TRIBUNAL DE JUSTIÇA DE PERNAMBUCO

Plano de Continuidade de Negócios

SECRETARIA DE PLANEJAMENTO ESTRATÉGICO E GESTÃO - SEPLAN

SECRETARIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO – SETIC

2024

Sumário

Introdução

O Tribunal de Justiça de Pernambuco (TJPE), comprometido com a excelência na prestação de serviços à sociedade, apresenta o Plano de Continuidade de Negócio (PCN). Este documento, elaborado em consonância com as diretrizes do Conselho Nacional de Justiça (CNJ) e da norma **ISO 22301**, tem como objetivo primordial garantir a resiliência da instituição perante a interrupções ou disrupções, assegurando a continuidade das atividades essenciais e a minimização dos impactos negativos.

Com o intuito de aprimorar a clareza e organização, este documento está estruturado em duas partes. A primeira é referente ao processo de governança do plano de continuidade do negócio, e a segunda trata da operacionalização das ações de continuidade do negócio.

PARTE 1 – Governança do Plano de Continuidade do Negócio

1. Objetivo

O PCN tem como objetivo estabelecer critérios de conduta jurídica e ações mitigatórias operacionais das áreas de negócio do TJPE em face de uma indisponibilidade dos sistemas críticos estabelecidos pela Alta Gestão, definindo papéis e responsabilidades para cada etapa e ação do processo de governança e operação do plano de continuidade do negócio.

O plano deve ser baseado no entendimento dos riscos, nas possíveis ameaças e seu impacto na continuidade da prestação de serviço jurisdicional, contemplando os requisitos mínimos de capacidade de execução de atividades fins.

2. Escopo

Ao concentrar as operações dos atos processuais no sistema PJe, foi natural a constatação de que o mesmo é o sistema de nível mais crítico em todo Poder Judiciário Estadual.
Consequentemente, foi acatada pelo Diretoria Geral e pela Secretaria de Planejamento e Gestão Estratégica (SEPLAN), a definição de um escopo reduzido para o sistema PJe, que corresponde à esta primeira versão do Plano de Continuidade dos Serviços de Negócio.

3. Conceitos

Para um correto entendimento do PCN, inicialmente é importante apresentar os conceitos relacionados a este plano.

- **Gestão de Continuidade (GCN):** Processo de gestão (GCN) que fornece uma estrutura para que se desenvolva uma resiliência institucional capaz de responder efetivamente aos incidentes e desastres por meio da salvaguarda da prestação jurisdicional e a imagem do Tribunal;
- **Continuidade de Negócio (CN)**: capacidade estratégica e tática de planejar e responder a incidentes e interrupções da prestação jurisdicional, minimizando seus impactos;
- **Tempo Objetivo de Recuperação (RTO):** período de tempo após um incidente em que o serviço deve ser retomado, ou a atividade deve ser retomada, ou os recursos devem ser recuperados;
- **Crise:** Período de instabilidade para o TJPE que pode ter origem interna ou externa, com a possibilidade de resultados não esperados que necessitam de decisões urgentes pela alta administração.
- **Desastre**: Evento repentino e não planejado que cause interrupção de processos e serviços ou a redução na qualidade da prestação jurisdicional de vulto global ou que afete o público externo ao TJPE;
- **Resiliência:** capacidade de uma organização de resistir aos efeitos de um incidente de continuidade de negócios;
- **Incidente:** evento que tenha causado algum dano ou colocado em risco algum ativo de informação crítico, interrompendo a execução de alguma atividade crítica;

4. Competências

A Gestão de Continuidade de Negócio é de competência da Administração Geral, sendo exercida de forma compartilhada pela SEPLAN e SETIC.

Os planos complementares integrantes do PCN, são de responsabilidade das unidades tecnicamente competentes à sua execução.

5. Estrutura e Responsabilidades

5.1 Estrutura:

A estrutura envolvida na continuidade de negócios do PJe no âmbito do TJPE são:

CGPJe - Comitê Gestor do PJe;

UNPJe – Unidade Gestora do PJe;

SETIC – UNPJe – Unidade Operacional do PJe;

As Secretarias SEPLAN e SETIC atuarão alinhadas com as diretrizes da Política de Segurança da Informação.

5.2. Responsabilidades:

CGPJe - Comitê Gestor do PJe;

- propor ajustes, aprimoramentos e modificações da Política de Gestão de Continuidade de Negócios no que se refere ao PJe;
- deliberar sobre controles, processos e procedimentos de Continuidade de Negócios referentes ao PJe;

UNPJe – Unidade Gestora do PJe;

- assegurar a execução de ações com base nos planos desenvolvidos, quando da ocorrência de incidente;

SETIC – UNPJe

Acompanhar e coordenar as ações de recuperação do incidente causador da interrupção do serviço PJe.

SEPLAN

Coordenar e planejar o ciclo de vida do PCN, como adaptações a mudanças organizacionais e/ou estruturais, revisões periódicas e monitoramento dos indicadores de gestão.

6. Manutenção do Plano

O PCN deverá ser revisado a cada 2 anos da última publicação ou quando ocorrer mudança significativa na estrutura operacional do serviço PJe.

PARTE 2 – Operacionalização da Continuidade do Negócio

7. Do Negócio

Os **Artigos 11 e 12 da Resolução nº 185 de 18/12/2013**, **que institui o Sistema Processo Judicial Eletrônico - PJe como sistema de processamento de informações e prática de atos**, tratam respectivamente da prorrogação dos prazos e das indisponibilidades previamente programadas.

7.1. Da Suspensão dos Prazos

Art. 11. Os prazos que vencerem no dia da ocorrência de indisponibilidade de quaisquer dos serviços referidos no art. 8º serão prorrogados para o dia útil seguinte, quando:

I – A indisponibilidade for superior a 60 (sessenta) minutos, ininterruptos ou não, se ocorrida entre 6h00 e 23h00; ou

II – Ocorrer indisponibilidade entre 23h00 e 24h00.

§ 1º As indisponibilidades ocorridas entre 0h00 e 6h00 dos dias de expediente forense e as ocorridas em feriados e finais de semana, a qualquer hora, não produzirão o efeito do caput.

§ 2º Os prazos fixados em hora ou minuto serão prorrogados até às 24h00 do dia útil seguinte quando:

I – Ocorrer indisponibilidade superior a 60 (sessenta) minutos, ininterruptos ou não, nas últimas 24 (vinte e quatro) horas do prazo; ou

II – Ocorrer indisponibilidade nos 60 (sessenta) minutos anteriores ao seu término.

§ 3º A prorrogação de que trata este artigo será feita automaticamente pelo sistema PJe.

7.2. Da Indisponibilidade Programada

Art. 12. A indisponibilidade previamente programada produzirá as consequências previstas em lei e na presente Resolução e será ostensivamente comunicada ao público externo com, pelo menos, 5 (cinco) dias de antecedência.

8. Da Indisponibilidade do PJE e Do Plantão Judiciário

A **Instrução Normativa Conjunta nº 10 de 12/08/2011 (DJE 16/08/2021)**, **que implanta o Sistema Processo Judicial Eletrônico – PJe no Plantão Judiciário Cível e Criminal no âmbito dos 1º e 2º graus**, disciplina a sua utilização e dá outras providências.

Art. 12. Após a implantação do sistema PJe nos plantões judiciários é vedado o recebimento de qualquer expediente, petição ou processo fora do Sistema PJe, salvo, em caráter excepcional, nas seguintes hipóteses:

I - Indisponibilidade do sistema PJe, nos termos dos §§1º e 2º deste artigo;

II - Quando o usuário externo não dispuser de certificado digital, em razão de caso fortuito ou de força maior devidamente comprovado, e desde que se trate da necessidade de se praticar ato urgente ou destinado a impedir o perecimento de direito.

§ 1º A indisponibilidade do sistema PJe é configurada quando ocorrer a falta de acesso ao sítio do Tribunal de Justiça de Pernambuco ou aos servidores WEB do PJe, bem como diante da ocorrência de falha em rotina do sistema que impossibilite o peticionamento eletrônico.

