

PCNTIC

Plano de Gestão de Continuidade de Negócios

2021

SUMÁRIO

Parte I – Generalidades

1. Introdução.....	03
2. Objetivo.....	05
3. Justificativa.....	05
4. Escopo.....	06
5. Conceitos e Definições.....	06

Parte II – Especificidades

6. Matriz de Serviços Essenciais do TJPA.....	09
7. Matriz de Ameaças.....	10
8. Matriz de responsabilidades.....	11
8.1. Matriz de Contatos.....	12
9. Fluxograma de Gerenciamento de desastres.....	13
10. Planos de Continuidade.....	14
10.1. PCO – Plano de Continuidade Operacional.....	14
10.2. PAC – Plano de Administração de Crises.....	15
10.3. PRD – Plano de Recuperação de Desastres.....	17
11. Matriz de Testes.....	19
12. Matriz de Aprovação.....	20

PARTE I – Generalidades

1. INTRODUÇÃO

O que é um Plano de Continuidade de Negócio?

É uma ferramenta de Gestão constituída por um documento no qual ficam definidas as estratégias a serem adotadas a fim de que se mantenha o **funcionamento das operações** de uma instituição, caso ela venha a enfrentar intempéries causadas por fatores internos ou externos à organização.

No documento em tela será elaborado um PCN para a Gestão de Tecnologia da Informação sob a tutela da Secretaria de Informática do Tribunal de Justiça do Estado do Pará.

Desta forma, pode-se dizer seguramente que o PCN é um **plano emergencial** que norteia a gestão de continuidade de negócio em situações não cotidianas que podem levar à solução de continuidade. Para o cenário considerado, tais situações, que variam da falta de energia elétrica a incêndios, passando por desastres naturais, ataques cibernéticos, panes de hardware e software entre outros "imprevistos", que têm como ponto em comum ferir os princípios CID (Confidencialidade, Integridade, Disponibilidade), pilares incontestes da segurança da informação.

O Plano de continuidade de negócio é composto pelos:

- Programa de Administração de Crise – PAC: Iniciado após detectada a crise. É voltado para o controle de todo o processo até que a operação retorne à normalidade;
- Plano de Continuidade Operacional – PCO: Acionado como primeiro procedimento do PAC, é voltado a recuperar a normalidade dos processos de negócio;
- Plano de Recuperação de Desastres – PRD: Acionado juntamente com o PCO. É focado na recuperação e restauração de componentes que suportam o PCN.

$$PCN = PAC + PCO + PRD$$

Qual objetivo de um Plano de Continuidade de Negócio?

O PCN, serve para nortear o trabalho dos gestores que buscam minimizar o impacto das intempéries operacionais (desastres) com segurança e eficiência de forma a reduzir ao máximo o impacto de tais situações na organização, evitando que as operações essenciais sejam interrompidas ou que operem de forma errônea. Assim sendo, o PCN deve orientar o gestor a fim de que, em caso de desastres, as operações críticas e essenciais não sejam interrompidas ou prejudicadas.

É fato que em tempos regulares previstos, ou no caso de uma mudança significativa no ambiente, o PCN precisa ser revisto e atualizado, de forma a espelhar a realidade existente na instituição.

Por que criar um Plano de Continuidade de Negócio

O PCN é fundamental para que a gestão de continuidade do negócio feita a partir dele assegure a resiliência organizacional, de forma que as operações não sejam interrompidas e que a normalidade seja estabelecida o mais breve possível.

Ademais, a Resolução Nº 370 de 28/01/2021, na sua Seção III - Dos Riscos, Segurança da Informação e Proteção de Dados, estabelece em seus artigos:

Art. 36. 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.

Art. 37. Cada órgão deverá elaborar Plano de Gestão de Riscos de TIC, com foco na continuidade de negócios, manutenção dos serviços e alinhado ao plano institucional de gestão de riscos, objetivando mitigar as ameaças mapeadas para atuar de forma preditiva e preventiva às possíveis incertezas.

Desta forma, o planejamento em questão visa atender à demanda supramencionada.

Como empregar e utilizar um Plano de Continuidade de Negócio?

Por meio do plano de continuidade de negócios (PCN), consegue-se, durante sua elaboração, identificar ameaças e riscos, prever cenários e situações que podem exercer impacto negativo sobre as operações da instituição.

