PLANO DE CONTINUIDADE DOS SERVIÇOS DE TIC - 2026

PODER JUDICIÁRIO
DO ESTADO DA BAHIA

Apresentação

Este documento apresenta o Plano de Continuidade de Serviços da Secretaria de Tecnologia da Informação e Modernização (SETIM) do Tribunal de Justiça do Estado da Bahia (TJBA) e estabelece as diretrizes, estratégias e responsabilidades necessárias para assegurar a continuidade, a resiliência e a recuperação dos serviços de Tecnologia da Informação e Comunicação (TIC) considerados essenciais ao cumprimento da missão institucional do Tribunal, especialmente no suporte à prestação jurisdicional e aos serviços prestados à sociedade.

Este Plano foi concebido e estruturado em conformidade com os princípios e requisitos da ABNT NBR ISO 22301 – Sistemas de Gestão de Continuidade de Negócios, adotando uma abordagem sistemática e baseada em risco para a preparação, resposta e recuperação frente a eventos disruptivos que possam comprometer a disponibilidade, a integridade ou a continuidade dos serviços de TIC. Alinha-se, ainda, às diretrizes da Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD 2021–2026) e às disposições da Resolução CNJ nº 396, de 7 de junho de 2021, que estabelecem a necessidade de mecanismos formais de continuidade e recuperação de serviços críticos no âmbito do Poder Judiciário.

No contexto do Sistema de Gestão de Continuidade de Negócios (SGCN) do TJBA, este Plano de Continuidade de Serviços da SETIM constitui um plano especializado de continuidade funcional, com foco nos serviços de TIC, e integra o conjunto de planos táticos e operacionais que suportam o Plano de Continuidade de Negócios (PCN) corporativo do Tribunal. Considera-se, portanto, como premissa de referência, a existência, a atualização periódica e a aplicabilidade do PCN institucional, bem como dos demais planos corporativos correlatos, tais como planos de gestão de riscos, segurança da informação, gestão de crises e comunicação institucional.

Dada a abrangência e a natureza deste Plano, não é seu objetivo substituir ou replicar os conteúdos do PCN corporativo, mas sim complementá-lo, detalhando os procedimentos, papéis, estratégias e mecanismos específicos necessários para garantir a continuidade dos serviços de TIC sob responsabilidade da SETIM, de forma integrada e coerente com as diretrizes institucionais de continuidade de negócios do TJBA.

Este Plano deve ser entendido como um documento dinâmico, sujeito a revisões periódicas e a melhorias contínuas, em consonância com o ciclo de gestão preconizado pela ISO 22301 (planejar, implementar, monitorar, analisar criticamente e melhorar). Sua efetividade depende não apenas de sua formalização documental, mas também do comprometimento, da capacitação das equipes envolvidas, da realização de testes e exercícios periódicos e da integração com os processos corporativos de governança, gestão de riscos e gestão de serviços de TIC da SETIM.

Histórico de revisões

DATA	VERSÃO	DESCRIÇÃO
2022	1.0	Criação da primeira versão do PCTIC
2026	1.1	1ª Revisão do PCTIC

Sumário

1. Introdução

O presente Plano de Continuidade dos Serviços de Tecnologia da Informação e Comunicação (PCTIC) da Secretaria de Tecnologia da Informação e Modernização (SETIM) do Tribunal de Justiça do Estado da Bahia (TJBA) estabelece diretrizes, princípios, responsabilidades e mecanismos operacionais para manter e/ou restaurar, em prazos aceitáveis, a prestação dos serviços de TIC que suportam as atividades judiciais, administrativas e extrajudiciais do Tribunal, inclusive aqueles que impactam diretamente o atendimento a partes interessadas externas e internas.

Este Plano tem como finalidade assegurar que, diante de incidentes graves, falhas relevantes ou eventos disruptivos (tecnológicos, operacionais, ambientais ou de segurança), a SETIM disponha de estratégias e planos de ação predefinidos para responder de modo coordenado, reduzindo o tempo de interrupção, preservando informações e viabilizando o retorno sustentado à normalidade, de forma compatível com a criticidade e a prioridade dos serviços afetados.

A elaboração e a manutenção deste Plano constituem iniciativa alinhada às diretrizes nacionais de continuidade aplicáveis ao Poder Judiciário e se apresentam como elemento estruturante da capacidade institucional de resiliência do TJBA. Trata-se de um documento de caráter estratégico, orientativo e integrador, que define premissas básicas e articula planos de níveis tático-operacional especializados para diferentes dimensões da continuidade e recuperação.

Este Plano é concebido em consonância com os princípios da ISO 22301 (Sistema de Gestão de Continuidade de Negócios – BCMS), que estabelece um arcabouço para planejar, implementar, operar, monitorar e melhorar continuamente a capacidade de continuidade de serviços diante de incidentes disruptivos.

Em particular, este documento observa a lógica de gestão preconizada pela norma ao:

- Definir escopo e fronteiras do que se pretende assegurar em continuidade, com delimitação clara de serviços, interfaces e dependências (escopo do plano de TIC dentro do BCMS institucional).
- Basear-se em análise de impacto e análise de riscos, premissa central para priorização de serviços, definição de objetivos de recuperação e seleção de estratégias.
- Estabelecer estruturas de acionamento, papéis e responsabilidades para resposta organizada e tomada de decisão em crise, integrando áreas técnicas e de gestão.
- Prever validação e testes periódicos, como requisito de garantia de efetividade, maturidade e melhoria contínua do plano.

Por se tratar de um Plano de Continuidade especializado em TIC, este documento é parte integrante do arcabouço de continuidade do TJBA e deve ser interpretado como um instrumento tático-operacional que complementa um Plano de Continuidade de Negócios (PCN) corporativo. Em razão da abrangência deste

Plano de TIC, considera-se como premissa de referência a existência, atualização e aplicabilidade do PCN institucional e de planos corporativos correlatos (ex.: gestão de crises, comunicação institucional e políticas internas). Essa premissa assegura coerência sistêmica e evita duplicidade de conteúdos, mantendo a especialização técnica do plano de TIC.

2. Justificativa e Objetivo

Falhas relevantes nos serviços de TIC afetam diretamente a continuidade da prestação jurisdicional e a entrega de serviços essenciais à sociedade, exigindo medidas de proteção, resposta e recuperação que sejam rápidas, coordenadas e eficazes.

Assim, este Plano visa prover condições para proteger e recuperar os processos críticos de TIC relacionados aos sistemas essenciais em situações de incidentes graves ou desastres, atuando como resposta estruturada aos resultados da Análise de Impacto nos Negócios e da Análise de Riscos.

Dessa forma, este Plano reforça a capacidade institucional de:

- Manter níveis mínimos aceitáveis de serviço durante a interrupção;
- Recuperar serviços e dados dentro de objetivos e prioridades definidos;
- Reduzir danos e impactos (operacionais, reputacionais, legais e de segurança);
- Orquestrar comunicação e coordenação entre equipes técnicas, gestão e partes interessadas.

A criticidade dos serviços de TIC contemplados por este Plano é determinada de forma objetiva a partir da cadeia de prestação de serviços disponibilizada ao público e às estruturas internas do TJBA, materializada nos seguintes canais oficiais de solicitação e atendimento:

Portal Service Desk Externo: disponível para o público externo, é destinado principalmente ao atendimento de advogados e delegatários, mediante ofertas de serviços publicadas para esse público.

Portal Service Desk Interno: disponível para o público interno, mediante autenticação (login e senha) na rede do TJBA. Esse portal é destinado ao atendimento das unidades internas, magistrados, servidores e estruturas administrativas do Tribunal.

Os serviços ofertados nesses portais são estruturados e correlacionados a categorias técnicas e filas de tratamento na ferramenta de ITSM em uso no Tribunal.

Assim, os serviços publicados nos portais funcionam como determinantes de criticidade, pois representam a “vitrine” institucional de entrega e, ao serem acionados, mobilizam processos internos de atendimento, suporte, escalonamento e sustentação que ativam serviços técnicos e componentes subjacentes geridos na ferramenta de gestão dos serviços de TIC “CASM”. Nessa ferramenta, observam-se serviços externos relacionados, por exemplo, a PJe, SAJ, PROJUDI, DAJE/SELO DIGITAL, e serviços internos ligados a suporte de sistemas, rede, equipamentos, identidade/acesso e demais necessidades corporativas.

No fluxo operacional do atendimento das solicitações de serviços de TIC, as solicitações registradas no Portal do Service Desk, tanto ***Interno*** (estruturas organizacionais ou áreas do TJBA) como ***Externo*** (outros interessados não

colaboradores do TJBA), passam pela estrutura de atendimento (Central de Atendimento) para conferência/triagem e, na sequência, são integradas à ferramenta de gestão de serviços de TIC, CASM, gerando registros que ativam os grupos técnicos responsáveis.

Esse encadeamento confirma que a criticidade não se limita ao “sistema final” percebido pelo usuário externo, mas inclui todos os serviços de TIC intermediários e componentes técnicos indispensáveis ao atendimento (plataforma de service desk, integrações, identidade e acesso, conectividade, infraestrutura de datacenter, segurança, entre outros).

3. Escopo

O escopo deste Plano de Continuidade de TIC abrange as estratégias necessárias à continuidade, contingência e recuperação dos serviços de TIC essenciais, com foco nos processos e capacidades sob responsabilidade da SETIM. O Plano pode ser acionado no âmbito da SETIM de forma isolada ou como parte coordenada do Plano de Continuidade de Negócios do TJBA.

Como instrumento integrador, este Plano estrutura a continuidade em planos operacionais especializados, que organizam a resposta e recuperação por dimensão:

- Plano de Continuidade Operacional (PCO): procedimentos alternativos e ações de contingência para manter serviços essenciais durante a crise;
- Plano de Administração de Crises (PAC): coordenação, comunicação e gestão de crise, com foco em alinhamento e comunicação eficaz;
- Plano de Recuperação de Desastres (PRD): recuperação do ambiente principal e retorno aos níveis originais de operação.

O Plano é suportado por registros e estruturas complementares (como a matriz do plano de gestão de riscos) que relacionam cenários disruptivos e ações correspondentes, garantindo rastreabilidade entre risco, decisão de acionamento e resposta operacional.

Estruturas envolvidas: atendimento, suporte, monitoramento e sustentação

A execução do Plano de Continuidade de TIC depende de atuação coordenada das estruturas organizacionais e técnicas que compõem a SETIM, com papéis complementares na sustentação dos serviços ponta a ponta. Participam deste plano as equipes e coordenações técnicas, com responsabilidades de administração do plano, execução de contingência, comunicação e recuperação.

No contexto atual, todas as estruturas da SETIM estão de alguma forma envolvidas na atuação de monitoramento e suporte técnico em diferentes níveis para sustentar e continuar os serviços de TIC.