§2º A indisponibilidade do sistema PJe que autoriza o recebimento de petições, expedientes e processos fora do sistema consiste tão somente naquela constante do Registro de Indisponibilidade (https://www.tjpe.jus.br/web/processo-judicial-eletronico/registro-de-indisponibilidade) ou reconhecida pelo serviço de plantão da SETIC.

§3º A instabilidade na conexão do próprio usuário externo ou do requerente não configura indisponibilidade e não autoriza o protocolamento fora do sistema PJe.

§4º Em caso de indisponibilidade do sistema PJe, a parte requerente deverá encaminhar os expedientes, pedidos e petições, juntamente com o registro de indisponibilidade, exclusivamente, para o e-mail da unidade judiciária plantonista, conforme escala publicada no site do Tribunal de Justiça de Pernambuco.

§5º Em caso de indisponibilidade total do site do TJPE e estando o e-mail institucional também indisponível, será divulgado nas redes sociais do Tribunal outros e-mails das unidades plantonistas para serem utilizados exclusivamente durante o período da referida indisponibilidade.

§6º O juiz plantonista somente admitirá o processamento dos expedientes recebidos por e-mail, se efetivamente constatada a indisponibilidade do sistema PJe.

§7º Não admitido o processamento, o juízo plantonista deverá informar ao requerente, por e-mail, determinando o protocolamento no Sistema PJe para que seja analisado o pedido.

§8º No 1º grau, os expedientes recebidos por e-mail, em virtude da indisponibilidade do sistema, serão protocolados no Sistema PJe pelos servidores plantonistas, no prazo máximo de 24 horas úteis após o retorno do sistema, seguindo-se com a redistribuição para a unidade judiciária competente, na forma do art. 11.

§9º No 2º grau, os expedientes recebidos por e-mail, em virtude da indisponibilidade do sistema, serão remetidos por e-mail pelo servidor plantonista para o Núcleo de Distribuição do 2º Grau – NUDIP, para ser protocolado no Sistema PJe no próximo dia útil.

9. Análise do Horário e Período de Indisponibilidade

A Análise do horário e período de indisponibilidade do PJe está relacionado ao impacto à prestação do serviço jurisdicional do TJPE, variando ao longo do experiente forense.

Horário	Dia Forense	Feriado e FDS	Plantão
Entre 0h00 e 6h00	1	1	4
Entre 6h00 e 23h00	3	2	4
Entre 23h00 e 24h00	2	2	4

10. Análise da Duração da Indisponibilidade

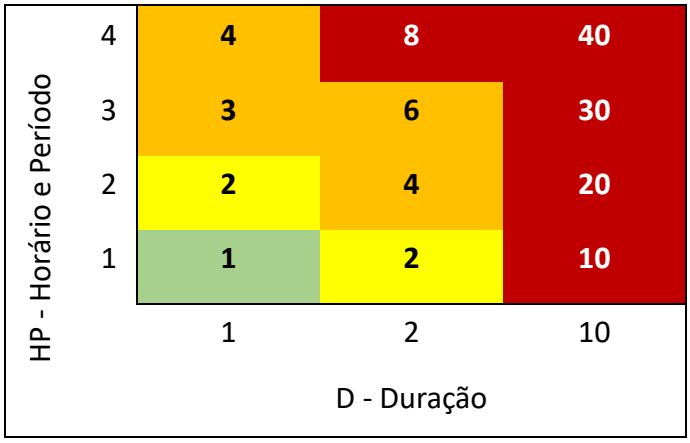
O tempo de indisponibilidade se refere ao prazo máximo definido pela unidade operacional do serviço afetado para o total restabelecimento das operações, definidos em horas de indisponibilidade e uma escala de avaliação. Sendo:

	<= 60 min	> 60 min	Plantão
Escala	1	2	10

11. Matriz de Criticidade

A matriz de Criticidade relaciona o horário e período com a duração da indisponibilidade do PJe. A matriz orienta as ações e os responsáveis pela tomada de decisão a todos os afetados pelo incidente, bem como o plano de comunicação.

Obtém-se o nível de criticidade multiplicando a escala de duração pela escala de horário e período (HP x D).



12. Procedimentos Operacionais Jurídicos em Caso de Indisponibilidade no PJe

Os procedimentos operacionais jurídicos descritos são essenciais para assegurar a continuidade das atividades judiciais e mitigar os impactos de falhas no sistema PJe. A adoção dessas medidas garante a transparência, a eficiência e a justiça no tratamento dos processos judiciais, mantendo a confiança das partes e a integridade do sistema judicial do Tribunal de Justiça de Pernambuco.

12.1. Notificação Imediata e Comunicação

a) **Informar as Partes Interessadas:** Notificação imediata a todos os juízes, servidores, advogados, e partes envolvidas sobre a falha no sistema PJe. Utilizar canais de comunicação previamente definidos, como e-mails, SMS, e avisos no site oficial do TJPE.

b) **Publicação de Comunicado Oficial:** Publicar um comunicado oficial no site do TJPE e nas redes sociais, explicando a situação, as medidas em andamento e as expectativas de retorno.

12.2. Estabelecimento de Prazos Alternativos

a) **Suspensão de Prazos Processuais:** Emitir uma portaria suspendendo os prazos processuais durante o período de inatividade do PJe. Esta suspensão deve ser amplamente divulgada para evitar prejuízos às partes.

b) **Prorrogação de Prazos:** Definir novos prazos para a realização de atos processuais que estavam previstos durante o período de falha, assegurando que nenhuma das partes seja prejudicada.

12.3. Protocolo Alternativo de Documentos

a) **Protocolo Temporário:** Implementar um protocolo temporário para a recepção de petições e outros documentos judiciais. Para viabilizar o exame de matérias urgentes durante o período de indisponibilidade.

b) O peticionamento de medidas urgentes deverá ser realizado pelo e-mail disponibilizado pelo TJPE.

12.4. Manutenção de Audiências e Sessões

a) **Adiamento de Audiências:** Adiar audiências e sessões que dependam diretamente do acesso ao PJe, com a devida comunicação às partes envolvidas e reprogramação para novas datas.

12.5. Garantia da Continuidade dos Atos Processuais Urgentes

a) Identificação de Processos Urgentes: Identificar e priorizar processos de natureza urgente (por exemplo, medidas cautelares, habeas corpus, e tutela de urgência) que não podem sofrer atrasos.

b) Procedimentos Alternativos para Urgências: Estabelecer mecanismos alternativos para a tramitação desses processos, incluindo a comunicação direta entre juízes, advogados e partes envolvidas.

12.6. Registro e Relatório de Incidentes

a) Documentação de Incidentes: Manter um registro detalhado de todos os incidentes ocorridos, incluindo a natureza da falha, as ações tomadas, e o tempo de resposta.

b) Relatório Pós-Incidente: Após a resolução da falha, elaborar um relatório completo com a análise do incidente, impactos, medidas de mitigação implementadas, e recomendações para evitar futuras ocorrências.

