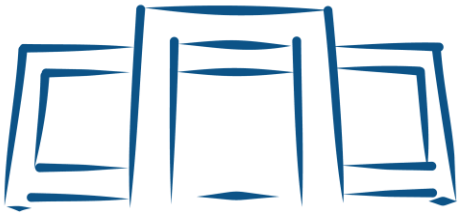


Plano de Continuidade de Serviços Essenciais de Tecnologia da Informação e Comunicação

PCSE-TIC

TRIBUNAL DE JUSTIÇA DO ESTADO DE RORAIMA
2024

Código:	001
Versão:	3.0
Data:	20/05/2024
Local:	Secretaria de Tecnologia da Informação
Organização:	Tribunal de Justiça do Estado de Roraima
Criado por:	Tatiana Brasil Brandão
Aprovado por:	Comissão de Gestão de TIC
Aprovado por:	Comitê de Governança de TIC
Nível de confidencialidade	Restrito

TRIBUNAL DE JUSTIÇA DO ESTADO DE RORAIMA

(Composição)

Des. Jésus Rodrigues do Nascimento
Presidente

Des. Ricardo de Aguiar Oliveira
Vice- Presidente

Esdras Silva Pinto
Juiz Auxiliar da Presidência

Des. Mozarildo Monteiro Cavalcanti
Corregedor – Geral de Justiça

Des. Erick Cavalcanti Linhares Lima
Ouvidor – Geral de Justiça

Des. Cristóvão José Suter Correia da Silva
Diretor da Escola do Poder Judiciário de Roraima

Membros

Des. Mauro José do Nascimento Campello
Des. Almiro José Mello Padilha
Desa. Tânia Maria Brandão Vasconcelos
Desa. Elaine Cristina Bianchi
Des. Leonardo Pache de Faria Cupello

SECRETARIA DE TECNOLOGIA DA INFORMAÇÃO

Secretário de Tecnologia da Informação

Tiago Mendonça Lobo

Secretário Adjunto

Gabriel Vieira

Subsecretários

Allef Weyller Batista Esbell

Boniek Amurim de Souza

Felippi Tuan da Silva Figueiredo

Paulo Adriano Brito Oliveira

Paulo Richard Perdiz Itapirema

Targino Carvalho Peixoto

Chefes de Setor

Amanda Cavalcante Sanguanini

Carlos Vinicius da Silva Souza

Cinara da Conceição Araújo

George Wilson Lima Rodrigues

Henrique Acquati Negreiros

Jádila Costa Cotrim

Marco Aurélio Carvalho Feitosa

Marlon Daniel Brands

Histórico de versões

Versão	Descrição	Responsável	Data
0.1	Minuta	Francisco das Chagas Braga, Boniek Amurim de Souza	18/10/2019
0.2	Revisão	Lilian Tajujá Rocha	15/11/2019
0.3	Aprovação	CGesTIC	19/11/2019
1.0	Aprovação	CGTIC	24/01/2020
2.0	Minuta	Tatiana Brasil Brandão	20/10/2021
2.0	Aprovação	CGTIC	10/11/2021
3.0	Revisão	Tatiana Brasil Brandão	15/05/2024
3.0	Aprovação	CGesTIC	

Definições

RPO	Objetivo do Ponto de Recuperação (*Recovery Point Objective*), representa o volume de dados perdidos em casos de falha nos serviços.
RTO	Objetivo de Tempo de Recuperação (*Recovery Time Objective*), período de tempo necessário para a realização de todas as tarefas necessárias para o restabelecimento dos serviços.
Stakeholders	É qualquer indivíduo ou organização que, de alguma forma, é impactado pelas ações de uma determinada organização.
Risco	Efeito da incerteza nos objetivos.
Resiliência	Capacidade de o Tribunal resistir aos efeitos de um incidente.
Ameaça	Causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização.
Vulnerabilidade	Fragilidade de um ativo que pode ser explorada por um ou mais ameaças.
Incidente	Qualquer evento que seja considerado suficientemente significativo para ser considerado um desastre e que possa causar uma interrupção.
Interrupção	Evento, previsível ou não, que cause um desvio negativo na entrega de produtos ou execução de serviços.
Continuidade	Capacidade de planejar e responder a incidentes em interrupções de negócios, objetivando manter os serviços em níveis aceitáveis.
Conformidade	Cumprimento de um requisito.
Correção	Ação para eliminar uma não conformidade detectada.
Evento	Ocorrência ou mudança em um conjunto específico de circunstâncias.

Documentos de Referência

ABNT NBR ISO/IEC 22301	Segurança da sociedade - Sistema de gestão de continuidade de negócios - Requisitos
Resolução CNJ n. 370/2021	Institui a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD).

Siglas

CGTIC	Comitê de Governança de Tecnologia da Informação e Comunicação
CGesTIC	Comissão de Gestão de Tecnologia da Informação e Comunicação
TIC	Tecnologia da Informação e Comunicação
PDTIC	Plano Diretor de Tecnologia da Informação e Comunicação
PETIC	Planejamento Estratégico de Tecnologia da Informação e Comunicação
ENTIC-JUD	Estratégia Nacional de TIC do Poder Judiciário
STI	Secretaria de Tecnologia da Informação
SUBPTIC	Subsecretaria de Projetos de TIC
TJRR	Tribunal de Justiça do Estado de Roraima
ISO	International Organization for Standardization
GCN	Gestão de Continuidade de Negócios
UPS	Uninterruptible Power Supply
CNJ	Conselho Nacional de Justiça
BIA	Business Impact Analysis
ITIL	Information Technology Infrastructure Library

Sumário

1. Apresentação

O presente documento foi desenvolvido de forma a proporcionar uma visão holística do funcionamento dos serviços oferecidos na área de Tecnologia da Informação do Tribunal de Justiça do Estado de Roraima, dentre eles infraestrutura, sistemas e suporte, bem como correlacionar seus respectivos níveis de imprescindibilidade.