Do ponto de vista do monitoramento operacional, existe uma estrutura específica da CPROD que realiza o monitoramento técnico dos componentes tecnológicos (ativos) que compõe os serviços e quando detectadas anomalias nesses componentes ocorre o acionamento baseado no agrupamento técnico de ativos/serviços por times, com grupos como CPROD, COTEC_SEGURANÇA, COTEC_LINUX_PJE, COTEC_BANCO e outros, refletindo a organização de acionamento e responsabilidades técnicas para infraestrutura, segurança, bancos e aplicações críticas.

Esse modelo reforça um princípio essencial de continuidade conforme indica a ISO 22301: a capacidade de resposta deve considerar dependências técnicas e operacionais reais (aplicações, rede, segurança, banco de dados, datacenter, integrações e canais de atendimento), com responsabilidades explícitas e rotinas de acionamento compatíveis com o nível de criticidade

A Figura 1 representa todos os processos envolvidos na Gestão de Continuidade de Negócios (GCN).

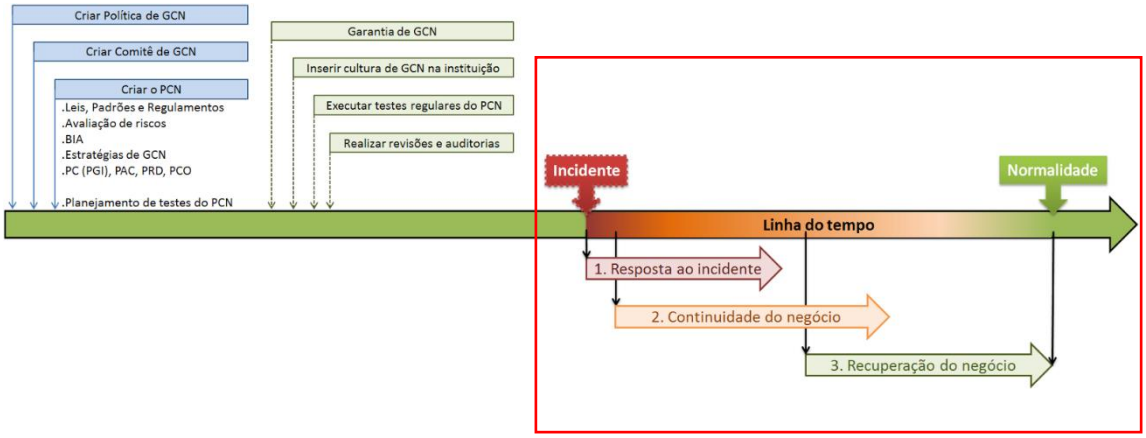


Figura 1: Representação do Processo de Continuidade de Negócios

A efetividade deste Plano requer que os objetivos de recuperação (como RTO e RPO) sejam derivados da Análise de Impacto nos Negócios e reavaliados periodicamente, garantindo que os serviços críticos tenham metas compatíveis com a tolerância institucional à interrupção.

Essa orientação de criticidade é empregada neste plano como um BIA/AIN (Análise de Impacto nos Negócios) simplificado, onde tenta se estabelecer que a priorização, impactos e tempos toleráveis de recuperação dos ativos e componentes dos serviços de TIC são definidos a partir da interferência direta ou indireta das ocorrências destes componentes nas opções de serviços oferecidos nos portais interno e externo dos serviços da SETIM.

Além disso, a SETIM promove, quando aplicável, testes e validações (ex.: testes de mesa, simulações e exercícios) para avaliar a consistência dos procedimentos e a prontidão das equipes, mantendo registros e promovendo melhoria contínua do plano, conforme previsto neste plano e convergente com a ISO 22301.

Ao consolidar o encadeamento Portais Service Desk (Interno/Externo) → CASM (ITSM) → Times técnicos (monitoramento e suporte) → Subplanos (PCO/PAC/PRD), este Plano estabelece uma base objetiva e auditável para:

- Identificar e justificar quais serviços são críticos (por sua exposição e compromissos com público externo e unidades internas);
- Definir e manter estratégias e procedimentos de continuidade para diferentes cenários disruptivos;
- Garantir governança, acionamento, comunicação e recuperação de serviços em níveis aceitáveis;
- Sustentar um ciclo de validação, aprendizado e melhoria contínua, aumentando a maturidade de continuidade da SETIM e do TJBA.

4. Definições

As definições e termos utilizados neste Plano de Continuidade dos Serviços de Tecnologia da Informação e Comunicação (PCTIC) seguem os conceitos que refletem as práticas institucionais adotadas pelo Tribunal de Justiça do Estado da Bahia (TJBA) e pela Secretaria de Tecnologia da Informação e Modernização (SETIM).

Sempre que aplicável, tais conceitos foram alinhados e harmonizados com as definições estabelecidas pela ABNT NBR ISO 31000 – Gestão de Riscos e pela ISO 22301 – Sistemas de Gestão da Continuidade de Negócios, de modo a assegurar coerência conceitual, aderência às boas práticas internacionais e consistência técnica entre risco, impacto, criticidade e continuidade.

Ameaça: Evento, agente ou circunstância potencial, interna ou externa, capaz de explorar uma vulnerabilidade de um ativo de TIC e causar impacto negativo aos serviços e/ou objetivos institucionais do TJBA.

Análise de Impacto nos Negócios (AIN ou BIA): Processo sistemático de identificação e avaliação dos impactos decorrentes da interrupção dos serviços de TIC, utilizado para definir criticidade, prioridades de recuperação, RTO – Tempo Objetivo de Retorno e POR – Ponto Objetivo de Retorno.

Ativo de TIC: Recurso de TIC que possui valor para o TJBA e que é utilizado para apoiar a prestação de serviços de Tecnologia da Informação e Comunicação, incluindo, mas não se limitando a: sistemas de informação, dados, aplicações, infraestrutura tecnológica, redes, equipamentos, pessoas, contratos, processos e serviços.

Backup: Cópia de segurança dos dados, sistemas ou configurações, realizada periodicamente, com o objetivo de permitir sua restauração em caso de perda, corrupção ou indisponibilidade. (Backup não representa, por si só, a estrutura de recuperação, mas é um dos principais meios para viabilizá-la).

Catálogo de Serviços de TIC: Conjunto estruturado e autorizado de serviços disponibilizados pela SETIM aos usuários internos e externos do TJBA, contendo informações sobre descrição do serviço, público atendido, critérios de solicitação, níveis de serviço associados, responsabilidades e canais de atendimento. O Catálogo de Serviços constitui a referência oficial para a prestação, gestão, priorização e continuidade dos serviços de TIC. (Alinhado às práticas de ITIL e à ISO 22301 – serviços no escopo do BCMS).

CMDB (Configuration Management Database – Base de Dados de Gerenciamento de Configuração): Repositório lógico que armazena informações sobre os Itens de Configuração de TIC e seus relacionamentos, permitindo compreender dependências técnicas e impactos de incidentes, mudanças, falhas e desastres sobre os serviços de TIC. A CMDB é um elemento essencial para análise de impacto, continuidade de serviços e recuperação de desastres e tende a ser mantida dentro de uma ferramenta de ITSM como a CASM.

Consequência (Impacto de um Risco): Resultado direto da materialização de um risco, representando o efeito negativo imediato sobre um ativo, processo, serviço ou objetivo específico, como indisponibilidade técnica, perda de dados, falha de sistema ou interrupção de um serviço de TIC. A consequência é avaliada no contexto da gestão de riscos e compõe a análise do risco junto com a probabilidade. (ISO 31000 – consequência ≠ impacto de negócio)**.**

Continuidade dos Serviços de TIC: Capacidade de manter ou restaurar os serviços críticos de TIC em níveis aceitáveis e dentro de prazos definidos, após a ocorrência de um incidente grave ou desastre.

Contingência: Conjunto de medidas, procedimentos e soluções alternativas previamente planejadas, adotadas para manter a operação em nível mínimo aceitável dos serviços de TIC durante a indisponibilidade total ou parcial dos recursos e ambiente principal.

Criticidade do Serviço de TIC: Nível de importância de um serviço de TIC para a continuidade das atividades institucionais do TJBA, determinado a partir da Análise de Impacto nos Negócios (AIN/BIA) e utilizado para priorização das ações de continuidade e recuperação.

Desastre: Evento disruptivo de grande magnitude que provoca interrupção severa e prolongada dos serviços de TIC, exigindo a execução coordenada do Plano de Continuidade, do Plano de Contingência e do Plano de Recuperação de Desastres.

Estruturas Técnicas Envolvidas: Unidades organizacionais da SETIM responsáveis pelo atendimento, suporte, monitoramento, sustentação e recuperação dos serviços de TIC, incluindo, entre outras, COATE, COTEC, CODAT, CPROD, COSIS e CSJUD.

Evento Disruptivo: Ocorrência que provoca interrupção relevante ou prolongada dos serviços de TIC, podendo exigir a ativação de planos de continuidade, contingência ou recuperação.

Impacto: Consequência da materialização de um risco, refletida em prejuízos operacionais, institucionais, legais, financeiros, reputacionais ou à segurança da informação.

Impacto de Negócio (Impacto da BIA / AIN): Efeito que a interrupção de um processo, serviço ou atividade essencial causa sobre os objetivos organizacionais, tais como a prestação jurisdicional, a conformidade legal, a imagem institucional, a continuidade administrativa ou a confiança das partes interessadas. O impacto de negócio é avaliado por meio da Análise de Impacto nos Negócios (BIA/AIN) e não depende da probabilidade, mas da gravidade da interrupção ao longo do tempo. (ISO 22301 – impacto de negócio é a base para criticidade, RTO e RPO).

Incidente de TIC: Evento não planejado que causa, ou pode causar, interrupção, degradação ou redução da qualidade de um serviço de TIC, sem necessariamente caracterizar um desastre.

Item de Configuração de TIC (IC ou CI – Configuration Item): Qualquer componente que precise ser gerenciado para entregar um serviço de TIC, incluindo hardware, software, sistemas, bases de dados, componentes de rede, documentos, contratos, serviços e até pessoas, bem como seus relacionamentos e dependências. Os Itens de Configuração são controlados ao longo de seu ciclo de vida para garantir a integridade e a rastreabilidade do ambiente de TIC.

Monitoramento: Atividade contínua de observação do desempenho, disponibilidade e integridade dos ativos e serviços de TIC, realizada por meio de ferramentas especializadas e pelas estruturas técnicas da SETIM, com o objetivo de detecção precoce de incidentes.

Níveis de Serviço de TIC: Conjunto de metas e parâmetros acordados que definem o desempenho esperado de um serviço de TIC, incluindo, entre outros, disponibilidade, tempo de resposta, tempo de resolução, capacidade e janelas de atendimento. Os níveis de serviço são formalizados por meio de Acordos de Nível de Serviço (SLA) e constituem referência para priorização, monitoramento e continuidade dos serviços.