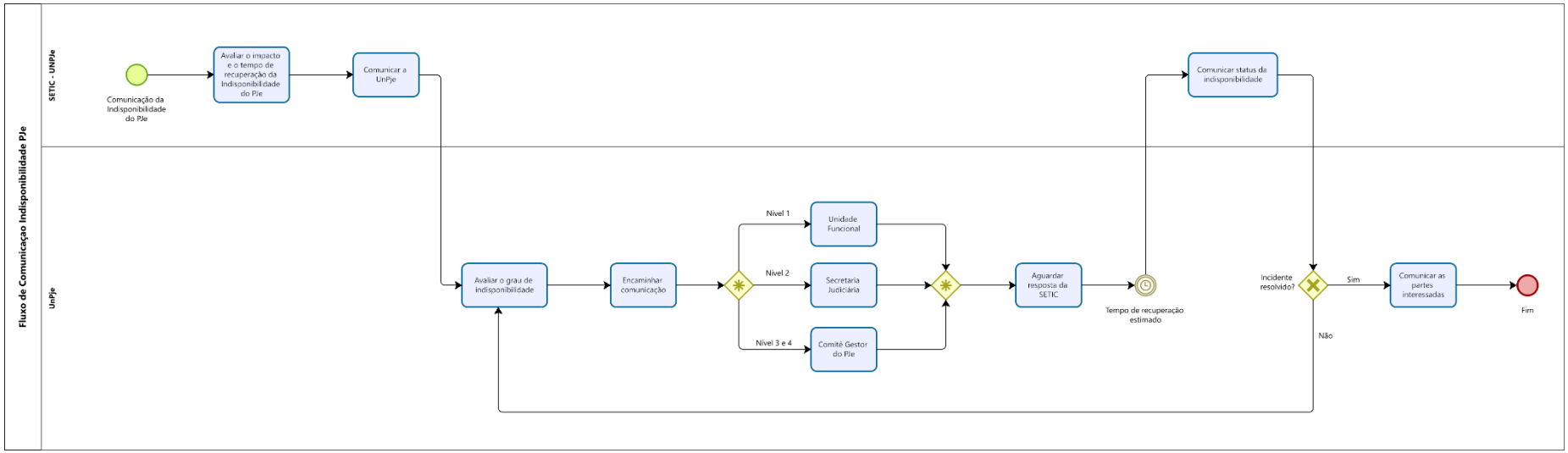
13. Plano de Comunicação

O objetivo do plano é definir o protocolo de comunicação, envolvendo as ferramentas de comunicação adequadas para cada público diante de um cenário de interrupção do sistema alvo deste documento.

A prioridade é assegurar que todos os agentes envolvidos com o sistema tenham sido notificados da catástrofe no nível de sua competência decisória, com as informações de localização, natureza, magnitude e impacto do desastre.

Qualquer colaborador está apto a identificar a indisponibilidade do serviço e comunicar imediatamente a central de serviços de TIC.

A seguir apresentamos o fluxo de comunicação do PCN.



14. Plano de Recuperação de Desastres

O Plano de Recuperação de Desastres (PRD ou PTCN) de TIC visa restabelecer rapidamente os dados, os sistemas e os ativos da infraestrutura de TIC do Tribunal de Justiça de Pernambuco (TJPE), após uma interrupção causada por algum desastre, como catástrofes naturais, ataques hacker ou falhas. É parte integrante do Plano de Continuidade de Negócio (PCN) e seu conteúdo segue em anexo na seção **Anexo A – Plano de Recuperação de Desastres**.

15. Métricas

As métricas visam o acompanhamento das ações do processo de continuidade do negócio, objetivando a garantia de entrega do serviço com o menor impacto às áreas de negócio, tendo como principais motivadores:

- Garantia que serviços de TI estarão disponíveis conforme necessário;
- Garantia de um impacto mínimo no negócio em caso de uma indisponibilidade ou mudança nos serviços de TI;
- Garantia que a infraestrutura e serviços de TI possam resistir e se recuperar de falhas devidas a erros, ataques ou desastres.

Métricas avaliadas:

- Frequência de revisão do plano de continuidade de TI;
- Quantidade de horas perdidas por usuários por mês devido à inoperância não planejada do sistema PJe;

16. Matriz de Contatos

Responsável	Unidade	Telefone	Email

17. Conclusão

Em um mundo em constante mutação, marcado por eventos imprevisíveis e disruptivos, a resiliência se torna um pilar fundamental para a sobrevivência e o sucesso das organizações. O Tribunal de Justiça de Pernambuco (TJPE), consciente de seu papel crucial na sociedade, reconhece a necessidade de se preparar para enfrentar os desafios e garantir a continuidade de seus serviços essenciais.

O Plano de Continuidade de Negócio (PCN) se configura como um escudo contra as adversidades, fornecendo ao TJPE a estrutura e os mecanismos necessários para lidar com interrupções, minimizando seus impactos e assegurando a prestação de serviços a seus jurisdicionados, mesmo em cenários adversos.

A implementação e o acompanhamento do PCN trazem diversos benefícios estratégicos para o TJPE, dentre eles:

Redução do Impacto de Interrupções: O PCN permite ao TJPE identificar, prevenir e responder de forma eficaz a incidentes, minimizando o tempo de inatividade e os prejuízos financeiros e à sua imagem.

Proteção da Reputação: A capacidade de manter a continuidade das operações, mesmo em situações de crise, reforça a confiança da sociedade no TJPE e protege sua reputação como instituição sólida e confiável.

Melhoria da Tomada de Decisões: O PCN fornece aos gestores do TJPE informações e ferramentas para tomar decisões assertivas em momentos críticos, garantindo a continuidade dos serviços essenciais.

Cumprimento de Normas e Regulamentações: O TJPE demonstra seu compromisso com o cumprimento das normas e regulamentações relacionadas à continuidade de negócios, prezando pela conformidade com:

- **A Resolução CNJ nº 370/2021, que instituiu a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD) para o sexênio 2021-2026**;
- **A Resolução CNJ nº 396/2021, que instituiu a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ).**

Desse modo, consolida sua posição como uma instituição responsável e comprometida com a boa governança.

O PCN não é um documento estático, mas sim um processo dinâmico que requer acompanhamento contínuo para garantir sua efetividade e adaptação às mudanças no ambiente interno e externo do TJPE.

A implementação e o acompanhamento do PCN representam um investimento na resiliência do TJPE, garantindo sua capacidade de se adaptar e superar adversidades, assegurando a continuidade da prestação de serviços à sociedade pernambucana com excelência, justiça e celeridade.

O TJPE reitera seu compromisso com a sociedade pernambucana de fornecer serviços de justiça de qualidade, com eficiência e celeridade, mesmo em face de desafios e situações adversas. A implementação e o acompanhamento do PCN demonstram este compromisso e garantem que o TJPE continuará a ser um pilar fundamental para o estado de direito e a construção de uma sociedade mais justa e segura para todos.

Anexo A – Plano de Recuperação de Desastres

PLANO DE RECUPERAÇÃO DE DESASTRE DE TIC

PRD-TIC 2024

Data: *07/03/2024*

Versão 1.0

Plano de Recuperação de Desastres de Tecnologia da Informação e Comunicação no âmbito do Poder Judiciário do Estado de Pernambuco

Presidente do Tribunal de Justiça do Estado de Pernambuco (gestão 2024- 2026)
Desembargador Ricardo Paes Barreto

1° Vice-Presidente
Desembargador Fausto Campos

2° Vice-Presidente
Desembargador Eduardo Sertório

Corregedor-Geral da Justiça
Desembargador Francisco Bandeira de Melo

Secretaria de Tecnologia da Informação e Comunicação
Juliana Neiva de Gouvêa Ribeiro

Equipe Técnica na elaboração deste documento (servidores da SETIC)

Moisés Neves Camêlo
Marcelo Ferreira de Lima
Diego Augusto de Araújo Madeira

HISTÓRICO DE ALTERAÇÕES

Versão	Data	Autor(es)	Descrição
1.0	07/03/2024	AGSI – Assessoria de Gestão em Segurança da Informação	Criação do Documento
2.0	21/03/2024	AGSI – Assessoria de Gestão em Segurança da Informação	Criação do Processo de Recuperação de Desastres
3.0	16/04/2024	AGSI – Assessoria de Gestão em Segurança da Informação	1º teste de recuperação de desastre no banco de dados do PJe 1º grau.
4.0	10/05/2024	AGSI – Assessoria de Gestão em Segurança da Informação	2º teste de recuperação de desastre no banco de dados do PJe 1º grau. Validação do documento com a equipe da AGSI.
5.0	16/05/2024	AGSI – Assessoria de Gestão em Segurança da Informação	3º teste de recuperação de desastre no banco de dados do PJe 1º grau, levantar banco de dados após restauração, apontamento do ambiente de homologação e testes validação com equipe da DISIS

SUMÁRIO

TABELAS

FIGURAS

1. APRESENTAÇÃO

O Tribunal de Justiça de Pernambuco tem como missão primordial a entrega de uma prestação jurisdicional acessível, de qualidade e célere para toda a sociedade. Para alcançar esses objetivos, é indispensável contar com meios eficazes que garantam a operacionalidade dos processos judiciais. Nesse contexto, a Tecnologia da Informação emerge como uma ferramenta essencial para suportar os processos de negócios e atividades fim.