Desta forma, na ocorrência de uma das intempéries identificadas no PCN, ou de outra que tenha consequências similares, é possível lidar com elas de maneira mais controlada, já que as ações estarão definidas e organizadas, de forma a serem executadas exigindo-se o mínimo de decisão, o que é uma boa prática em casos de crises como as enfrentadas durante a ocorrência de um desastre.

Quando criar e utilizar um Plano de Continuidade de Negócio?

Um PCN precisa ser elaborado antes da ocorrência do desastre. Nele se prevêem a ocorrência do desastre, suas consequências, e a forma de mitigá-lo, incluindo todos os recursos necessários para que a execução do PCN torne as operações afetadas à normalidade o mais rapidamente possível.

Por outro lado, estando atualizado o PCN e, no caso da ocorrência de um desastre, cumpre aos gestores tê-lo à mão para consultá-lo e assim aplicar suas recomendações, de forma a operacionalizar solução adequada que retorne à normalidade as operações de tecnologia da informação e comunicação do TJPA.

2. OBJETIVO

O presente Plano de Continuidade de Negócio, mapeará ameaças e os riscos que elas representam para o negócio do Tribunal de Justiça do Estado do Pará, através dos serviços de providos por tecnologia da informação e comunicação os quais são geridos pela Secretaria de Informática através de suas coordenações e chefias.

Após tal mapeamento serão descritos os PAC, PCO e PRD necessários para reestabelecer à normalidade a operação do negócio do TJPA.

3. JUSTIFICATIVA / MOTIVAÇÃO

Os serviços de tecnologia da informação e comunicação constituem-se hoje em ativos críticos para o negócio do Tribunal de Justiça do Estado do Pará, de forma que planejar formas de resguardar tais serviços e os dados que eles encerram, além de recuperá-los à normalidade no caso da ocorrência de desastres, é fator primordial para a sobrevivência desta casa, e dos serviços que ela presta à sociedade.

4. ESCOPO

O presente plano de continuidade de negócios foi elaborado para atender aos serviços atinentes à Secretaria de Informática - SECINFO do Tribunal de Justiça do Estado do Pará, estando intrinsecamente atrelado aos serviços e ativos sob a tutela desta unidade organizacional.

De uma forma geral, os itens a serem resguardados pelo PCN em questão são:

- *Serviços, incluindo os bancos de dados correspondentes:* Sistemas judiciais (ex: PJE e Libra), administrativos (MentorRH e GLPI, entre outros) e arrecadadores (tais como, custas judiciais);
- *Infraestrutura de Serviços:* Datacenters, servidores, configurações específicas de soluções proprietárias, infraestrutura de virtualização e sistema de backup;
- *Infraestrutura de comunicação:* Switches, roteadores e links de dados das redes LAN e Metro que compõe o sistema de comunicação do TJPA;
- *Segurança da Informação:* Sistemas de certificado digital, Firewall e WAF, análise de vulnerabilidades entre outros.

5. CONCEITOS E DEFINIÇÕES

A fim de que se compreenda em detalhes todas as especificações contidas neste PCN, há que se considerar a normatização dos termos nele utilizados, de forma a não deixar que haja ambiguidades na sua compreensão. Por este motivo, seguem definições adotadas neste documento na "Matriz de Conceitos e Definições":

Matriz de Conceitos e definições

Termo	Conceito ou Definição
atividade	Processo ou conjunto de processos executados pelo TJPA, que produzam ou suportem um ou mais produtos ou serviços.
atividade crítica	Atividade que deve ser executada de forma a garantir a consecução dos produtos e serviços fundamentais do TJPA, de tal forma que permita atingir os seus objetivos mais importantes e sensíveis ao tempo.
ativos de informação	Meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso.