Níveis Operacionais de TIC (OLA – Operational Level Agreement): Acordos internos estabelecidos entre equipes, unidades ou fornecedores da SETIM que definem responsabilidades, prazos e compromissos operacionais necessários para o cumprimento dos Níveis de Serviço de TIC acordados com os usuários. Os Níveis Operacionais de TIC sustentam os SLAs e são fundamentais para resposta a incidentes e recuperação de serviços.

Plano de Continuidade de Negócios (PCN): Documento que estabelece estratégias, diretrizes e procedimentos para assegurar que os processos e serviços essenciais da organização possam ser mantidos ou restaurados em níveis aceitáveis após a ocorrência de eventos disruptivos. O PCN é orientado ao negócio e integra planos especializados, como planos de continuidade de TIC, planos de contingência, planos de comunicação e planos de recuperação de desastres. (ISO 22301 – o PCN é um dos principais instrumentos operacionais do Sistema de Gestão de Continuidade de Negócios)

Plano de Administração de Crises (PAC): Subplano responsável pela coordenação da tomada de decisão, da comunicação institucional e do gerenciamento da crise decorrente de eventos disruptivos que afetem os serviços de TIC.

Plano de Continuidade dos Serviços de TIC (PCTIC): Documento que estabelece diretrizes, responsabilidades e procedimentos para assegurar a continuidade e a recuperação dos serviços de TIC críticos do TJBA em situações de incidentes graves ou desastres. O PCTIC não substitui o Plano de Continuidade de Negócios (PCN) do TJBA, constituindo-se como plano especializado de TIC, subordinado e complementar às diretrizes e decisões estabelecidas no PCN institucional

Plano de Continuidade Operacional (PCO): Subplano que define os procedimentos operacionais alternativos e ações emergenciais para garantir a continuidade mínima dos serviços de TIC durante a interrupção.

Plano de Recuperação de Desastres (PRD): Subplano que estabelece os procedimentos técnicos e operacionais para restaurar o ambiente principal de TIC e retornar os serviços aos níveis normais de operação após um desastre.

Recovery (Recuperação): Conjunto de atividades destinadas a restaurar serviços, sistemas, dados ou infraestrutura de TIC após a ocorrência de um incidente grave ou desastre, utilizando, entre outros recursos, backups, ambientes alternativos e procedimentos definidos no PRD.

Risco: Efeito da incerteza sobre os objetivos do TJBA, resultante da interação entre ameaça, vulnerabilidade e ativo de TIC, expresso pela combinação da probabilidade de ocorrência de um evento e de suas consequências.

RPO (Recovery Point Objective – Ponto Objetivo de Recuperação): Quantidade máxima aceitável de perda de dados, medida em tempo, relacionada ao último ponto de recuperação disponível.

RTO (Recovery Time Objective –Tempo Objetivo de Recuperação): Tempo máximo aceitável para a restauração de um serviço de TIC após sua interrupção.

Serviço de TIC: Conjunto estruturado de recursos tecnológicos, processos e pessoas, disponibilizado pela SETIM para atender necessidades institucionais do TJBA ou do público externo, conforme catalogação nos Portais Service Desk e na ferramenta CASM.

Sistema de Gestão de Continuidade de Negócios (SGCN ou BCMS – Business Continuity Management System): Conjunto estruturado de políticas, processos, responsabilidades, recursos e práticas que permitem à organização planejar, implementar, operar, monitorar, revisar e melhorar continuamente sua capacidade de responder e se recuperar de eventos disruptivos. O SGCN fornece o arcabouço de governança no qual se inserem o PCN, o PCTIC e demais planos de continuidade. (ISO 22301 – o SGCN é o sistema de gestão; os planos são seus produtos).

Vulnerabilidade: Fragilidade ou deficiência de um ativo de TIC, processo, controle ou configuração que pode ser explorada por uma ameaça.

5. Definições de Estratégias de Continuidade e Contingência de TIC

As definições de estratégias de continuidade e contingência de TIC estabelecem os conceitos fundamentais que orientam a seleção, o planejamento e a aplicação das soluções técnicas e organizacionais destinadas a assegurar a manutenção ou a recuperação dos serviços de Tecnologia da Informação e Comunicação diante de incidentes, falhas graves ou desastres.

Essas estratégias são definidas com base na Análise de Impacto nos Negócios (BIA/AIN), nos objetivos de recuperação (RTO e RPO) e na criticidade dos serviços, e têm como finalidade reduzir o tempo de interrupção, minimizar impactos ao negócio e garantir a resiliência operacional.

As estratégias de continuidade e contingência não se confundem com os planos em si, mas representam as abordagens e alternativas que sustentam a execução dos planos de continuidade, contingência e recuperação de desastres de TIC.

Estratégias de Continuidade: Conjunto de abordagens, soluções técnicas e organizacionais definidas com base na Análise de Impacto nos Negócios (BIA/AIN) e na gestão de riscos, destinadas a garantir a manutenção ou a recuperação dos serviços de TIC em níveis aceitáveis após eventos disruptivos. As estratégias de continuidade orientam a escolha de ambientes alternativos, mecanismos de redundância, formas de backup, replicação e contingência operacional.

Estratégias de Continuidade de TIC: Estratégias específicas aplicadas aos serviços, sistemas, dados e infraestrutura de TIC, que definem como e onde os serviços serão mantidos ou restaurados em caso de indisponibilidade do ambiente principal, considerando criticidade, RTO, RPO, custo, complexidade e riscos associados.

Estratégias de Contingência de TIC: Conjunto de medidas temporárias e alternativas adotadas para manter a operação mínima aceitável dos serviços de TIC durante a indisponibilidade total ou parcial do ambiente principal, sem necessariamente restaurar o ambiente definitivo. A contingência antecede ou complementa a recuperação.

5.1. Estratégias para ambientes físicos alternativos de tecnologia

Hot Site: Ambiente alternativo totalmente equipado, configurado e operacional, capaz de assumir imediatamente a execução dos serviços de TIC críticos em caso de indisponibilidade do ambiente principal. Caracteriza-se por baixíssimo RTO e, geralmente, baixo RPO, com alto custo de implementação e manutenção.

Warm Site: Ambiente alternativo parcialmente equipado e configurado, que requer a execução de procedimentos adicionais (ativação, carga de dados, ajustes de configuração) antes de entrar em operação. Apresenta RTO intermediário e custo menor que o Hot Site.

Cold Site: Ambiente alternativo que dispõe apenas de infraestrutura básica (espaço físico, energia, conectividade), sem sistemas ou dados previamente instalados. Requer maior esforço para ativação, resultando em RTO elevado, sendo indicado para serviços de menor criticidade.

Replication Site: Ambiente alternativo que recebe dados replicados periodicamente ou de forma contínua a partir do ambiente principal, permitindo restauração mais rápida dos serviços. A efetividade da estratégia depende do método de replicação e da frequência de atualização dos dados.

Mirroring Site (Espelhamento): Estratégia de continuidade baseada na duplicação simultânea e em tempo real dos dados e, em alguns casos, das aplicações, entre o ambiente principal e um ambiente alternativo. Proporciona RPO próximo de zero e RTO muito baixo, sendo indicada para serviços de altíssima criticidade.

5.2. Estratégias de tecnologia baseadas em nuvem

Cloud Site: Ambiente alternativo de continuidade implementado em infraestrutura de computação em nuvem, pública, privada ou híbrida, capaz de hospedar sistemas e serviços de TIC em situação de contingência ou recuperação. Pode ser configurado como Hot, Warm ou Cold Site, conforme o nível de preparo e automação.

Cloud Backup: Estratégia de backup na qual cópias de dados são armazenadas em infraestrutura de nuvem, garantindo maior resiliência geográfica e proteção contra falhas locais. O Cloud Backup suporta estratégias de recuperação, mas não substitui, por si só, um ambiente de execução dos serviços.

Onsite Backup: Backup armazenado no mesmo local físico ou datacenter do ambiente principal. Possui recuperação rápida, porém menor resiliência a desastres físicos ou ambientais.

Offsite Backup: Backup armazenado em local físico distinto do ambiente principal, proporcionando maior proteção contra desastres locais e eventos de grande impacto, ainda que com maior tempo de recuperação.

5.3. Outras estratégias relevantes de continuidade e contingência de TIC

Redundância: Estratégia que utiliza componentes duplicados ou múltiplos (servidores, links, equipamentos de rede, fontes de energia) para evitar ponto único de falha e aumentar a disponibilidade dos serviços de TIC.

Failover: Mecanismo automático ou manual que transfere a operação de um serviço de TIC do ambiente principal para um ambiente alternativo quando ocorre falha ou indisponibilidade.

Load Balancing (Balanceamento de Carga): Estratégia que distribui a carga de processamento entre múltiplos componentes ou ambientes, contribuindo para alta disponibilidade e continuidade do serviço.

Procedimentos Manuais ou Alternativos: Estratégia de contingência que prevê a execução temporária de atividades por meios não automatizados ou por sistemas substitutos, quando os sistemas principais de TIC estiverem indisponíveis.

Terceirização ou Acordos de Apoio Emergencial: Estratégia que utiliza fornecedores, contratos ou parcerias previamente estabelecidas para suportar a continuidade ou recuperação dos serviços de TIC em situações excepcionais.

Ciclo de Gestão da Continuidade de Serviços de TIC (PDCA), sendo:

- Planejar: BIA, riscos, definição de estratégias;
- Executar: ativação, contingência, recuperação;
- Verificar: testes, indicadores, lições aprendidas;
- Agir: revisões, atualizações, melhoria contínua.

6. Análise de Impacto dos Serviços de TIC (AIN/BIA)

A Análise de Impacto nos Negócios (AIN/BIA) é o instrumento utilizado para identificar, justificar e graduar a criticidade dos serviços de TIC sob responsabilidade da SETIM, determinando prioridades de recuperação e metas de RTO (Tempo Objetivo para Retorno) e RPO (Ponto Objetivo de Retorno).

No contexto deste plano, o BIA é o elo entre: (i) a prestação de serviços do TJBA para o público externo e para as unidades internas; (ii) os objetivos institucionais e obrigações regulatórias; e (iii) as estratégias de continuidade, contingência e recuperação de TIC.

A metodologia adotada neste capítulo segue a lógica recomendada pela ISO 22301, em que a priorização se baseia no impacto de negócio ao longo do tempo, e não apenas em causas técnicas. Complementarmente, para garantir consistência com a governança já institucionalizada na SETIM, as graduações de impacto utilizadas no BIA são ancoradas na escala e critérios já adotados no Plano de Gestão de Riscos de TIC 2025/2026.

