Poder Judiciário

Tribunal de Justiça da Paraíba

Diretoria de Tecnologia da Informação

Plano de Continuidade de TI

DITEC

TRIBUNAL DE JUSTIÇA DA PARAÍBA

SUMÁRIO

1 APRESENTAÇÃO

Uma vez que falhas nos serviços de TIC impactam diretamente a continuidade da prestação da justiça, 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 da Análise de Impacto nos Negócios e Análise de Riscos.

2 ESCOPO

O Plano de Continuidade de TI (PCTI) 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 TIC do TJPB e serviços essenciais judiciais.

3 SERVIÇOS ESSENCIAIS

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

Serviço	**Criticidade**[1]	**RPO**[4]	**RTO**[3]	**Impacto**[2]			
				Financeiro	**Legal**	**Imagem**	**Operacional**
PJE 1G	Alta	Backup mais recente	1 dia	Indefinido	Alto	Alto	Alto
PJE 2G	Alta	Backup mais recente	1 dia	Indefinido	Alto	Alto	Alto
Custas Online	Alta	Backup mais recente	1 dia	Indefinido	Alto	Alto	Alto
PJE CGJ	Média	Backup mais recente	2 dias	Indefinido	Medio	Alto	Alto
Sistemas STI	Média	Backup mais recente	2 dias	Indefinido	Baixo	Alto	Alto

DigitalizaPJE	Média	Backup mais recente	2 dias	Indefinido	Baixo	Baixo	Baixo
Diário da Justiça Eletrônico	Baixa	Backup mais recente	3 dias	Indefinido	Medio	Baixo	Baixo
Consulta Processual Online	Baixa	Backup mais recente	3 dias	Indefinido	Baixo	Médio	Médio
CEMAN-e	Baixa	Backup mais recente	3 dias	Indefinido	Baixo	Baixo	Baixo
ADM Eletrônico	Alta	Backup mais recente	1 dia	Indefinido	Medio	Alto	Alto
Central de Compras - SGC	Alta	Backup mais recente	1 dia	Indefinido	Medio	Medio	Medio
Portal do TJPB / Intranet	Alta	Backup mais recente	1 dia	Indefinido	Alto	Médio	Médio
Selo Digital	Alta	Backup mais recente	1 dia	Indefinido	Alto	Alto	Alto
Recursos Humanos	Alta	Backup mais recente	1 dia	Indefinido	Baixo	Alto	Alto
RGP Frequência	Média	Backup mais recente	2 dias	Indefinido	Baixo	Baixo	Baixo
OTRS DIADM	Baixa	Backup mais recente	3 dias	Indefinido	Baixo	Medio	Medio
OTRS DITEC	Baixa	Backup mais recente	3 dias	Indefinido	Medio	Alto	Alto
Malote Digital	Baixa	Backup mais recente	3 dias	Indefinido	Medio	Baixo	Medio
WebCartório	Baixa	Backup mais recente	3 dias	Indefinido	Alto	baixo	Medio

Active Directory	Alta	Backup mais recente	1 dia	Indefinido	Baixo	Baixo	Alto
Barramento de Serviços	Alta	Backup mais recente	1 dia	Indefinido	Alto	Alto	Alto
TJSEG / CAS	Alta	Backup mais recente	1 dia	Indefinido	Baixo	Baixo	Alto
Links de Internet	Alta	Backup mais recente	1 dia	Indefinido	Alto	Alto	Alto
E-mail institucional / Webmail	Media	Backup mais recente	2 dias	Indefinido	Medio	Baixo	Alto
VPN	Baixa	Backup mais recente	3 dias	Indefinido	Baixo	Baixo	Baixo

1 (A)lto, (M)édio, (B)aixo, (I)ndefinido.
2 (A)lto, (M)édio, (B)aixo, (I)ndefinido.
3 Período de tempo dentro do qual os níveis mínimos dos serviços e/ou sistemas devem ser recuperados após a ocorrência de uma interrupção.
4 Ponto em uma linha de tempo em que os dados devem ser recuperados após a ocorrência de uma ruptura.

