Plano de Continuidade de Serviços de TI - TRE-MA

Sumário

Controle de Versões 1
1. Objetivo e Escopo 1
2. Serviços Essenciais 2
3. Sistemas Estratégicos 2
4. Principais Ameaças 3
5. Papéis e Responsabilidades 4
6. Invocação do Plano 5
7. Processo e subprocessos 6
8. Estratégias de Continuidade 7
9. Plano de Continuidade dos Serviços de TIC 7
10. Teste e manutenções 11
11. Avaliação de Riscos e Plano de Respostas à Incidentes 12
12. Revisão de plano e realização de testes 12
ANEXO I 13

Controle de Versões

Versão	Data	Autor	Notas da Revisão
0.1	**16/03/2022**	**Wellington Moraes**	Versão Inicial.
0.2	**24/06/2022**	**Wellington Moraes**	Revisão.

1. Objetivo e Escopo

O Plano de Continuidade de Serviços de TI estabelece estratégias e planos gerais de ação para garantir a continuidade e a disponibilidade dos serviços essenciais e sistemas estratégicos do TRE-MA quando na ocorrência de falhas, incidentes graves ou desastres (Resolução CNJ Nº 370/2021, Art. 36).

2. Serviços Essenciais

Os serviços elencados na **Tabela 1** são considerados essenciais para o acionamento e execução deste plano, conforme Portaria TRE-MA 1055/2021.

Serviço	Responsável
BANCO DE DADOS	SEDIN
LINK DE DADOS - TRE/TSE	SERED
LINK DE DADOS - TRE/ZONAS	SERED
LINK DE DADOS - TRE/INTERNET	SERED

3. Sistemas Estratégicos

Os sistemas elencados na **Tabela 2** são considerados estratégicos para o acionamento e execução deste plano, conforme Portaria TRE-MA 1055/2021.

Sistema	Responsável
BANCO DE DADOS	SEDIN
CORREIO	SERED
DJE	SESJU
ELO	COUSE
PJE	SESJU
SEI	SEDIN
SERVIDOR INTRANET	WEB
SERVIDOR INTERNET	WEB
SGRH	SEDIN

4. Principais Ameaças

Este plano deve ser acionado quando da ocorrência de crise ou parada de serviços essenciais ou sistemas estratégicos. A **Tabela 3** elenca os principais eventos para o acionamento e execução deste plano.

EVENTO	POSSÍVEIS CAUSAS
Interrupção de energia Elétrica	- Fator externo à rede elétrica do prédio ou da localidade com duração da interrupção superior a 12 horas. - 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.
Falha na Climatização da sala cofre	- Falha/Defeito nos equipamentos de climatização. - Superaquecimento dos ativos do Data Center.
Indisponibilidade de links de comunicação	- Rompimento de fibra ótica decorrente da execução de obras públicas, manutenção, desastres, roubo, vandalismo ou acidentes. - Interrupção dos serviços de conectividade com as operadoras de telecomunicação. - Falha de switch gerenciador de segmento de rede.
Indisponibilidade de Backup	- Cópia de segurança dos dados não disponível ou sem integridade.
Falha humana	- Acidente ao manusear equipamentos críticos. - Erro na execução de comandos.
Incêndio	- Incêndios que comprometam os serviços de TIC.
Desastres Naturais	- Terremotos, tempestades, alagamentos e etc.
Falha de hardware	- Falha que necessite reposição de peça ou reparo, cujo reparo ou aquisição dependa de processo Licitatório.
Vulnerabilidades de software	- Falha na aplicação de patches de segurança - Software obsoleto sem atualizações do fabricante
Ataque cibernético	- Ataque virtual que comprometa o desempenho, os dados ou configuração dos serviços essenciais.

5. Papéis e Responsabilidades

Para mitigar ou solucionar potenciais problemas com os serviços essenciais e sistemas estratégicos são necessários procedimentos, que preliminarmente precisam estar associados a papéis e responsáveis indicados.