Para fins deste BIA, adota-se como premissa que os serviços ofertados pelo Portal Service Desk Externo tendem a compor o grupo de maior criticidade, por representarem a interface direta do TJBA com atores externos que materializam interesses sociais e obrigações públicas (principalmente advogados e delegatários). A indisponibilidade desses serviços produz impacto imediato e mensurável em múltiplas dimensões:

- Imagem institucional e confiança pública: falhas percebidas externamente tendem a amplificar repercussão e a reduzir a confiança na capacidade do Tribunal de operar serviços digitais essenciais, gerando desgaste institucional.
- Impacto regulatório (CNJ e governança de TIC): indisponibilidades recorrentes e degradações podem gerar apontamentos e pressões de conformidade, especialmente quando afetam serviços ligados ao funcionamento digital do Judiciário e às diretrizes de governança/gestão de TIC.
- Impacto financeiro: falhas externas podem acarretar custos adicionais de tratamento, contratações emergenciais, glosas e até indenizações (quando houver dano material associado), além de pressão sobre contratos e níveis de serviço.
- Impacto social: embora o público externo seja "segmentado" (advogados/delegatários), ele representa interesses de jurisdicionados e da sociedade civil, pois atua como meio para acesso e operacionalização de demandas judiciais e extrajudiciais. Assim, a indisponibilidade afeta o serviço ao cidadão de forma indireta, porém relevante.

Em resumo: no BIA da SETIM, a criticidade não é atribuída "porque o sistema é famoso", mas porque o serviço externo é um ponto de contato institucional com impacto reputacional, regulatório, financeiro e social, devendo, portanto, receber maior prioridade de recuperação e controles mais robustos de continuidade.

Figura 2: Portal Service Desk Externo

De forma complementar, os serviços do Portal Service Desk Interno também são de alta criticidade, porém predominantemente em nível corporativo, pois sustentam o funcionamento das unidades internas do TJBA e dos profissionais que executam o objeto finalístico (atividade jurisdicional e administrativa). A indisponibilidade desses serviços tende a ter efeitos mais intensos em produtividade e continuidade operacional interna.

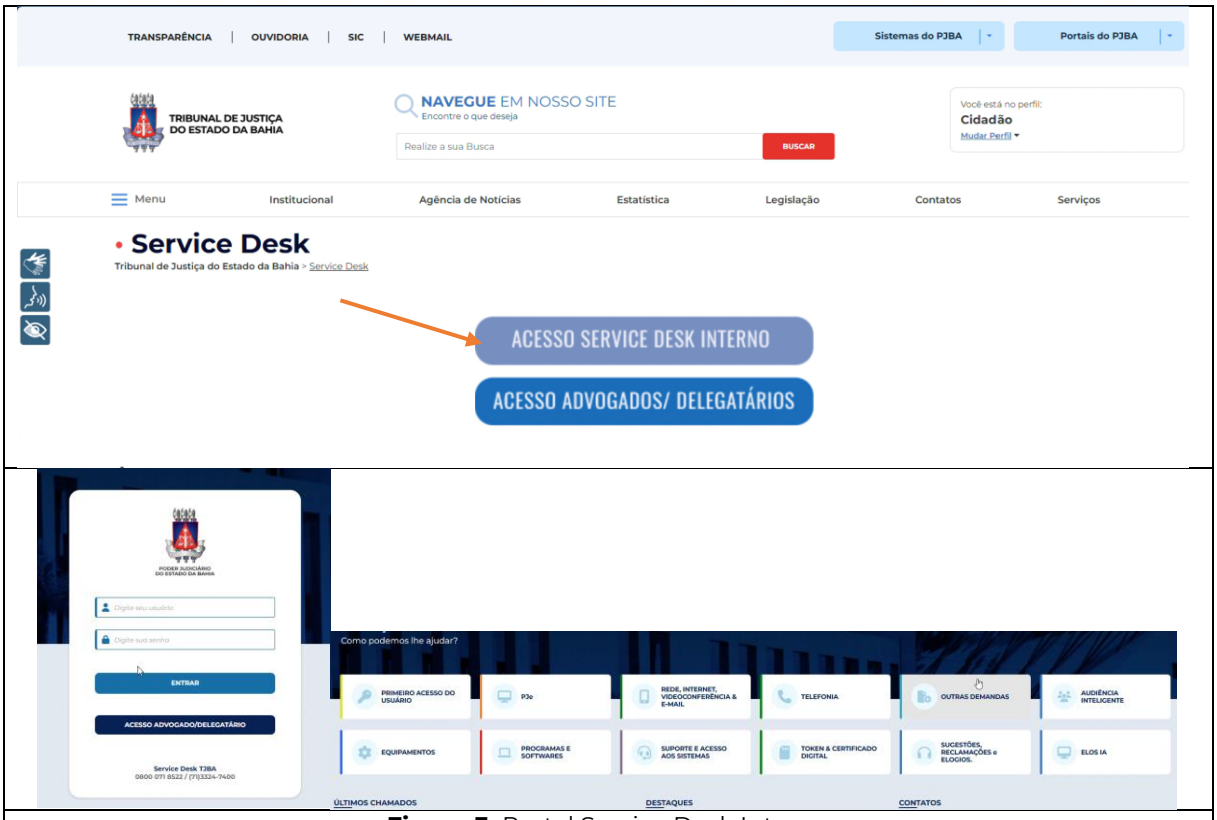


Figura 3: Portal Service Desk Interno

Para manter padronização com a governança vigente, a graduação de impacto do BIA utiliza como referência a escala de impacto do Plano de Gestão de Riscos da SETIM (1, 2, 5, 8, 10) e sua lógica de comprometimento do objetivo do ativo/serviço.

Essa escala é utilizada no plano de riscos para avaliação de impacto e probabilidade, com apuração do Nível de Risco (NRI/NRR). No BIA, ela é reutilizada como "gradiente de severidade do impacto de negócio", preservando coerência institucional. No BIA, o foco é o impacto ao longo do tempo e a tolerância do negócio (MTPD/MAO), enquanto no risco o impacto é "consequência do evento" combinado com probabilidade. A escala é a mesma, porém, a interpretação no BIA é orientada pela continuidade.

Nível	Pontos	Definição operacional (base SETIM)	Interpretação no BIA para serviços externos (Portal Externo)
Muito Baixo	1	Compromete minimamente; efeitos desprezíveis no resultado	Sem repercussão externa; impacto quase imperceptível, contornável sem urgência
Baixo	2	Compromete em alguma medida; não impede resultado principal	Reclamações pontuais; baixo potencial de repercussão/regulação; contorno simples
Médio	5	Compromete parte relevante; transtornos e perda parcial de entrega	Afeta atendimento externo por período relevante; aumento de incidentes, filas e risco de não conformidade
Alto	8	Compromete a maior parte do objetivo; reduz muito o resultado	Repercussão significativa; risco regulatório evidente; paralisa parte importante de serviços externos
Muito Alto	10	Compromete totalmente; inviabiliza o resultado	Paralisação do serviço externo crítico; forte pressão institucional/regulatória; possibilidade de perdas e sanções relevantes

Quadro 1: Graduação de Impactos do BIA (referência SETIM: 1 / 2 / 5 / 8 / 10)

A definição de janelas de tempo relevantes para mensurar impacto e tolerância de indisponibilidade utiliza como referência o método de BIA que trabalha com intervalos (ex.: imediato, 1h, 4h, 8h, dias) para determinar tempo máximo aceitável de indisponibilidade (MAO/MTPD). No contexto desse plano, esses intervalos são convertidos em metas de RTO e RPO, coerentes com a criticidade dos serviços e com o uso de RTO/RPO já observado em versões anteriores desse tipo de plano para sistemas essenciais.

Janela de indisponibilidade (BIA)	Interpretação (Impacto cresce ao longo do tempo)	Referência de RTO sugerida	Referência de RPO sugerida	Diretriz prática (exemplos)
Imediato – até 15 min	Impacto inicial; foco em detecção e resposta	RTO ≤ 1h	RPO ≤ 15 min	Acionar NOC/monitoramento; triagem e comunicação inicial
15 min – 1h	Impacto começa a ser percebido externamente	RTO ≤ 2h	RPO ≤ 30 min	Escalonamento; ativar contingência leve
1h – 4h	Janela típica de criticidade alta para canal externo	RTO ≤ 4h	RPO ≤ 1h	Ativar plano de contingência/DR parcial conforme estratégia
4h – 8h	Indisponibilidade passa a gerar pressão institucional	RTO ≤ 8h	RPO ≤ 4h	Ativação de estratégia completa (warm/hot, conforme serviço)
8h – 24h	Impacto severo, potencial regulatório e reputacional	RTO ≤ 24h	RPO ≤ 8h	Mobilização ampliada; priorização institucional; comunicação pública
1 – 3 dias	Impacto muito alto; risco de sanções e perdas significativas	RTO ≤ 72h	RPO ≤ 24h	Crise institucional; ações extraordinárias; replanejamento de capacidade
> 3 dias	Impacto extremo; continuidade do negócio fica ameaçada	RTO: definir por serviço	RPO: definir por serviço	Ativar governança de crise; soluções emergenciais de longo prazo

Quadro 2: Janelas de tempo do BIA (MTPD/MAO) e referências de RTO/RPO

Para construir o BIA dos serviços externos, o ponto de partida é o inventário do Catálogo de ofertas de serviços de tecnologia do Portal Service Desk Externo, correlacionado aos serviços/categorias dos serviços prestados pelas coordenações da SETIM e registrados na ferramenta de ITSM CASM. A identificação de “macro serviços” foi inferida conforme a visão obtida do catálogo de serviços e o relacionamento com os serviços do CASM.