Busca-se assim apresentar um manual prático que sirva de norte para tomadas de decisões em casos de eventos que tenham o condão de interromper serviços aqui conceituados como essenciais para o Tribunal, pois de nada valeria uma Justiça célere e atuante se estivesse indisponível ao jurisdicionado, sem previsibilidade de retomada dos seus serviços estruturantes.

Ao final espera-se clarear o entendimento daquilo que é serviço de TI essencial ao Tribunal, qual a autonomia do TJRR em casos de eventuais falhas em seus sistemas e/ou instalações, quais são as ações a serem realizadas para manter o Tribunal funcionando em caso de interrupção, quais serviços devem ser prioritariamente restabelecidos e sobre quem cabe a responsabilidade de iniciar o protocolo de recuperação de desastre.

2. Objetivo

O Plano de Continuidade de Serviços Essenciais de Tecnologia da Informação e Comunicação, denominado PCSE-TIC, tem por objetivo definir ações, estratégias e responsabilidades que visem manter, recuperar e assegurar o mínimo de impacto no negócio além de garantir a continuidade das atividades desenvolvidas pelo Tribunal de Justiça do Estado de Roraima (TJRR), em casos de eventuais interrupções não programadas, envolvendo recursos inerentes à área de Tecnologia da Informação (infraestrutura, sistemas e recursos humanos).

Para o atingimento da proposta, este PCSE-TIC fundamenta-se em quatro pilares: definição e identificação dos serviços essenciais, elaboração de diretrizes que minimizem a probabilidade de ocorrência de interrupções dos serviços, orientações que busquem garantir a capacidade de restabelecimento tempestivos dos serviços e atribuição de papéis e responsabilidades.

Definir ações e atividades referentes à continuidade dos serviços essenciais de tecnologia da informação e comunicações (TIC) do TJRR. Estas ações e atividades são as estratégias de continuidade definidas para que em caso de incidentes que causem uma interrupção dos serviços essenciais de TIC para TJRR e em consequência a indisponibilidade dos processos e atividades do negócio,

estes serviços essenciais de TIC sejam recuperados em ambiente alternativo e seja garantido ao Tribunal um nível de continuidade de seus processos de forma previamente acordado.

Neste documento é apresentado o cenário atual de tecnologia de continuidade do TJRR e o cenário futuro em termos de estratégias de continuidade. São descritos aqui também a delimitação do incidente de interrupção, as ameaças que podem causar incidentes, bem como os recursos necessários para a continuidade, além dos tempos de recuperação e ponto da informação, ação, necessários para uma correta continuidade dos serviços de TIC.

Também são definidas neste documento as atribuições de cada equipe especializada em cada tipo de serviços essenciais, bem como a recuperação destes serviços em caso de interrupção.

3. Justificativa

Um incidente de interrupção é um evento ou fato negativo que se concretizado por uma ameaça, tem como consequência a interrupção dos serviços essenciais de TIC e com isso, gerar um impacto inaceitável para o TJRR. Seu impacto se faz sentir de forma imediata e há necessidade de acionamento de alternativas de continuidade para que os serviços essenciais de TIC do TJRR estejam disponibilizados em um nível previamente acordado.

Uma vez que falhas nos serviços de TIC impactam diretamente na continuidade da prestação jurisdicional no âmbito da Justiça de Roraima, almeja-se com este plano prover medidas de proteção rápidas e eficazes para os processos críticos de TIC, relacionados aos sistemas essenciais em casos de incidentes graves ou desastres.

4. Escopo

Considerada como instrumento de boas práticas e presente nos melhores frameworks de gerenciamento de serviços de Tecnologia da Informação, o Plano de Continuidade de Serviços Essenciais de TI encontra embasamento na necessidade de atendimento regulatório, seguindo recomendação constante no art.21, da Resolução n. 370/2021.

Idealizado para ser utilizado no âmbito de serviços de TI, o presente planejamento poderá ser parte integrante do Plano de Continuidade do Negócio do Tribunal de Justiça, eis que não fazem parte do escopo desta documentação as

ações voltadas para outras áreas e demais serviços essenciais para o correto e regular funcionamento do TJRR.

5. Área

O PCSE-TIC será executado no âmbito da Secretaria de Tecnologia da Informação. Cabe ainda à STI propor atualizações visando melhorias e/ou adequação à realidade do Tribunal de Justiça.

O Comitê de Gestão de Tecnologia da Informação e Comunicação (CGSTIC) será responsável pelas diretrizes do PCSE-TIC, incluídas na deliberação acerca de organização, melhoria revistas e atualizadas anualmente.

6. Serviços Essenciais de TIC

Os serviços de TIC essenciais pelo Tribunal de Justiça são aqueles considerados críticos e que se interrompidos poderão causar impacto inaceitável para o TJRR, órgãos parceiros e sociedade. Após procedimento de análise de impacto em cada uma das subáreas de TI chegou-se a seguinte ativos:

Segmento	Ativos
Conectividade	Links de comunicação entre os prédios e órgãos parceiros. Links de acesso à Internet principal e redundante (Provedores de internet), Firewalls, DNS, DHCP.
Hardwares	Servidores, storages, switches core, switches de distribuição, switches de acesso, roteadores, switches gerenciáveis, nobreaks;
Softwares	Serviços baseados em servidores de aplicação, banco de dados, controladores de domínio e compartilhamento de arquivos
Sistemas	Projudi, Scriba, SEI, ERP-Thema

- **Conectividade** - os links de comunicação entre os prédios do TJRR transportam, compartilham informações e serviços do judiciário de forma interna e externamente aos servidores, magistrados e ao público em geral. Os links de internet são disponibilizados através de contratos com empresas terceirizadas (Provedores de internet), Oi, Embratel e Starlink, tendo como

link principal o Circuito de Dados da Oi, o de backup o Circuito da Embratel/Claro e a Starlink como contenção em caso de rompimento da fibra no Estado. A Solução de Firewall Check Point é fornecida através de contrato com a empresa terceirizada CDTI.