Comitê de Crises Cibernéticas:

Responde em nível institucional pelo acionamento e monitoramento da execução do plano e demais ocorrências relacionadas. 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.

Equipe de Tratamento e Resposta a Incidentes:

Receber, analisar, classificar, tratar e responder às notificações e atividades relacionadas a incidentes de segurança em redes de computadores (Portaria TRE-MA Nº. 738/2017).

Equipe de Segurança Cibernética:

Conduzir a elaboração e manter atualizado o Plano de Gestão de Continuidade de Serviços, no que se refere à TIC (Resolução TRE-MA 9.882/2021).

Equipe de Infraestrutura:

Fornecer a infraestrutura de servidor físico e virtuais necessária para que a TI execute suas operações e processos essenciais durante um desastre.

Equipe de Redes:

Avaliar os danos específicos de qualquer infraestrutura de rede e fornecer dados e conectividade de rede, incluindo WAN, LAN ou de infraestrutura externa junto aos prestadores de serviço.

Equipe de Aplicações / Sistemas:

Garantir que os sistemas estratégicos funcionem como exigido para atender aos objetivos de negócios em caso de e durante um desastre.

Equipe de Backup:

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

Equipe de Instalações Elétricas:

Responsável por avaliar danos e monitorar continuamente o nível de serviço quanto a instalações elétricas, nobreaks e geradores em situações de desastre.

6. Invocação do Plano

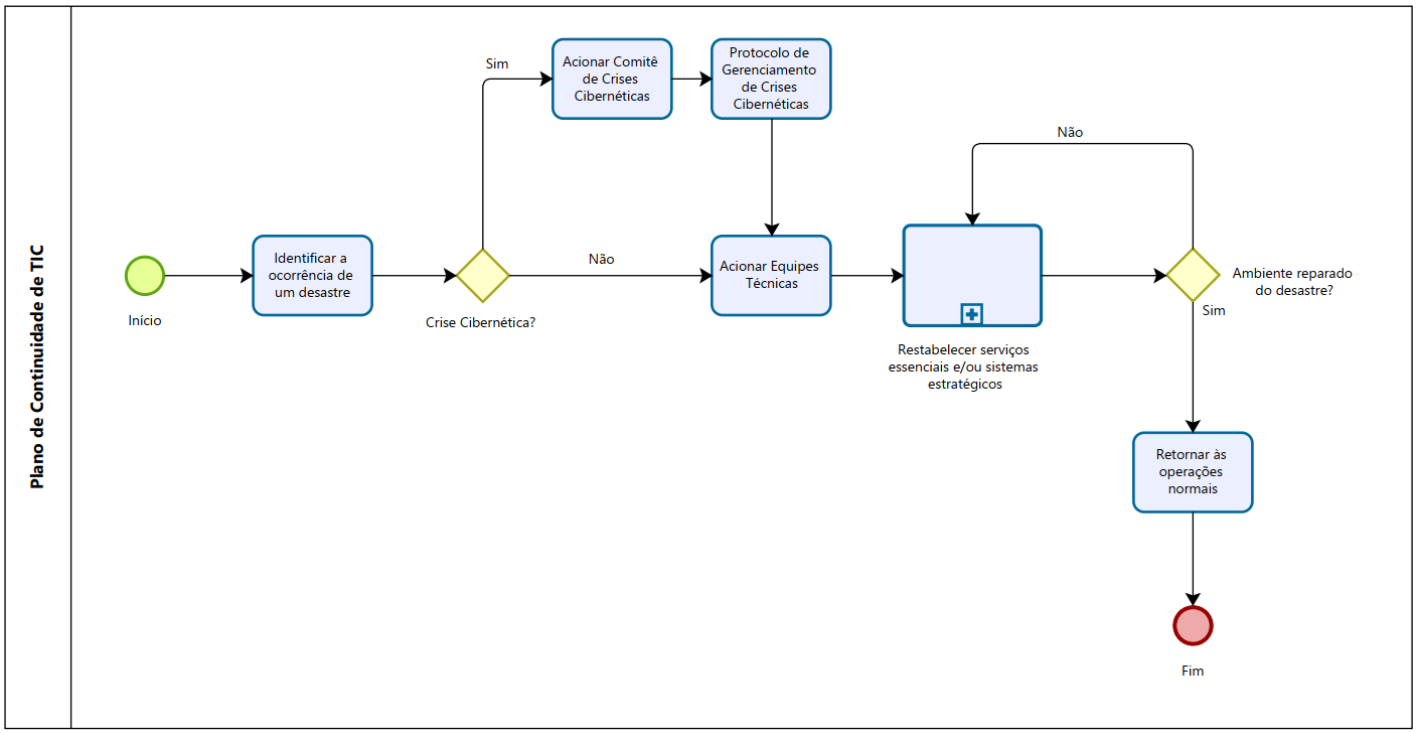
Este plano será acionado quando da ocorrência de algum dos cenários de desastres, a insurgência ou ocorrência de um risco desconhecido ou caso uma vulnerabilidade tenha grande possibilidade de ser explorada. O plano também poderá ser invocado em casos de testes ou por determinação do Comitê de Crises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

