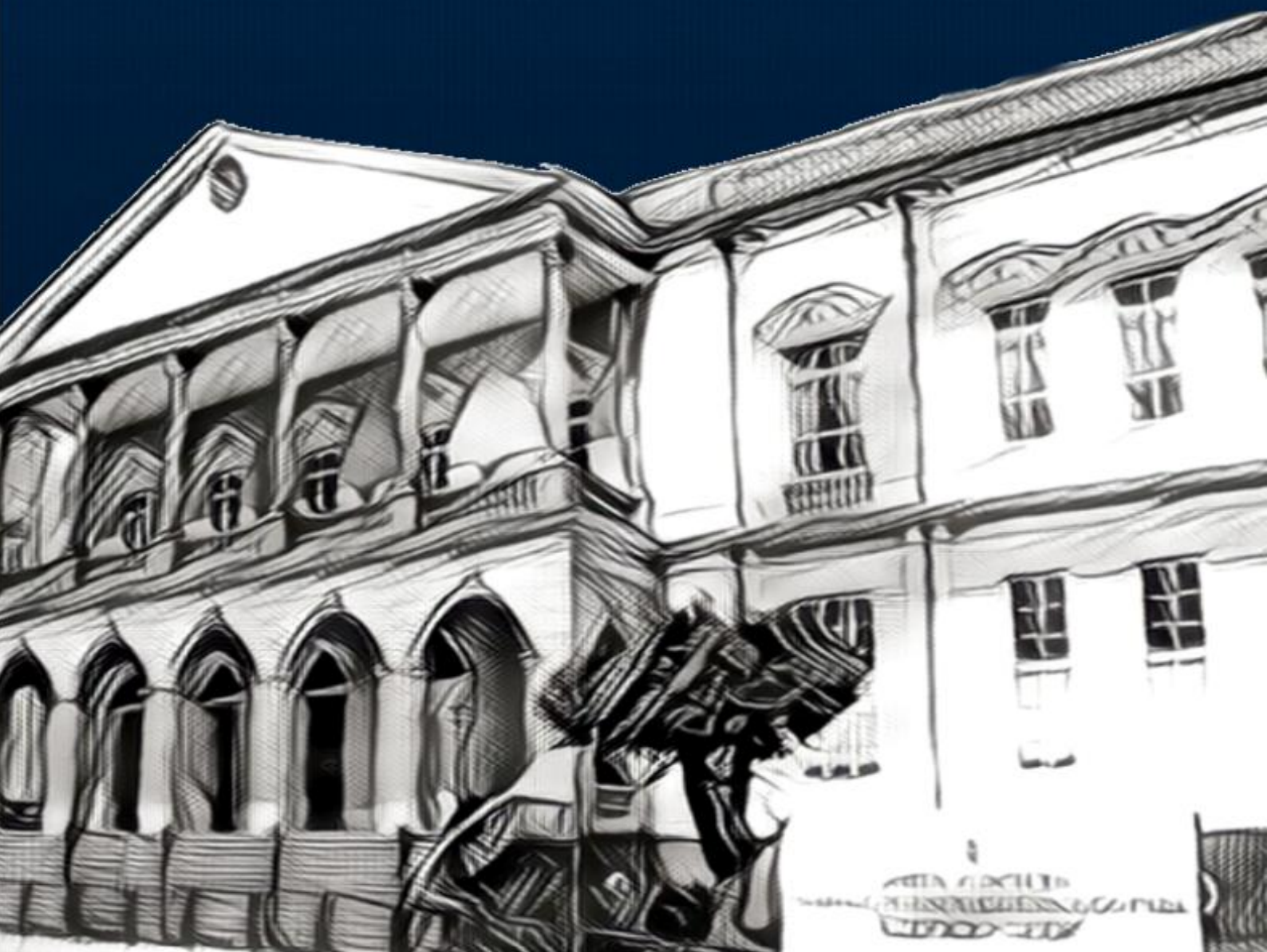
TRIBUNAL DE JUSTIÇA
DO ESTADO DO PARÁ

PLANO DE CONTINUIDADE DE NEGÓCIO (PCN) 2025 – 2027



TRIBUNAL DE JUSTIÇA
DO ESTADO DO PARÁ

PLANO DE CONTINUIDADE DE NEGÓCIO (PCN)

– SECRETARIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO –

2025 – 2027

PRESIDENTE DO TJPA

DESEMBARGADOR ROBERTO GONÇALVES DE MOURA

VICE-PRESIDENTE DO TJPA

DESEMBARGADOR LUIZ GONZAGA DA COSTA NETO

DESEMBARGADOR CORREGEDOR GERAL DE JUSTIÇA

DESEMBARGADORA MARIA ELVINA GEMAQUE TAVEIRA

SECRETARIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

SECRETÁRIO DE TIC

DIEGO BAPTISTA LEITÃO

SECRETÁRIO ADJUNTO DE TIC

BRUNO RODRIGUES CARDOSO

COORDENADOR DE APLICAÇÕES

ÁLVARO ROGERS CARDOSO ALVÃO

COORDENADORA DE ATENDIMENTO AO USUÁRIO

ALINE SANTOS DE OLIVEIRA

COORDENADORA DE GOVERNANÇA

LUCIANA MACHADO SILVEIRA MELLO

COORDENADOR DE INFRAESTRUTURA TECNOLÓGICA

ARILSON GALDINO DA SILVA

ASSESSORES DE INFORMÁTICA

ANDREY DIEGO DA SILVA ALBUQUERQUE

MARCIO GOES DO NASCIMENTO

MAURICIO DE FREITAS BRAGA

MIGUEL JOSE DE ALMEIDA PERNAMBUCO

PAULA NANCY LIMA DIOCESANO GUERREIRO

WELLEN DE PAULA MONTEIRO AMADOR

CHEFES DE DIVISÃO / SERVIÇO

ALEXANDER RICHARD VINSON

BRUNO VIEIRA DOS SANTOS

CARLOS DIEGO POJO DE BRITO

DANIEL FONTES PEREIRA

DENISON LEANDRO SERRAO SOARES

FÁBIO VENICIUS FERREIRA DOS REIS

IGOR PINTO SIMÕES

JOSÉ DE ANDRADE GOYANA JUNIOR

MARCUS SERGIO FERREIRA NEVES

MARILIA PAULOS TELES

MURILO DE MELO SILVA

PAULO ROBERTO LOURINHO DOS SANTOS

RAMON SANTOS DO NASCIMENTO

JORGE ANDRÉ SILVA ABDON

WANDERSON BENEDITO SOUZA DA COSTA

COMISSÃO DE INFORMÁTICA
(PORTARIA Nº 1570/2025-GP)

DESEMBARGADOR ALEX PINHEIRO CENTENO
J. EDMAR SILVA PEREIRA
Jª. KÁTIA PARENTE SENA
ARILSON GALDINO DA SILVA
BRUNO RODRIGUES CARDOSO
DIEGO BAPTISTA LEITÃO
PAULA NANCY LIMA DIOCESANO GUERREIIRO

COMITÊ DE GOVERNANÇA DE SEGURANÇA DA INFORMAÇÃO
(PORTARIA Nº 1093/2025-GP)

DESEMBARGADOR ALEX PINHEIRO CENTENO
Jª. PATRÍCIA DE OLIVEIRA SÁ MOREIRA
ARILSON GALDINO DA SILVA
DIEGO BAPTISTA LEITÃO
MIGUEL LUCIVALDO ALVES SANTOS
MAURÍCIO CRISPINO GOMES
HELLEN GEYSA DA SILVA MIRANDA BRANCALHÃO
TIAGO SILVA GUIMARÃES
PAULO VICTOR RAMOS CORRÊA
CEL. QOPM MARLON SILVA NASCIMENTO
FÁBIO DJAN OLIVEIRA DE LIMA
WILL MONTENEGRO TEIXEIRA

COMITÊ DE GOVERNANÇA DE TIC
(PORTARIA Nº 3477/2025-GP)

JOÃO VALÉRIO DE MOURA JUNIOR
DIEGO BAPTISTA LEITÃO
MIGUEL LUCIVALDO ALVES SANTOS
MAURÍCIO CRISPINO GOMES
TIAGO SILVA GUIMARÃES
LUCIANA SÁ FERNANDES
LUCIANA MACHADO SILVEIRA MELLO
PAULA NANCY LIMA DIOCESANO GUERREIRO
JEAN KARLO QUINTELA DE SOUZA
CARLOS ALBERTO MAGALHÃES BREMGARTNER
LORENA RAMOS DO VALE

COMITÊ DE GESTÃO DE TIC
(PORTARIAS Nº 2309/2025 E 2900/2025-GP)

ARILSON GALDINO DA SILVA
ALINE SANTOS DE OLIVEIRA
ÁLVARO ROGERS CARDOSO ALVÃO
BRUNO RODRIGUES CARDOSO
DIEGO BAPTISTA LEITÃO
LUCIANA MACHADO SILVEIRA MELLO
PAULA NANCY LIMA DIOCESANO GUERREIRO

FICHA DE CONTROLE DE VERSÃO E PUBLICIDADE DE DOCUMENTOS

Identificação do Documento			
Título:	Plano de Continuidade de Negócio	Sigla:	PCN
Tipo do documento:	() Norma () Política **(X) Plano** () Protocolo Outro: _____		
Elaborado por:	SECRETARIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO		
Publicidade			
Classificação:	() Público **(X) Institucional** () Departamental () Restrito () Controlado		
Forma de Publicação:			
Documentos Relacionados:	PSI Plano de Gestão de Riscos	ID:	

Versão	Data	Autoria	Descrição da Alteração	Aprovado Por
01	27/09/2021	Paulo Lourinho	PCN/2021	
01.01	25/04/2022	Paulo Lourinho	PCN/2021	
2	11/10/2023	Paulo Lourinho	PCS/2023	
2.1	16/11/2023	Paulo Lourinho	PCS/2023 - Matrizes de Serviços Essenciais	
2.2	29/11/2023	Paulo Lourinho	Mudança na Matriz de Ameaças	
2.3	30/06/2024	Paulo Lourinho	Definição de serviço essencial. Criação da matriz de apetite a risco, mudança de matriz de ameaça para matriz de risco, mudança da matriz de conceitos e definições para um "glossário no final do documento"	
V3	27/11/2024	Paulo Lourinho	Reestruturação Completa no Plano	
V4	28/07/2025	Paulo Lourinho Fábio Azevedo Alexander Tschertasch	Renomeado para PCN e reestruturado completamente. Cronograma de Implementação dos Protocolos e Execução dos Testes.	Comitê de Governança de Segurança da Informação (CGSI)
4.1	21/08//2025	Paulo Lourinho	Atualização do Cronograma de Implementação dos Protocolos e Execução dos testes.	