- **Hardwares** - Os servidores, storages, switches cores e nobreaks de grande porte, ambos são acomodados em nosso ambiente seguro Data Center, instalados no Data Center no Prédio Administrativo.
- **PROJUDI** - O Sistema PROJUDI é a solução do TJRR para a tramitação processual nos dois graus de jurisdição. O software possibilita que todo o trâmite de feitos judiciais ocorra por meio eletrônico, informatizando também diversas rotinas cartorárias. Na definição do próprio CNJ, trata-se de "um sistema de informática que reproduz todo o procedimento judicial em meio eletrônico, substituindo o registro dos atos processuais realizados no papel, por armazenamento e manipulação dos autos em meio digital".
- **Scriba** - O SCRIBA é um software para realização de audiências por videoconferência , que reúne todas as informações em um só lugar, gravar e transcrever áudio e vídeo, reduz custos operacionais e promove o aumento da produtividade. Ele está integrado ao sistema de controle de processos judiciais - Projudi, por esse motivo depende da disponibilidade do Projudi para permitir a realização da gravação e da transcrição das audiências diretamente da tela de gestão da pauta diária da Unidade Judicial.
- **SEI** - O Sistema Eletrônico de Informações, desenvolvido pelo Tribunal Regional Federal da 4ª Região (TRF4), é uma ferramenta de gestão de documentos e processos eletrônicos, e tem como objetivo promover a eficiência administrativa.
- **ERP-Thema** - É um sistema completo para o cálculo da folha de pagamento e gestão de recursos humanos e o e-Social, atendendo de forma integrada grande parte dos processos de RH do TJRR. Possui integração com sistema contábil e financeiro, gerando os empenhos de todos os tipos de folha de pagamento, encargos e provisões de forma automática. Todos os documentos, atos legais, certificados, comprovantes, etc, referente ao servidor, podem ser digitalizados, arquivados e historiados pelo sistema, dispensando a utilização de arquivos físicos gerando economia e segurança para esta corte.

7. Principais riscos identificados

O PCSE-TIC foi desenvolvido para ser acionado quando da ocorrência de cenários de desastres que apresentam risco à continuidade dos serviços essenciais. O quadro abaixo procura dar uma dimensão do universo de riscos dentro da realidade de TIC, cada um possuindo graus diversos de severidade no contexto de

TIC deste tribunal, e que serão tratados com mais detalhes dentro do Plano de Recuperação de Desastres (PRD) que compõe o PCSE-TIC

De fato, a relação de eventos de desastre que se segue não pretende esgotar todas as possibilidades de acontecimentos danosos, porém objetiva apresentar de forma macro um mapeamento inicial que deve ser aperfeiçoado ao longo do tempo, com as revisões previstas na utilização deste plano.

Tipo	Risco	Causas
Tecnológico	Falhas em links de comunicação;	• Rompimento de fibra óptica decorrente da execução de obras públicas, desastres ou acidentes na capital e interior. • Mal funcionamento de switch gerenciador de segmento de rede. • Interrupção dos serviços de conectividade com as operadoras de telecomunicação por mais de 12 horas
	Falhas em hardware e software;	• Equipamento não condizente com as especificações técnicas; • Equipamentos sem manutenções corretivas realizadas; • Equipamentos com obsolescência; • Falha que necessite reposição de hardware crítico ou reparo, e cujo reparo ou aquisição dependa de processo licitatório.
	Indisponibilidade de backups	• Cópia de segurança dos dados não disponíveis ou sem integridade nos servidores de backup. • indisponibilidade do site backup. • Armazenamento de fitas cheio. • limite de velocidade de escrita do drive na fita. • Não monitoramento do sistema de backup. • Aquisição de Fitas de backup.
	Ataques cibernéticos.	• Acesso não autorizado a informações sensíveis constantes em servidores • Ataque virtual que comprometa o desempenho, os dados ou a configuração dos serviços essenciais.
	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. • acionamento dos UPS.

Tipo	Risco	Causas
Ambiental		• Impossibilidade de acionar o Grupo gerador no momento de uma queda de energia.
	Incêndios;	• Aquecimento excessivo • Curto circuito elétrico
	Falha em infraestrutura predial;	• Desabamento do Prédio
	Desastres Naturais.	• Inundações. • Abalos sísmicos.
	Falha na climatização	• Falha na Unidade de Climatização e não emissão de Alertas de monitoração. • Superaquecimento dos ativos devido falha no dimensionamento de carga no data center. • Falha na Unidade de Climatização e não emissão de Alertas de monitoração.
Humano	Greves.	
	Terrorismo.	Ataques internos - ativos do Data Center.
	Violência ou sequestro.	
	Desconhecimento ou erro induzido.	Manipulação indevida de equipamentos e sistemas.