4 PRINCIPAIS AMEAÇAS

Este plano deve ser acionado quando da ocorrência de cenários de desastres 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	Superaquecimento dos ativos devido a falha no

sala cofre	dimensionamento de carga na sala cofre.
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 PAPEIS E RESPONSABILIDADES

COMITÊ DE DESASTRE/RECUPERAÇÃO/COMUNICAÇÃO (CDR):

Avaliar o plano periodicamente e decidir pelo seu acionamento quando da 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 DITEC.

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 CGTI.**

EQUIPE DE INSTALAÇÕES/AMBIENTE:

Responsável pelas instalações físicas que abrigam sistemas de TIC e pela garantia que as instalações de alternativa são mantidas adequadamente. Avalia os danos e supervisiona os reparos.

- O líder desta equipe administrará e manterá o **Plano de Recuperação de Desastre.**

EQUIPE DE REDES:

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

EQUIPE DE INFRAESTRUTURA/APLICAÇÕES:

Fornecer a infraestrutura de servidor físico e virtuais necessária para que a TI execute suas operações e processos essenciais durante um desastre.
Garantir que as aplicações essenciais funcionem como exigido para atender aos objetivos de negócios em caso de e durante um desastre. Eles serão os principais responsáveis por assegurar e validar o desempenho das aplicações essenciais e podem ajudar outras equipes de TIC CDR conforme necessário.

EQUIPE DE OPERAÇÕES:

Fornecer aos funcionários as ferramentas de que necessitam para desempenhar suas funções da forma mais rápida e eficiente possível. Eles precisarão provisionar todos os funcionários do TJPB na solução de contingência e aqueles que trabalham remotamente com as ferramentas específicas à sua atuação.

- O líder desta equipe administrará e manterá o **Plano de Continuidade Operacional.**

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 pré-estabelecidas.

EQUIPE DE SEGURANÇA DA INFORMAÇÃO:

Prover mecanismos de segurança no ambiente principal e alternativo. Resguardar aplicações e dados, evitando que desdobramentos de segurança afetem o acionamento da continuidade, cuja proteção estará contida na política de segurança.

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 CDR em conjunto com a alta administração do TJPB.

Os integrantes da COMITÊ RDC 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	SETOR
INFRAESTRUTURA	Líder da equipe de infraestrutura - GESUP	3216-1644	gesup@tjpb.jus.br	GESUP
REDES	Líder da quipe de redes - GESUP	3216-1644	gesup@tjpb.jus.br	GESUP
INFRA/APLICAÇÔES	Líder da equipe de Aplicações - GESUP	3216-1644	gesup@tjpb.jus.br	GESUP
SEGURANÇA DA INFORMAÇÃO	Líder da equipe de SI - Governança	3216-1644	joao.matos@tjpb.jus.br	GESUP
OPERAÇÕES	Gerente de suporte - GESUP	3216-1644	gesup@tjpb.jus.br	GESUP
BACKUP	Líder da equipe de infraestrutura - GESUP	3216-1644	gesup@tjpb.jus.br	GESUP
VALIDAÇÃO AMBIENTE	Gerentes de Sitema e Desenvolvimento - GESIS/GEDES		gesis@tjpb.jus.br/gedes@tjpb.jus.br	GESIS/ GEDES

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 desastres, 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 TIC retome seus níveis originais de operação no ambiente principal.

8 ESTRATÉGIAS DE CONTINUIDADE

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

TIPO : *Warm site*[1]

DESCRIÇÃO:

Cópias de backup dos sistemas essenciais armazenadas em local alternativo:

Atualmente o TJPB não possui nenhuma estrutura preparada para armazenamento externo, porém está no planejamento de contratações a salvaguarda em nuvem, assim como iniciou-se estudos para solução de armazenamento mínimo em um dos fóruns da capital. A necessidade de um site backup remoto é crucial para que seja aplicável a continuidade dos serviços em caso de desastre no prédio ou datacenter do TJPB.

Opções em estudo

- Fórum de mangabeira ou corregedoria
  - Colocação de storage antigo, porém funcional para armazenamento remoto dos backups mais recentes dos serviços essenciais to TJPB. O risco é considerado alto devido a falta de estrutura física, mas seria o mínimo para uma recuperação em caso de desastre.
  - Não possui qualquer tipo de hardware configurado no local.
  - Não dispõe de conexão redundante
  - Downtime alto.
- Nuvem
  - Objetivo é viabilizar o armazenamento externo em local com infra-estrutura de datacenter. A GESUP iniciou as tratativas para ver a viabilidade desse serviço.
  - Pode-se evoluir para um *Hot Site* como estratégia de contratação.