continuidade dos serviços essenciais	Conjunto de práticas, procedimentos, processos, planos e ferramentas de trabalho que maximizam a possibilidade de que o órgão, dispondo de um sistema de gestão de continuidade documentado, mantenha o fornecimento dos serviços essenciais de TIC após a ocorrência de determinados cenários de desastre.
desastre	Evento repentino e não planejado que causa perda para todo ou parte do TJPA e gera sérios impactos em sua capacidade de entregar os serviços essenciais ou críticos por um período de tempo superior ao tempo objetivo de recuperação.
gestão de continuidade	Processo abrangente de gestão que identifica ameaças potenciais para uma organização e os possíveis impactos nas operações de negócio, caso elas se concretizem. Este processo fornece uma estrutura para que se desenvolva uma resiliência organizacional que seja capaz de responder efetivamente e salvaguardar os interesses das partes interessadas, a reputação e a imagem do Tribunal e suas atividades de valor agregado.
Grupo Funcional	Seção ou Assidência com papel e responsabilidades na execução de procedimentos descritos no PCN.
hot site	Tipo de estratégia na qual os aplicativos são balanceados e trabalham com servidores ativos nos dois data centers, ou seja, em caso de indisponibilidade do data center principal os usuários dos sistemas não percebem a interrupção.
Incidente	Qualquer evento suficientemente significativo, que possa causar a interrupção do negócio.
interrupção	Evento, previsível ou não, que cause um desvio negativo na entrega de produtos ou execução de serviços, de acordo com os objetivos do TJPA.
Plano de Continuidade Operacional (PCO)	documentação dos procedimentos e informações necessárias para que o Tribunal mantenha seus ativos de informação críticos e a continuidade de suas atividades críticas em um nível previamente definido, em casos de desastres.
Programa de Administração de Crise (PAC)	Plano de ação claramente definido e documentado, para ser usado quando ocorrer um incidente que basicamente cubra as principais pessoas, recursos, serviços e outras ações que sejam necessárias para implementar o processo de gerenciamento de incidentes de TIC.
Plano de Recuperação de Serviços de TIC	documentação dos procedimentos e informações necessárias para que o órgão operacionalize o retorno das atividades críticas de TIC à normalidade.
responsável pelo ativo	indivíduo legalmente instituído por sua posição e/ou cargo, responsável primário pela viabilidade e sobrevivência dos ativos de informação.
RTO	Recovery Time Objective: Tempo estabelecido para que um sistema seja recuperado de uma solução de continuidade.
RPO	Compreende o ponto de recuperação dos dados, ou seja, uma vez recuperada a solução, qual a quantidade de dados máxima que poderá ser perdida sem que o negócio seja afetado.
serviços essenciais	conjunto de ativos de informação que, por meio de integração e orquestração, entrega valor aos usuários e ao órgão, mediante recursos de TIC empregados. Os serviços essenciais estão divididos em negócio (área fim), infraestrutura e segurança da informação, (área de TIC e engenharia)
sistemas essenciais	sistemas de informação do TRT da 8a Região definidos como estratégicos e com alto impacto no negócio em caso de indisponibilidade.
criticidade	Representa o quão drástica é uma situação para o negócio do TJPA.

impacto	Desconformidade causada por um incidente ou desastre.
ameaça	Qualquer atividade maliciosa, intencional ou acidentalmente, seja através de meios eletrônicos ou não, que possa explorar uma vulnerabilidade e, assim, obter acesso, danificar ou destruir um determinado ativo ou serviço.
solução de continuidade	Interrupção de um serviço por falha em algum de seus componentes.

A matriz abaixo define numa escala de 3 pontos a intensidade percebida por atores envolvidos no processo e no item cuja intensidade se pretende dimensionar. A rigor esta escala trata da percepção dos envolvidos e, portanto, é até certo ponto, subjetiva.

Dependendo do contexto analisado, a grandeza pode representar uma percepção positiva, neutra ou negativa, em uma situação em que represente análise qualitativa ou ainda pode representar uma probabilidade quando se tratar uma análise quantitativa.

Matriz de escala de 3 pontos

Grandeza	Conceito ou Definição
Alto	Representa uma grandeza muito significativa no contexto analisado, de forma a se sobressair sobre demais pontos considerados no cenário analisado.
Médio	Representa uma grandeza ainda significativa, embora não seja tão intensa. É contudo, ainda bastante relevante no contexto analisado.
Baixo	Representa uma grandeza de pouco significado que, no entanto, ainda acarreta consequências perceptíveis no cenário analisado, embora seja de menor impacto.