SUMÁRIO

CONTEXTUALIZAÇÃO

O Plano de Continuidade de Negócio (PCN), da Secretaria de Tecnologia de Informação e Comunicação do TJPA, é um documento de planejamento tático, pertencente ao domínio da Segurança da Informação e, sendo assim, deve ser referenciado no documento que institui a Política de Segurança da Informação, na instituição em questão.

1. DEFINIÇÃO DE DESASTRE, ACIDENTE E INCIDENTE

Embora não diretamente, a norma NBR ISSO 22301, define:

- **Incidente:** Termo mais amplo e utilizado diretamente na norma, referindo-se a qualquer evento que possa causar, ou já está causando, interrupção nas operações. A norma foca no planejamento e na resposta a incidentes para evitar que se tornem crises maiores ou desastres.
- **Desastre**: Embora menos detalhado, é entendido como uma forma mais severa de incidente, com impacto de longo prazo.
- **Acidente**: Geralmente é tratado como eventos específicos que podem ou não afetar a continuidade do negócio, mas que, geralmente, resulta em danos ou perdas, muitas vezes associado a segurança física de pessoas ou equipamentos.

Para o contexto em questão, um desastre, acidente ou incidente representa a ocorrência de um evento adverso, de origem natural ou não, capaz de causar danos significativos, com solução de continuidade total ou parcial, nos serviços de Tecnologia da Informação e Comunicação do TJPA.

Tal evento adverso pode ser um item previsto ou não nas matrizes de riscos componentes da BIA[1] deste PCN, mas deve afetar pelo menos um dos itens das matrizes de serviços essenciais de TIC do TJPA, ferindo pelo menos um dos princípios CID de segurança da informação.

A matriz a seguir resume os conceitos apresentados:

Termo	Definição (ISO)	Notas	Exemplos
Incidente	Evento fora do normal que **pode causar interrupção, perda, emergência ou crise** (ISO 22300:2021, § 3.1.122)	Genérico – engloba todos os tipos de ocorrência	Queda de servidor; atraso na rede
Acidente	Evento inesperado e indesejado, de impacto limitado (nota em ISO 22300, § 2.1.6)	Subcategoria de incidente, sem escalar	Vazamento de água sem danos; falta de energia mínima com gerador ativo
Desastre	Situação com perdas generalizadas, **excedendo capacidade interna** (ISO 22300:2021, § 2.1.11)	Requer BCP/DRP conforme BCMS (ISO 22301)	Incêndio no data center; enchente grave; ataque cibernético crítico

[1] Business Impact Analisys [ver glossário]

Relação entre os termos:

- Todo **acidente** é um **incidente**, mas nem todo incidente é acidente.
- Todo **desastre** é um **incidente**, mas com gravidade muito superior.

Sob a perspectiva da previsibilidade, o ITIL classifica e define os conceitos de Requisição de Serviço, Incidente e Problema, conforme consolidado na matriz apresentada a seguir:"

Conceito	Definição	Objetivo	Exemplo
Requisição	Solicitação padrão de um serviço ou recurso	Atender uma demanda planejada	Instalar MS Office; criar conta de acesso; resetar senha de usuário.
Incidente	Interrupção/redução de qualidade de um serviço	Restaurar o serviço rapidamente	E-mail caiu; rede está lenta
Problema	Causa raiz desconhecida de um ou mais incidentes	Eliminar a causa raiz e evitar recorrência	Analisar falhas constantes no servidor de banco de dados

No contexto geral deste PCN será utilizado o termo **"Incidente"**.

É mister salientar que o ativo afetado por um incidente, deve estar sob a responsabilidade de, pelo menos, uma equipe, a qual executará os procedimentos elencados no PCS (PGC, PCO, PRD) para a ocorrência em questão.

2. DEFINIÇÃO DE ATIVO

Entende-se como ativo qualquer recurso essencial para a operação da organização. Isso inclui, mas não se limita a:

- **Pessoas** – Servidores, equipes ou terceiros essenciais para as operações;
- **Processos** - Procedimentos e fluxos de trabalho críticos para a entrega de produtos ou serviços;
- **Informações** - Dados em sistemas digitais, físicos ou na nuvem;
- **Tecnologia** - Sistemas, softwares, redes e hardware indispensáveis;
- **Infraestrutura** - Edifícios, equipamentos e utilidades necessários para a continuidade do negócio;
- **Fornecedores e Parceiros** - Entidades externas cuja colaboração é crítica;
- **Reputação e Marca** - Imagem da organização, que pode ser prejudicada por interrupções.

Somente os ativos considerados **críticos** para a realização da missão do TJPA, ou seja, aqueles que afetam significativamente o negócio do PJPA, devem ser tratados neste PCS.

3. PLANO DE CONTINUIDADE DE NEGÓCIO

3.1 O QUE É UM PLANO DE CONTINUIDADE DE NEGÓCIO? (DEFINIÇÃO)

O Plano de Continuidade de Negócio (PCN), é uma ferramenta de gestão, subordinada à Política de Segurança da Informação do TJPA, e constituída por um documento (este documento) no qual ficam definidas as táticas a serem adotadas a fim de que se mantenha o funcionamento das operações essenciais de serviços de TIC deste tribunal, caso tais serviços venham a enfrentar intempéries causadas por fatores internos ou externos à organização que causem solução de continuidade (interrupção) nestas operações.

Desta forma, pode-se dizer seguramente que o PCN é um plano que norteia a gestão de continuidade de serviços de TIC, em situações não cotidianas que denotem solução de continuidade. Para o cenário considerado, tais situações, podem variar da falta de energia elétrica a incêndios, perpassando por desastres naturais, ataques cibernéticos, panes de *hardware* e *software*, entre outros eventos, que têm como ponto em comum ferir os princípios CID, pilares incontestes da segurança da informação.

3.2 PARA QUE CRIAR UM PLANO DE CONTINUIDADE DE NEGÓCIO? (FINALIDADE)

O PCN é essencial para garantir uma gestão eficaz da continuidade do negócio, assegurando a resiliência organizacional. Por meio dele, busca-se evitar a interrupção das operações de serviços críticos de Tecnologia da Informação e Comunicação (TIC) e restabelecer a normalidade dentro de um intervalo de tempo previsto em acordo.

Adicionalmente, a Resolução Nº 370, de 28 de janeiro de 2021, em sua Seção III - Dos Riscos, Segurança da Informação e Proteção de Dados, dispõe, em seus artigos, as seguintes diretrizes:

> Art. 36. Cada órgão deverá elaborar um 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.

3.3 POR QUE CRIAR UM PLANO DE CONTINUIDADE DE NEGÓCIO? (MOTIVAÇÃO)

Para além da obrigação regulamentar, que atende a conformidade, o PCN, serve para nortear o trabalho dos gestores que buscam **minimizar o impacto das intempéries operacionais** (incidentes) que causem interrupção, garantindo segurança e eficiência de forma a reduzir ao máximo o impacto de tais situações na organização, evitando assim que as operações essenciais sejam interrompidas ou que operem de forma errônea, ou ainda sem o desempenho satisfatório. Isto posto, o PCN deve orientar o gestor a fim de que, em caso de incidentes (materialização de riscos), as operações críticas e essenciais não sejam interrompidas ou prejudicadas.

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

Dessa forma, na ocorrência de uma das intempéries previstas no PCN, ou de outra com consequências similares, torna-se possível lidar com a situação adversa de maneira controlada, uma vez que as ações já estarão previamente definidas e organizadas. Isso permite sua execução com o mínimo de necessidade de decisões ou improvisações, alinhando-se às boas práticas recomendadas para a gestão de crises, especialmente em cenários de desastre.

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.

4. ESTRUTURA DO PLANO DE CONTINUIDADE DE NEGÓCIO

Este PCN é composto por quatro partes principais:

- **Contextualização:** (Esta parte) Tem como objetivo normalizar os termos e estabelecer a padronização necessária para a estruturação e aplicação do Plano de Continuidade de Negócio (PCN);
- **Parte I - Diretrizes:** Estabelece as orientações gerais do Plano de Continuidade de Negócio (PCN), detalhando os parâmetros para análise, os indicadores de desempenho e as responsabilidades. Além disso, define a estrutura e a documentação necessária para implementar ações de contingência e garantir a continuidade dos serviços essenciais de TIC, considerando as peculiaridades e necessidades do ambiente organizacional.
- **Parte II – Análise de Impacto de Negócio (BIA):** Abrange a identificação e a avaliação dos serviços críticos de tecnologia que sustentam os processos essenciais do TJPA. Por meio da Análise de Impacto nos Negócios (BIA), são analisadas as dependências, os riscos e as consequências de eventuais interrupções, permitindo a priorização de ações de continuidade. Além disso, define as responsabilidades dos stakeholders

envolvidos, garantindo um alinhamento claro das funções e das expectativas no processo de continuidade.