8. Cenários de indisponibilidade

Identificação do incidente		Tratamento do incidente
Descrição	**Causa**	**Procedimentos de recuperação**
Indisponibilidade nos serviços de rede	• Falta de energia no Data Center • Defeito no sistema de refrigeração Data center • Problemas de curtos circuitos ou incêndio	• Acionamento de Ups de grande e médio porte. • Os sistemas alternativos de geração de energia serão acionados automaticamente em 1 minuto. • Abertura de chamado na Gemelo, equipamentos com garantia de manutenção. • Acionamento de gás FM200 no ambiente. • Comunicar/informar ao Secretário de TI.
	Falha no ativo de rede (switches e outros)	• Carregamento do script de backup de configuração. • O equipamento defeituoso será substituído e encaminhado para manutenção.
	Danos ao cabeamento local, tomadas, conectores e outros	• acionamento da central de serviços - atendimento nível 1. • A empresa contratada será acionada para proceder com o

Identificação do incidente		Tratamento do incidente
Descrição	**Causa**	**Procedimentos de recuperação**
		reparo.
	Danos nas fibras ópticas que interligam os diversos prédios da capital, e links que atendem as demais comarcas no estado.	• Acionamento de um link extra ou link backup, diferente da tecnologia utilizada que permita a liberação de serviços críticos que necessitam exclusivamente da internet e rede até que os serviços normais sejam restabelecidos. • A empresa contratada será acionada para proceder com o reparo.
	Falha no servidor - hardware	• A empresa contratada será acionada para proceder com o reparo, através de abertura de chamados. O TJRR manterá servidores e storage em cluster com a HA (High Availability), mantendo a possibilidade de falha de pelo menos 1 equipamento.
	Falha no servidor - software	• Uma imagem do servidor será restaurada com a substituição dos dados de backup da VM pelo último backup realizado. O tempo de

Identificação do incidente		Tratamento do incidente
Descrição	**Causa**	**Procedimentos de recuperação**
		recuperação de cada serviço deve ser definido (Servidores de Aplicação, de Arquivos, de Domínio, de banco de dados, etc.)
Indisponibilidade no Software Scriba	1. Integração com o Projudi falhou; 2. Impossível conectar remotamente 3. Impossível Gravar 4. Transcrição não funcionou 5. Falhas no áudio ou vídeo	Primeiro Nível - A central de atendimento deve ser acionada para prestar suporte ao usuário
		Segundo Nível - A SSJ deve ser acionada para prover o reparo no software.
		Terceiro Nível - A SUBINF será acionada para reparos na infraestrutura.
Indisponibilidade do Projudi	Impossível conectar	Primeiro Nível - A central de atendimento deve ser acionada para prestar suporte ao usuário
		Segundo Nível - A SSJ deve ser acionada para prover o reparo no software.
		Terceiro Nível - A SUBINF será acionada para reparos na infraestrutura.

Obs. Em caso de ataques cibernéticos o Plano de resposta a Incidentes Cibernéticos deve ser acionado.

9. Responsabilidades

O tratamento de um evento de desastre requer a atuação multidisciplinar de vários perfis profissionais, tornando necessário que se atribuam responsabilidades e papéis definidos para os grupos de trabalho, formados por servidores lotados em diversos setores da Secretaria de Tecnologia da Informação e também de outras Secretarias.

Os grupos definidos podem possuir participantes lotados em várias Subsecretarias e Setores do organograma da STI. Estes componentes podem participar cumulativamente de vários grupos, maximizando a equipe técnica disponível.

Abaixo segue os grupos e suas atribuições para consecução do PCSE-TIC:

COMITÊ DE GESTÃO DE TIC CGESTIC:

- 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.
- Inclui autoridades em nível institucional e tomadores de decisão da Secretaria de Tecnologia da Informação.

EQUIPE DE REDES:

- Avaliar os danos específicos de qualquer infraestrutura de rede no fornecimento de dados e conectividade de rede de voz, incluindo WAN, LAN e quaisquer conexões de telefonia interna dentro do TJRR ou de infraestrutura externa junto aos servidores.

EQUIPE DE GESTÃO INFRAESTRUTURA:

- Responsável pela infraestrutura que abriga os sistemas de TIC e pela garantia que haja estruturas alternativas (lógicas ou físicas) mantidas adequadamente.
- Avaliar os danos e supervisionar a execução do Plano de Recuperação de Desastres.
- O líder desta equipe administrará e manterá o Plano de Recuperação de Desastres.

EQUIPE DE APLICAÇÕES:

- Garantir que as aplicações essenciais funcionem como exigido para atender aos objetivos de negócios, durante ocorrência do desastre. Eles serão os principais responsáveis por assegurar e validar o desempenho das aplicações essenciais e podem ajudar outras equipes de TIC, conforme necessário.
- O líder desta equipe administrará e manterá o Plano de Continuidade Operacional juntamente com a equipa de Infraestrutura.

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 os servidores do TJRR na solução de contingência.
- Monitorar e recuperar as estruturas de armazenamento do BD.

EQUIPE DE COMUNICAÇÃO:

- Responsável por informar sobre a evolução das providências em andamento visando restaurar o serviço inoperante junto a servidores, autoridades, fornecedores e Assessoria de comunicação, que se encarregará de prestar informações à Mídia, se for o caso.
- O líder desta equipe administrará e manterá o Plano de Administração de Crises.

EQUIPE DE BACKUP:

- Responsável por 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.

Invocação do Plano

O PCSE-TIC 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 CGesTIC em conjunto com a alta administração do TJRR.

O acionamento das demais equipes será realizado pelos integrantes do Comitê, de acordo com as características de cada ocorrência, havendo o registro do evento através do Formulário de invocação do Plano onde serão consignados informações como data do incidente, descrição sucinta do ocorrido e quais as equipes acionadas.

REGISTRO DE ACIONAMENTO DO PCSETIC		
	Data e hora ____/___/____ **Início** ____:____	**Data e Hora** ____/___/____ **Fim** ____:____
Descrição		
Resultado		

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

Os protocolos e procedimentos de recuperação deverão ser imediatamente iniciados visando correção dos danos.

10. Matriz de Acionamento do plano

O acionamento ocorrerá após a constatação de algum dos cenários de desastres descritos neste documento. Na possibilidade de ocorrência de evento com risco desconhecido, mas que haja elevado grau de detectabilidade do risco ou da ameaça, o plano também poderá ser invocado.