PARTE II – Especificidades

6. MATRIZ DE SERVIÇOS ESSENCIAIS DO TJPA

As matrizes abaixo registram os serviços considerados essenciais no TJPA. Tais serviços são divididos por suas categorias: serviços de negócio, de infraestrutura, de segurança. As matrizes incluem perspectivas de criticidade e impacto e expectativas de RPO e RTO.

Matriz de Serviços essenciais de negócio

Serviço	Criticidade	RTO	RPO	Impacto			
				financeiro	legal	imagem	operacional
Judiciais	Alta	2 hs	Último backup válido	baixo	alto	alto	alto
Administrativos	Alta	4 hs	Último backup válido	médio	médio	médio	alto
Arrecadores	Alta	2 hs	Último backup válido	alto	alto	alto	alto

Matriz de Serviços essenciais de infraestrutura

Serviço	Criticidade	RTO	RPO	Impacto			
				financeiro	legal	imagem	operacional
Virtualização	Alta	2 hs	Último backup válido	Baixo	Baixo	Alto	Alto
Ambiente Devops	Alta	2 hs	Ambiente de contingência	Baixo	Baixo	Alto	Alto
Servidor de Aplicação	Alta	2 hs	Último backup válido	Baixo	Baixo	Alto	Alto
Serviços de Rede	Alta	2 hs	Último backup válido	Baixo	Baixo	Alto	Alto
Serviços de Storage	Alta	2 hs	Último backup válido	Baixo	Baixo	Alto	Alto
Serviços de Compute	Alta	2 hs	Ambiente de contingência	Baixo	Baixo	Alto	Alto
alto Serviços de Monitoramento	Alta	2 hs	Último backup válido	Baixo	Baixo	Alto	Alto
Datacenter	Alta	2 hs	Ambiente de contingência	Baixo	Baixo	Alto	Alto
Comunicação de Dados	Alta	2 hs	Ambiente de contingência	Baixo	Baixo	Alto	Alto

Matriz de Serviços essenciais de segurança da informação

Serviço	Criticidade	RTO	RPO	Impacto			
				financeiro	legal	imagem	operacional
Firewall	Alta	2 hs	Ambiente de Contingência	Médio	Baixo	Alto	Alto
WAF	Alta	2 hs	Ambiente de Contingência	Médio	Baixo	Alto	Alto
Segurança de endpoint	Alta	2 hs	Ambiente de Contingência	Médio	Baixo	Alto	Alto
Análise de vulnerabilidades	Alta	2 hs	Ambiente de Contingência	Médio	Baixo	Alto	Alto

7. MATRIZ DE AMEAÇAS

Evidencia eventos que podem ocorrer resultando na solução de continuidade, bem como as causas que podem levar a estes eventos.

Matriz de Ameaças

Ameaça	Probabilidade	Impacto para o negócio	Causa provável
Interrupção no fornecimento de Energia elétrica	baixa	alto	> fator externo: Concessionária de energia; > fatores internos: falta de combustível no gerador, manutenção inadequada nos circuitos elétricos, carga excessiva nos circuitos
Pane na infraestrutura de datacenter	baixo	alto	>Hardware ou software em pane;
Indisponibilidade de redes LAN ou Metro e Links	média	alto	> fator externo: rompimento de fibra; > Fator interno: Ativo de rede defeituoso
Falha Humana	média	alto	> Incidente ao manusear equipamentos ou software crítico.
Ataque cibernético interno	baixo	médio	> Ataque cibernético efetivado por servidor ou terceirizado com permissões de acesso aos ativos do TJPA.
Ataque cibernético externo (incluindo ransomware)	alto	alto	> Ataque cibernético efetivado por elemento externo ao TJPA, sem prévias permissões de acesso.
Incêndio	baixo	alto	> Incêndios que comprometam serviços de TIC
Desastres Naturais	baixo	alto	> Alagamentos, raios, terremotos, etc.

8. MATRIZ DE RESPONSABILIDADES

Define a responsabilidade das equipes e seus líderes quanto à execução de itens deste plano. Assim, “um desastre representa a ocorrência de um item previsto na matriz de ameaças, o qual afeta um dos itens da matriz de serviços essenciais, que deve estar sob a responsabilidade de uma equipe, a qual executará os procedimentos elencados no PCN para a ocorrência em questão”.