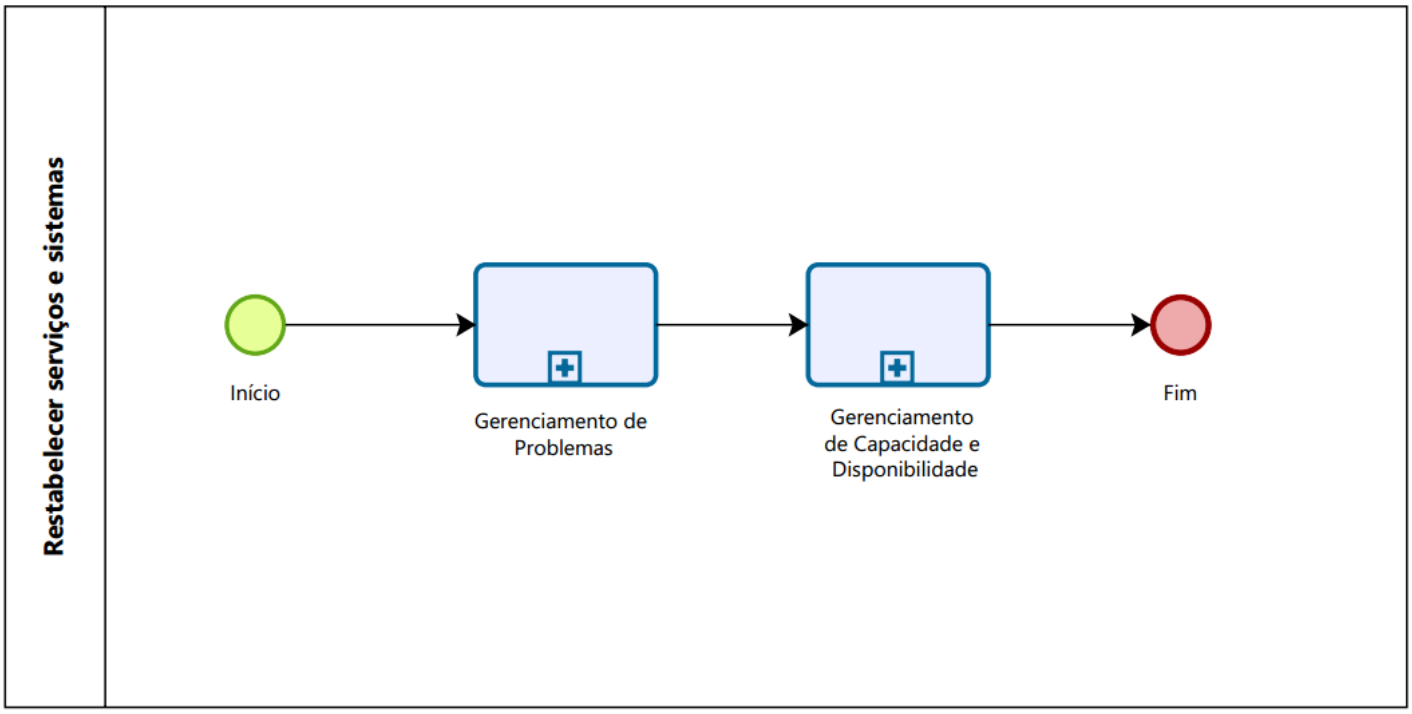
Os integrantes da Equipe de Tratamento e Resposta a Incidentes serão responsáveis por acionar os contatos e partes interessadas, prioritariamente por telefone, ou pessoalmente caso seja possível.