Público-alvo	Macro Serviço de TIC (Portal Externo)	Tipo de solicitação	Funcionalidades / Sistemas	Serviço acionado no CASM
Delegatário	Gestão de Acessos – Aplicações Extrajudiciais (DAJE / Selo Digital)	cadastro/acesso erro/falha Informação	Selo Digital; Usuário de integração	Sistema.Aplicacao.Extrajudicial.Daje/Selo Digital.Aprovacao Coarc
Delegatário	Gestão de Acessos – Sistemas Extrajudiciais (Núcleo Extrajudicial)	cadastro/acesso erro/falha Informação	Gestão de Serventias; SCC; Malote Digital; Justiça Aberta; PJeCOR	Sistema.Aplicacao.Extrajudicial.Aprovacao Nucleo Extrajudicial
Delegatário	Gestão de Acessos – Sistema Corporativo TJBA	cadastro/acesso erro/falha Informação	PJe 1º Grau	**Sistema Corporativo TJBA**
Advogado	Cadastro – eProc 1º Grau (cadastro de advogados)	cadastro	eProc 1º Grau	Sistema.Aplicacao.Judicial.Eproc 1g.Cadastro de Advogados
Advogado	Cadastro – PROJUDI (permissão de acesso)	cadastro	PROJUDI	Sistema.Aplicacao.Judicial.Projudi.Permissao De Acesso
Advogado	Cadastro – SAJ 1º Grau (permissão de acesso)	cadastro	SAJ 1º Grau	Sistema.Aplicacao.Judicial.SajPg.Permissao De Acesso
Advogado	Cadastro – Sistema Corporativo TJBA	cadastro	PJe 1º; PJe 2º; SAJ 2º; SAIPRO	**Sistema Corporativo TJBA**
Advogado	Alteração/Atualização – PROJUDI (melhoria)	alteração	PROJUDI	Fornecedor.Netra.103/25.Sistema_Aplicacoes.Judicial.Projudi.Melhoria
Advogado	Alteração/Atualização – SAJ 1º Grau (melhoria)	alteração	SAJ 1º Grau	Fornecedor.Netra.103/25.Sistema_Aplicacoes.Judicial.SajPg.Melhoria
Advogado	Alteração/Atualização – Sistema Corporativo TJBA	alteração	eProc 1º; PJe 1º; PJe 2º; SAJ 2º; SAIPRO	**Sistema Corporativo TJBA**
Advogado	Incidente (Erro/Falha) – eProc 1º Grau	erro	eProc 1º Grau	Sistema.Aplicacao.Judicial.Eproc 1g.Erro_Falha
Advogado	Incidente (Erro/Falha) – PJe 1º Grau (informação/erro conforme registro)	erro	PJe 1º Grau	Sistema.Aplicacao.Judicial.PjePg.Informacao
Advogado	Incidente (Erro/Falha) – PROJUDI (informação/erro conforme registro)	erro	PROJUDI	Sistema.Aplicacao.Judicial.Projudi.Informacao
Advogado	Incidente (Erro/Falha) – SAJ 1º Grau	erro	SAJ 1º Grau	Fornecedor.Netra.103/25.Sistema_Aplicacoes.Judicial.SajPg.Erro_Falha
Advogado	Incidente (Erro/Falha) – Sistema Corporativo TJBA	erro	PJe 2º; SAJ 2º; SAIPRO	**Sistema Corporativo TJBA**
Advogado	Informação/Orientação – eProc 1º Grau	informação	eProc 1º Grau	Sistema.Aplicacao.Judicial.Eproc 1g.Informação
Advogado	Informação/Orientação – PROJUDI	informação	PROJUDI	Sistema.Aplicacao.Judicial.Projudi.Informacao

Público-alvo	Macro Serviço de TIC (Portal Externo)	Tipo de solicitação	Funcionalidades / Sistemas	Serviço acionado no CASM
Advogado	Informação/Orientação – SAJ 1º Grau	informação	SAJ 1º Grau	Sistema.Aplicacao.Judicial.Saj Pg.Informacao
Advogado	Informação/Orientação – Sistema Corporativo TJBA	informação	PJe 1º; PJe 2º; SAJ 2º; SAIPRO	**Sistema Corporativo TJBA**
Carta Precatória	Cadastro – Habilitação para distribuição (PJe)	Cadastro alteracao erro Informação	PJe	Sistema.Aplicacao.Judicial.Pje Pg.Habilitação para distribuição de carta precatória
Carta Precatória	Cadastro – Habilitação para distribuição (PROJUDI)	Cadastro alteracao erro Informação	PROJUDI	Sistema.Aplicacao.Judicial.Projudi.Habilitação para distribuição de carta precatória

Quadro 3: Macro Serviços de TIC do Portal Externo (inventário para o BIA)

Como ler o Quadro 3: cada linha representa um macro serviço (agrupamento por público-alvo + tipo de solicitação + serviço acionado no CASM), com as funcionalidades/sistemas externos que dependem dele.

Com base nas tabelas acima, o capítulo de BIA pode ser operacionalizado em fichas por macro serviço externo contendo:

- Descrição do serviço e público atendido (advogados / delegatários / carta precatória);
- Dependências críticas (Portal Externo → Central de Atendimento → CASM → grupos técnicos, fornecedores e infraestrutura);
- Dimensões de impacto (Imagem, Regulatório/CNJ, Financeiro, Social, Operacional) graduadas pela Tabela de impactos do BIA.
- Janelas de tempo (MTPD/MAO) pela Tabela de metas de RTO/RPO;
- Priorização de recuperação (Tier 0/1/2 ou Vital/Essencial/Importante) e vinculação às estratégias (Warm/Cold/Cloud etc.);
- Evidências: histórico de incidentes, SLAs/OLAs, volume de chamados, métricas do CASM, e resultados de testes de continuidade.

Os serviços de Tecnologia da Informação e Comunicação (TIC) disponibilizados no Portal Service Desk Interno foram estruturados a partir de uma visão orientada à continuidade, governança e impacto institucional, considerando como Macro Serviços de TIC as 12 opções apresentadas no menu inicial do portal.

Figura 4: Macro Serviços de TIC do Portal Interno (inventário para o BIA)

Essa abordagem adotou deliberadamente uma visão consolidada e funcional dos serviços, refletindo a forma como as unidades internas do Tribunal acessam e

percebem a entrega de TIC no seu cotidiano operacional, em consonância com as boas práticas de gestão de serviços e continuidade estabelecidas no âmbito da SETIM.

Cada uma dessas opções do menu inicial do Portal Interno representa um agrupamento lógico de demandas homogêneas, permitindo reduzir a granularidade excessiva do catálogo técnico detalhado e facilitar a análise de criticidade, impacto de negócio e priorização para fins de continuidade.

Assim, os Macro Serviços definidos no Portal Service Desk Interno funcionam como a camada de abstração corporativa, essencial para a condução do BIA (Análise de Impacto nos Negócios), para a definição de RTO e RPO e para a comunicação com instâncias de governança, auditoria e alta administração.

Esses Macro Serviços foram correlacionados diretamente com os serviços cadastrados no Catálogo de Serviços da ferramenta de ITSM CASM, de modo a assegurar rastreabilidade completa entre a experiência do usuário interno, os serviços técnicos subjacentes e as estruturas de atendimento, suporte, sustentação e recuperação.

Essa correlação garante que cada opção do Portal Interno acione, no CASM, os serviços consolidados correspondentes, preservando dependências técnicas, grupos responsáveis, SLAs/OLAs e fluxos de escalonamento necessários para a execução eficaz dos planos de continuidade, contingência e recuperação.

Dessa forma, a construção dos serviços do Portal Service Desk Interno baseada em Macro Serviços e sua vinculação ao catálogo do CASM asseguram coerência entre gestão de serviços, gestão de riscos e gestão da continuidade, permitindo que o Plano de Continuidade de TIC da SETIM seja acionável, auditável e alinhado às diretrizes da ISO 22301 e às práticas institucionais já consolidadas no TJBA.

A seguir os serviços e Macro serviços do Portal de Service Desk Interno:

Serviço de Acesso do Usuário

Acesso do Usuário	Serviço de Cadastro, Alteração, Bloqueio e Desbloqueio de Acesso de Usuários aos Sistemas Corporativos do TJBA
Acesso do Usuário	Serviço de Gestão de Perfis, Papéis e Permissões de Usuários em Sistemas Corporativos

Serviços de demandas do Sistema PJe

Sistema PJe	Serviço de Informação, Configuração, Instalação e Suporte ao Sistema de Aplicação Judicial PJe Office
Sistema PJe	Serviço de Suporte Operacional e Tratamento de Incidentes do Sistema PJe – 1º e 2º Graus

Sistema PJe	Serviço de Apoio à Utilização, Atualização e Orientação sobre Funcionalidades do Sistema PJe

Serviços relacionados à Equipamentos

Equipamentos	Serviço de Solicitação, Instalação, Substituição e Retirada de Equipamentos de TIC (Desktop, Notebook, Monitor e Periféricos)
Equipamentos	Serviço de Manutenção Corretiva e Preventiva de Equipamentos de TIC
Equipamentos	Serviço de Movimentação, Remanejamento e Configuração Física de Equipamentos

Serviços relacionados à Softwares

Softwares	Serviço de Instalação, Atualização e Configuração de Softwares Corporativos Homologados
Softwares	Serviço de Suporte Técnico a Softwares Institucionais
Softwares	Serviço de Solicitação de Avaliação e Homologação de Novos Softwares

Serviços relacionados à demandas de Rede – Internet e Links

Rede – Internet e Links	Serviço de Suporte, Configuração e Tratamento de Incidentes de Rede Local (LAN)
Rede – Internet e Links	Serviço de Suporte à Conectividade, Internet e Links de Comunicação
Rede – Internet e Links	Serviço de Configuração e Suporte a Wi-Fi Institucional

Serviços de Suporte à Sistemas

Suporte Sistemas	Serviço de Suporte Técnico e Tratamento de Incidentes em Sistemas Corporativos do TJBA
Suporte Sistemas	Serviço de Apoio Operacional e Orientação ao Usuário em Sistemas Administrativos e Judiciais

Serviços de demandas para Telefonia

Telefonia	Serviço de Solicitação, Configuração e Manutenção de Telefonia Fixa e Móvel
Telefonia	Serviço de Suporte a Ramais, Aparelhos Telefônicos e Softphones

Serviços relacionados aos Certificados Digitais

Certificados Digitais	Serviço de Solicitação, Instalação, Renovação e Suporte a Certificados Digitais e Tokens

Demandas de Sugestões e Reclamações

Sugestões e Reclamações	Serviço de Registro, Encaminhamento e Acompanhamento de Sugestões, Reclamações e Elogios sobre Serviços de TIC

Outras Demandas

Outras Demandas	Serviço de Atendimento a Demandas de TIC Não Classificadas nos Demais Macro Serviços

Serviços de Audiência Inteligente

Audiência Inteligente	Serviço de Suporte Técnico, Configuração e Operação de Soluções de Audiência Inteligente

Serviços de Inteligência Artificial

Inteligência Artificial	Serviço de Suporte, Operação e Sustentação de Soluções de Inteligência Artificial Institucionais

A Análise de Impacto nos Negócios (AIN/BIA) aplicada aos serviços de TIC ofertados no Portal Service Desk Interno, com o propósito de: (i) estabelecer a criticidade relativa dos macros serviços de TIC; (ii) definir janelas de tolerância de indisponibilidade (MTPD/MAO); e (iii) padronizar metas de recuperação (RTO/RPO) a serem utilizadas nesse plano, assegurando coerência com a governança de TIC e com os processos operacionais de atendimento, escalonamento e monitoramento mantidos pela SETIM

No contexto interno, a criticidade não decorre primariamente de exposição pública, mas do impacto sobre a continuidade corporativa do TJBA, incluindo a execução de atividades judiciais e administrativas, a disponibilidade de conectividade e a operação de sistemas e recursos essenciais.