Nos casos de reprodução simulada, o acionamento deverá ser precedido de comunicação interna com antecedência mínima estabelecida no Plano de Testes e Validações.

Todos e quaisquer acionamentos devem ser rigorosamente documentados, devendo constar o motivo do acionamento, data, operação realizada, quais equipes foram mobilizadas e a resposta ao incidente.

Quem?	Secretário de Tecnologia da Informação do TJRR
Quando?	Incidentes de interrupção de serviços superior a 01 hora
Onde?	Secretaria de Tecnologia da Informação
Em quanto tempo?	03 horas

Quem executará?	Equipe de recuperação de desastre da área afetada.

11. Equipe de recuperação de desastres

A equipe de recuperação de desastres é composta pelas seguintes equipes:

- Comitê de Gestão de TIC
- Equipe de Infraestrutura
- Equipe de operações
- Equipe de Backup

12. Recomendações

Considerando as limitações propostas neste Plano, limitando-se a restabelecimento de serviços e garantia de sua continuidade num período previamente elaborado, recomenda-se:

Atualização dos serviços essenciais: visa avaliar cada ativo de TI em casos de interrupção, considerando seu impacto para o Tribunal, para órgãos parceiros e demais jurisdicionados. Nesta avaliação deve ser considerado ainda o tempo de recuperação e seu respectivo ponto de informação.

Atualização do apetite ao risco: visa identificar em qual quantidade e tipo de risco o Tribunal de Justiça está disposto a buscar ou manter. Equivale a reavaliar seguindo os critérios de probabilidades de ocorrências atrelados à gravidade do dano caso o incidente aconteça.

Elaboração do Plano de Testes e Validação, Plano de Administração de Crise: tem o propósito de assegurar a validade dos procedimentos descritos neste plano de continuidade de serviços, proporcionando a melhoria contínua, tendo como principal insumo os resultados dos planos de reprodução simulada.

13. Comunicação com fornecedores

Os fornecedores deverão ser acionados sempre que necessário dentro dos parâmetros dos contratos.

14. Plano de Continuidade Operacional (PCO)

O Plano de Continuidade Operacional (PCO) descreve os procedimentos de contingência em uma situação de falha ou interrupção nos ativos que sustentam esses processos. Este PCO deve ser revisado, anualmente ou quando ocorrer mudanças significativas na organização, atualizado e gerenciado conjuntamente pelos líderes das equipes de gestão de infraestrutura e aplicações.

Escopo e Objetivo:

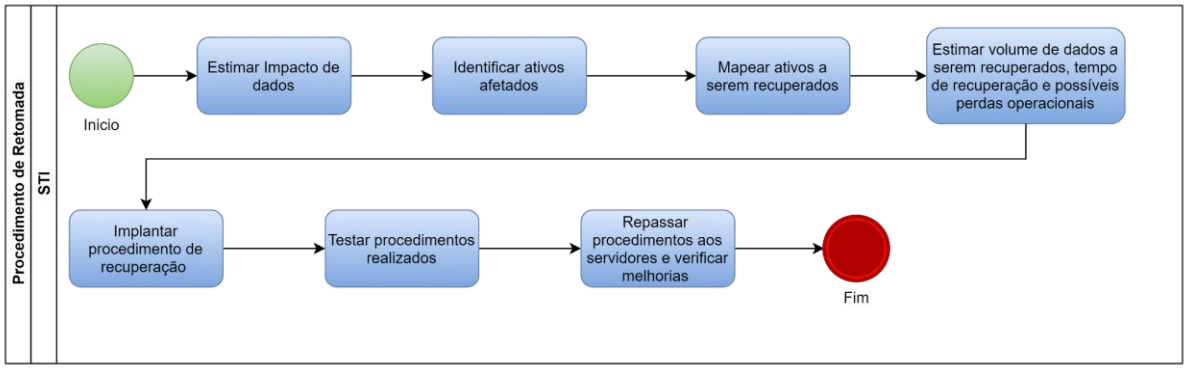
Este documento tem como objetivo restabelecer o funcionamento dos principais ativos que compõem as operações da Secretaria de Tecnologia da Informação do TJRR, reduzindo o tempo de queda e os impactos provocados por eventual incidente.

O PCO é composto por um conjunto de procedimentos definidos, destinados a manter a continuidade dos serviços vitais do Judiciário de Roraima, considerando a ausência de componentes que os suportem, devido à ocorrência de eventos previamente identificados e definidos. Através desse PCO os gestores e as equipes do TJRR saberão como agir na falta ou falha de algum componente que o suporte, garantindo a continuidade do processo, reduzindo o impacto no judiciário.

Este PCO aplica-se ao prédio Administrativo, prédio no qual se encontra atualmente o DATA CENTER Modular principal que provê os serviços ao Judiciário, e no Fórum Criminal Site Backup.

Lista de Atividades:

As etapas aqui realizadas são denominadas “Procedimentos de Retomada”:



- Estimar impacto de perda de dados;
- Identificar ativos afetados;
- Mapear ativos a serem recuperados;
- Estimar volume de dados a serem recuperados, tempo de recuperação e possíveis perdas operacionais;
- Implantar procedimentos de recuperação;
- Testar procedimentos realizados;
- Repassar procedimentos aos servidores e verificar melhorias.