- **Parte III – Implementação e Gestão:** (É a parte consultada em caso de incidentes) Aborda a execução prática das táticas de continuidade e o gerenciamento de crises, com o objetivo de garantir a operação dos serviços essenciais do TJPA, mesmo diante de adversidades. Ela detalha a definição, aplicação e gestão dos seguintes protocolos operacionais:
  - **Protocolo de Gerenciamento de Crise (PGC):** Ativado imediatamente após a identificação de uma crise, este protocolo coordena o controle e a comunicação de todo o processo de contingência, assegurando uma resposta organizada até que os serviços sejam estabilizados. Somente é encerrado após a conclusão do PRD.
  - **Protocolo de Continuidade Operacional (PCO):** Aplicado após a execução do PGC declarar desastre. Ele assegura que os serviços críticos continuem funcionando, ainda que em estado contingencial, minimizando os impactos sobre a operação.
  - **Protocolo de Recuperação de Crises (PRC):** Implementado após a conclusão do PCO, este protocolo foca na restauração completa e definitiva da operação normal dos serviços afetados.

Os protocolos operacionais (PGC, PCO e PRD) são desenvolvidos em conformidade com os serviços críticos de TIC identificados no PCN. Cada protocolo é personalizado para atender às necessidades específicas de um serviço, garantindo uma abordagem direcionada e eficiente.

O relacionamento entre os componentes do PCN, pode ser visualizado no diagrama abaixo (Figura 1). Tal figura denota a subordinação dos protocolos operacionais ao PCN, explicitando que deve haver tantos protocolos (PGC, PCO e PRD) quantos são os ativos para os quais se criaram planos de continuidade e contingência.

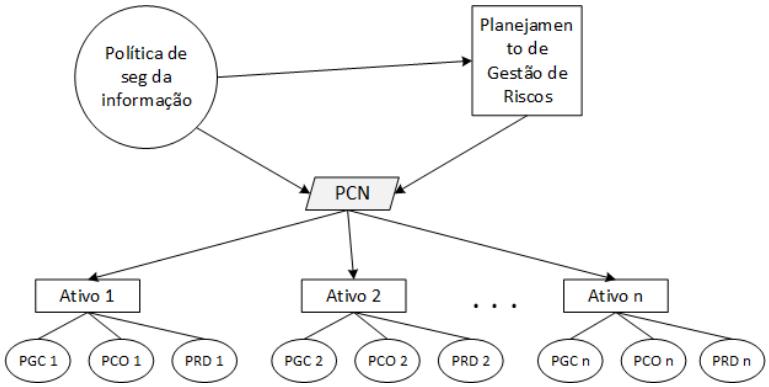


Figura 1: Diagrama de estrutura do PCS

Desta forma, o **Plano de Continuidade de Negócio** referencia (contém, mas não é igual - ⫋) os protocolos PGC, PCO e PRD, como seus componentes operacionais, os quais devem ser específicos para cada ativo crítico. A quantidade de protocolos necessários corresponde ao

número de ativos que precisam ser recuperados em caso de incidentes, conforme ilustra a figura abaixo:

PCN ⊋ (PGC * n) + (PCO * n) + (PRD * n)

Figura 2: Componentes do PCS

O objetivo deste Plano de Continuidade de Negócios (PCN) é alcançado por meio de três pilares principais:

- Gestão de Riscos: Identifica, avalia e implementa medidas para mitigar riscos que possam comprometer a continuidade dos serviços críticos.
- Gestão de Mudanças: Estabelece diretrizes para realizar alterações no ambiente de TIC de forma controlada, prevenindo interrupções nos serviços essenciais.
- Gestão de Incidentes: Define processos para detecção, resposta e resolução de incidentes, assegurando que os serviços sejam restaurados no menor tempo possível.

A Gestão de Riscos é abordada na Parte II (Análise de Impacto nos Negócios - BIA), enquanto a Gestão de Mudanças e a Gestão de Incidentes são tratadas na Parte III deste PCN.

5. ESTRATÉGIA DO PLANO DE CONTINUIDADE DE NEGÓCIO

A alta gestão do Tribunal de Justiça do Estado do Pará (TJPA) deve garantir a existência de uma estrutura mínima capaz de assegurar a continuidade das operações, mesmo diante de eventos que possam ocasionar interrupções significativas nos serviços essenciais. A estratégia de continuidade de negócios deve estar alinhada às melhores práticas e normas de gestão reconhecidas internacionalmente, como a ABNT NBR ISO/IEC 27001:2022 (Sistemas de Gestão de Segurança da Informação) e a ABNT NBR ISO 22301:2020 (Sistemas de Gestão de Continuidade de Negócios).

Entre as ações essenciais para o êxito do Plano de Continuidade de Negócios (PCN), destaca-se a elaboração da Política de Segurança da Informação (PSI). Essa política deve conter diretrizes claras para a gestão da continuidade e ser formalizada em documento específico, servindo de referência para toda a organização.

O PCN, por sua vez, deve contemplar:

5.1 DIRETRIZES, PARÂMETROS E INDICADORES

Com o objetivo de padronizar entendimentos e práticas, o plano deve especificar:

- O objetivo geral do PCN, alinhado aos princípios de resiliência organizacional;
- Os grupos funcionais designados para a execução, acompanhamento e monitoramento das ações previstas;
- Métricas e critérios para análise e avaliação da eficácia do plano;
- Referência explícita aos protocolos de contingência correlatos (PGC, PCO e PRD);
- Procedimentos para revisão periódica, aprimoramento e monitoramento contínuo do PCN e de seus protocolos associados;

- Realização regular de testes práticos para validar estratégias e ações, com o devido registro das evidências;
- Resultados esperados em termos de mitigação de impactos e redução do tempo de recuperação (RTO e RPO).

5.2 CONHECIMENTO ORGANIZACIONAL E ANÁLISE DE IMPACTO NOS NEGÓCIOS (BIA)

Para promover um entendimento profundo sobre os processos e serviços críticos da instituição, o PCN deve incluir:

- Identificação e priorização dos ativos tecnológicos essenciais;
- Mapeamento das dependências entre processos críticos e os ativos de suporte;
- Análise de riscos abrangendo ameaças internas e externas, em conformidade com a ISO/IEC 31000:2018 (Gestão de Riscos).

5.3 RECURSOS NECESSÁRIOS PARA A IMPLEMENTAÇÃO DO PCN

Para viabilizar a execução eficaz do plano, devem ser providos:

- Capacitação e treinamentos contínuos para as equipes de gestão e operação envolvidas no planejamento, elaboração e execução do PCN;
- Hardware e software apropriados, incluindo redundâncias para equipamentos críticos previamente definidos;
- Infraestrutura de comunicação resiliente e redundante (ex.: links de internet de backup, data centers alternativos);
- Fornecimento de energia elétrica para garantir a operação dos equipamentos essenciais às equipes de continuidade;
- Acesso a instalações físicas do TJPA, considerando a necessidade de recuperações fora do horário regular de funcionamento;
- Condições adequadas de conforto e segurança para as equipes técnicas, incluindo refrigeração, iluminação, abastecimento de água, café, higiene e banheiros;
- Consultorias e suporte especializados, quando necessário, para análise, revisão e implementação das ações previstas no PCN.

5.4 TÁTICA DE BACKUP E PROTEÇÃO DE DADOS

A continuidade de negócio exige a existência de um Plano de Backup que assegure a proteção dos dados institucionais, em especial aqueles classificados como críticos na Análise de Impacto nos Negócios (BIA). Este plano deve ser alinhado com as diretrizes deste PCN e atender ao estabelecido na Política de Segurança da Informação (PSI) do TJPA, que exige mecanismos sistemáticos de cópia, proteção e recuperação da informação.

O plano de backup deve detalhar e garantir procedimentos que:

- Assegurem a rotina de cópias de segurança (backup) dos dados críticos;
- Mantenham verificações periódicas de integridade e recuperação dos backups;

- Estabeleçam **tempos máximos aceitáveis de perda de dados (RPO)**, definidos na BIA;
- Realizem **testes periódicos de restauração de backup**, conforme definido na Parte III deste plano.

6. ALINHAMENTO NORMATIVO

O PCN deve ser estruturado em conformidade com as exigências normativas aplicáveis, como a **Resolução nº 370 de 28/01/2021** do CNJ, que estabelece diretrizes sobre riscos, segurança da informação e proteção de dados. A resolução determina que os órgãos judiciários elaborem planos de continuidade de negócios e gestão de riscos alinhados aos objetivos institucionais.

Além disso, o TJPA deve adotar metodologias de mercado amplamente reconhecidas, como o **CobiT 2019** e o **ITIL 4**, para estruturar as ações e processos relacionados à continuidade de negócios e governança de TIC.

PARTE I – DIRETRIZES

7. OBJETIVO

O Plano de Continuidade de Negócio (PCN) tem como objetivo principal **mapear e tratar os serviços críticos de Tecnologia da Informação e Comunicação (TIC) do Tribunal de Justiça do Estado do Pará (TJPA), geridos pela Secretaria de Tecnologia da Informação (SECINF), com vistas a assegurar a resiliência e a continuidade desses serviços.**

O PCN visa identificar as principais ameaças a esses serviços, avaliar os riscos associados e implementar estratégias eficazes de mitigação, resposta e recuperação. Essas ações têm como propósito minimizar impactos, preservar a operação dos serviços essenciais protegendo os ativos críticos para assegurar a prestação jurisdicional à sociedade e assim alinhar a continuidade das atividades às metas institucionais do TJPA.

8. JUSTIFICATIVA / MOTIVAÇÃO

Os serviços de Tecnologia da Informação e Comunicação (TIC) representam ativos estratégicos e indispensáveis para a continuidade das operações do Tribunal de Justiça do Estado do Pará (TJPA). Garantir a proteção desses serviços e dos dados por eles processados, bem como estabelecer métodos eficazes de recuperação em situações de crise, é crucial para manter a resiliência institucional e a continuidade das atividades judiciais.

