Tabela 04: Medidas de contingência e continuidade.

11. PAC – PLANO DE ADMINISTRAÇÃO DE CRISE

O plano estabelece diretrizes a serem seguidas em caso de um cenário de desastre. Essas diretrizes abrangem a gestão, administração, mitigação ou interrupção dos efeitos relacionados à interação entre os agentes envolvidos e/ou afetados, por meio de ações coordenadas e comunicação eficiente, até superar a crise.

11.1 Objetivos

O propósito do programa é assegurar a comunicação contínua entre todas as partes antes, durante e após um desastre, gerenciando a crise e promovendo uma compreensão clara das ações a serem tomadas.

- Garantir a segurança das vidas das pessoas.
- Minimizar os transtornos decorrentes de incidentes e promover esforços conjuntos para superar a crise.
- Orientar servidores e colaboradores por meio de informações e procedimentos de conduta.
- Informar a população de forma oportuna, fornecendo esclarecimentos adequados ao ocorrido.

11.2 Execução do plano

Efetuar a comunicação em situações de desastre requer a interação com diversas áreas, especialmente as impactadas, com o intuito de informá-las sobre os efeitos na continuidade dos serviços e o tempo de recuperação. O Conselho de Desastres (CD) assume a responsabilidade de contatar essas repartições e compartilhar informações pertinentes a cada grupo, setor ou segmento. O processo de comunicação com cada parte seguirá o seguinte protocolo:

- **Comunicar às autoridades**

A principal responsabilidade da CD será garantir que as autoridades competentes sejam prontamente informadas sobre a catástrofe, especialmente se envolver riscos para as pessoas. Isso incluirá o fornecimento de informações precisas sobre a localização, natureza, magnitude e impacto do desastre. Os telefone emergenciais estão contidos na tabela 05, que deverá ser preenchida com os dados solicitados em caso de desastre.

Autoridade	Telefone	Data e Hora do registro	Número da ocorrência
Bombeiros	(19) 3802-7983		
Guarda Civil Municipal	(19) 3802-7980		
Polícia Militar	190		
SAMU	192		

Tabela 05: Telefones emergenciais.

- **Comunicação pós-desastre**

Após uma reunião a CD, desenvolverá um programa conciso para contatar as partes afetadas. O objetivo é informar e transmitir a todos a visão dos esforços necessários para restabelecer os serviços inativos.

- **Comunicação com servidores e terceirizados**

A Comissão de Desastres (CD) deverá disponibilizar um canal de contato específico com o objetivo de manter todos os Departamentos da PMETH informados sobre a ocorrência de um desastre e a inatividade dos serviços essenciais de TI. Deve-se explorar diversas estratégias de comunicação, como telefonemas (fixos ou celulares), plataformas de redes sociais, divulgações oficiais, ou qualquer outra tática a ser determinada de acordo com as circunstâncias.

- **Comunicação com as repartições públicas**

Entrar em contato diretamente com as repartições impactadas pelo desastre e fornecer informações de contato. Deve-se comunicar a natureza, o impacto e a extensão do desastre, bem como as ações de contingência em andamento

- **Comunicação da normalização das operações de TI**

Deverá informar a todas as partes mencionadas anteriormente assim que as operações retornarem à normalidade.

- **Finalização do PAC**

Com o retorno dos sistemas essenciais e estabilidade do sistema afetado, a CD deverá elaborar um relatório com a relação das atividades necessárias após a ocorrência do desastre, como remanejamento dos canais de informação, abertura e acompanhamento de chamados correlatos ao ocorrido.

12. PRD – PLANO DE RECUPERAÇÃO DE DESASTRES

O plano estabelece os cenários de inabilidade e os procedimentos planejados correspondentes, especificando as atividades prioritárias para restaurar o nível de operação dos serviços no ambiente afetado, dentro de um prazo aceitável.

12.1 Objetivos

O objetivo deste plano é assegurar que os servidores e demais ativos de rede voltem a operar após uma conjuntura de desastre. Outros objetivos do PRD:

- Avaliar os prejuízos nos ativos e conexões do datacenter e propor métodos de recuperação.
- Impedir que outros incidentes se desencadeiem na instalação principal.
- Restaurar a operação normal do datacenter em um período considerado aceitável.