LISTA DE ACIONAMENTO DE CONTATOS

EQUIPE	RESPONSÁVEL	TELEFONE	CONTATO
Aplicações / Sistemas	Chefe SEDIN	2107-8877	sedin@tre-ma.jus.br
Backup	Chefe SERED	2107-8799	sered@tre-ma.jus.br
ETIR	Secretário TI	2107-8751	gabstic@tre-ma.jus.br
Infraestrutura	Chefe SERED	2107-8799	sered@tre-ma.jus.br
Redes	Chefe SERED	2107-8799	sered@tre-ma.jus.br
Segurança Cibernética	Chefe SESEC	2107-8986	sesec@tre-ma.jus.br
Instalações Elétricas	Chefe SEMAP	2107-8968	semap@tre-ma.jus.br

7. Processo e subprocessos





8. Estratégias de Continuidade

A estratégia de continuidade para o cenário atual dos serviços essenciais e sistemas estratégicos está estabelecida da seguinte forma:

Tipo: *Warm site* - mantém uma infraestrutura mínima/reduzida em relação ao site primário, ao qual há constante atualização das informações para este site reduzido ou é idealizado para rapidamente serem restaurados os backups do site principal.

Cópias de backup dos sistemas essenciais armazenadas em local alternativo: atualmente o TRE-MA possui estrutura redundante ativo-passivo contemplando os serviços de armazenamento (storage) e processamento (blade).

Backups em fita, disco e nuvem: de acordo com a Política de Backup.

9. Plano de Continuidade dos Serviços de TIC

São apresentados a seguir os planos de continuidade para cada serviço essencial e sistema estratégico, definindo as ações prioritárias para cada cenário de inoperância identificado.

9.1 Medidas primárias associadas aos eventos de interrupção

EVENTO	Ações primárias
Interrupção de energia Elétrica	- Providenciar atendimento para pessoas em situações de risco (elevadores, próximos a curtos-circuitos, etc.). - Monitorar o acionamento do grupo gerador. - Desligamento controlado de servidores de rede e estações de trabalho em caso de insuficiência de fornecimento de energia auxiliar pelo grupo gerador ou por nobreaks. - Contato com a distribuidora local de energia. - Suporte e orientação às unidades e Zonas Eleitorais quanto à operação de sistemas informatizados e o acesso (ou abandono) de ambientes nas condições do desastre. - Se causa interna (curto-circuito, etc.): a) providenciar a segurança do local. b) acionar as empresas contratadas para a manutenção respectiva. c) acompanhar as ações corretivas específicas. - Atualizar Administração sobre expectativa de tempo de retorno à normalidade.