AÇÕES DE CONTINGÊNCIA/RECUPERAÇÃO:

- Mapear perda de dados e ativos, restabelecer toda a estrutura afetada e, após o ambiente principal estar operacional, prover a recuperação dos dados em backups.

OBSERVAÇÕES:

- As ações de contingência e recuperação são detalhadas nos subplanos a seguir.

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.

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:

- 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 a continuidade das operações de TI durante uma crise ou cenário de desastre.
- Estabelecer uma equipe para cada plano PCO, PRD e PAC
- Definir os formulários, checklists e relatórios a serem entregues pelas equipes ao executar a contingência.

GESTÃO

A GESUP é a unidade responsável 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 e 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.

Acionamento do plano

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

- Coordenar prazos e orquestrar as ações de contingência.
- Informar as equipes ações de contingência com a priorização dos serviços essenciais.

Contingência de Warm Site

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 jobs 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 validado o funcionamento do 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, inerente 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

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

São objetivos específicos do PAC:

- Garantir a segurança à vida das pessoas;
- Minimizar transtornos sobre os desdobramentos de 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 DO PLANO

Comunicação na ocorrência de um Desastre

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*		

- **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 funcionários**

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

Números de contatos a serem disponibilizados:

Telefone: (83) :
Contatos de E-mail:
Central de Serviços (service desk):

*Caso não haja conectividade ou linha telefônica disponível, ceder essas informações por meio de publicações, ou outra estratégia definida no momento.

Comunicar unidades e setores do tjpb

Acionar diretamente às unidade afetadas pelo desastre e fornecer contato. Informar a natureza, o impacto e a abrangência da catástrofe, como também as ações de contingência em andamento.

Comunicar colaboradores externos, cidadãos e mídia

A equipe de comunicação, em consonância com a Comunicação do TJPB, deverá fornecer informações pertinentes aos colabores externos: Advogados, 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

Comunicar a todas as partes acima supracitadas quando ocorrer o retorno das operações à normalidade.

ENCERRAMENTO DO PAC

Uma vez validado o funcionamento do retorno dos sistemas essenciais e estabilidade do datacenter a EQUIPE DE COMUNICAÇÃO entrará em contato com as partes descritas neste plano provendo 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

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.

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.

São objetivos PRD:

- 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

EXECUÇÃO DO PLANO

- **Identificar ativos danificados**

As equipes de INSTALAÇÃO/BACKUP/SERVIDORES/REDE deverão identificar e listar todos os ativos danificados da ocorrência do desastre.

- **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.

- **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 DE DR. 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.

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

- **Substituição de ativos e equipamentos**

Em caso de perda de ativos, deverá ser imediatamente informado ao comitê de DR a necessidade de aquisição 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 INSTALAÇÕES deve 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.

- **Reconfiguração de ativos e equipamento**

A equipe de **INSTALAÇÕES** deverá verificar que as configurações dos ativos reparados ou substituídos estão em funcionamento pleno. Caso não estejam, prover cronograma estimado para configurar estes ativos informando à **EQUIPE DE COMUNICAÇÃO** e **CDR**.

- **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;

- **Recuperar dados do backup**

Proceder a recuperação dos dados para as aplicações, seja do storage ou fitas de backup.

◦ Validar as configurações e funcionalidades dos sistemas:

▪ A validação pode ser realizada pelos testes automatizados de monitoramento dos serviços

▪ Por equipe designada pela equipe de configuração dos sistemas (GESIS)

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.

12 DOCUMENTO DE VALIDAÇÃO E TESTE

O PCTIC será testado e validado em reunião entre os líderes de cada subplano 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 *1	Motivo	Status *2

*1 Teste de mesa; Caminho percorrido;Simulação
*2 Programado;Executado;Planejado;Agendado

APROVAÇÃO DO PCTIC

A versão ____ do PCTIC fica aprovada em ____ /____/____ por deliberação das partes envolvidas.

Diretoria de Tecnologia e Comunicação

Gerência de Suporte

Assessoria Especial da Presidência