12.2 Execução do plano

- **Listar dispositivos danificados**

A equipe da divisão de Tecnologia da Informação (DTI) tem a responsabilidade de reconhecer e elaborar uma lista de todos os ativos prejudicados durante a ocorrência do evento catastrófico.

- **Identificar acessos interrompidos**

A DTI deverá identificar e relatar as interrupções nas conexões e acessos decorrentes do desastre, especificando se afetam a rede local, WAN ou envolvem o provedor de serviços.

- **Identificar os serviços descontinuados**

A equipe da DTI deverá mapear os serviços descontinuados, incluindo detalhes sobre a perda de ativos e interrupções de conexão. Este relatório deve abranger os elementos essenciais para a total operacionalidade da aplicação, como servidores, máquinas virtuais (VM), banco de dados, firewall, armazenamento, roteadores e *switches*, incluindo configurações pertinentes, como proxy, DNS, rotas, VLANs, entre outros.

- **Elaboração do cronograma de recuperação**

Após mapear perdas e impactos, a equipe da DTI desenvolverá um cronograma de recuperação para as aplicações, considerando a priorização dos serviços essenciais

ou a determinação de nível institucional, os RTOs estabelecidos para cada serviço e a disponibilidade da força de trabalho.

- **Substituição de ativos**

No evento de perda de ativos, é imperativo comunicar imediatamente ao Comitê de Direção (CD) a necessidade de adquirir os ativos irrecuperáveis. Deve-se avaliar o impacto do tempo de aquisição no RTO de cada serviço, buscando possíveis soluções alternativas, dentro da legalidade, durante o processo de aquisição. Para ativos danificados, é essencial analisar as coberturas contratuais e garantias disponíveis.

- **Reconfiguração de ativos**

A equipe deve assegurar o pleno funcionamento das configurações dos ativos reparados ou substituídos. Se não estiverem operacionais, é necessário fornecer um cronograma estimado para a configuração desses ativos.

- **Ambiente de testes**

A DTI deverá estabelecer um ambiente de testes de recuperação para garantir a total restauração das aplicações/serviços afetados pelo incidente ou desastre. Esses testes devem abranger a verificação de se os níveis de capacidade e disponibilidade dos serviços retornam ao estado anterior ao desastre.

- **Recuperação dos dados do backup**

Realizar a recuperação dos dados para as aplicações impactadas, validando as configurações e funcionalidades dos sistemas. A confirmação pode ocorrer por meio de testes automatizados de monitoramento dos serviços ou pela equipe de TI.

- **Encerramento do PRD**

Após a conclusão do procedimento de recuperação, as informações serão reunidas em um relatório específico, detalhando o horário de restabelecimento de cada serviço, os equipamentos adquiridos, os procedimentos de recuperação executados e os fornecedores acionados.

13. DOCUMENTO DE VALIDAÇÃO DE TESTE

A equipe da Divisão de Tecnologia da Informação conduzirá testes e validações bienais no Plano de Continuidade de Serviços de TIC. Qualquer incorporação de novos fatores de risco ou a inclusão de um serviço adicional no plano também desencadeará revisões e ajustes necessários.

Sendo executados testes de:

- O teste de mesa: procedimento de natureza simples, envolvendo uma análise crítica e ensaios de execução dos procedimentos e informações delineadas no plano. Este processo tem como finalidade a atualização e validação dos procedimentos e informações contidas no PCTI.
- Simulação de paralisação: teste de complexidade média no qual é criada uma situação "artificial", como a interrupção de um processo em horários distintos das operações diárias (finais de semana, após o expediente, etc.). O resultado é utilizado para validar se os planos contêm informações necessárias e suficientes, permitindo a recuperação bem-sucedida de um arranjo de contingência específica.

A tabela 06 deverá ser preenchida, caso algum teste seja realizado.

Data	[1]Espécie	Motivo	[2]Status

Tabela 06: Testes.

[1] Espécie: Se o teste foi um teste de mesa, ou uma simulação de paralisação.
[2] Status: A situação do teste, se está programado ou executado.

VERSÃO 1.0 – DEZEMBRO DE 2023