A implementação de um Plano de Continuidade de Negócio (PCN) é imprescindível para preparar o TJPA para enfrentar eventos adversos, mitigando impactos e assegurando a prestação ininterrupta dos serviços essenciais à sociedade, além de proteger informações vitais à administração da justiça.

9. ESCOPO

Este Plano de Continuidade de Negócio (PCN) foi elaborado para atender aos ativos críticos de Tecnologia da Informação e Comunicação (TIC) sob a responsabilidade da Secretaria de Informática (SECINF) do Tribunal de Justiça do Estado do Pará (TJPA). Ele abrange os serviços, infraestruturas geridas por essa unidade organizacional, estando alinhado e subordinado à Política de Segurança da Informação do Tribunal.

O principal ativo de negócio do TJPA é, indubitavelmente, o Processo Judicial Eletrônico (PJe), sistema responsável pelo registro e pela tramitação de todos os processos judiciais no âmbito do Tribunal. Naturalmente, o funcionamento do PJe depende de uma infraestrutura composta por diversos outros ativos de tecnologia, entre os quais se destacam:

- Ativos de Infraestrutura de Serviços:
  - Datacenters, infraestrutura de virtualização, sistemas operacionais, serviços de rede, armazenamento e sistemas de backup.
- Ativos de Infraestrutura de Comunicação:
  - Switches, roteadores e links de dados das redes LAN, Metro e WAN, que sustentam a comunicação de dados interna e externa do TJPA.
- Ativos de Segurança da Informação:
  - Soluções como sistema de certificados digitais, firewalls, WAF, gestão de vulnerabilidades e controle de acesso.

No contexto deste plano, os ativos de TIC são elementos indispensáveis para o processo de negócio do TJPA. Assim, ao proteger esses ativos, assegura-se a resiliência e a continuidade das operações essenciais do TJPA.

10. BENEFÍCIOS

A adoção de um Plano de Continuidade de Negócio (PCN) voltado especificamente para o Processo Judicial Eletrônico (PJe) pelo Tribunal de Justiça do Estado do Pará (TJPA) é indispensável para assegurar a resiliência deste sistema, considerado o principal ativo de negócio da instituição. O PJe é o núcleo que sustenta a tramitação e gestão de todos os processos judiciais no âmbito do TJPA, e sua indisponibilidade representa risco direto à prestação jurisdicional e ao cumprimento da missão institucional.

Nesse contexto, as análises necessárias para a elaboração do PCN e a formalização do plano resultam em benefícios significativos, tais como:

- **Identificação dos processos críticos relacionados ao PJe** e avaliação dos impactos decorrentes de interrupções, possibilitando uma compreensão aprofundada sobre as dependências tecnológicas e operacionais que asseguram o pleno funcionamento do sistema. Esse mapeamento revela oportunidades de melhoria na gestão do PJe e dos ativos de TIC correlatos, contribuindo para o fortalecimento das operações diárias e para uma resposta mais eficaz em situações de crise.
- **Avaliação do grau de exposição a riscos do PJe**, permitindo o planejamento de ações preventivas e corretivas adequadas para manter a operação durante contingências e agilizar a recuperação após incidentes.

- **Redução dos impactos sobre magistrados, servidores, advogados e jurisdicionados**, assegurando a continuidade da prestação de serviços essenciais e preservando a reputação institucional do TJPA perante a sociedade e os órgãos parceiros.
- **Aumento expressivo da capacidade de resiliência do TJPA** em face de falhas ou eventos adversos que possam comprometer a disponibilidade e integridade do PJe, independentemente da causa.
- **Padronização e documentação de processos e ativos relacionados ao PJe**, facilitando a gestão, o treinamento de equipes, auditorias e revisões periódicas, além de contribuir para uma operação mais eficiente e segura do sistema.

11. UNIDADE GESTORA E EXECUTORA DO PCN

A Secretaria de Tecnologia da Informação e Comunicação (SECINF) do TJPA, por meio das Coordenadorias de Infraestrutura de TIC (CIT), de Atendimento ao Usuário (CAU) e de Aplicações (CA), é responsável por elaborar, gerir e executar o Plano de Continuidade de Negócios (PCN). A Coordenadoria de Governança em TIC (COGV) avalia sua efetividade, alinha o PCN aos objetivos estratégicos e monitora a realização de testes, as revisões e as atualizações necessárias.

11.1 DIRETRIZES BASILARES DA GESTÃO E EXECUÇÃO DO PCN

As diretrizes a seguir têm como objetivo orientar a elaboração, gestão e execução do PCN:

- O PCN deve **estar alinhado** com a missão, visão e metas estratégicas do TJPA, assegurando que a continuidade dos serviços críticos esteja integrada aos objetivos institucionais.
- A alta administração deve **participar ativamente da elaboração, validação e aprovação** do PCN, assegurando o comprometimento estratégico com a continuidade dos negócios.
- Os colaboradores devem **ser informados sobre as fases de desenvolvimento** do PCN, contribuir na identificação de ameaças e riscos que possam afetar os serviços

essenciais, e sugerir ações mitigatórias que não tenham sido previamente contempladas no plano.

- A elaboração do PCN deve **priorizar os riscos com maior impacto**, expandindo o alcance do plano conforme a maturidade do TJPA na proteção de seus ativos críticos.
- O **treinamento contínuo e a conscientização de todos os colaboradores** são fundamentais para garantir a efetividade do plano de continuidade, permitindo que o TJPA gerencie seus riscos e esteja preparado para implementar ações de contingência quando necessário.
- Deve-se **promover a adoção de frameworks reconhecidos e capacitações específicas** para a elaboração, gestão e atualização do PCN, bem como dos protocolos operacionais que o complementam.

12. UNIDADES ENVOLVIDAS

- Coordenadoria de Suporte Técnico - CST;
- Coordenadoria de Aplicações - CA;
- Coordenadoria de Atendimento ao Usuário – CAU
- Coordenadoria de Governança – COGV

13. NORMATIVOS UTILIZADOS

A elaboração e gestão do Plano de Continuidade de Negócios (PCN) do PJe no TJPA baseia-se nos seguintes normativos e referências:

- **Resolução CNJ n.º 370/2021** – Institui a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD) para 2021–2026 e, em seu Art. 36, obriga cada órgão a elaborar Plano de Gestão de Continuidade de Negócios ou de Serviços. No Art. 37, exige também Plano de Gestão de Riscos de TIC.
- **ABNT NBR ISO/IEC 22301:2020** – Define os requisitos para um Sistema de Gestão de Continuidade de Negócios (SGCN), cobrindo planejamento, implementação, operação, monitoramento, análise e melhoria contínua.
- **ABNT NBR ISO/IEC 22313:2020** – Diretrizes para aplicação prática da ISO 22301, detalhando como estruturar o ciclo PDCA de continuidade.
- **ABNT NBR ISO/IEC 22317:2015** – Fornece orientações para condução da Análise de Impacto nos Negócios (BIA), etapa crítica na identificação de processos e serviços essenciais.
- **ABNT NBR ISO/IEC 22318:2020** – Recomendações para definição de estratégias de continuidade especificamente para recursos de TIC.

- ISO/IEC 27031:2011 – "Diretrizes para prontidão de TIC para continuidade de negócios", voltada a assegurar que os arranjos técnicos e organizacionais de TIC estejam aptos a suportar o PCN.
- ISO/IEC 24762:2008 – Estabelece requisitos para provedores de serviços de recuperação de desastres e continuidade de TIC, incluindo aspectos de governança e processos de serviço.

- ABNT NBR ISO/IEC 27001:2022 – Requisitos para um Sistema de Gestão de Segurança da Informação (SGSI), cujo domínio A.17 (Continuidade dos Negócios) reforça controles de TIC no PCN.
- ABNT NBR ISO/IEC 27002:2022 (seção A.17) – Código de práticas de segurança da informação, com controles específicos para planejamento, implementação e testes de continuidade de TIC.
- ABNT NBR ISO/IEC 27005:2019 – Orientações para gestão de riscos de segurança da informação, complementar ao PCN na identificação e tratamento de ameaças a ativos de TIC.

A partir desses normativos, todas as definições, ações, métricas e testes do PCN do PJe devem seguir estritamente seus requisitos e recomendações.

14. RELAÇÃO COM OUTROS NORMATIVOS INTERNOS

- Política de Segurança da Informação - PSI/TJPA;
- Manual de Governança de Tecnologia da Informação e Comunicação - PG-TIC/TJPA;
- Protocolos de Administração de Crise para os serviços de TIC - PAC;
- Protocolos de Continuidade Operacional para os serviços de TIC - PCO;
- Protocolos de Recuperação de Crises para os serviços de TIC – PRC;
- Plano de Cópia e Restauração de Dados - PCRD.

15. ATRIBUIÇÃO DE RESPONSABILIDADES

Para garantir a efetividade do Plano de Continuidade de Negócio (PCN), é essencial mapear e registrar formalmente todas as responsabilidades relacionadas à sua elaboração, ativação, manutenção e monitoramento.

No âmbito do TJPA, a continuidade dos serviços de Tecnologia da Informação e Comunicação (TIC) é gerida e executada por Grupos Funcionais, cada um com atribuições específicas. Essas responsabilidades estão organizadas de forma clara na matriz apresentada a seguir, de modo a assegurar que todas as etapas e processos do PCN sejam devidamente conduzidos.