A Tecnologia da Informação (TIC) desempenha um papel importante no cumprimento da missão do Tribunal, fornecendo suporte às atividades judicantes. No entanto, a indisponibilidade ou interrupção desses serviços pode acarretar sérias consequências, como o descumprimento de prazos processuais, a falta de atendimento aos jurisdicionados, perda de dados e a necessidade de retrabalho.

Diante dessa realidade, faz-se necessário um plano estratégico que descreva os cenários de inoperância e os procedimentos planejados para lidar com tais eventualidades. Este plano tem como objetivo definir atividades prioritárias para restabelecer o nível de operação dos serviços no ambiente afetado dentro de um prazo tolerável.

Destaca-se que falhas nos serviços de TIC têm um impacto direto na continuidade da prestação da justiça. Portanto, este plano visa prover medidas de proteção rápidas e eficazes para os processos críticos de TI, especificamente relacionados ao banco de dados do Processo Judicial Eletrônico (PJe) do 1º grau, em casos de incidentes graves ou desastres.

Por meio da implementação deste plano, o Tribunal de Justiça de Pernambuco reafirma seu compromisso com a excelência na prestação jurisdicional, garantindo a continuidade dos serviços de Tecnologia da Informação e, consequentemente, o acesso à justiça de forma eficiente e eficaz para toda a sociedade.

Este documento está estruturado da seguinte forma:

- Objetivo e Escopo;
- Abreviações e Definições;
- Serviço Essencial;
- Principais Ameaças;
- Comunicação
- Papeis e Responsabilidades;
- Processo de Recuperação de Desastres;
- Estratégia de Recuperação de Desastres;
- Execução do Plano de Recuperação de Desastres;
- Protocolo de Revisão e Atualização do PRD

Diante disso, a recuperação dos serviços de TIC devem ser gerenciados de forma eficiente e eficaz. Este documento define o PRD que compõe o Plano de Continuidade de Negócio (PCN). O PRD deverá ser aplicado no âmbito da Secretaria de Tecnologia da Informação e Comunicação (SETIC).

A Resolução nº 370/2021 do CNJ, que estabelece a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD), para o período 2021 a 2026, dispõe no Art. 36 que "Cada órgão deverá elaborar Plano de Gestão de Continuidade de Negócios ou de Serviços no qual estabeleça estratégias e planos de ação que garantam o funcionamento dos serviços essenciais quando na ocorrência de falhas."

Nesse contexto, o presente plano contempla um conjunto de atividades que permitem identificar e implementar as medidas de proteção necessárias para restaurar o Banco de Dados do Sistema do Processo Judicial Eletrônico - PJE, contribuindo para o fortalecimento da governança de TIC, a tomada de decisões e o alcance dos objetivos institucionais.

2. OBJETIVO E ESCOPO

O objetivo primordial do PRD é garantir a continuidade dos serviços essenciais de TIC do Tribunal de Justiça de Pernambuco (TJPE) em níveis aceitáveis durante incidentes de segurança da informação. O escopo limita-se ao Banco de Dados do Sistema Processo Judicial Eletrônico (PJe) do 1º Grau. Portanto, qualquer outro cenário que não implique na necessidade da restauração do backup frio do banco de dados do PJe não está coberto por este PRD.

Este PRD busca assegurar que a recuperação total dos serviços seja realizada dentro de prazos aceitáveis, minimizando assim os impactos negativos sobre a prestação jurisdicional. Dessa forma, ele proporciona um nível de resiliência dos serviços e sistemas de TIC diante de eventos que possam causar sua interrupção, contribuindo para a melhoria contínua da prestação jurisdicional.

O escopo do plano abrange todas as áreas da Secretaria de Tecnologia da Informação (SETIC) do TJPE, incluindo infraestrutura de TI, redes, segurança da informação, suporte técnico, desenvolvimento de sistemas, governança e gestão de TI e o Comitê Gestor do PJe. Isso garante que todas as operações críticas relacionadas ao PJe sejam abordadas de forma abrangente e integrada.

Portanto, o Plano de Recuperação e Desastre de TIC do TJPE desempenha um papel fundamental na proteção do Sistema de Processo Judicial Eletrônico - PJE e na garantia da continuidade da prestação jurisdicional, ao mesmo tempo em que promove a resiliência das operações do Tribunal frente a potenciais incidentes e desastres.

3. ABREVIAÇÕES E DEFINIÇÕES

ABREVIAÇÕES:

- **CNJ**: Conselho Nacional de Justiça
- **ENTIC-JUD**: Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário
- **PCSTIC**: Plano de Contratações de Solução de TIC
- **PCTIC**: Plano de Capacitação de TIC
- **PDTIC**: Plano Diretor de Tecnologia da Informação e Comunicação
- **PRD**: Plano de Recuperação e Desastre
- **PSI**: Política de Segurança da Informação
- **SEI**: Sistema Eletrônico de Informações
- **SIC**: Segurança da Informação e Comunicação
- **SETIC**: Secretaria de Tecnologia da Informação e Comunicação
- **TJPE**: Tribunal de Justiça de Pernambuco
- **TIC**: Tecnologia da Informação e Comunicação

DEFINIÇÕES:

Análise de Impacto no Negócio (BIA): processo de análise dos efeitos de uma interrupção nos serviços de uma organização;
Ameaça: causa potencial de um incidente indesejado, que possui potencial para comprometer ativos através de exploração de vulnerabilidades.

Apetite a risco: nível de risco que a instituição está disposta a aceitar para atingir os objetivos identificados no contexto analisado.

Ativos de TIC: qualquer elemento de valor para organização, seja tangível ou intangível, que esteja relacionado à Tecnologia da Informação e Comunicação.

Causa de Risco: razão que pode promover a ocorrência do risco.

CCC – Comitê de Crises Cibernéticas: comitê responsável por apoiar e implementar o Protocolo de Gerenciamento de Crises Cibernéticas.

CGTIC – Comitê de Governança de Tecnologia da Informação e Comunicação: comitê responsável por apoiar e orientar as iniciativas, projetos e investimentos em Tecnologia da Informação e Comunicação, observando a estratégia institucional, dentre outros.

CGESTIC – Comitê Gestor de Tecnologia da Informação e Comunicação: comitê responsável pelos planos táticos e operacionais, análise de demandas, acompanhamento da execução de planos, estabelecimento de indicadores operacionais, dentre outros.

CGSI – Comitê de Gestão de Segurança da Informação: comitê responsável por apreciar, assessorar e aprovar a implementação das ações de segurança da informação e garantir a implementação da Política de Segurança de Tecnologia da Informação.

Consequências: resultado de um evento que afeta os objetivos estabelecidos.

Escopo: é a soma total de todos os produtos do processo de trabalho e seus requisitos ou características.

Evento: incidente ou ocorrência originada a partir de fontes internas ou externas que afetem a implementação da estratégia ou a realização dos objetivos.

Fonte de Risco: elemento que, individualmente ou combinado, tem potencial para dar origem a um risco específico, podendo ou não estar sob controle.

Gestão da continuidade de negócios: processo de gestão que visa aumentar a resiliência da organização diante dos impactos decorrentes de ameaças, promovendo a capacidade de resposta aos mesmos;

Impacto: efeito da ocorrência do evento nos objetivos.

Interrupção máxima aceitável (MAO): tempo para que os impactos, decorrentes da interrupção de um serviço/fornecimento de produto, tornem-se inaceitáveis;

Nível de Risco: representação numérica da magnitude do risco, que é expressa pelo produto das variáveis "impacto" e "probabilidade".

Parte interessada (*Stakeholder*): pessoa ou organização que pode afetar, ser afetada ou perceber-se afetada por uma decisão ou atividade.

Plano de Contingência: documento que apresenta detalhadamente os procedimentos e recursos a serem utilizados em caso de ocorrência de eventos que possam afetar a segurança de pessoas, do patrimônio ou de sistemas de informação, bem como outros que possam interromper a continuidade da prestação de serviços jurisdicionais.