Algumas premissas de criticidade e contagem do tempo de indisponibilidade (MTPD/MAO) incluem:

- Serviços em regime 24x7 (críticos por natureza operacional)

  Considera-se que os macro serviços relacionados com o Sistema PJe, Acesso do Usuário, Telefonia, Redes, Internet e Links e Suporte Sistemas/Operações de Produção e sustentação do datacenter, funcionam de forma ininterrupta (24x7). Entretanto, por restrições orçamentárias e limitações contratuais inerentes às contratações de terceiros (serviços prestados por empresas contratadas via licitação), define-se que o tempo máximo de indisponibilidade passa a produzir criticidade relevante para fins de BIA a partir de 24 horas corridas.

  Até esse limiar, as ocorrências são tratadas dentro do ciclo de resposta operacional (monitoramento, gestão de incidentes e ações de contorno), com escalonamento técnico conforme necessário e dentro das réguas de escalação definidas na coordenação CPROD.

- Demais serviços não indicados pelas coordenações da SETIM com componentes e itens de configuração críticos a tratativa é pela ferramenta de ITSM com registro, acionamento e contorno podendo ocorrer em até 2 dias úteis.

  Os demais macro serviços de tecnologia do Portal Service Desk Interno, define-se que a indisponibilidade passa a produzir impacto relevante no BIA a partir de 2 dias úteis. Tudo o que ocorre até essa janela é tratado dentro dos processos de Gestão de Incidentes e de ações de contorno, não caracterizando, por si só, uma ruptura que exija ativação de estratégias extraordinárias de continuidade

Para manter coerência metodológica com o modelo institucional, a graduação de impacto utilizada no BIA continua sendo a mesma adotada para os serviços externos, escala já empregada também no Plano de Gestão de Riscos da SETIM (gradiente **1, 2, 5, 8, 10**), preservando o entendimento de comprometimento do objetivo/valor do serviço.

Nível	Pontos	Definição (base SETIM)	Interpretação no BIA para Serviços Internos
Muito Baixo	1	Compromete minimamente o objetivo	Impacto desprezível; sem prejuízo relevante ao TJBA
Baixo	2	Compromete em alguma medida	Prejuízo limitado; contornável sem pressão institucional
Médio	5	Compromete parte relevante	Impacto perceptível; acumula backlog e risco de descumprimentos
Alto	8	Compromete a maior parte	Impacto severo; reduz significativamente a capacidade operacional
Muito Alto	10	Compromete totalmente	Interrompe o resultado essencial; afeta continuidade corporativa

Quadro 4: Graduação de Impacto no BIA (escala SETIM 1/2/5/8/10)

A criticidade operacional dos macro serviços do portal interno é reforçada por evidências de monitoramento contínuo e acionamento registrados junto à

coordenação CPROD, com indicação dos elementos de infraestrutura e aplicações monitorados são listados por Categoria / Serviço / Host / Grupo, em que:

- CPROD sustenta a monitoria (NOC) e a coordenação inicial de acionamentos de conectividade e rede (roteadores, switches, datacenter, links e conectividade de unidades.
- COTEC_SEGURANÇA aparece associada a elementos críticos de perímetro e proteção (firewalls e balanceador), reforçando escalonamento técnico especializado.
- COTEC aparecem diretamente associados ao ecossistema PJe (aplicação e banco), evidenciando operação e resposta técnica sobre sistemas críticos.
- Outros grupos (ex.: COTEC_LINUX, COTEC_WINDOWS) aparecem associados a aplicações corporativas, o que reforça sustentação e operação de produção em diversos domínios.

Essa evidência é utilizada como fator de sustentação da criticidade no BIA: serviços cuja cadeia técnica possui monitoramento e acionamento 24x7 tendem a possuir maior relevância operacional e demandam metas de recuperação mais rigorosas.

Buscando a padronização requerida por esse tipo de plano, estabelece-se que todos os macro serviços classificados como 24x7 possuem RTO padronizado com prazo ≤ 8 horas (meta institucional para restabelecimento).

Observação: o MTPD/MAO para fins de criticidade relevante permanece 24 horas corridas (premissa de tolerância por restrição contratual/orçamentária), mas o RTO é definido como meta operacional para acelerar retomada sempre que possível.

Macro Serviço (Portal Interno)	Evidência (Categoria/Serviço/Hosts)	Grupos de acionamento (SETIM)	Criticidade BIA	MTPD/MAO (início impacto relevante)	RTO (padronizado 24x7)	RPO (meta)
Sistema PJe	Categoria “Pje”; serviço “Aplicação PJe”; hosts pje1gapp*, pje2gapp*, consultapublicapje, pje_* (banco)	COTEC_LINUX_PJE, COTEC_BANCO (monitoria NOC/CPROD)	Muito Alta	24h corridas	≤ 8h	≤ 1h
Rede – Internet e Links	Roteadores RT-, Switches SW-, Firewalls FW-*, FortiADC; serviços “Conectividade Sede”, “Internet Unid Especial”, “Rede Local Sede”	CPROD e COTEC_SEGURANÇA	Muito Alta	24h corridas	≤ 8h	N/A
Telefonia	Evidência de infraestrutura/acionamento (PABX consta no inventário de acionamento do mesmo arquivo)	CPROD (monitoria) + coordenações de telecom/COATE conforme cadeia	Alta	24h corridas	≤ 8h	N/A
Acesso do Usuário	Não listado claramente na aba 1, mas é dependência transversal para operação interna	Tipicamente COTEC_WINDOWS / COTEC_SEGURANÇA	Alta	24h corridas	≤ 8h	≤ 8h

Macro Serviço (Portal Interno)	Evidência (Categoria/Serviço/Hosts)	Grupos de acionamento (SETIM)	Criticidade de BIA	MTPD/MAO (início impacto relevante)	RTO (padronizado 24x7)	RPO (meta)
		(conforme IAM/AD)				
Suporte Sistemas (inclui operações de produção quando aplicável)	Hosts de aplicações corporativas sob COTEC_LINUX/COTEC_WINDOWS/COTEC_BANCO (sustentação)	COTEC_LINUX, COTEC_WINDOWS, COTEC_BANCO (monitoria NOC/CPROD)	Alta	24h corridas	≤ 8h	≤ 24h (baseline)
Audiência Inteligente	Dependência forte de Rede/Internet; macro serviço não aparece como categoria na aba 1	COATE/COTEC + infraestrutura CPROD conforme incidente	Média	2 dias úteis	≤ 2 dias úteis	N/A/≤24h
Equipamentos	Não consta como categoria de infraestrutura 24x7 na aba 1 (itens são tratados via ITSM)	COATE (atendimento), escalonamento conforme necessidade	Média	2 dias úteis	≤ 5 dias úteis	N/A
Softwares	Demandas de instalação/configuração não aparecem como itens de infraestrutura 24x7	COATE/COTEC conforme software	Média	2 dias úteis	≤ 5 dias úteis	N/A
Certificados Digitais	Suporte operacional e atendimento; não é item típico de monitoramento 24x7	COATE/COTEC	Média	2 dias úteis	≤ 5 dias úteis	N/A
Inteligência Artificial	Pode depender de hosts Linux/app monitorados, mas sem categoria explícita na aba 1	DIS/COTEC_LINUX conforme solução	Média	2 dias úteis	≤ 5 dias úteis	≤ 24h (quando houver dados)
Sugestões e Reclamações	Serviço de governança/relacionamento; não depende de monitoramento 24x7	COATE	Baixa	2 dias úteis	≤ 10 dias úteis	N/A
Outras Demandas	Categoria guarda-chuva; criticidade depende do conteúdo	COATE/triagem e escalonamento	Variável (baseline média/baixa)	2 dias úteis	≤ 10 dias úteis	N/A

Quadro 5: Matriz BIA do Portal Interno (Macro Serviço x 24x7 x RTO/RPO)

O Quadro 6 é recomendado para auditoria e governança, pois evidencia o vínculo entre o serviço (catálogo) e a capacidade de monitoramento/acionamento 24x7:

Macro Serviço	Categorias / Serviços	Hosts	Grupo de acionamento
Rede – Internet e Links	Roteador / Conectividade Sede; Switch / Rede Local; Firewall / Conectividade; Balanceador	RT-INTERNET-ITS-PE-01/02; RT-INTERNET-ALGAR*; SW-CORE*; SW-TJBA*; FW3200; FIREWALL-TJBA; FortiADC	**CPROD**; **COTEC_SEGURANÇA**

Sistema PJe	Pje / Aplicação PJe (e bancos relacionados)	pje1gapp*; pje2gapp*; consultapublicapje; pje_16; pje_2g*	**COTEC_LINUX_PJE**; **COTEC_BANCO**
Suporte Sistemas / Produção	Diversas aplicações corporativas monitoradas	esaj; projapp*; selo*; tamuz; saturno; SRVSAJ*; etc.	**COTEC_LINUX**; **COTEC_WINDOWS**; **COTEC_BANCO**

Quadro 6: Evidências de monitoramento 24x7 por macro serviço

O Monitoramento 24x7: realizado pela CPROD (NOC), que detecta eventos e indisponibilidades, aciona rotinas de resposta e efetua escalonamento conforme os grupos de acionamento definidos.

Os chamados do Portal Interno: originam-se no Service Desk Interno (CASM), são tratados pela Central de Serviços e encaminhados para COATE e COTEC, que então realizam escalonamento para as coordenações técnicas correspondentes (ex.: COTEC_LINUX_PJE, COTEC_BANCO, COTEC_SEGURANÇA), em consonância com a estrutura de grupos de acionamento do monitoramento.

Essa integração garante coerência entre a perspectiva do usuário (catálogo/ITSM) e a perspectiva técnica (monitoramento/acionamento), tornando o BIA operacionalmente executável.

A seguir, o Quadro 7 traz um resumo dos serviços mais representativos no Portal Interno do Service Desk, conforme o catálogo do ITSM/CASM refletido nas ofertas de serviço (itens internos). Esta tabela é propositalmente "sucinta" para o BIA (macro visão). O detalhamento completo por item pode ficar como Anexo do Catálogo.