Matriz de Responsabilidades

Equipe	Responsabilidade
COMITÊ DE DESASTRE/RECUPERAÇÃO/COMUNICAÇÃO (CDR)	<p>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.</p> <p>Inclui autoridades em nível institucional e tomadores de decisão da SECINFO</p> <p>Responsável por todas as comunicações durante um desastre. Especificamente, eles se comunicarão com os funcionários, clientes, autoridades, fornecedores e até mesmo com a mídia, se necessário.</p> <ul style="list-style-type: none"> • O líder desta equipe administrará e manterá o Plano de Administração de Crise. • O Comitê CDR será composto pelos mesmos integrantes do CGTI.
Coordenadoria de Suporte Técnico	<p>O líder desta equipe administrará e manterá o Plano de Recuperação de Desastre.</p>
SSSB (Infraestrutura, aplicações, backup)	<p>Responsável pelas instalações físicas que abrigam sistemas de TIC e pela garantia que as instalações de alternativa são mantidas adequadamente. Avalia os danos e supervisiona os reparos.</p> <p>Fornecer infraestrutura de servidor físico e virtuais necessária para que a TI execute suas operações e processos essenciais durante um desastre.</p> <p>Garantir que as aplicações essenciais funcionem como exigido para atender aos objetivos de negócios em caso de e durante um desastre. Eles serão os principais responsáveis por assegurar e validar o desempenho das aplicações essenciais e podem ajudar outras equipes de TIC CDR conforme necessário.</p> <p>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.</p> <p>> O líder desta equipe irá liderar os PCO relacionados a estes itens.</p>
Divisão de Banco de Dados	<p>Responsável pelas configurações e manutenções dos ambientes de bancos de dados, incluindo execução e recuperação dos backups.</p> <p>> O líder desta equipe irá liderar os PCO relacionados exclusivamente a bancos de dados.</p>

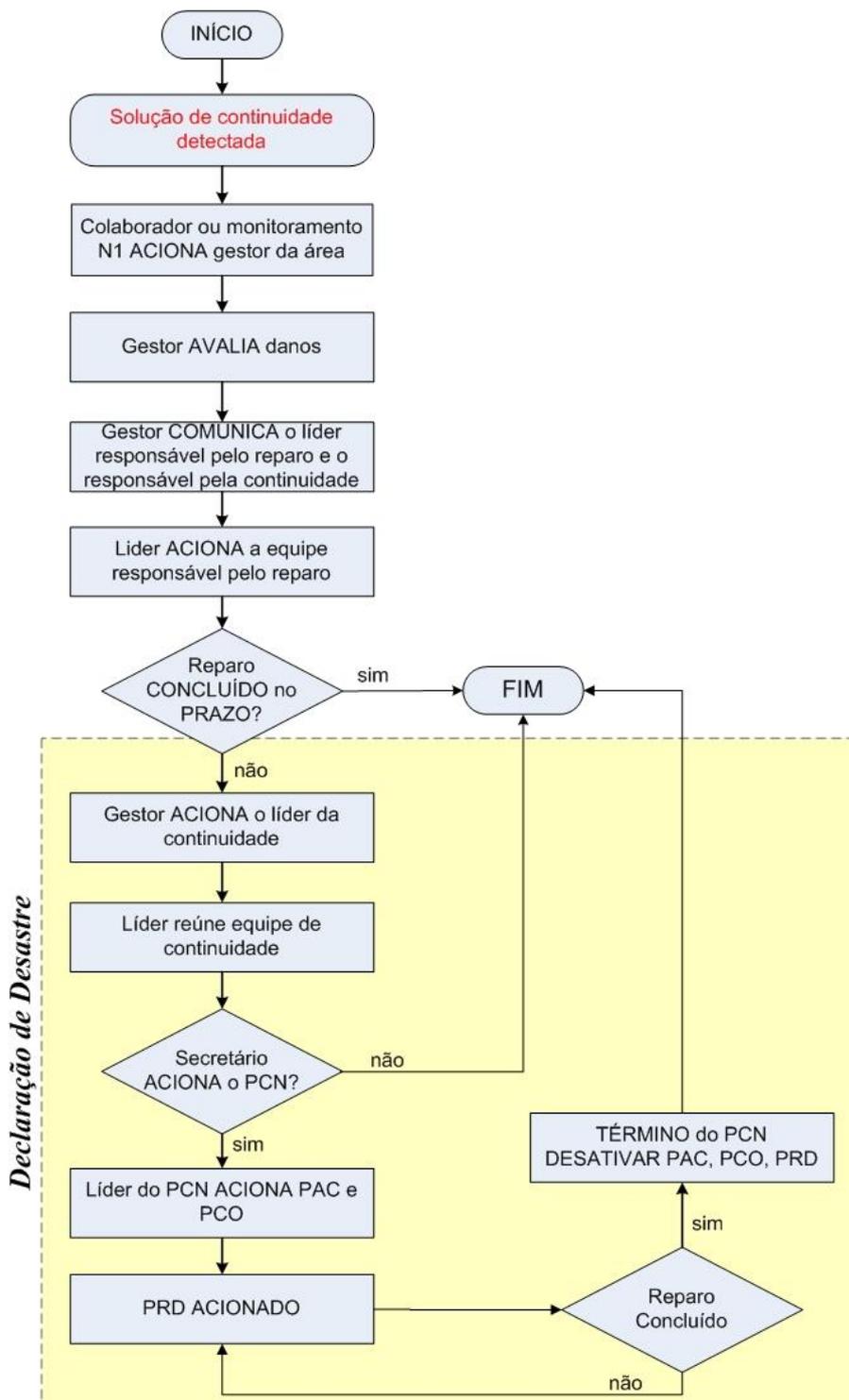
Serviço de Infraestrutura de Redes	Avaliar os danos específicos de qualquer infraestrutura de rede e para fornecer dados e conectividade de rede, incluindo WAN, LAN ou de infraestrutura externa junto aos prestadores de serviço. > O líder desta equipe irá liderar os PCO relacionados exclusivamente à comunicação de dados.
Segurança da Informação	Responsável por ativos que provêm o controle de acesso a sistemas e a comunicação de dados. > O líder desta equipe irá liderar os PCO relacionados exclusivamente à segurança da informação