Plano de Continuidade Operacional (PCO): procedimento documentado que orienta as organizações a responder, recuperar e restaurar os seus serviços para um nível de operação mínimo após a ocorrência de uma interrupção;

Plano de Recuperação de Desastre (PRD): procedimento documentado que orienta as organizações a responder, recuperar e restaurar os seus serviços para um nível normal de operação após a ocorrência de uma interrupção;

Plano de Administração de Crise (PAC): procedimento documentado que orienta a organização durante uma crise, estabelecendo os papéis e seus responsáveis, bem como a comunicação entre os seus atores;

Plano de Continuidade de Negócios (PCN): plano composto pelos três planos acima, dedicados aos processos de negócio essenciais da instituição;

Plano de Continuidade de TIC (PCTIC): subconjunto do plano acima dedicado aos serviços de TIC que suportam os processos de negócio essenciais da instituição;

Procedimento de Teste: Procedimento a ser seguido para a execução de teste ou ensaio de planos de administração de crise, continuidade operacional e/ou de recuperação de desastre;

Probabilidade: possibilidade de ocorrência do evento.

Ponto objetivado de recuperação (RPO): ponto em uma linha de tempo em que os dados devem ser recuperados após a ocorrência de uma ruptura;

Relatório de Incidente de Segurança da Informação (RISI): Relatório contendo as informações sobre incidentes de segurança da informação.

Resiliência: poder de recuperação ou capacidade de uma organização resistir aos efeitos de um desastre.

Risco: evento capaz de afetar positiva ou negativamente os objetivos e metas do Poder Judiciário do Estado de Pernambuco.

Risco-Chave: risco com elevado impacto nos objetivos da instituição.

Risco Inerente: é aquele ao qual a instituição está exposta, considerando os controles existentes, mas quando não são estabelecidos nem adotados tratamentos para alterar a probabilidade ou o impacto dos eventos.

Risco Residual: risco remanescente após estabelecimento e adoção de tratamento.

Serviço de TIC: serviço baseado no uso da Tecnologia da Informação provido a um ou mais clientes para apoiar os processos de negócio da instituição;

Tempo objetivado de recuperação (RTO): período de tempo em que os níveis mínimos dos serviços devem ser recuperados após a ocorrência de uma interrupção;

4. SERVIÇO ESSENCIAL

São os seguintes serviços considerados essenciais no ecossistema do Sistema do Processo Judicial Eletrônico - PJE, para o acionamento e execução deste plano em caso de recuperação e desastre.

Serviço	Finalidade	Criticidade[1]	RPO[4]	RTO[3]	Impacto[2]			
					Financeiro	Legal	Imagem	Operacional
PJe Usuário	Acesso ao PJe por usuários internos e externos	Alta	1 (uma) hora	15 horas	Indefinido	Alto	Alto	Alto
PJe Integração Ajuizamento	Integração do Ajuizamento Eletrônico ao PJe	Alta	1 (uma) hora	15 horas	Indefinido	Alto	Alto	Alto
PJe Integração	Integração das Procuradorias e outros órgãos ao PJe	Alta	1 (uma) hora	15 horas	Indefinido	Alto	Alto	Alto
PJe Debug	Utilizado para a realização de publicação de fluxos	Alta	1 (uma) hora	15 horas	Indefinido	Alto	Alto	Alto
PJe Agendamento	Utilizado para execução de jobs do quartz	Alta	1 (uma) hora	15 horas	Indefinido	Alto	Alto	Alto

Tabela 1 – Serviços Essenciais ao PJE

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 desastre.

Considerando os tempos de backup, o backup full ocorre entre 8 e 9 horas uma vez por semana e incrementado em de hora e hora, que custa em entre 1 e três minutos e quarenta segundos o Backups full fica guardado no disco por 7 dias e 30 dias um ciclo.

5. PRINCIPAIS AMEAÇAS

Este documento estratégico visa identificar e mitigar os riscos que podem comprometer a operação eficaz dos sistemas e serviços de Tecnologia da Informação (TI), abrangendo ameaças intencionais ou não intencionais, humanas ou da natureza, que possam afetar o banco de dados do PJe e cujas contingências existentes não sejam suficientes para o restabelecimento do serviço, exigindo a restauração do banco de dados por meio do backup frio.

As ameaças que podem causar dano ao backup implicando na necessária recuperação por meio do backup frio atuam de forma a comprometer ou corromper logicamente a estrutura ou dados do banco de dados de PJe, eventualmente fazendo com que tais comprometimentos e corrupções sejam refletidos inclusive em cópias mantidas por meio de estratégias de espelhamento. São exemplos: softwares maliciosos que podem atuar nas mais diversas camadas da solução, interação direta humana intencional para causar distorção nos dados do banco de dados, interação humana não intencional que leve a corrupção de dados, condições de falhas no sistema não foram endereçadas nos testes de desenvolvimento e introduzem distorções nos dados, etc.

6. COMUNICAÇÃO

Para fins de execução deste plano, a SETIC seguirá o plano de comunicação estabelecido no PCN, devendo manter suas equipes e partes interessadas informadas sobre a situação atual, os impactos nas operações e as medidas em andamento para mitigar os efeitos da interrupção.

Para fins de comunicação interna da SETIC, cujo fluxo não esteja contemplado no PCN deve-se utilizar a matriz de contatos abaixo. A comunicação deve ocorrer por aplicativos de mensagens e outras ferramentas institucionais de comunicação:

Nome	Cargo	Equipe
Juliana Neiva de Gouveia Ribeiro	Secretária de TIC	SETIC
Raphael José Dcastro	Secretário Adjunto de TIC	SETIC
Marcelo Ferreira de Lima	Assessor de Gestão em Segurança da informação	AGSI
Felipe Simão Henriques de Araújo	Diretoria de Operações de TIC	DIOP
João Tiago Ferreira Soares Pessoa	Diretoria de Sistemas	DISIS
Arthur Vasconcelos Lins	Diretoria de Suporte Técnico de TIC	DIST
Saulo José de Araújo Moreira	Secretário de Comunicação	ASCOM

Tabela 2 – Matriz de contatos

7. PAPEIS E RESPONSABILIDADES

As diretrizes, papéis e responsabilidades no que se refere a estrutura de tomada de decisão e as responsabilidades das partes envolvidas no Plano de Desastre e Recuperação de TIC são definidos da seguinte forma:

Papeis	Responsabilidades
Comitê de Gestão de Tecnologia da Informação e Comunicação da SETIC (CGESTIC-SETIC) G9	• 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; • Responsável por todas as comunicações durante o desastre. Especificamente, eles se comunicarão com servidores, clientes, autoridades, fornecedores e ASCOM; • Normatizar, fomentar e acompanhar a implementação e operação do processo de gestão de riscos de TIC, exceto de riscos de segurança da informação; • Deliberar sobre priorização de ações cuja necessidade resulte de planos de tratamento de riscos de TIC, exceto de riscos de segurança da informação.
Responsável	- Secretário (a) G9

Papeis	Responsabilidades
Assessoria de Gestão em Segurança da Informação (AGSI)	• 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; • Coordenar e monitorar a execução das atividades relativas ao plano de recuperação e desastres, relacionadas ao ambiente tecnológico da instituição; • Propor ações de sensibilização e capacitação em recuperação e desastre; • 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; •
Responsável	- Assessor de Gestão em Segurança da Informação

Papeis	Responsabilidades
Sala de Crise	• A Sala de Situação física deve ter isolamento acústico apropriado para garantir a reserva das reuniões e ser acessível apenas pelos integrantes que estão no plano de recuperação de desastres e aqueles cujo acesso foi autorizado previamente pelo G9; • A Sala de Situação virtual deve utilizar plataforma de comunicação institucional contratada pelo Tribunal de Justiça de Pernambuco, que garanta o sigilo da comunicação entre os integrantes por meio da Internet e deve permitir o controle dos que desejam ingressar e/ou permanecer na sala virtual; • Na utilização de sala virtual cada participante deverá tomar os devidos cuidados com a segurança do seu acesso remoto, o que inclui: o Estar em um local que não permita que outras pessoas ouçam as reuniões ou enxerguem a tela do seu dispositivo; o Não gravar reuniões sem a previa autorização; e o Desligar aplicativos, softwares e dispositivos desnecessários e que inadvertidamente possam capturar conteúdo em áudio;
Responsável	- Secretário (a) G9