Recursos Necessários:

Durante um incidente, os recursos humanos e materiais necessários para a continuidade operacional devem ser relacionados de forma a refletir a necessidade de acordo com a gravidade do evento. Em caso de alguma operação de emergência no DATA CENTER principal, deverão ser realizados algumas ações que possa garantir a operação do funcionamento dos serviços, entre elas está descrito:

- Abertura de chamado no NOC da Gemelo, repasse das informações referente aos problemas.
- Em caso de parada parcial do Data Center, como falha dos climatizadores de ar, nobreaks ou gerador de energia, devem ser avaliadas possibilidades de outros contratos para suprir as necessidades, através de locações ou manutenções corretivas de curto prazo;
- Na possibilidade de parada total do Data Center sem perda de dados, deverão ser avaliadas as possibilidades de execução parcial dos serviços nas infraestruturas do prédio administrativo.
- Em caso de algum desastre na infraestrutura do prédio Administrativo, providenciar a remoção do DATA CENTER Modular para um local seguro.

Obs: Demais atividades não previstas deverão passar pelo Comitê de Gestão de TIC.

Fechamento/Encerramento do Plano de Continuidade Operacional:

O Plano será encerrado assim que constatado que o funcionamento de todos os sistemas essenciais esteja totalmente de forma estável no ambiente do Data Center. A equipe responsável pelo retorno deverá emitir um relatório via SEI informando as atividades realizadas, para então fornecer os dados necessários para um comunicado de retorno das atividades do TJRR.

15. 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.

O PRD deve ser revisado e atualizado conjuntamente pelos líderes das equipes de GESTÃO DE INFRAESTRUTURA e Equipe de Aplicações.

Escopo e Objetivo:

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 do PRD:

- Avaliar danos aos ativos, serviços essenciais e conexões do datacenter, provendo meios para sua recuperação.
- Evitar desdobramentos de outros incidentes na instalação principal.
- Restabelecer o datacenter ou serviço/sistema essencial, dentro do prazo tolerável.

Possíveis Cenários de Inoperância:

A partir da determinação e levantamento de potenciais riscos frente às possíveis situações que se apresentam dentro do ambiente da STI, procuramos referenciar no quadro abaixo os principais incidentes, suas possíveis causas e medidas macro mais adequadas para recuperação destes cenários de inoperância. São eles:

Incidente	Causas	Procedimentos Macro de Recuperação
		• informar a SIL. • Acionamento da Roraima Energia

Incidente	Causas	Procedimentos Macro de Recuperação
Falha de alimentação de energia elétrica Problemas na concessionária	Externa	para o restabelecimento dos serviços elétricos. ● Solicitação de previsão de conclusão das providências. ● Comunicar integrante do Comitê DR gestor.
	Interna	● Acionar a Subsecretaria de Infraestrutura para verificação dos geradores emergenciais e da Subestação de Energia. ● Acionar setor de administração predial solicitando verificação de cabeamento elétrico até a subestação de energia para verificar disjuntores, fusíveis, etc, considerando os 2 circuitos independentes (Sala/Ar condicionado)
	Danos ao nobreak	● Solicitar ao fiscal de contrato que acione a empresa contratada para manutenção do mesmo e execução de reparos (limpeza, trocas de baterias, ou conserto de placa, etc).
Problemas/Danos no sistema de refrigeração de Ar do DATA CENTER.	Falhas nos circuitos elétricos Dentro da Subestação do TJRR	● informar a SIL. ● Comunicar Comitê DR ● Abrir chamado na Administração Predial para avaliação e reparos. ● Solicitar previsão para término dos reparos.
	Falhas nos circuitos elétricos Dentro do DATA CENTER	● Comunicar Comitê DR ● Abrir chamado no Service Desk (NOC) da empresa de manutenção do Data Center ● Monitoramento do SLA acordado ● Solicitar previsão para término dos reparos.
	Falha de alimentação de energia para o circuito Ar	● Comunicar ao Comitê DR. ● Abrir chamado na Administração Predial para avaliação e reparos. ● Abrir chamado no Service Desk

Incidente	Causas	Procedimentos Macro de Recuperação
	condicionado	(NOC) da empresa de manutenção do Data Center. ● Solicitar previsão para término dos reparos. ● Monitoramento do SLA acordado.
Indisponibilidade dos serviços /aplicações pela rede Interna	Danos a Switch	● Verificação de cabeamento UTP e Fibra; ● Verificação da existência de equipamento reserva, Acionar a garantia, se for o caso. ● Reconfiguração do novo equipamento através da biblioteca de configurações. ● Instalar e testar equipamento
	Danos ao cabeamento	● Substituir ou reparar o cabo ou danificado. ● Verificação de segmento/porta lógica para via de conexão alternativa. ● Abertura de chamado junto a empresa responsável pelo contrato de manutenção de cabeamento estruturado.
	Danos em servidor de aplicação/ Arquivos/ autenticação	● Verificação de montagem de máquina virtual ou disponibilidade de equipamento reserva. ● Acionar a garantia, se for o caso ● Identificação do backup de dados mais recente e restauração das informações. ● Ativação do equipamento em produção, baseado na biblioteca de configurações. ● Testes e homologação.
	Remoção/perda de Dados pelos usuários.	● Identificar meios pelos quais foram possíveis se fazer a remoção e tratá-los em conformidade com a Política de Segurança da Informação adotada. ● Identificação do backup de dados mais recente e restauração das informações removidas. ● Restauração do backup e Testes.

Incidente	Causas	Procedimentos Macro de Recuperação
Indisponibilidade dos serviços de internet.	Links de internet indisponíveis	• Alteração de rotas para o link de internet redundante. • Abertura de chamados através do 0800 junto aos provedores de internet. • Identificação de chamados e repasse das informações ao Comitê de TIC. • Monitoramento do SLA acordado
	Servidor de internet/Firewall indisponível	• Acionamento do master para o Slave. • Testes.
	Backup mais recente de usuário não existe.	• Orientação de abertura de chamados para formalização da Demanda. • Verificar existência de backup anterior. Recomendar ao usuário a inclusão de seus arquivos no drive Corporativo (Google Workspace)
Indisponibilidade de restauração de backups	Mídia indisponível	• Verificação da disponibilidade de mídia alternativa. • Identificação do backup de dados mais recente e restauração das informações, se for o caso. • Notificar o comitê DR sobre a data/hora do backup que será recuperado. • Verificar causas de indisponibilidade e revisar processo de execução. • Testes
Indisponibilidade de comunicação com as Comarcas do TJRR	Links indisponíveis	Notificar/informar ao Comitê DR sobre a ocorrência. • Verificação de infraestrutura interna nas comarcas. • Abrir chamado no Service Desk da concessionária dos Links de comunicação • Monitoramento do SLA acordado.