8.1. Matriz de Contatos

Matriz de Contatos

Equipe	Cargo	Pessoa	E-mail
Coordenadoria de Suporte Técnico	Coordenador CST	Arlson Silva	arilson.silva@tjpa.jus.br
SSSB (Infraestrutura, aplicações, backup)	Chefe do SSSB	Paulo Lourinho	paulo.lourinho@tjpa.jus.br
DBD (Divisão de Banco de Dados)	Chefe da DBD	Thalles Lima	thalles.lima@tjpa.jus.br
SIR (Serviço de Infraestrutura de Redes)	Chefe do SIR	Denison Soares	denison.soares@tjpa.jus.br
Segurança da Informação	Líder Técnico	Thiago de Castro	thiago.rosario@tjpa.jus.br

9. FLUXOGRAMA DE GERENCIAMENTO DE DESASTRES



10. PLANOS DE CONTINUIDADE

10.1. PCO - Plano de Continuidade Operacional

Este plano descreve os cenários de inoperância e seus respectivos procedimentos alternativos planejados, definindo as atividades prioritárias para garantir a continuidade dos serviços essenciais.

ESCOPO: É escopo deste plano garantir ações de continuidade durante e depois da ocorrência de uma crise ou cenário de desastre tratando-se apenas das ações de contingência definidas na estratégia.

OBJETIVOS:

- Prover meios para manter o funcionamento dos principais serviços de TIC e a continuidade das operações de TI, dos sistemas essenciais;
- Estabelecer procedimentos, controles e regras alternativas que possibilitem a continuidade das operações de TI durante uma crise ou cenário de desastre;
- Estabelecer uma equipe para cada plano PCO, PRD e PAC;
- Definir os formulários, checklists e relatórios a serem entregues pelas equipes ao executar a contingência;

GESTÃO: A CST é a unidade responsável por implementar, manter e melhorar o PCO e toda documentação inerente.

EXECUÇÃO DO PCO: Avaliação de Impacto de Desastre: Identificada a ocorrência de um incidente ou crise e o Líder da Equipe competente deve verificar a dimensão do impacto, extensão e possíveis desdobramentos do ocorrido.

- Divulgar a informação a todas as equipes envolvidas.
- Acionamento do plano

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

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

AÇÕES DE CONTINGÊNCIA: Devem ser adotadas para cada processo ou serviço essencial.