Papeis	Responsabilidades
Equipe de Operações (DIOP)	• Fornecer aos servidores envolvidos no plano de desastre e recuperação as ferramentas de que necessitam para desempenhar suas funções da forma mais rápida e eficiente possível; • Eles precisarão provisionar todos os envolvidos a solução de contingência e aqueles que trabalham remotamente com as ferramentas específicas à sua atuação; • 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; • 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; • 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; • Assegurar e validar o desempenho das aplicações essenciais e podem ajudar outras equipes da SETIC conforme necessário;
Responsável	- Diretor da DIOP - Equipe de Data Center - Equipe de Banco de Dados

Papeis	Responsabilidades
Comitê de Crises Cibernéticas	• Levantar informações confirmadas, detalhadas e atualizadas sobre o incidente que gerou a crise com todas as áreas relevantes; • Elaborar e revisar estratégias e planos de comunicação interna e externa durante o ciclo da crise; • Elaborar plano de retorno à normalidade; • Identificar e descartar boatos acerca da crise; • Avaliar soluções no período de crise, considerando viabilidade e impactos; • Evitar o vazamento de informações tratadas pelo próprio Comitê sobre a crise classificando-as de acordo com grau de sigilo, sempre com fundamento na legalidade e objetivando a eficiente e efetiva superação da crise; • Observar a aplicação do Protocolos de Prevenção de Incidentes Cibernéticos e de Investigação de Ilícitos Cibernéticos nas decisões para o tratamento da crise; • Orientar adequadamente os envolvidos na resolução da crise quanto a estratégias e priorizações; e • Delimitar o que pode ser compartilhado e o procedimento a ser adotado para o compartilhamento de informações com outras entidades que também possam estar sob risco, com base na avaliação do incidente que originou a crise; • Aprovar solicitações de apoio a outros órgãos e pessoas, físicas e jurídicas, sem vínculo com Tribunal de Justiça de Pernambuco; • Aprovar o compartilhamento de informações com outras entidades, observadas as obrigações legais e normativas; • Aprovar comunicado ao Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos do Poder Judiciário (CPTRIC-PJ), órgão superior vinculado ao Conselho Nacional de Justiça. • Responsável por todas as comunicações durante o desastre. Especificamente, eles se comunicarão com servidores, clientes, autoridades, fornecedores e ASCOM;
Responsável	• Coordenador do Comitê de Crises Cibernéticas, que pode ser o Secretário(a) de Tecnologia da Informação e Comunicação (SETIC) ou o Assessor(a) de Gestão de Segurança da Informação da SETIC;

8. EXECUÇÃO DO PLANO DE RECUPERAÇÃO E DESASTRE (PRD)

A etapa de execução de um plano de recuperação e desastre de Tecnologia da Informação (TIC) é um passo fundamental na garantia da continuidade operacional e na mitigação de potenciais impactos adversos sobre os serviços essenciais do TJPE. Este processo estratégico visa restabelecer rapidamente as operações do PJe após a ocorrência de incidentes graves, conforme citado na sessão 5 deste documento.

São atividades PRD:

- Identificar a ocorrência de desastre que afete a base de dados do PJe 1º grau;
- Comunicar as partes interessadas;
- Elaborar cronograma de recuperação;
    - O coordenador da crise 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
- Avaliar os danos causado no Banco de Dados do Pje 1º grau;
    - As equipes de UGDC (Unidade de Gestão do Data Center) e UBD (Unidade de Banco de Dados) deverão identificar e listar todos os ativos danificados da ocorrência do desastre.
- Restaurar o backup dentro do prazo tolerável;
    - 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;
  - Ou por equipe designada pelo coordenador de crises.
- Restabelecer o PJe;
- Apresentar resultados e lições aprendidas.

Esta seção foi apresentada uma visão geral da execução do PRD e na seção 9 abordará o processo detalhado de recuperação e desastre para o banco de dados do PJe, com seu fluxo de atividades, atores, responsabilidades e artefatos.

9. PROCESSO DE RECUPERAÇÃO E DESASTRE PARA BANCO DE DADOS DO PJE

Esta seção tem o objetivo de apresentar o conjunto de estratégias e procedimentos, definidos e detalhados no processo de recuperação de desastres de TIC visando o banco de dados do PJe 1º grau. Conforme ilustrado na Figura 1 e no Apêndice B.