Grupo	Componentes	Atribuição de Responsabilidade
Estratégico de Contingência e Continuidade **(GECC)**	-Secretário -Chefe de gabinete **-** Coordenador de Governança	- Avaliar o PCS periodicamente; - Decidir pelo acionamento ou não do último PCS aprovado, quando da declaração de uma crise; -Responder, em nível institucional, pela execução do PCS e demais ocorrências relacionadas; -Tomar decisões estratégicas no caso da ocorrência de contingências significativas
Comunicação de Contingência e Continuidade **(GCCC)**	-Assessores de imprensa - Coordenadores técnicos da SECINF	-Efetuar todas as comunicações a imprensa, entidades externas e internas, a fim de garantir a disseminação adequada do cenário de crise (execução do PGC) -O líder desta equipe administrará e manterá o Protocolo de Gestão de Crise (PGC).
Gestão de Contingência e Continuidade (GGCC)	-Coordenador de suporte; -Coordenador de desenvolvimento; -**Líder da continuidade**	-Supervisionar as atividades do grupo operacional, assegurando os recursos necessários para operação do PCS; -Gerir os cenários de contingência e apoio ao processo de decisão do Grupo Executivo;
Operacional de Contingência e Continuidade (**GOCC)**	- Chefe responsável pelo serviço -Analistas de suporte -Analistas de desenvolvimento - Engenheiros	-Executar protocolos (PCO e PRD) do PCS; -Em caso de cenários de crises não previstos, analisar o contexto, optar e executar protocolos de continuidade operacional e recuperação de crise conforme orientações do GGCC; -Especificar e solicitar previamente, recursos necessários para a prevenção e mitigação de crises.
Apoio de Contingência e Continuidade - **(GCCA)**	-Analistas de administração -Analistas de logística	-Prover recursos necessários para que os grupos executivo, tático e operacional efetuem suas atividades de maneira adequada. Tais recursos podem ser, equipamentos, *softwares*, alimentação e transporte, entre outros.

16. ANÁLISE DOS ATIVOS

A gestão de continuidade de negócio requer uma análise detalhada dos ativos de Tecnologia da Informação e Comunicação (TIC) que sustentam os serviços essenciais. Essa análise, é chamada **Análise de Impacto de Negócio**, também conhecida como *Business Impact Analysis* (BIA), visa identificar os ativos críticos, suas interdependências e os riscos associados, de modo a priorizar ações de mitigação e contingência.

A análise dos ativos é composta por três etapas principais:

- **Identificação dos ativos críticos:** Identifica os componentes de TIC mais relevantes para o negócio, como sistemas, infraestrutura e equipamentos, considerando sua relevância estratégica para os objetivos institucionais do TJPA.
- **Mapeamento das dependências entre ativos:** Analisa como os ativos críticos dependem de outros ativos e serviços, estabelecendo uma cadeia de interdependências que reflete o impacto de falhas em cascata.
- **Mapeamento dos riscos associados aos ativos:** Avalia os riscos que podem comprometer a funcionalidade dos ativos críticos, consolidando essas informações em matrizes de risco específicas, usadas para embasar os Protocolos de Continuidade Operacional (PCO).

Os ativos essenciais são organizados em três categorias principais, conforme seu papel no suporte às operações do TJPA:

- Ativos Essenciais de Negócio: Compreende o sistema Judicial Eletrônico -PJE
- Ativos Essenciais de Infraestrutura: Incluem datacenters, redes, espaços físicos e softwares necessários para o funcionamento do ativo essencial de negócio.
- Ativos Essenciais de Segurança da Informação: Envolvem equipamentos e softwares destinados à proteção do ambiente computacional, como firewalls, sistemas de detecção de ameaças e soluções de controle de acesso.

A análise de riscos é normatizada pela ABNT NBR ISO 31000:2018 - Gestão de riscos - Diretrizes. O diagrama que resume esta análise consta no anexo IIII deste PCN.

17. IMPACTOS AVALIADOS

Os impactos analisados nas matrizes de risco (mapeamento dos riscos associados a ativos) incluem:

- Impacto financeiro: Perda de recursos ou aumento de custos devido à interrupção.
- Impacto legal: Descumprimento de normas ou prazos legais.
- Impacto reputacional: Danos à reputação institucional.
- Impacto operacional: Consequências negativas no funcionamento diário da organização.

Esse processo estruturado assegura que os serviços críticos do TJPA sejam protegidos e restaurados com eficiência em situações de contingência.

18. ESCALA DE AVALIAÇÃO

Para avaliar e mensurar componentes da continuidade de negócio (como ativos essenciais), utiliza-se uma escala de cinco pontos para indicadores como probabilidade e impacto. Essa escala estabelece um padrão empírico, baseado na percepção de indivíduos com experiência prática no cenário analisado. O bom senso do grupo é essencial para definir essas grandezas, que devem considerar também dados e registros históricos, documentados ou não, sobre os ativos.

A escala é definida como segue:

Nível	Conceito (Grandeza)	Pontuação
Muito Baixo	Grandeza mínima, praticamente irrelevante para o cenário analisado.	1
Baixo	Grandeza pequena, com efeitos limitados e de pouca influência no contexto.	2
Médio	Grandeza moderada, perceptível e que exige atenção para avaliação adequada.	3
Alto	Grandeza significativa, com impacto relevante que pode influenciar decisões ou processos.	4
Muito Alto	Grandeza crítica, de alta importância, com potencial de alterar significativamente o cenário analisado.	5

19. PROTOCOLOS DA CONTINUIDADE DE NEGÓCIO

O Plano de Continuidade de Negócio (PCN) define protocolos específicos para cada ativo crítico. Esses protocolos detalham ações claras para:

- Estabelecer procedimentos de comunicação e gestão de crise;
- Cessar a solução de continuidade, permitindo a operação do ativo, ainda que de forma limitada, dentro de um SLA previamente acordado;
- Retomar a normalidade operacional do ativo, no prazo previamente estabelecido (RTO), com tolerância a perdas de dados conforme limites definidos.

Os protocolos são ativados após a Declaração de Crise e incluem os seguintes:

19.1 PROTOCOLO DE GESTÃO DE CRISE (PGC)

Este protocolo define ações para gerir cenários de crise, eliminando ou mitigando impactos por meio de comunicação eficaz e coordenação de esforços entre as partes envolvidas.

- Escopo: Gestão e comunicação de crise, bem como ativação do Protocolo de Continuidade Operacional (PCO) correspondente, garantindo entendimento claro das ações antes, durante e após a crise.
- Objetivos:
  - Garantir a segurança das pessoas;
  - Minimizar os impactos do incidente, promovendo esforços coordenados;
  - Orientar colaboradores com informações e procedimentos;
  - Informar partes interessadas, incluindo a sociedade, com clareza e em tempo adequado.
- Gestão e Execução:
  - GECC;
  - GCCC;
  - GGCC.

- **Ação:** Comunicação às autoridades competentes, partes interessadas, funcionários, colaboradores externos, cidadãos e mídia, garantindo informações consistentes sobre a crise e o status das ações de recuperação.
- **Encerramento:** Notificação formal do retorno dos ativos à operação normal, além da elaboração de um relatório detalhado com as atividades realizadas e lições aprendidas.

19.2 PROTOCOLO DE CONTINUIDADE OPERACIONAL (PCO)

O PCO descreve os procedimentos para garantir a continuidade de ativos críticos durante cenários de crise ou desastre.

- **Escopo:** Ações corretivas para colocar ativos críticos em operação em modo de contingência.
- **Objetivos:**
  - Manter a operação dos ativos essenciais durante crises;
  - Estabelecer regras e controles alternativos;
  - Definir equipes, formulários e relatórios necessários para a contingência.
- **Gestão e Execução**
  - GGCC;
  - GOCC;
  - GACC.
- **Ação**
  - Avaliar o impacto da crise e acionar os planos correspondentes conforme decisão do CECC.
  - Priorizar ativos críticos e coordenar ações de contingência.
- **Encerramento**
  - Informar o status do retorno dos ativos e consolidar informações para relatórios pós-contingência.

19.3 PROTOCOLO DE RECUPERAÇÃO DE CRISE (PRC)

Este protocolo descreve os procedimentos para restaurar ativos críticos ao seu estado normal de operação após crises ou desastres.

- **Escopo**
  - Garantir a recuperação dos ativos afetados, abrangendo conexões e configurações do ambiente crítico.
- **Objetivos**
  - Avaliar danos e prover meios de recuperação;
  - Evitar impactos secundários em outros ativos e serviços;
  - Restaurar os ativos no prazo tolerável definido.
- **Gestão e Execução**
  - GGCC;

  - GOCC;
  - GACC.
- Ação
  - Gerar relatório detalhado com perdas, danos, aquisições necessárias e força de trabalho.
  - Elaborar cronograma de recuperação priorizando ativos críticos.
- Encerramento
  - Emitir relatório final com horário de restabelecimento, aquisições realizadas, procedimentos executados e fornecedores acionados.

Nos anexos do PCN encontram-se modelos para cada protocolo descrito acima.

20. TESTES E EXERCÍCIOS DO PCN

O Plano de Continuidade de Negócios (PCN) e seus protocolos serão submetidos a testes pelas equipes responsáveis, visando avaliar sua eficácia e identificar possíveis melhorias. Os resultados desses testes serão discutidos em reuniões periódicas entre os líderes de cada protocolo, onde serão aprovados ou ajustados conforme necessário.

Os testes serão documentados em um registro de evidências denominado "Matriz de Testes", que será armazenado inclusive em meio físico, em pasta apropriada na SECINF. O modelo da Matriz de Testes está incluído no planejamento deste PCN.

Os resultados das avaliações serão registrados na "Matriz de Avaliação", a qual documenta quais gestores tomaram conhecimento do plano e suas respectivas avaliações, validando ou refutando o PCN. O modelo adotado para a Matriz de Avaliação também está presente no planejamento deste PCN.

A realização periódica de testes regulares é fundamental para assegurar a efetividade do Plano de Continuidade de Negócio (PCN), bem como a capacidade de resposta às situações de crise, contingência e recuperação de crises. Os testes têm como objetivo identificar falhas nos protocolos, avaliar a prontidão das equipes e garantir que os ativos críticos possam ser restaurados dentro dos parâmetros estabelecidos.