Os procedimentos macro de recuperação citados na tabela acima, serão conduzidos pela execução formal das seguintes etapas definidas abaixo sob a supervisão da **Equipe de GESTÃO DE INFRAESTRUTURA.**

Momento de Ativação do Plano:

A ativação do presente plano se dará na ocorrência de um dos cenários descritos na tabela acima, ou ainda por conta de ocorrência de evento ainda não mapeado pela STI, que tenha gerado interrupção nos serviços essenciais, seguindo o fluxo de fases definido abaixo.

Identificação de Ativos Inoperantes:

As equipes de BACKUP, EQUIPAMENTOS SERVIDORES, REDE e OPERAÇÕES deverão identificar e listar todos os Ativos/Serviços inoperantes em decorrência do desastre. As informações de cada ativo inoperante devem ser condensadas em levantamento contendo no **mínimo identificação, IP, breve descrição de sua função, indicação se está em período de garantia, se há redundância física disponível, responsável, fornecedor.**

Identificação de acessos interrompidos

A Equipe de Infraestrutura de rede do TJRR deverá identificar a existência de interrupções de conexões e acessos gerados após o desastre, informando sua abrangência(rede local, rede WAN ou provedor de serviços), quando aplicável.

Identificação de serviços descontinuados

A equipe de GESTÃO DE INFRAESTRUTURA 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. No 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.

Elaboração de cronograma de recuperação

A equipe de GESTÃO DE INFRAESTRUTURA após o mapeamento das perdas e impactos elaborará um breve cronograma de recuperação dos serviços/aplicações atingidos pelo desastre levando em consideração:

- A priorização dos serviços essenciais, ou se for o caso, outra determinação de prioridades de nível institucional desde que formalmente solicitada à STI e aceita pelo Comitê de DR;

- A utilização da rotina existente de tratamento de recuperação existente, para cada um dos ativos de informação;
- Disponibilidade e compromisso da equipe envolvida; e
- A força de trabalho disponível.

Substituição de ativos e equipamentos

Em caso de perda dos ativos (equipamentos), 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 TJRR, comunicando ao COMITÊ DE DR se há alguma solução alternativa a ser tomada enquanto é realizada a aquisição.

A equipe de OPERAÇÕES e GESTÃO DE INFRAESTRUTURA deve verificar dentre os ativos danificados que estão cobertos por garantia e se a mesma poderá ser acionada neste caso através da lista de 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 OPERAÇÕES deverá verificar se as configurações dos ativos reparados ou substituídos estão em pleno funcionamento. Caso não estejam, prover cronograma estimado para configurar estes ativos informando ao COMITÊ DE DR.

Teste de homologação/ambiente

O ambiente principal do datacenter deverá ser testado antes do recovery dos dados do backup, a fim de garantir que o processo de recuperação ocorra conforme o planejado.

Os testes incluem:

- Avaliar performance para garantir os mesmos níveis de capacidade e disponibilidade dos serviços essenciais, antes do desastre;
- Validar as configurações.

Recuperar dados do backup

Nos casos de recuperação de dados para as aplicações, este será realizado pela Equipe de BACKUP, INFRAESTRUTURA em conjunto com com a cópia de

segurança mais recente disponível, notificando o líder do PRD, a equipe de aplicações e o Comitê de DR da data e hora do mesmo.

Encerramento do Plano de Recuperação de Desastres (PRD)

Na finalização do procedimento de recovery, as informações da recuperação de serviços serão consolidadas em parecer específico informando horário de restabelecimento de cada serviço, equipamentos adquiridos (se for o caso), procedimentos de recuperação realizados e fornecedores acionados.

16. Plano de Administração de Crises PAC

Este plano especifica as ações tomadas ante os cenários de desastres. As ações incluem gerir, administrar, eliminar ou neutralizar os impactos, inerentes ao relacionamento entre os agentes envolvidos e/ou serviços afetados, até a superação da crise, através da orquestração das ações e de uma comunicação eficaz.

Objetivo

O objetivo desse plano é garantir a comunicação, gerenciar crises e viabilizar uma compreensão entre todos os envolvidos nas ações antes, durante e após a ocorrência de um desastre.

Segue abaixo os objetivos do PAC:

- Minimizar transtornos sobre os desdobramentos de incidente e estimular o esforço em conjunto para superação da crise;
- Garantir a segurança à vida das pessoas;
- Orientar as equipes de gestão e aos servidores do poder judiciário com informações concretas; e
- Informar a sociedade de modo geral 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 e equipes, principalmente as que foram 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 segmento.

A comunicação com cada parte ocorrerá da seguinte forma:

1. **Comunicar às autoridades locais:**

Essa parte caberá a **Equipe de Comunicação,** essa equipe irá assegurar que as autoridades competentes tenham sido notificadas do desastre/catástrofe, principalmente se envolver risco às pessoas, repassando as seguinte informações de localização, natureza, magnitude e impacto do desastre.

Autoridade Local	Número para Contato	Data e hora do registro	Número da Ocorrência
Polícia	190		
Bombeiros	192		
Samu	192		

2. **Comunicação logo após um desastre:**

Logo após a correção de um desastre deverá ser feita uma reunião com os líderes de Equipe, onde 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 retorno dos serviços inativos.