Falha na Climatização da sala cofre	- Verificação e manutenção corretiva dos ativos de TI associados à situação. - Acionamento da prestadora do serviço. - Acompanhamento das ações corretivas específicas. - Atualizar Administração sobre expectativa de tempo de retorno à normalidade.
Indisponibilidade de links de comunicação	- Ativação de conexão auxiliar, quando disponível, priorizando o tráfego relacionado aos serviços essenciais previstos neste Plano. - Verificação e manutenção corretiva dos ativos de TI associados à situação. - Acionamento da prestadora do serviço. - Acompanhamento das ações corretivas específicas. - Atualizar Administração sobre expectativa de tempo de retorno à normalidade.
Indisponibilidade de Backup	- Restaurar e manter cópias em locais alternativos (nuvem, fita ou disco).
Falha humana	- Restaurar serviço afetado. - Restaurar backups. - Mapear necessidade de capacitações/treinamento.
Incêndio	- Providenciar atendimento para pessoas em situações de risco; - Acionar alarmes, equipes médicas, corpo de bombeiros e brigadas de incêndio. - Acionar sistemas de combate a incêndio.
Desastres Naturais	- Providenciar atendimento para pessoas em situações de risco; - Acionar equipes médicas e corpo de bombeiros; - Ativar serviços de TI no site backup.
Falha de hardware	- Acionamento da prestadora do serviço de suporte. - Verificar presença de equipamento alternativo que possa suceder ou substituir o equipamento danificado. - Verificar possibilidade de hospedar em servidor de virtualização (quando adequado) instância que substitua os serviços prestados pelo equipamento danificado. - Instalar sistema substituto, recuperando os dados do sistema original (ou do backup mais recente). - Acionar o CGTIC para dar início à análise sobre aquisição emergencial de equipamento ou serviço.

Vulnerabilidades de software	- Migrar software para novo servidor. - Providenciar, adquirir ou desenvolver substituto para o sistema obsoleto. - Isolar o sistema obsoleto em ambiente apropriado com restrições elevadas.
Ataque cibernético	- Analisar necessidade de suspender conexões entre redes locais, outras redes da Justiça Eleitoral e a Internet. - Analisar necessidade de restringir ou suspender acesso de usuários a recursos da rede do TRE-MA. - Mapear e desativar ou corrigir vulnerabilidades. - Desconectar da rede os sistemas afetados, substituindo-os se necessário e possível, de forma a não comprometer os serviços essenciais a serem mantidos por este Plano.

9.2 Procedimentos Gerais de Retomada

De modo geral, as atividades de contingência/recuperação são as seguintes:

a. Identificar ativos afetados;
b. Estimar impacto de perda de dados;
c. Mapear ativos a serem recuperados;
d. Estimar tempo de recuperação e possíveis perdas operacionais;
e. Executar procedimentos de recuperação;
f. Testar procedimentos realizados;
g. Validar recuperação;
h. Enviar comunicado de retorno das atividades à instituição;

Banco de Dados

Cenário	Responsável	Ação Preventiva	Ação Corretiva
Data Center Indisponível	SERED	Monitoramento	Manutenção Corretiva
Banco de Dados Indisponível	SEDIN	Monitoramento	Manutenção Corretiva

Link de Internet

Cenário	Responsável	Ação Preventiva	Ação Corretiva
Data Center Indisponível	SERED	Monitoramento	Manutenção Corretiva
Linha de Dados Indisponível	SERED	Monitoramento / Link Backup	Chamado: Operadora

Link de Intranet

Cenário	Responsável	Ação Preventiva	Ação Corretiva
Data Center Indisponível	SERED	Monitoramento	Manutenção Corretiva

Linha de Dados com o TSE Indisponível	SERED	Monitoramento / Link Backup	Chamado: TSE
Linha de Dados com as Zonas Indisponível	SERED	Monitoramento / Link Backup	Chamado: Operadora

Servidor de Intranet

Cenário	Responsável	Ação Preventiva	Ação Corretiva
Data Center Indisponível	SERED	Monitoramento	Manutenção Corretiva
Servidor de Intranet Indisponível	WEB	Monitoramento	Manutenção Corretiva

Sistema Eletrônico de Informações (SEI)

Cenário	Responsável	Ação Preventiva	Ação Corretiva
Data Center Indisponível	SERED	Monitoramento	Manutenção Corretiva
Aplicação Indisponível	SEDIN	Monitoramento	Manutenção Corretiva
Banco de Dados Indisponível	SEDIN	Monitoramento	Manutenção Corretiva