Matriz de ação de Contingência

Instrução	Duração	Observação	Resultado
Verificar status da aplicação de backup e estimar impacto de perda dados (janela)			
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			
Atestar retorno do funcionamento do ambiente principal com Líder do PRD			
Teste de aplicação de backup após desastre			
Validar políticas de backup implementadas			

ENCERRAMENTO DO PCO: Uma vez validado o funcionamento do retorno dos sistemas essenciais e estabilidade do datacenter deverá ser emitido um parecer relatando as atividades realizadas neste PCO.

- Informar à equipe de CDR o retorno das atividades.

10.2. PAC – Programa de Administração de Crise

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

ESCOPO: Comunicação e gerenciamento de crises, viabilizando uma compreensão linear a todos os envolvidos das ações antes, durante e após a ocorrência de um desastre.

OBJETIVOS:

- Garantir a segurança à vida das pessoas;
- Minimizar transtornos sobre os desdobramentos de incidente e estimular o esforço em conjunto para superação da crise.

- Orientar os funcionários e demais colaboradores com informações e procedimentos de conduta.
- Informar a sociedade em tempo e com esclarecimentos condizentes com o ocorrido.

EXECUÇÃO DO PAC

- **Comunicação na ocorrência de um Desastre:** Na ocorrência de um desastre será necessário entrar em contato com diversas áreas, principalmente as afetadas para informá-las de seu efeito na continuidade dos serviços e tempo de recuperação. A equipe de comunicação será responsável por contatar estas unidades e passar as informações pertinentes a cada grupo, setor ou seguimento.

A comunicação com cada parte ocorrerá da seguinte forma:

- **COMUNICAR AS AUTORIDADES:** A prioridade da equipe de comunicação será assegurar que as autoridades competentes tenham sido notificadas da catástrofe, principalmente se envolver risco às pessoas, fornecendo as seguintes informações de localização, natureza, magnitude e impacto do desastre.

Autoridade	Contato	Data/hora do registro	Número da ocorrência
Polícia	190		
Bombeiros	190		
SAMU	192		

- **COMUNICAÇÃO APÓS UM DESASTRE:** Após reunião com líderes do PRD e PCO, a equipe de comunicação elaborará um breve programa de comunicação para acionar as partes envolvidas e afetadas de modo a manter todos bem-informados e passar a todos a perspectiva dos esforços necessários para o restabelecimento dos serviços inativos.
- **COMUNICAÇÃO COM OS COLABORADORES:** A equipe de comunicação deverá prover um meio de contato específico para este fim, com intuito de que as unidades do TJPA se mantenham informadas da ocorrência de um desastre e da inatividade dos serviços essenciais de TI.

- **COMUNICAR UNIDADES E SETORES DO TJPA:** Acionar diretamente as unidades afetadas pelo desastre e fornecer contato. Informar a natureza, o impacto e a abrangência da catástrofe, como também as ações de contingência em andamento;
- **COMUNICAR COLABORADORES EXTERNOS, CIDADÃOS E MÍDIA:** A equipe de comunicação, em consonância com a Comunicação do TJPB, deverá fornecer informações pertinentes aos colaboradores externos: Advogados, cidadãos e outros órgãos. Buscar publicar em meios oficiais e de ampla divulgação, com aval do comitê de continuidade e institucional, informações sobre o ocorrido.
- **COMUNICAR RETORNO DAS OPERAÇÕES:** Comunicar a todas as partes acima supracitadas quando ocorrer o retorno das operações à normalidade.

ENCERRAMENTO DO PAC: Uma vez validado o funcionamento do retorno dos sistemas essenciais e estabilidade do datacenter a EQUIPE DE COMUNICAÇÃO entrará em contato com as partes descritas neste plano provendo as informações de retorno das operações com as informações de status dos serviços essenciais.

Compor relatório com relação das atividades necessárias após a ocorrência dos desastres como remanejamento dos canais de informação, abertura e acompanhamento de chamados correlatos ao ocorrido.

10.3. PRD – Plano de Recuperação de Desastres

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.

ESCOPO: É escopo deste plano garantir o retorno das operações do ambiente principal depois da ocorrência de uma crise ou cenário de desastre tratando-se apenas dos ativos, conexões e configurações deste ambiente.