Macro Serviço	Serviços de TIC (CASM) – consolidados e reescritos
Acesso do Usuário	Reset de senha de rede; Primeiro acesso; Permitir/Revogar acesso a sistemas (quando aplicável)
Sistema PJe	Serviço de Informações/Configuração/Instalação do PJe Office; Serviço de Configuração/Instalação/Incidente do PJe 1G; Serviço de Permissão/Reset/Incidente do PJe 2G; PJe Mídias (permissão, reset, incidentes, informações)
Rede – Internet e Links	Instalação/remanejamento de ponto de rede; Falha no acesso à internet; VPN; Criação de e-mail; Videoconferência (salas, permissões, falhas, mídias)
Telefonia	Solicitação de ramal; Instalação/substituição de aparelho; Falhas em telefonia fixa/móvel; Troca de celular/modem
Suporte Sistemas	Permissão/erro-falha em sistemas administrativos (SIGA, SEI etc.); sistemas judiciais (SAJ, PROJUDI, SEEU etc.); extrajudiciais (DAJE/Selo Digital etc.)
Equipamentos	Erro/ falha e instalação de desktop/ notebook/ monitor/ scanner/ impressora; reposição de toner; solicitação/substituição/devolução de equipamentos.
Softwares	Instalação de programas/softwares; configurações correlatas
Certificados Digitais	Atendimento a token/certificado digital
Sugestões e Reclamações	Registro e tratamento de sugestões/reclamações/elogios

Outras Demandas	Categoria “outras demandas” (tratativa conforme triagem)
Audiência Inteligente	Audiência Virtual (Teams) e AUDIN (permissões/erro-falha)
Inteligência Artificial	Serviços de acesso/suporte a soluções de IA (ex.: ELOS IA)

Quadro 7: Catálogo Interno Consolidado (Macro Serviço → Serviços CASM consolidados)

Com base nas premissas de funcionamento 24x7, nos limiares de criticidade relevante (24h corridas e 2 dias úteis) e na evidência objetiva de monitoramento e acionamento 24x7, o BIA do Portal de Service Desk Interno define uma matriz de criticidade e metas padronizadas de recuperação.

O RTO padronizado de 8 horas para os macro serviços 24x7 estabelece meta operacional consistente e mensurável, enquanto os demais macro serviços seguem metas em dias úteis, alinhadas ao modelo de atendimento por ITSM e às restrições de capacidade contratual.

Esse conjunto fornece rastreabilidade, governança e base técnica para priorização de continuidade e para validação periódica desse plano por meio de testes e simulações.

7. Equipes envolvidas

Este capítulo estabelece a estrutura de equipes, papéis e responsabilidades da Secretaria de Tecnologia da Informação e Modernização (SETIM) para atuação no Plano de Continuidade de Serviços de TIC (PCTIC), assegurando alinhamento com:

- os requisitos da ABNT NBR ISO 22301;
- os resultados da Análise de Impacto nos Negócios (BIA);
- e a estrutura organizacional formal do TJBA.

O objetivo é garantir que, diante de incidentes relevantes, interrupções prolongadas ou cenários de desastre, existam times claramente definidos, com responsabilidades objetivas, fluxos de acionamento conhecidos e capacidade de coordenação integrada, evitando decisões ad hoc ou dependentes de pessoas específicas.

Esse plano será administrado, avaliado e acionado no âmbito da Secretaria de Tecnologia da Informação e Modernização - SETIM do TJBA tendo sua manutenção, organização e melhoria revistas e atualizadas periodicamente pelas Coordenações já mencionadas no BIA/AIN desse plano, principalmente CPROD, COTEC e COATE que atuarão no Atendimento Técnico, Suporte Técnico e Operações de administração e sustentação dos ambientes e estruturas de Produção.

Em conformidade com a ISO 22301, a atuação em continuidade é organizada em três níveis complementares:

- Nível Estratégico (Gestão de Crise e Governança): Responsável por decisões institucionais, priorização de serviços, comunicação e autorização de exceções.
- Nível Tático (Coordenação da Continuidade):Responsável por coordenar a execução dos planos, articular equipes técnicas e acompanhar a recuperação.
- Nível Operacional (Resposta Técnica e Recuperação): Responsável pela execução direta das ações técnicas de contingência, recuperação e restabelecimento.

Essa separação evita sobreposição de decisões, reduz riscos de conflito de autoridade e garante rastreabilidade das ações durante eventos críticos.

A imagem a seguir representa graficamente o organograma funcional da SETIM para o Plano de Continuidade de Serviços de TIC.

7.1. Estrutura de equipes de continuidade da SETIM

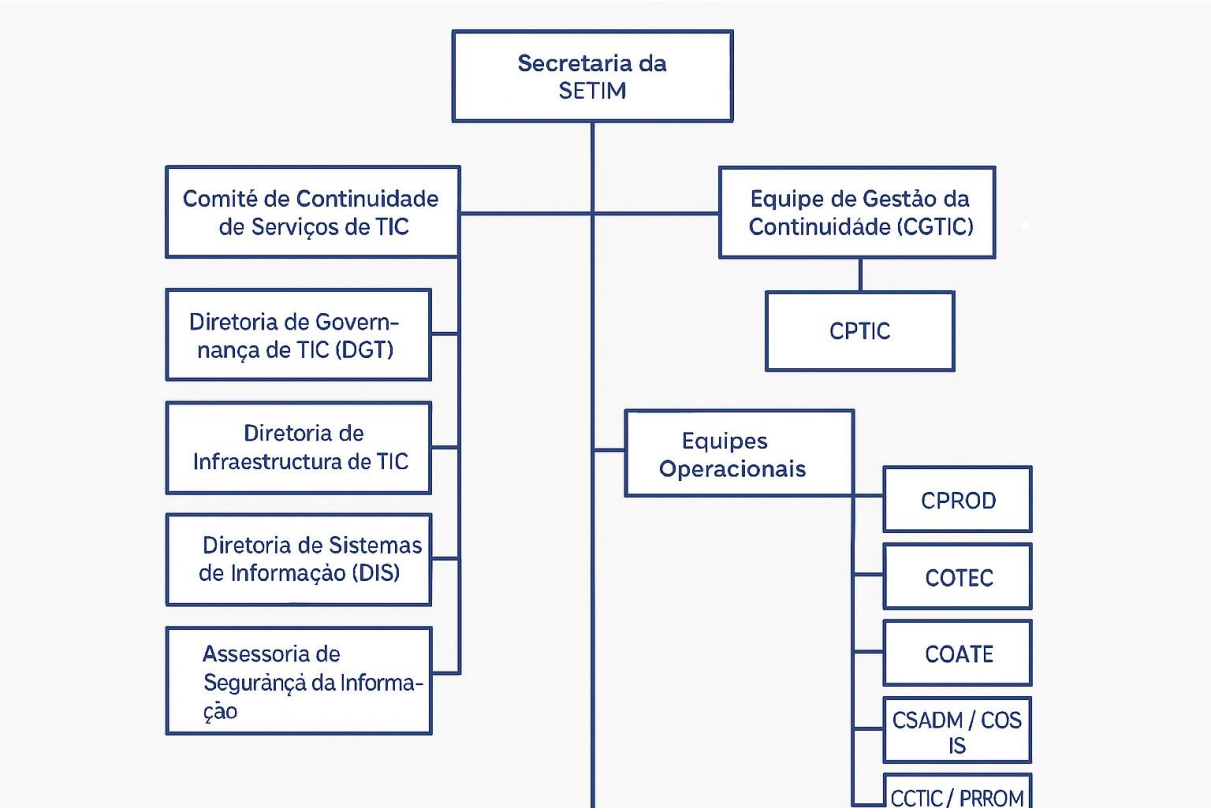


Figura 2: organograma funcional da SETIM para o Plano de Continuidade de Serviços

COMITÊ DE CONTINUIDADE DE SERVIÇOS DE TIC (NÍVEL ESTRATÉGICO)

Composição institucional:

- Secretaria da SETIM
- Assessoria Técnica da SETIM
- Diretoria de Governança de TIC (DGT)
- Diretoria de Infraestrutura de TIC (DIN)
- Diretoria de Sistemas de Informação (DIS)
- Assessoria de Segurança da Informação

Papel do comitê no Plano de Continuidade: O Comitê de Continuidade de Serviços de TIC é o órgão decisório estratégico durante situações de crise ou interrupções relevantes, sendo responsável por:

- declarar formalmente a ativação do Plano de Continuidade;
- priorizar macro serviços críticos conforme o BIA;
- autorizar medidas excepcionais (ex.: mudanças emergenciais, uso de soluções temporárias);
- deliberar sobre comunicação institucional com a Presidência do TJBA e demais instâncias;
- decidir sobre encerramento do modo de contingência e retorno à operação normal.

Esse comitê atua de forma colegiada, garantindo que decisões estratégicas não fiquem concentradas em uma única área técnica.

EQUIPE DE GESTÃO DA CONTINUIDADE DE SERVIÇOS (NÍVEL TÁTICO)

Coordenação central:

- Coordenação de Governança de TIC (CGTIC)
- Unidades de apoio:
- Assessoria Técnica da SETIM
- Coordenação de Projetos de TIC (CPTIC)

Papel dessa equipe no Plano de Continuidade: A Equipe de Gestão da Continuidade é responsável por operacionalizar as decisões estratégicas, atuando como elo entre o Comitê e as equipes técnicas. Suas atribuições incluem:

- coordenar a execução dos planos específicos de continuidade e recuperação;
- acompanhar indicadores de indisponibilidade, RTO e RPO definidos no BIA;
- consolidar informações técnicas e apresentar situação executiva ao Comitê;
- garantir o registro formal dos eventos, decisões e lições aprendidas;
- acionar, quando necessário, planos de recuperação alternativos ou escalonamentos adicionais.

A CGTIC atua como custodiante metodológica do plano, assegurando aderência às normas e alinhamento com a governança de riscos.

7.2. Equipes operacionais de resposta e recuperação (Nível Operacional)

COORDENAÇÃO DE PRODUÇÃO E COMUNICAÇÃO – CPROD

Escopo principal: atuar em nível de gestão e execução de operações no Datacenter, telecomunicações, links, telefonia, monitoramento e operação 24x7.

Atuação no PCTIC: A CPROD é a linha de frente operacional nos cenários de indisponibilidade de infraestrutura crítica. Suas responsabilidades incluem:

- monitoramento contínuo dos ambientes de produção;
- identificação e contenção inicial de falhas;
- execução de procedimentos de contingência (failover, redundâncias, rotas alternativas);
- acionamento de fornecedores e contratos críticos;
- suporte técnico direto às demais coordenações durante a recuperação.

A CPROD é responsável pela execução técnica dos primeiros movimentos de resposta, especialmente para os macro serviços classificados como 24x7 no BIA.

COORDENAÇÃO DE SUPORTE TÉCNICO – COTEC

Escopo principal: Infraestrutura lógica, servidores, sistemas básicos, plataformas de apoio e sustentação técnica.

Atuação no PCTIC: A COTEC atua na recuperação técnica de ambientes, sendo responsável por:

- restabelecer serviços de infraestrutura afetados;
- executar procedimentos de recuperação de sistemas e plataformas;
- apoiar tecnicamente a CPROD e as coordenações de sistemas;
- garantir a integridade e estabilidade dos ambientes após a recuperação.