Correio Eletrônico

Cenário	Responsável	Ação Preventiva	Ação Corretiva
Data Center Indisponível	SERED	Monitoramento	Manutenção Corretiva
Aplicação Indisponível	SERED	Monitoramento	Manutenção Corretiva
Linha de Dados com o TSE Indisponível	SERED	Monitoramento	Chamado: TSE

Processo Judicial Eletrônico (PJE)

Cenário	Responsável	Ação Preventiva	Ação Corretiva
Aplicação Indisponível	TSE	Monitoramento	Chamado: TSE

Diário de Justiça Eletrônico (DJE)

Cenário	Responsável	Ação Preventiva	Ação Corretiva
Aplicação Indisponível	TSE	Monitoramento	Chamado: TSE

ELO

Cenário	Responsável	Ação Preventiva	Ação Corretiva
Linha de Dados com o TSE Indisponível	SERED	Monitoramento / Link Backup	Chamado: TSE
Linha de Dados com as Zonas Indisponível	SERED	Monitoramento / Link Backup	Chamado: Operadora
Aplicação Indisponível	TSE	Monitoramento	Chamado: TSE

SGRH

Cenário	Responsável	Ação Preventiva	Ação Corretiva
Aplicação Indisponível	SESUM	Monitoramento	Manutenção Corretiva
Banco de Dados Indisponível	SEDIN	Monitoramento	Manutenção Corretiva

9.12 Encerramento do Plano de Continuidade Operacional

O plano será encerrado assim que o funcionamento de serviços essenciais e/ou sistemas estratégicos estiverem restabelecidos e o Data Center estável. A equipe responsável pelo retorno deve emitir um parecer, relatando as atividades realizadas, para então fornecer os dados necessários para um comunicado de retorno das atividades à instituição.

10. Teste e manutenções

Cada unidade responsável deverá elaborar e publicar internamente plano de testes anual ou semestral do ano anterior à sua realização, seguindo a tabela de periodicidade abaixo.

Para cada um dos testes abaixo, cria-se uma condição de falha e mitigação. Durante cada teste todos os sistemas críticos devem ter seu funcionamento aferido.

Após cada teste, deve ser produzido e publicado um relatório com as ações realizadas, resultados obtidos e oportunidades de melhoria. Os planos de contingência devem ser revistos no caso de alguma falha nos testes.

Cenário	Teste	Periodicidade	Responsável
Link de internet	Testes de desempenho e de acionamento da redundância	Anual	SERED
Banco de Dados	Testes de restauração de cópia de segurança (parcial e total)	Semestral	SEDIN
Backup Fita	Testes de restauração de cópia de segurança (total)	Semestral	SERED
Backup Disco	Testes de restauração de cópia de segurança (total)	Semestral	SERED
Backup Nuvem	Testes de restauração de cópia de segurança (total)	Semestral	SERED

11. Avaliação de Riscos e Plano de Respostas à Incidentes

A avaliação de riscos de incidentes cibernéticos deverá ser feita pelo proprietário do ativo, com base no inventário de ativos que suportam os serviços e sistemas críticos, e ser revista a cada 6 meses, conforme previsto nas normas de gestão de riscos corporativa e de gestão de ativos, assim como, deverá ser elaborado plano de respostas à cada risco encontrado contendo os procedimentos de resposta específico, conforme modelo no anexo I.

Deverá ser elaborado relatório com as lições aprendidas e encaminhado para o Comitê de Crises Cibernéticas para que seja feita análise criteriosa conforme Protocolo de Gerenciamento de Crises Cibernéticas do poder Judiciário (PGCRC-PJ).

12. Revisão de plano e realização de testes

O Plano de Continuidade deverá ser revisado anualmente e testada a sua validação a cada 6 meses.

ANEXO I

Modelo de Plano de Resposta a Incidentes