OBJETIVOS DO PRD:

- Avaliar danos aos ativos e conexões do datacenter e prover meios para sua recuperação;

- Evitar desdobramentos de outros incidentes na facilidade principal;
- Restabelecer o datacenter dentro do prazo tolerável;

EXECUÇÃO DO PRD:

- Identificar ativos danificados: As equipes de INSTALAÇÃO/BACKUP/SERVIDORES/REDE deverão identificar e listar todos os ativos danificados da ocorrência do desastre;
- Identificar acessos interrompidos: A EQUIPE DE REDE deverá identificar as interrupções de conexões e acessos gerados após o desastre, informando se a abrangência está na rede local, rede WAN ou com o provedor de serviços.
- Listar serviços descontinuados: A equipe do PRD deverá mapear quais serviços foram descontinuados contendo as informações de perda de ativo e de conexão com intuito de levar ao conhecimento do COMITÊ DE DR. O relatório deverá abranger todos os componentes necessários à plena operação da aplicação como servidores, máquinas virtuais, banco de dados, firewall, storage, routers e switches, bem como respectivas configurações de proxy, dns, rotas, vlans etc.
- Elaborar cronograma de recuperação: O líder do PRD após o mapeamento das perdas e impactos elaborará um breve cronograma de recuperação das aplicações levando em consideração:
 - A priorização dos serviços essenciais, ou determinação de nível institucional;
 - O RTO definido para cada serviço essencial;
 - A força de trabalho disponível.
- Substituição de ativos e equipamentos: Em caso de perda de ativos, deverá ser imediatamente informado ao comitê de DR a necessidade de aquisição de ativos perdidos que não puderem ser recuperados. A equipe irá mensurar quanto tempo a aquisição irá impactar o RTO de cada serviço comunicando ao CDR se há alguma solução alternativa a ser tomada enquanto é realizada a aquisição. Então, a equipe de INSTALAÇÕES deve verificar quais ativos foram danificados estão cobertos por

garantia e se poderá ser acionada neste caso através dos fornecedores. As informações pertinentes à alteração do tempo de recuperação dos serviços serão passadas às equipes do PCO e PAC.

- Reconfiguração de ativos e equipamento: A equipe de INSTALAÇÕES deverá verificar que as configurações dos ativos reparados ou substituídos estão em funcionamento pleno. Caso não estejam, prover cronograma estimado para configurar estes ativos informando à EQUIPE DE COMUNICAÇÃO e CDR
- Teste de ambiente: O ambiente principal do datacenter antes do recovery dos dados do backup deverá ser testado a fim de garantir que o processo de recuperação ocorra conforme o planejado. Os testes incluem:
 - Garantir os mesmos níveis de capacidade e disponibilidade dos serviços essenciais antes do desastre;
- Recuperar dados do backup: Proceder a recuperação dos dados para as aplicações, seja do storage ou fitas de backup,
- Validar as configurações e funcionalidades dos sistemas:
 - A validação pode ser realizada pelos testes automatizados de monitoramento dos serviços;
 - Por equipe designada pela equipe de configuração dos sistemas.

ENCERRAMENTO DO PRD: Ao término do procedimento de recuperação, as informações serão consolidadas em parecer específico informando horário de restabelecimento de cada serviço, equipamentos adquiridos, procedimentos de recuperação realizados e fornecedores acionados.

11. MATRIZ DE TESTES

O PCN e seus subplanos serão testados pelas equipes competentes e os testes serão validados em reunião entre os líderes de cada subplano, uma vez 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.

Os testes serão registrados na "Matriz de testes", cujo modelo figura a seguir:

MATRIZ DE TESTES

Data	Tipo	Motivo	Status

Data: Refere-se ao dia da execução ou validação do teste;

Tipo: o teste pode ser, de mesa, caminho percorrido, simulação, entre outros

Motivo: O Motivo pelo qual o teste foi necessário:

Status: programado, executado, planejado, agendado

12. MATRIZ DE AVALIAÇÃO

Tomaram conhecimento do presente plano, os seguintes gestores:

MATRIZ DE AVALIAÇÃO

Nome	Cargo	Data	Resultado	Assinatura

Resultado: Aprovado, aprovado com ressalvas, reprovado