3. **Comunicação com Servidores:**

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

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

As informações que serão dadas irão se referir:

- Se é seguro a entrada no ambiente afetado, onde tenha acontecido o desastre/Catástrofe.
- Onde devem se deslocar em caso de não terem acesso ao TJRR.

- Que tipo de serviços ainda estão disponíveis para eles.
- Expectativas de trabalho durante o desastre.

Comunicar as Comarcas, gabinetes e Secretarias do TJRR.

- Acionar diretamente as comarcas, gabinete ou secretarias afetadas pelo desastre e fornecer contato para que possam tirar dúvidas ou extrair mais informações.
- Natureza, impacto e abrangência da catástrofe.
- Ações de contingência em andamento.
- Processos/sistemas e serviços cobertos pelo plano de continuidade (Serviços essenciais).

Comarca/Gabinete /Secretarias	Número para Contato	Data/Hora do Contato	Local
Gabinete da Presidência TJRR	(95) 3198-2810 (95) 3198-2811		2º Piso do Palácio da Justiça
Assessoria Militar	(95) 3198-2833		Térreo - Palácio da Justiça.
Secretaria de Tecnologia da Informação (STI) - Gabinete	(95) 3198-2825		1º Piso do Prédio Administrativo.
Núcleo Comunicação e de Relações Institucionais (NUCRI)	(95) 3198-2827		2º Piso do Palácio de Justiça.
Secretaria de Gestão Administração (SGA) Gabinete	(95) 3198-4112		3º Piso do Prédio Administrativo.
Secretaria de infraestrutura e Logística (SIL)	(95) 3198-4110		2º Piso do prédio Administrativo.
Comarca de Alto Alegre	(95) 3198-4174 (95) 3198-4175		Fórum Ottomar de Sousa Pinto Rua Antônio Dourado de Santana, 595 - Centro.

Comarca de Bonfim	(95) 3198-4171 (95) 3198-4172 (95) 3198-4173		Fórum Ruy Barbosa Rua Maria Deolinda de Franco Megias, s/nº, Bonfim - Centro.
Comarca de Caracaraí	(95) 3198-4166 (95) 3198-4198		Fórum Juiz Paulo Martins de Deus Praça do Centro Cívico, s/nº - Centro.
Comarca de Mucajaí	(95) 3198-4169 (95) 3198-4170 (95) 3198-4192 (95) 3198-4168		Fórum Juiz Antônio de Sá Peixoto Av. Nossa Senhora de Fátima, s/nº - Centro.
Comarca de Pacaraima	(95) 3198-4167 (95) 3198-4176		Fórum Advogado Humberto Teles Machado de Sousa Av. Guiana, s/nº - Centro.
Comarca de Rorainópolis	(95) 3198-4178 (95) 3198-4179		Fórum Des. José Lourenço Furtado Portugal Av. Pedro Daniel da Silva, s/nº.
Comarca de São Luiz.	(95) 3198-4180 (95) 3198-4181		Fórum Juiz Umberto Teixeira Av. Ataliba Gomes de Laia, 100 - Centro.

Informar Fornecedores e Prestadores de Serviços do TJRR:

Lista de principais fornecedores Anexo I

Fornecedor	Contato	Data e hora

Informar Parceiros Externos, Cidadãos e Mídia:

A equipe de comunicação em conjunto com o Núcleo de Comunicação e Relações Institucionais (NUCRI) do TJRR deverá disponibilizar informações aos parceiros colaboradores externos, cidadãos e outros órgãos.

- Validar toda situação de acordo com o cenário.
- Realizar publicações em meios oficiais e de ampla divulgação para a sociedade, com o aval do comitê gestor DR, acerca das informações sobre o ocorrido.
- Após a divulgação, preencher a tabela com os dados abaixo.

Parceiro/Colaborador /empresa/Pessoa	Contato	Meio de Publicação	E-mail

Informar/Comunicar o retorno das Operações:

A equipe de comunicação em conjunto com o Núcleo de Comunicação e de Relações Institucionais (NUCRI) do TJRR deverá comunicar a todas as partes acima supracitadas quando ocorrer o retorno das operações à normalidade.

Finalização/Encerramento do Plano de Administração de Crises (PAC):

Após validado a estabilidade do DATACENTER e o funcionamento do retorno dos sistemas judiciais e administrativos essenciais, 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. Deverá ser elaborado um relatório compondo as relações das atividades necessárias após as ocorrências do desastre, como remanejamento dos

canais de informação, abertura e acompanhamento de chamados relacionados ao ocorrido.

17. Plano de Testes e Validação

Validações e Testes do PCSE-TIC

Cumprindo o propósito de reavaliar os procedimentos planejados visando a melhoria contínua, o PCSE-TIC 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.

A execução dos passos planejados deve ser registrada 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:

- Testes de Mesa
- Assegurar que cada integrante (Equipe) esteja familiarizado com o PCTIC
- Simular uma situação real de interrupção.

Status:

- Programado
- Executado
- Planejado
- Agendado

Data	Tipo	Motivo	Status

Aprovação do Plano de Continuidade de Serviços Essenciais de Tecnologia da Informação e Comunicação do Tribunal de Justiça do Estado de Roraima.

A versão _____ do PCTI fica aprovada em _____/_____/_____ por aprovação das partes envolvidas.

_____

Secretário de Tecnologia da Informação TJRR

_____

COMITÊ DE DISASTER/RECOVERY (DR) CGSTIC:

_____

EQUIPE DE GESTÃO INFRAESTRUTURA:
EQUIPE DE REDES
EQUIPE DE BACKUP

_____

EQUIPE DE APLICAÇÕES:

_____

EQUIPE DE OPERAÇÕES

_____

EQUIPE DE COMUNICAÇÕES