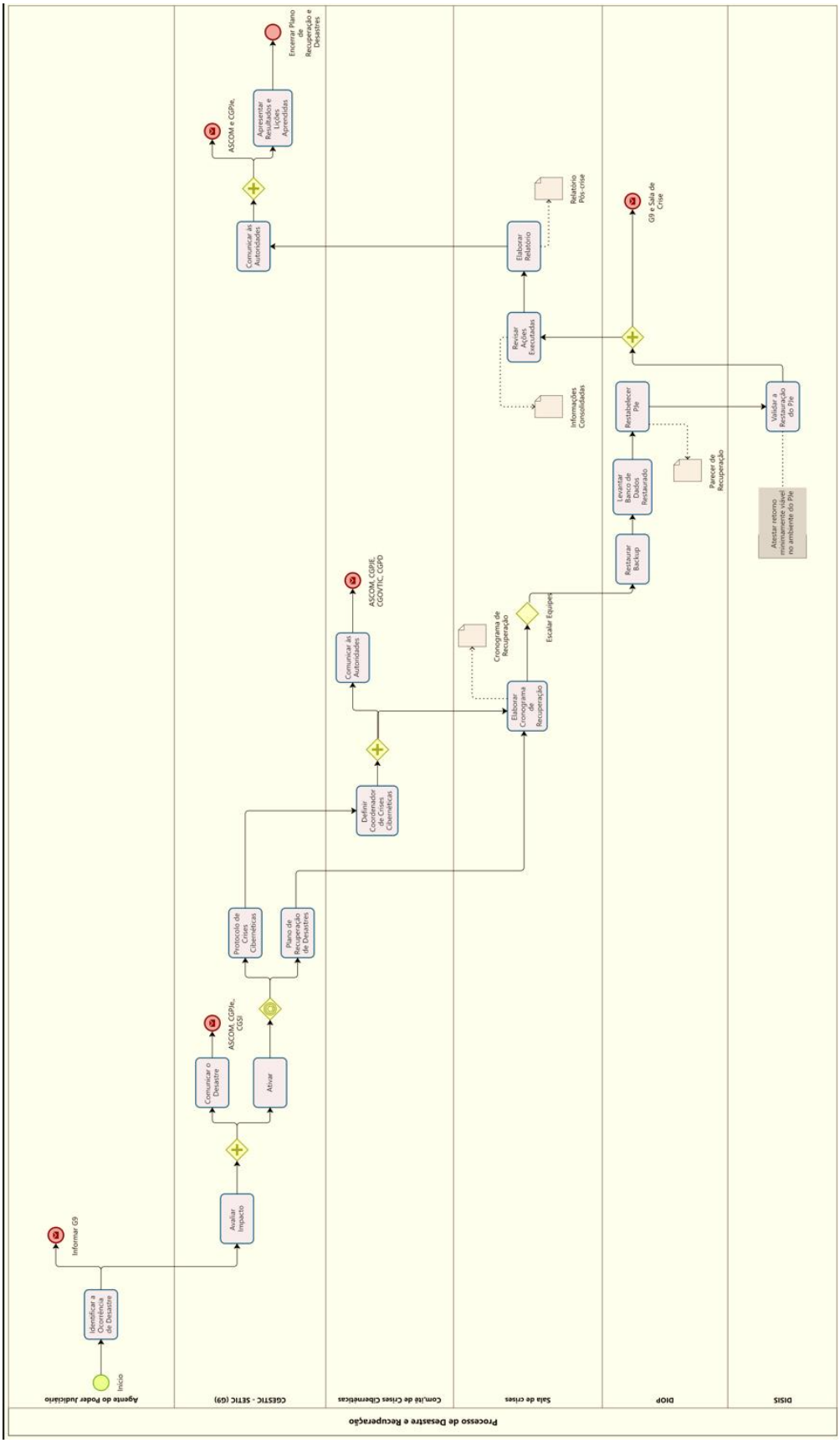


Figura 1 - Fluxo do Processo de Recuperação de Desastres de TIC

9.1. Descritivo do processo do Plano de Recuperação de Desastres

Atividade: Identificar a Ocorrência de Desastre	
Objetivo	Identificar a ocorrência de desastre, informar ao CGESTIC (G9) para avaliar o impacto, comunicar às autoridades e direcionar as atividades.
Responsável	Agente do Poder Judiciário
Entradas	- Indisponibilidade do PJe; - Alertas de Segurança da Informação (ataques cibernéticos);
Saídas	- CGESTIC (G9) avaliar o impacto.
Descrição	Uma ocorrência de desastre está relacionada a perda ou interrupção no Banco de Dados do PJe, que pode ocorrer devido a ataques cibernéticos, falhas de equipamentos computacionais ou utilização das tecnologias sem conhecimento, sendo uma falha ocasionada pela operação humana. A comunicação deverá ser feita pelos canais de comunicação informados neste plano (e-mail e telefone).

Atividade: Avaliar Impacto	
Objetivo	Esta atividade corresponde, basicamente, à realização de uma Análise de Impacto que a parada do PJe pode causar no TJPE, esse dimensionamento foi mapeado nos testes de recuperação de desastres apresentado na sessão 10 deste documento, como também, pode ser extraída do *BIA (*Business Analisys Impact*), verificar Apêndice C, em que utiliza os dados provenientes de análises de riscos realizadas anteriormente. É importante que representantes do negócio contribuam para a identificação dos impactos e prazos aceitáveis.
Responsável	- CGESTIC (G9)
Entradas	- BIA;
Saídas	- Ativar Plano de Recuperação de Desastres - Ativar Protocolo de Crises Cibernéticas.
Descrição	Avaliar o impacto causado por indisponibilidade na base de dados do PJe, mapear procedimentos e os requisitos para recuperá-los em um prazo aceitável para o TJPE, de acordo com o nível de criticidade de cada um. Para tal, são identificados os eventos potenciais e os prováveis impactos sobre a Tribunal, os processos afetados e os critérios que serão usados para quantificar e qualificar esses impactos. Considerando os riscos reconhecidos, tempo e ponto objetivados de recuperação (RTO e RPO), e os requisitos tecnológicos.

*Existe um BIA que elaborado no ano de 2012, mas que não retrata a realidade atual do cenário do PJe e que precisa ser refeito.

Atividade: Comunicar às Autoridades	
Objetivo	Identificar quais são as necessidades comunicativas dos interessados e definir a maneira mais apropriada para que a sua distribuição ocorra.
Responsável	- CGESTIC (G9)
Entradas	- Informações da natureza, magnitude e impacto do desastre.
Saídas	- Utilizar os canais oficiais de comunicação da instituição (e-mail, MS Teams, telefone).
Descrição	A comunicação deve ser regular, fornecendo atualizações frequentes e transparentes. Além disso, é fundamental compartilhar informações sobre as necessidades adicionais, como recursos ou assistência específica, para que a SETIC possa oferecer suporte adequado.

Atividade: Ativar Atividades de Crises	
Objetivo	O protocolo deverá ser ativado no caso de evento adverso na base de dados do PJe. Abrangendo ameaças intencionais ou não intencionais, humanas ou da natureza, que possam afetar o banco de dados do PJe e cujas contingências existentes não sejam suficientes para o restabelecimento do serviço, exigindo a restauração do banco de dados
Responsável	- CGESTIC (G9)
Entradas	- BIA
Saídas	- Definir coordenador e sala da crise;
Descrição	– Levantar informações confirmadas, detalhadas e atualizadas sobre o incidente que gerou a crise com todas as áreas relevantes; – Elaborar e revisar estratégias e planos de comunicação interna e externa durante o ciclo da crise; – Elaborar plano de retorno à normalidade; – Identificar e descartar boatos acerca da crise; – Avaliar soluções no período de crise, considerando viabilidade e impactos; – Evitar o vazamento de informações tratadas pelo próprio Comitê sobre a crise classificando-as de acordo com grau de sigilo, sempre com fundamento na legalidade e objetivando a eficiente e efetiva superação da crise; – Observar a aplicação do Protocolos de Prevenção de Incidentes Cibernéticos e de Investigação de Ilícitos Cibernéticos nas decisões para o tratamento da crise; – Orientar adequadamente os envolvidos na resolução da crise quanto a estratégias e priorizações; e – Delimitar o que pode ser compartilhado e o procedimento a ser adotado para o compartilhamento de informações com outras entidades que também possam estar sob risco, com base na avaliação do incidente que originou a crise.

Atividade: Definir Coordenador	
Objetivo	Decidir sobre a ativação do plano de recuperação de desastres ou protocolo de crises cibernéticas, subsidiado com informações dos demais integrantes do G9 e com base nos critérios estabelecidos no plano e no protocolo.
Responsável	- Secretário (a) da SETIC
Entradas	- Ocorrência de impacto relevante sobre as atividades críticas do PJe; - Ocorrência de dano material grave ao TJPE; - Ocorrência de dano de imagem grave ao TJPE; - Interesse acentuado da mídia e população em geral sobre o incidente.
Saídas	- As ações de resposta ao incidente persistirão por longo período;
Descrição	– Decidir sobre a suspensão de serviços, processos de negócio e sistemas informatizados; – Indicar um porta-voz único para comunicações ao público, para evitar informações equivocadas ou imprecisas; – Aprovar o conteúdo das comunicações, independentemente do formato e do meio, de maneira tempestiva e eficiente; – Aprovar solicitações de apoio a outros órgãos e pessoas, físicas e jurídicas, sem vínculo com Tribunal de Justiça de Pernambuco; – Aprovar o compartilhamento de informações com outras entidades, observadas as obrigações legais e normativas; e – Aprovar comunicado ao Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos do Poder Judiciário (CPTRIC-PJ), órgão superior vinculado ao Conselho Nacional de Justiça; e – Determinar o espaço físico e virtual que serão utilizados como Sala de Situação.

Atividade: Elaborar Cronograma de Recuperação	
Objetivo	O coordenador da crise, após o mapeamento das perdas e impactos elaborará um breve cronograma de recuperação das aplicações levando em consideração o RTO definido e a força de trabalho disponível.
Responsável	- Coordenador de Crises Cibernéticas
Entradas	- RTO e RPO
Saídas	- Cronograma de Recuperação
Descrição	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. E o documento do cronograma de recuperação será encaminhado para as equipes que executarão o contingenciamento.

Atividade: Restaurar Backup	
Objetivo	Proceder a recuperação dos dados para as aplicações, seja do storage ou fitas de backup.
Responsável	- Equipe Data Center (UGDC-DIOP)
Entradas	- Backup mais recente
Saídas	- Job de restauração de backup concluído com sucesso
Descrição	- 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. - Identificar jobs de backup cujos dados em questão foram afetados. - Estimar volume de dados a serem recuperados, tempo de recuperação dos dados e possíveis perdas operacionais - Priorizar a recuperação da base de dados para restabelecer o serviço do PJe.

Atividade: Levantar Banco de Dados Restaurado	
Objetivo	Subir o banco de dados do PJe 1º no local que foi restaurando após o desastre.
Responsável	- Equipe de Banco de Dados;
Entradas	- Script para subir BD
Saídas	- Disponibilizar BD
Descrição	- Restaurar timeout de statement para o PJe 1º; - Reiniciar banco; - Executar vaccum full na base de produção PJe 1º; - Habilitar rotina do CRON; ~Habilitar bouncer; - E disponibilizar o banco de dados do PJe 1º para equipe de gestão de aplicações (GEDAI), que fará a operação de apontar a aplicação do PJe 1º para a base restaurada.