20.1 OBJETIVOS DOS TESTES

- Validar os protocolos do PCN, incluindo o Protocolo de Gestão de Crise (PGC), o Protocolo de Continuidade Operacional (PCO) e o Protocolo de Recuperação de Crises (PRC);
- Avaliar a eficácia das ações de mitigação e recuperação descritas nos protocolos;
- Identificar gaps e vulnerabilidades nos processos relacionados aos ativos críticos;
- Garantir que os níveis de SLA, RTO e RPO possam ser atingidos conforme os cenários previstos;
- Treinar as equipes envolvidas nos planos de continuidade e recuperação.

20.2 TIPOS DE TESTES

- Testes de Mesa (Tabletop Tests)
  - Exercícios simulados realizados em ambiente controlado, onde as equipes analisam cenários hipotéticos e avaliam os procedimentos do PCN sem impactar os ativos críticos.
- Testes Parciais (Walkthrough Tests)
  - Execução de procedimentos específicos de contingência e recuperação em um ambiente controlado, focando em ativos ou serviços selecionados.
- Testes Reais (Full Scale Tests)
  - Simulações abrangentes que reproduzem um cenário de crise real, com a execução completa dos protocolos do PCN, incluindo a ativação de contingência e recuperação dos ativos.

20.3 FASES DE EXECUÇÃO DOS TESTES

- Planejamento
  - Definição do escopo do teste, ativos críticos envolvidos, equipes participantes e métricas de avaliação.
  - Agendamento prévio para evitar impacto não planejado nos ativos e serviços.
- Execução
  - Realização do teste conforme o tipo e escopo definido, simulando cenários de crise e ativando os protocolos correspondentes.
  - Registro detalhado de todas as etapas e resultados obtidos.
- Avaliação e Documentação
  - Análise dos resultados para identificar falhas ou ineficiências nos procedimentos.
  - Registro das lições aprendidas e propostas de melhoria em relatórios específicos.
- Aprimoramento do PCN
  - Atualização dos protocolos com base nas lições aprendidas durante os testes.
  - Planejamento de novos testes para validar as correções implementadas.

20.4 FREQUÊNCIA DOS TESTES

Os testes do PCN devem ser realizados em periodicidade definida pelo Comitê de Continuidade e aprovada pelo TJPA, garantindo alinhamento com a criticidade dos ativos e os requisitos de conformidade. A frequência sugerida é:

- **Testes de Mesa:** Semestralmente;
- **Testes Parciais:** Anualmente;

- **Testes Reais:** Bienalmente.

Adicionalmente, testes deverão ser conduzidos sempre que surgirem novos fatores de risco, ocorrerem mudanças na análise de impacto ou forem incluídos novos serviços no PCN.

20.5 RESPONSABILIDADES

- **Grupo de Gestão de Contingência e Continuidade (GGCC):** Responsável pelo planejamento, coordenação e análise dos testes.
- **Grupo Operacional de Contingência e Continuidade (GOCC):** Responsável pela execução das ações previstas nos testes.
- **Grupo de Apoio de Contingência e Continuidade (GACC):** Suporte técnico e logístico durante a execução dos testes.

20.6 RELATÓRIOS DE TESTES

Os resultados de cada teste devem ser documentados em relatórios contendo:

- Ativos testados e protocolos ativados;
- Resultados alcançados, incluindo tempos de resposta (RTO e RPO);
- Falhas identificadas e propostas de correção;
- Lições aprendidas e recomendações para aprimoramento.

Os relatórios devem ser apresentados ao Comitê de Continuidade para análise e aprovação, garantindo a evolução contínua do PCN.

21. CRONOGRAMA DE IMPLEMENTAÇÃO DOS PROTOCOLOS E EXECUÇÃO DOS TESTES

Abaixo apresenta-se o cronograma de atividades para elaboração, validação e testes dos principais protocolos que compõem o Plano de Continuidade de Negócio - PCN do TJPA, de forma a garantir a efetividade das ações em caso de crises, interrupções ou desastres que impactem os serviços essenciais de TIC, são os prazos:

AÇÕES	PRAZOS (MESES)									
	JUL/2025	AGO/2025	SET/2025	OUT/2025	NOV/2025	DEZ/2025	JAN/2026	FEV/2026	MAR/2026	MAIO/2026
Planejamento do Projeto de Protocolos		•								
Criação do Protocolo de Gestão de Crise (PGC)			•	•	•	•	•	•		
Criação do Protocolo de Continuidade Operacional (PCO)			•	•	•	•	•	•		
Criação do Protocolo de Recuperação de Crise (PRC)			•	•	•	•	•	•		
Planejamento dos Testes						•				
Execução dos Testes							•	•		
Avaliação e Documentação do Testes							•	•		
Atualização dos Protocolos (pós-teste de mesa)							•	•		
Avaliação Final e Aprimoramento do PCN									•	•

PARTE II – ANÁLISE DE IMPACTO DE NEGÓCIO (BIA)

Esta Parte do Plano de Continuidade de Negócios (PCN) aborda a **Análise de Impacto nos Negócios (BIA)**, cujo objetivo é identificar e avaliar os processos críticos da organização e os impactos potenciais decorrentes de interrupções nesses processos.

A BIA permite compreender as consequências de interrupções nos processos críticos, fornecendo informações essenciais para o desenvolvimento de estratégias eficazes de continuidade de negócios.

Ao confrontar os resultados da BIA com a matriz de apetite a risco, é possível determinar as ações apropriadas para tratamento dos riscos identificados, assegurando a resiliência e a continuidade das operações da organização.

22. IDENTIFICAÇÃO DOS ATIVOS CRÍTICOS

Para todas as matrizes de ativos essenciais a seguir, as colunas de criticidade e de todos os subitens de impacto são mensuradas pela escala de 5 pontos, enquanto os RTO, POR são mensurados em horas e o SLA [2], é definido em porcentagem (%).

MATRIZ DE ATIVOS ESSENCIAIS DE NEGÓCIO - SISTEMAS JUDICIAIS

Nº	Ativo	RTO (h)	RPO (h)	SLA (%)	Prob	Impacto				
						Rep	Fin	Leg	Ope	Res (1-5)
1	PJE 1ª Grau	8	6	99	1	5	2	4	3	3,5
2	PJE 2ª Grau	8	6	99	1	5	2	4	3	3,5

MATRIZ DE ATIVOS ESSENCIAIS DE INFRAESTRUTURA - DATACENTER A

Nº	Ativo	RTO (h)	RPO (h)	SLA (%)	Prob	Impacto				
						Rep	Fin	Leg	Ope	Res (1-5)
3	Compute Lenovo Blade	8	6	99,50	1	4	3	2	3	3
4	Compute Nutanix	8	6	99,80	2	4	3	2	2	2,75
5	Storage Dorado V3	8	6	99,50	1	4	3	2	2	2,75
6	Switch SAN	8	6	99,50	1	4	3	2	2	2,75

MATRIZ DE ATIVOS ESSENCIAIS DE INFRAESTRUTURA – SOFTWARE DE DATACENTER

Nº	Ativo	RTO (h)	RPO (h)	SLA (%)	Prob	Impacto				
						Rep	Fin	Leg	Ope	Res (1-5)
7	Jboss	8	6	99,50	2	4	3	3	3	3,25
8	Openshift	8	6	99,50	3	4	3	3	3	3,25
9	DNS	8	6	99,50	2	4	3	3	3	3,25
10	NTP	8	6	99,50	1	4	3	3	3	3,25
11	Nutanix Acropolis Hypervisor	8	6	99,50	2	4	3	3	3	3,25

MATRIZ DE ATIVOS ESSENCIAIS DE INFRAESTRUTURA - REDES E COMUNICAÇÃO DE DADOS

Nº	Ativo	RTO (h)	RPO (h)	SLA (%)	Prob	Impacto				
						Rep	Fin	Leg	Ope	Res (1-5)
12	Switch Core	6	6	99	1	4	5	3	4	4
13	Link Internet	6	6	99,5	2	4	3	3	4	3,5

[2]Para a definição dos termos RTO, RPO e SLA, ver glossário

MATRIZ DE ATIVOS ESSENCIAIS DE INFRAESTRUTURA - ESPAÇO FÍSICO E SISTEMAS AUXILIARES, DATACENTER A (DCA)

Nº	Ativo	RTO (h)	RPO (h)	SLA (%)	Prob	Rep	Fin	Leg	Ope	Res (1-5)
14	Fornecimento de Energia Elétrica	24	24	99,50	1	1	1	1	2	1,25
15	Sistema de ar-condicionado de precisão	8	24	99,50	1	1	1	1	2	1,25

MATRIZ DE ATIVOS ESSENCIAIS DE SEGURANÇA DA INFORMAÇÃO – HARDWARE

						Impacto				
Nº	Ativo	RTO (h)	RPO (h)	SLA (%)	Prob	Rep	Fin	Leg	Ope	Res (1-5)
16	Firewall de Perímetro	2	48	95%	1	5	1	4	5	3,75
17	WAF	4	48	90%	1	5	1	3	5	3,5

MATRIZ DE ATIVOS ESSENCIAIS DE BANCOS DE DADOS

						Impacto				
Nº	Ativo	RTO (h)	RPO (h)	SLA (%)	Prob	Rep	Fin	Leg	Ope	Res (1-5)
18	PG Bouncer	2	2	90%	2	2	2	2	3	2,25
19	DB PJE 1G	5	5	99%	2	5	5	5	5	5
20	DB PJE 2G	5	5	99%	2	5	4	5	5	4,75

23. MAPEAMENTO DAS DEPENDÊNCIAS ENTRE ATIVOS

Para o mapeamento da dependência entre os serviços críticos de tecnologia do TJPA, deve ser utilizada a seguinte legenda:

Figura 5: Legenda de componentes do mapeamento de ativos

PJE 1G E PJE 2G

O Ativo PJE (1G e 2G) foi mapeado como segue:

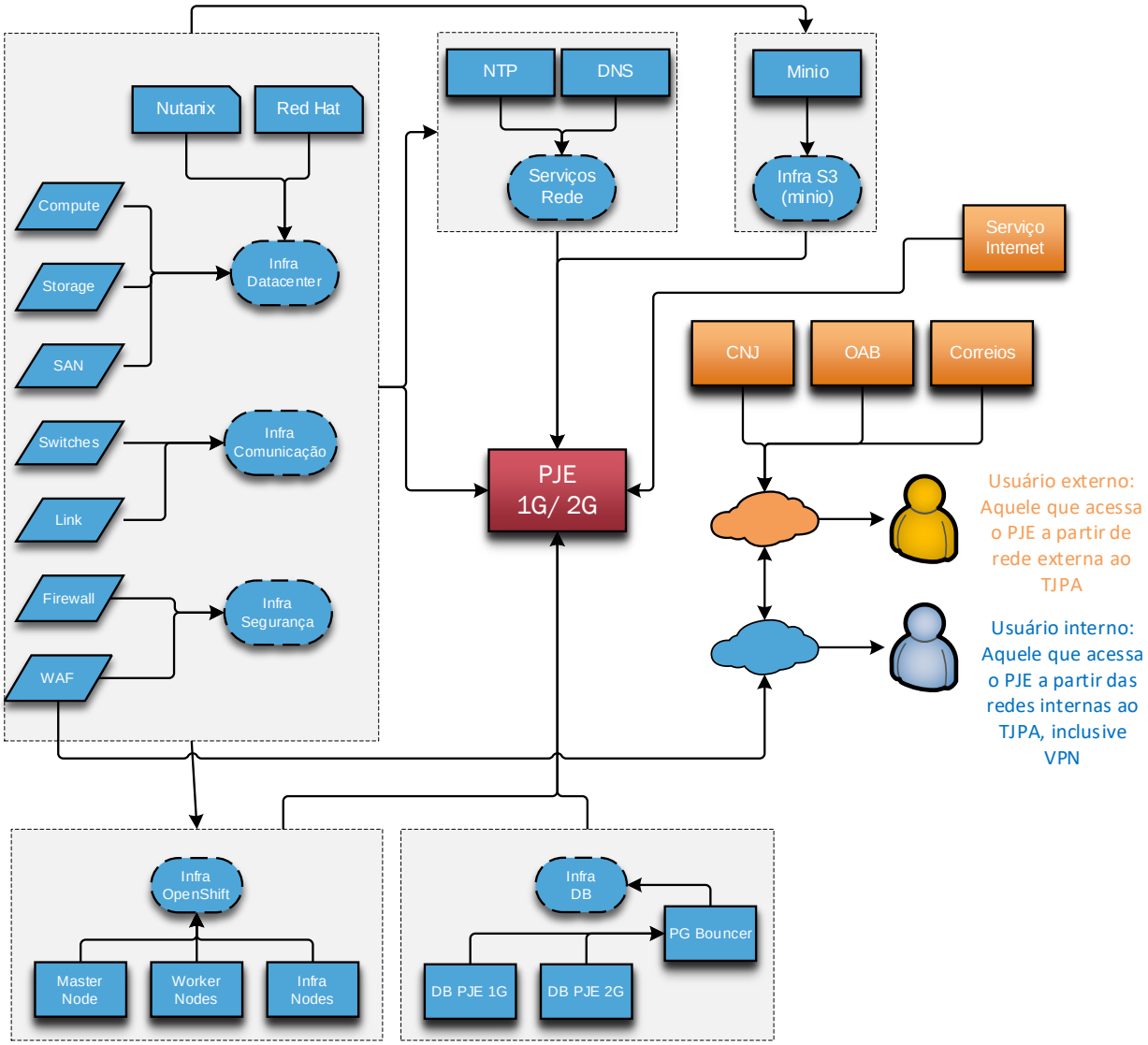


Figura 6: Mapeamento de dependências do PJE 1G e 2 G

24. RESPONSABILIDADES DOS GRUPOS FUNCIONAIS

A definição clara de responsabilidades, comumente referida pelo termo em inglês *accountability*, é essencial para a gestão eficaz das atividades inerentes tanto aos Protocolos de Gestão de mudanças, quanto aos protocolos de gestão de incidentes (PGC, PCO, PRD) relacionados aos serviços críticos protegidos pelo PCN. Essas responsabilidades são atribuídas aos grupos funcionais mencionados no [item 15] deste PCN, os quais são compostos por membros específicos, identificados **nominalmente**, assegurando que cada indivíduo tenha ciência de suas atribuições.

No contexto deste plano, as atribuições são designadas aos grupos por meio da "Matriz de Atribuições por Atividade". Os membros individuais responsáveis por cada atribuição são especificados na "Matriz de Contatos".

24.1 ATRIBUIÇÕES

As responsabilidades de gestão das atividades do PCN são delineadas para cada grupo funcional na matriz RACI apresentada a seguir. A Matriz RACI é uma ferramenta que define claramente os papéis e responsabilidades de cada membro ou grupo em relação às atividades do projeto, assegurando uma compreensão comum das funções atribuídas.

24.2 MATRIZ DE ATRIBUIÇÕES POR ATIVIDADE

Atividade	Grupo	R	A	C	I
Avaliação, testes e revisão do PCN	GECC	Cord Continuid	secretário	GECC	Todos os grupos
Desenvolvimento do PGC	GGCC	Comunicação	Assessor	COGV	Todos os grupos
Acionamento do PGC	GECC	Secretário	Secretário	GECC	Todos os grupos
Encerramento do PGC	GECC	GECC	Secretário	GECC	Todos os grupos
Testes e Revisão do PGC	GGCC	Comunicação	COGV	CIT/CA	Todos os grupos
Desenvolvimento do PCO	GOCC	CIT/ CA	CIT	COGV	Todos os grupos
Acionamento do PCO	GOCC	GECC	GECC	GECC	Todos os grupos
Encerramento do PCO	GOCC	GECC	GECC	COGV	Todos os grupos
Testes e Revisão do PCO	GOCC	CIT /CA	COGV	COGV/ GECC	Todos os grupos
Desenvolvimento do PRC	GCCC	CIT/CA	CIT	COGV	Todos os grupos
Acionamento do PRC	GCCC	GECC	GECC	GECC	Todos os grupos
Encerramento do PRC	GCCC	GECC	GECC	COGV	Todos os grupos
Testes e Revisão do PRC	GCCC	CIT/CA	COGV	COGV	Todos os grupos
Atualização da Matriz de Contatos	GGCC	GCCC	Comunicação	COGV	Todos os grupos
Providenciar materiais necessários	GACC	GACC	Secretário	COGV	Todos os grupos

Legenda da Matriz RACI:
- R (Responsável): Quem executa a atividade.
- A (Aprovador): Quem aprova e é responsável final pela atividade.
- C (Consultado): Quem deve ser consultado para fornecer informações ou conselhos.
- I (Informado): Quem deve ser informado sobre o andamento ou resultados da atividade.

Essa estrutura assegura que todas as atividades relacionadas aos protocolos de continuidade e contingência sejam claramente atribuídas, facilitando a coordenação e a comunicação entre os grupos funcionais envolvidos no PCN.

25. CONTATOS

25.1 MATRIZ DE CONTATOS

Esta matriz guarda contatos de pessoas nominadas, incluindo seus cargos, líderes dos grupos Funcionais do PCS. Que têm atribuições neste plano, bem como em seus protocolos.

Unidade Organizacional	Grupo	Cargo / Função	Pessoa	Celular
SECINFO	GECC	Secretário	Diego Leitão	
CIT	GGCC	Coordenador	Arilson Galdino	
CA	GGCC	Coordenador	Álvaro Alvão	
CAU	GGCC	Coordenador	Aline Oliveira	
Continuidade	GCCC	Líder da Continuidade	Fábio Reis	
Apoio	GACC	Líder do Apoio à Continuidade		

As matrizes de contatos para as equipes de comunicação, operacional e de apoio estão definidas em cada protocolo.

PARTE III - IMPLEMENTAÇÃO E GESTÃO

26. GESTÃO DE MUDANÇAS

A Gestão de Mudanças é fundamental para assegurar que todas as alterações no ambiente de Tecnologia da Informação e Comunicação (TIC) sejam realizadas de maneira controlada, minimizando riscos e garantindo a continuidade dos serviços críticos.

Objetivo

Estabelecer procedimentos e diretrizes para a implementação de mudanças no ambiente de TIC, assegurando que sejam realizadas de forma planejada, controlada e documentada, evitando interrupções nos serviços essenciais.

- Escopo: Esta seção abrange todas as mudanças planejadas ou emergenciais nos ativos de TIC, incluindo hardware, software, redes e processos relacionados, que possam impactar a continuidade dos negócios.
- Princípios de Gestão de Mudanças: A gestão de mudanças é norteada pelos princípios a seguir:
  - Planejamento: Todas as mudanças devem ser cuidadosamente planejadas, considerando os potenciais impactos e riscos associados.
  - Avaliação de Riscos: Antes da implementação, cada mudança deve passar por uma avaliação de riscos para identificar e mitigar possíveis efeitos adversos.

  - **Aprovação:** As mudanças devem ser aprovadas por um comitê ou autoridade designada, garantindo que todas as partes interessadas estejam cientes e de acordo.
  - **Comunicação:** Informar todas as partes afetadas sobre a natureza, cronograma e impacto esperado da mudança.
  - **Documentação:** Manter registros detalhados de todas as etapas do processo de mudança, incluindo solicitações, aprovações, planos de implementação e resultados.
- Procedimentos de Gestão de Mudanças
  - **Solicitação de Mudança:** Formalizar a solicitação de mudança, detalhando a natureza, justificativa e impacto esperado.
  - **Avaliação e Análise:** O comitê de mudanças avalia a RFC, analisa os riscos e benefícios, e decide sobre a viabilidade da mudança.
  - **Planejamento da Implementação:** Desenvolver um plano detalhado que inclua recursos necessários, cronograma, medidas de contingência e plano de reversão.
  - **Aprovação Formal:** Obter aprovação formal do plano de mudança antes da implementação.
  - **Implementação:** Executar a mudança conforme o plano aprovado, monitorando em tempo real para identificar e resolver quaisquer problemas imediatamente.
  - **Revisão Pós-Implementação:** Após a implementação, realizar uma revisão para avaliar o sucesso da mudança, documentar lições aprendidas e atualizar procedimentos conforme necessário.
- Papéis e Responsabilidades
  - **Solicitante da Mudança:** Responsável por iniciar a RFC e fornecer todas as informações necessárias.
  - **Comitê de Mudanças:** Grupo responsável por avaliar, aprovar e priorizar as solicitações de mudança.
  - **Gestor de Mudanças:** Coordena o processo de gestão de mudanças, assegurando o cumprimento das políticas e procedimentos estabelecidos.
  - **Equipe de Implementação:** Executa as atividades relacionadas à implementação da mudança conforme o plano aprovado.
- Monitoramento e Melhoria Contínua
  - **Indicadores de Desempenho:** Estabelecer métricas para avaliar a eficácia do processo de gestão de mudanças, como número de mudanças bem-sucedidas, tempo médio de implementação e incidentes pós-mudança.
  - **Auditorias Periódicas:** Realizar auditorias regulares para assegurar a conformidade com as políticas de gestão de mudanças e identificar oportunidades de melhoria.
  - **Feedback:** Coletar feedback das partes envolvidas para aprimorar continuamente o processo de gestão de mudanças.

Implementando esta estrutura de Gestão de Mudanças, o Tribunal de Justiça do Estado do Pará (TJPA) poderá assegurar que as alterações no ambiente de TIC sejam conduzidas de maneira eficiente e controlada, minimizando riscos e garantindo a continuidade dos serviços críticos.

26.1 PROCESSO DE GESTÃO DE MUDANÇAS

Consultar Anexo IV

27. GESTÃO DE INCIDENTES

O processo de gestão de incidentes é acionado quando ocorre um incidente, seja ele decorrente de um risco previamente identificado ou não, que resulte em interrupção ou degradação de um dos ativos críticos dos serviços de TIC do TJPA. O objetivo é restaurar a operação normal do serviço o mais rápido possível, minimizando o impacto nas operações de negócio.

27.1 PROCESSO DE GESTÃO DE INCIDENTES

Devido a sua complexidade, o processo de gestão de incidentes é representado por um macroprocesso que se divide em 3 subprocessos, como a seguir:

Consultar Anexo V

27.2 DIRETRIZES DO PROCESSO DE GESTÃO DE INCIDENTES

- O gerenciamento de incidentes (este PCN) e seus protocolos complementares devem estar prontos para serem executados a qualquer momento;
- O analista responsável pode ser um especialista pelo serviço, no caso do horário de expediente, ou um analista de sobreaviso, em caso de incidentes fora do horário comercial;
- As chefias, coordenadorias e lideranças envolvidas, assim como o próprio secretário de informática, necessitam ter uma segunda pessoa para acionamento em caso de impossibilidade de se acionar o titular.
- Treinamentos na execução dos protocolos envolvidos devem ser promovidos periodicamente a fim de tornar natural sua execução caso necessário;
- A gestão de incidentes requer a existência manutenção e operação de um plano de backup efetivo conforme requisitos negociais para salvaguarda das informações das aplicações;

- Testes dos protocolos também devem ser executados periodicamente a fim de averiguar sua aplicabilidade.

27.3 GESTÃO DE BACKUP E RESTAURAÇÃO DE DADOS

O backup é parte indissociável da continuidade e da recuperação das operações. Nesta seção são estabelecidos os critérios técnicos e operacionais que devem obrigatoriamente orientar a realização dos backups dos dados críticos, de modo a assegurar a continuidade ininterrupta dos serviços de TIC.

27.3.1 PLANO DE BACKUP

O TJPA manterá e executará um Plano de Backup conforme determinado na PSI e em consonância com este PCN. O plano deve conter:

- Planejamento de retenção de dados (curto, médio e longo prazo);
- Classificação da criticidade dos dados e frequência de backup (diária, semanal, mensal);
- Tecnologias utilizadas (local, nuvem, híbrido);
- Mecanismos de criptografia e controle de acesso aos arquivos;
- Responsáveis pelas rotinas de backup e testes de restauração;
- Procedimentos de notificação em caso de falha ou indisponibilidade do sistema de backup.

27.3.2 RESTAURAÇÃO E TESTES

A restauração dos dados deve ser testada periodicamente, conforme definido no cronograma do Plano de Backup. Os testes devem simular cenários de perda de dados e observar:

- O tempo de restauração (RTO);
- O ponto de restauração (RPO);
- A consistência e integridade das informações restauradas;
- A efetividade dos responsáveis e ferramentas envolvidas;
- A rastreabilidade e documentação dos procedimentos executados.

27.3.3 INTEGRAÇÃO COM A BIA

As definições de RPO e RTO registradas na BIA do PGRTIC guiarão as decisões sobre frequência de backup e tempo máximo de recuperação dos dados de cada ativo essencial.

28. MATRIZ DE PROTOCOLOS DE CONTINGÊNCIA E CONTINUIDADE

Ativo	Itens tratados	PGC	PCO	PRC
Infraestrutura de Datacenter	Compute Lenovo e Nutanix, storage, SAN, Vmware, Red Hat, NTP, DNS, Minio OpenShift	PGC-01	PCO-01	PRC-01
Infraestrutura de Comunicação	Switches, Links e Roteadores	PGC-02	PCO-02	PRC-02
Infraestrutura de Segurança	WAF e Firewall	PGC-03	PCO-03	PRC-03
Infraestrutura de Bancos de Dados	PgBouncer, PJE 1G e PJE 2G (PostrgreSQL)	PGC-04	PCO-04	PRC-04

29. MATRIZ DE TESTES

Plano/ Protocolo	Data	Tipo	Motivo	Status	Resultado

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.
Resultado: Relata o resultado do Teste executado com sucesso, insucesso ou inconclusivo.

30. MATRIZ DE AVALIAÇÃO

Esta matriz regista quais gestores tomaram conhecimento do presente plano, e quais suas avaliações sobre este plano, de forma a validar ou refutar o PCN.

28.1 MATRIZ DE AVALIAÇÃO

Nome	Cargo	Data	Resultado	Assinatura

Resultado: Aprovado, aprovado com ressalvas, reprovado

GLOSSÁRIO

Termo ou Sigla	Conceito ou definição
ameaça	Qualquer atividade maliciosa, intencional ou acidental, seja através de meios eletrônicos ou não, que possa explorar uma vulnerabilidade e, assim, obter acesso, danificar ou destruir um determinado ativo ou serviço.
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 de informação; os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso.
BIA	Do inglês Business Impact Analysis, é conjunto de técnicas, métodos e ferramentas que tem por finalidade a identificação e análise de serviços ou atividades críticas de negócios, compreendendo assim o impacto advindo da solução de continuidade em tais serviços.
CID	Sigla que referencia as 3 prioridades básicas e fundamentais da segurança da informação: Confidencialidade, Integridade e Disponibilidade.
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 crise.
criticidade	Representa o quão drástica é uma situação para o negócio do TJPA.
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 Assistência com papel e responsabilidades na execução de procedimentos descritos no PCN.
impacto	Desconformidade causada por um incidente ou desastre.
Protocolo de Recuperação de Crise (PRC)	Documentação dos procedimentos e informações necessárias para que o órgão operacionalize o retorno das atividades críticas de TIC à normalidade.
Protocolo 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 crises.
Protocolo de Gestão de Crise (PGC)	Documento operacional de ação claramente definido para ser utilizado quando ocorrer uma crise. Tal documento deve cobrir as principais pessoas, recursos, serviços e outras ações que sejam necessárias para implementar o processo de gerenciamento de crise.
responsável pelo ativo	Indivíduo legalmente instituído por sua posição e/ou cargo, responsável primário pela viabilidade e sobrevivência dos ativos de informação.
risco	Possibilidade de que um evento afete negativamente o alcance dos objetivos (TCU). É a probabilidade de uma ameaça explorar certa vulnerabilidade em um ativo ou serviço de TIC, de forma a comprometer a continuidade de negócio de uma organização.
RPO	*Recovery Point Objective*: Compreende o ponto de recuperação dos dados, ou seja, uma vez que o ativo retorne à operação, qual a quantidade de dados máxima (em unidades de tempo) que poderá ser perdida sem que o negócio seja afetado; está focado na integridade dos dados; é expresso em horas.
RTO	*Recovery Time Objective*: Tempo estabelecido para que um sistema seja recuperado de uma solução de continuidade; está ligado à disponibilidade do sistema; é expresso em horas.
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)
SLA	Da sigla em inglês para Service Level Agreement (acordo de nível de serviço), refere-se a uma deliberação entre os clientes e a área TIC sobre a disponibilidade a ser atingida; neste caso específico em relação ao tempo de disponibilidade do ativo PJe em certo período. O SLA é um tempo de porcentagem dentro de certo período que o sistema precisa estar operando satisfatoriamente. Caso não seja cumprido, é declarado uma crise. A partir desta declaração, passa a contar o RTO.
solução de continuidade	Interrupção de um serviço por falha em algum de seus componentes.