Atividade: Restabelecer PJe	
Objetivo	Apontar aplicação de produção do PJe para base restaurada.
Responsável	- GEDAI
Entradas	- Start da aplicação PJe produção 1º grau
Saídas	- Disponibilizar para testes de validação
Descrição	Disponibilizar para equipe UNJPe efetuar os testes de validação.

Atividade: Validar a Restauração do PJe	
Objetivo	Atestar retorno do funcionamento do ambiente principal do PJe, com o objetivo de deixá-lo minimamente operacional e o retorna das atividades básicas.
Responsável	- UNJPe (DISIS)
Entradas	- Teste no ambiente de produção
Saídas	- Comunicar ao G9 e sala de crise
Descrição	Ao término do procedimento de recuperação e restabelecimento do PJe, as informações serão consolidadas em parecer específico informando horário de restabelecimento do serviço.

Atividade: Revisar Ações Executadas	
Objetivo	Validar ações executadas para recuperação do desastre, com o objetivo de revisar o RTO e RPO a fim de garantir que o processo de melhoria continuada de recuperação.
Responsável	Coordenador de Crises
Entradas	- Parecer informando horário e procedimentos de recuperação - RTO e RPO
Saídas	- Informações consolidadas
Descrição	Consolidar todas as informação desde a origem do desastre, execução e fim do PRD.

Atividade: Elaborar Relatório	
Objetivo	Elaborar relatórios de tratamento sobre os incidentes ocorridos e encaminhar para a CGESTIC (G9).
Responsável	- Comitê de Crises - Assessor em Gestão da Segurança da Informação
Entradas	- Informações consolidadas
Saídas	- Relatório Pós-crise
Descrição	Manter os registros, histórico dos incidentes e dos acionamentos das atividades e os seus resultados. Caso o CGESTIC não esteja de acordo com os dados contidos no relatório, será necessário refazer a análise.

Atividade: Apresentar Resultados e Lições Aprendidas	
Objetivo	Prover informações as partes interessadas, a respeito dos resultados e as lições aprendidas na recuperação de desastre.
Responsável	- CGESTIC (G9)
Entradas	- Relatório Pós-crise
Saídas	- Encerrar o plano
Descrição	Revisar e ajustar o plano de recuperação de desastres conforme as lições aprendidas, a fim de garantir que o processo de recuperação ocorra conforme o planejado.

10. PROTOCOLO DE REVISÃO, ATUALIZAÇÃO PERIÓDICA DO PLANO E SIMULAÇÃO DE DESASTRE

Este plano deve ser revisado anualmente, ou sempre que houver mudanças significativas no ambiente do Sistema de Processo Judicial Eletrônico que possam afetar a viabilidade deste PRD, ou nas situações em que novos riscos sejam identificados.

Caberá ao Secretário (a) do CGESTIC (G9) e ao Assessoria de Gestão em Segurança da Informação (AGSI) proceder com a revisão e atualização do PRD, que deverá envolver também as equipes envolvidas que tenham a necessidade de aderir a novos requisitos de conformidade.

As reuniões de revisão do PRD devem ter registros em ATA dos seus principais pontos discutidos, decisões tomadas e ações acordadas, de forma que possam ser utilizadas como evidência para atendimento dos requisitos de melhoria contínua, auxiliando na gestão adequada do processo de revisão e atualização do PRD.

O protocolo de revisão e atualização periódica do PRD deve ser acompanhado dos resultados do exercício do plano de testes de backup, com o objetivo de identificar lacunas, ajustar ações e procedimentos conforma necessário e garantir a prontidão da equipe em caso de interrupção real. Os exercícios devem ser realistas e abrangentes, envolvendo todos os níveis do TJPE/SETIC e abordando diferentes cenários de interrupção no âmbito dos serviços prestados pela SETIC.

As alterações e atualizações realizadas neste documento devem ser registradas utilizando procedimentos adequados de controle de alterações, de forma a manter a integridade e versionamento de todas as alterações efetuadas no PRD.

Como também, os testes que simulam a recuperação de desastres de TIC, no âmbito da base de dados do PJe do 1º grau, conforme apresentado na Tabela 2, com o objetivo de garantir os mesmos níveis de capacidade e disponibilidade dos serviços essenciais antes do desastre, analisar o resultado dos testes e da avaliação dos incidentes críticos e testar os procedimentos, a fim de registrar oportunidade de melhoria tanto na recuperação de desastre, quanto aos documentos em vigor, para serem implementados no próximo ciclo.

Data	Tipo *1	Motivo	Status *2
16/04/2024	Simulação	Com objetivo de simular a recuperação após desastre, o primeiro teste apresentou falha na finalização da recuperação.	Executada com Falha
03/05/2024	Simulação	Com objetivo de simular a recuperação após desastre, pois no último teste falhou no final. O segundo teste houve falha por falta de espaço necessário.	Executada com Falha
14/05/2024	Simulação	Com objetivo de simular a recuperação após desastre, o terceiro teste foi executado com sucesso e sem falhas. Será necessário efetuar mais testes para verificar o crescimento dos *archives*. A equipe de Banco de Dados fará a validação da restauração.	Executada com Sucesso
15/05/2024	Simulação	Após a recuperação do banco de dados do PJe, a equipe gestora dos bancos de dados da SETIC informou que durou **9 horas** para levantar a base recuperada. Próximo passo será apontar o ambiente de homologação do PJe, para a base recuperada.	Executada com Sucesso
23/05/2024	Simulação	Em seguida foi necessário a equipe de gestora das aplicações (GEDAI) apontarem o ambiente de homologação do PJe para a base recuperada.	Executada com Sucesso
30/05/2024	Simulação	Por fim a equipe da UNJPe da DISIS efetuou os testes de validação da base de dados recuperado. Os testes validaram que restauração do backup após a simulação de desastre, foram executados com sucesso e sem falhas.	Executada com Sucesso

Tabela 3 – Controle de Revisão e Atualizações

*1 Teste de mesa; Caminho percorrido; Simulação

*2 Programado; Executado; Planejado; Agendado

Diante dos testes de simulação apresentado na **Tabela 2**, considerando o **RPO (*Recovery Point Objective*)** que tenha perda de dados e informações, o período mínimo necessário para recuperação das informações armazenadas na base de dados do PJe em cópias de segurança de retornar as atividades do processo, será de um período de aproximadamente **5 horas** e **46 minutos** e de um espaço em disco de 12,5TB para alocar os dados.

E será considerado a métrica de **RTO (*Recovery Time Objective*)** de **16 horas**, para o tempo máximo que o PJe retorne as suas operações minimamente aceitáveis.

A versão _____ do PRD fica aprovada em __/__/__ por deliberação das partes envolvidas.

_____

Secretário (a) de Tecnologia da Informação e Comunicação

_____

Assessoria de Gestão em Segurança da Informação

11. CONSIDERAÇÕES FINAIS

Este plano e suas subsequentes atualizações devem ser aprovados pelo G9 e pelo Comitê de Crises Cibernéticas. Posteriormente deve ser publicada em local de fácil acesso para todos e distribuída para todas as partes interessadas da SETIC. Este documento é versão pública deste que passou por revisão para supressão de informações consideradas sensíveis (ex.: nomes de servidores, bases de dados, etc.). Mas a versão de circulação interna do documento conta com todas as informações tecnicamente relevantes para o Plano de Recuperação de Desastres.

A área da Tecnologia da Informação e Comunicação (TIC) se mostra cada vez mais estratégica para o Tribunal, e entender os riscos de TIC que podem afetar os objetivos institucionais é um caminho crucial para uma gestão de excelência e contribui para a tomada de decisão. Tais técnicas podem não ser suficientes para garantir que eventos negativos ocorram, no entanto, o domínio sobre estes eventos serve para reduzir a probabilidade que ocorram ou o impacto ao efetivamente ocorrerem.

Em suma, a adoção do Plano de Recuperação e Desastre de TIC é parte integrante positiva para a efetividade da gestão governamental.