A COTEC é fundamental na fase de estabilização pós-incidente, garantindo que o retorno à operação seja seguro e sustentável.

COORDENAÇÃO DE ATENDIMENTO TÉCNICO – COATE

Escopo principal: Central de Serviços, atendimento ao usuário, registro e acompanhamento de chamados.

Atuação no PCTIC: Durante eventos de continuidade, a COATE:

- atua como ponto único de contato com os usuários internos;
- registra, classifica e acompanha incidentes relacionados à indisponibilidade;
- comunica orientações operacionais definidas pelo Comitê;
- mantém os usuários informados sobre status e prazos estimados;
- apoia a priorização de demandas emergenciais conforme o BIA.

A COATE não executa a recuperação técnica, mas é essencial para gestão da percepção do impacto e para a organização do fluxo de atendimento.

COORDENAÇÕES DE SISTEMAS (DIS)

- Coordenação de Sistemas Judiciais – CSJUD
- Coordenação de Sistemas Administrativos – CSADM (COSIS)

Atuação no PCTIC: As coordenações de sistemas são responsáveis por:

- validar a integridade funcional dos sistemas após a recuperação;
- apoiar a execução de planos específicos de contingência de sistemas;
- priorizar funcionalidades críticas conforme o BIA;
- coordenar ajustes emergenciais com fornecedores de software;
- garantir que o retorno do sistema atenda aos requisitos mínimos de negócio.

Essas coordenações de sistemas de informação atuam fortemente na fase de retomada funcional, assegurando que o serviço recuperado seja efetivamente utilizável.

COORDENAÇÃO DE CONTRATAÇÃO DE SOLUÇÕES DE TIC – CCTIC / CPROM

Atuação no PCTIC: A CCTIC/CPROM atua de forma suporte estratégico, sendo responsável por:

- apoiar contratações emergenciais quando autorizadas;
- acionar cláusulas de contingência contratual;
- orientar tecnicamente a formalização de aditivos ou exceções;
- garantir conformidade legal durante contratações emergenciais.

COORDENAÇÃO DE PROJETOS DE TIC – CPTIC

Atuação no PCTIC: A CPTIC atua no planejamento da recuperação estruturada, sendo responsável por:

- apoiar a reorganização de cronogramas pós-incidente;
- estruturar planos de correção definitiva;
- registrar lições aprendidas e propor melhorias sistêmicas;
- integrar ações corretivas ao portfólio de projetos de TIC.

A estrutura de equipes definida neste Plano de Continuidade assegura que a SETIM disponha de papéis claros, coordenação integrada e alinhamento com as melhores práticas internacionais, reduzindo riscos de improvisação, sobreposição de responsabilidades ou decisões isoladas durante eventos críticos.

Essa organização, aliada ao BIA e aos planos técnicos específicos, fortalece a resiliência operacional da TIC do TJBA.

8. Riscos de Continuidade

Este capítulo consolida os riscos com potencial de afetar a continuidade dos serviços de TIC prestados pela SETIM ao TJBA, incluindo: (i) serviços suportados pelo Portal Service Desk Externo (cidadão/usuários externos quando aplicável); (ii) serviços do Portal Service Desk Interno (unidades e áreas internas); e (iii) riscos associados a componentes críticos com monitoramento e acionamento 24x7.

Em alinhamento com a ISO 22301, a lógica aplicada aqui é: um risco é relevante para continuidade quando seu impacto pode interromper, degradar significativamente ou inviabilizar serviços/processos críticos dentro das janelas de tolerância definidas no BIA (principalmente para macro serviços 24x7 e serviços com dependências transversais como rede, identidade e datacenter).

Para cumprir as exigências de continuidade (identificar riscos que possam gerar incidentes disruptivos), os riscos foram selecionados quando ao Impacto, indica potencial de: indisponibilidade, interrupção prolongada, paralisação, descontinuidade, degradação severa, perda de acesso, ou impactos equivalentes que afetem o funcionamento das áreas internas do TJBA ou serviços externos.

Para cada risco selecionado, foi feita uma inferência de quais macro serviços internos e quais famílias de serviços externos podem ser afetados, usando:

- Área responsável → indica qual coordenação/diretoria conduz tratamento e, portanto, qual cadeia técnica está associada;
- Objeto e Ativo de TI → indicam “o que” é impactado (processo/serviço e ativo tecnológico);
- Evidência 24x7 do monitoramento CPROD → quando o risco envolve rede/datacenter/servidores PJe/segurança, presume-se maior criticidade operacional e aderência ao bloco 24x7 do BIA.

O BIA do Service Desk Interno estabeleceu que PJe, Rede/Internet/Links, Telefonia, Acessos e Operações de Produção são serviços de operação contínua (24x7), cuja indisponibilidade passa a gerar criticidade relevante a partir de 24 horas corridas (com RTO padronizado definido no capítulo BIA).

Isso tem implicação direta na gestão dos riscos de continuidade:

- Riscos que atingem infraestrutura-base (datacenter, rede, conectividade, identidade) têm efeito “em cascata”, pois degradam múltiplos macro serviços simultaneamente (inclusive portais interno e externo).
- Riscos cibernéticos disruptivos (ex.: ransomware, exploração de vulnerabilidades, falhas de governança de mudanças) tendem a gerar indisponibilidade de múltiplos sistemas e devem ser tratados como cenários prioritários de continuidade (testes de mesa, runbooks e simulações).
- Riscos de fornecedores/contratos afetam diretamente a capacidade de restaurar serviços no prazo, especialmente quando o serviço é crítico e depende de licitações e terceiros (restrição já considerada no BIA).

O Quadro 8 sintetiza os 51 riscos relevantes para continuidade, agrupados por categoria executiva (uma consolidação gerencial das ameaças), mostrando volume e severidade (maior NRR). A lista detalhada por risco e por ameaça está no anexo/planilha gerada.

CATEGORIA EXECUTIVA DE AMEAÇA	QTD_RISCOS	MAIOR_NRR
Falhas de conectividade e rede	16	44.8
Indisponibilidade de datacenter/servidores/backup/DR	9	40
Falhas de processo/governança (ITSM, mudanças, catálogo)	7	64
Risco de fornecedores e contratos	7	44.8
Ciberataques / Exploração de vulnerabilidades	5	50
Desastres físicos / Falhas estruturais	4	64
Capacidade operacional / sobrecarga	2	44.8
Riscos de IA	1	28

Quadro 8: Síntese dos 51 riscos relevantes para continuidade

***Observação**: a severidade aqui usa o NRR (nível de risco residual) presente no registro de riscos, já considerando a situação dos controles.*

PRINCIPAIS GRUPOS DE RISCO (EXPLICAÇÃO POR CATEGORIA) E LIGAÇÃO COM SERVICE DESK E MONITORAMENTO

- **Falhas de conectividade e rede (16 riscos)**

  Este grupo reúne riscos com impacto típico de perda de acesso, paralisação de unidades/comarcas, e indisponibilidade de serviços por falhas de operadoras, redundância insuficiente, pontos únicos de falha e componentes de rede.

  Esses riscos afetam diretamente:

  - **Portal Service Desk Interno** (porque os usuários internos perdem conectividade para abrir/acompanhar solicitações e para operar os sistemas);
  - **Portal Service Desk Externo e serviços digitais ao público** (quando o portal/sistemas externos dependem da mesma infraestrutura);
  - **macro serviços internos críticos do BIA**: Rede–Internet–Links, Telefonia (quando sobre IP) e Suporte/Sistemas.

  Evidência 24x7: a lista de monitoramento contém amplo conjunto de roteadores, switches e firewalls associados a conectividade e rede local, com acionamento do grupo CPROD e escalonamentos específicos (ex.: COTEC_SEGURANÇA para firewalls).

- **Indisponibilidade de datacenter/servidores/backup/DR (9 riscos)**

  Este grupo cobre riscos que podem gerar interrupção prolongada por falhas em datacenter, cluster de servidores, sistemas de backup, ausência/insuficiência de DR e limitações de continuidade/replicação.

O efeito típico é sistêmico: indisponibilidade simultânea de múltiplos serviços do TJBA.

Esse conjunto se conecta diretamente aos macro serviços do Service Desk (interno e externo) porque:

- sem datacenter/servidores, serviços judiciais, administrativos e portais podem ficar indisponíveis;
- sem backup/DR, a retomada pode extrapolar as tolerâncias do BIA.

Evidência 24x7: CPROD monitora componentes críticos e aplicações (incluindo ambientes e bancos, conforme grupos de acionamento), sustentando resposta mais rápida para eventos de produção.

- **Falhas de processo/governança (ITSM, mudanças, catálogo) (7 riscos)**

  Este grupo é particularmente importante para continuidade porque eleva o risco de indisponibilidades causadas por falhas internas, como:

  - mudanças sem avaliação formal (incluindo segurança);
  - processos ITSM/ITIL inconsistentes;
  - catálogos desatualizados e falhas de governança operacional.

  Na prática, isso se manifesta no Service Desk como:

  - aumento de incidentes reincidentes;
  - dificuldade de classificação e encaminhamento;
  - atraso na restauração e no acionamento correto;
  - e risco ampliado de falhas por mudança (mudança que derruba serviços).

- **Risco de fornecedores e contratos (7 riscos)**

  Riscos de contratações, gestão contratual, desertos de licitação, falhas de fiscalização, rescisões e indisponibilidade/instabilidade de fornecedores impactam diretamente a continuidade porque reduzem a capacidade de:

  - manter disponibilidade (SLA e suporte);
  - repor peças/ativos;
  - renovar contratos essenciais;
  - e executar planos de recuperação com apoio de terceiros.

  Esse grupo tem aderência direta ao BIA porque as restrições contratuais e orçamentárias influenciam o tempo de recuperação factível e os limiares de criticidade adotados.

- **Ciberataques / exploração de vulnerabilidades (5 riscos)**

  Inclui riscos como ransomware, movimentação lateral, phishing, e exploração de vulnerabilidades em sistemas e serviços. O impacto de continuidade é alto porque esses eventos:

  - podem indisponibilizar serviços críticos por longos períodos;
  - podem exigir isolamento de rede e parada controlada;

- e podem afetar integridade/confiança, exigindo restauração e validação ampliada.

A planilha do monitoramento de itens críticos (firewalls, conectividade e hosts relevantes), suporta detecção mais rápida, mas não substitui runbooks de DR cibernético e simulações (ISO 22301).

- **Desastres físicos / falhas estruturais (4 riscos)**

  Abrange riscos como incêndio/pane elétrica/dano estrutural e eventos de desastre físico.

  Esses riscos tipicamente têm baixa frequência e alto impacto, exigindo:

  - redundância de site;
  - alternativas operacionais;
  - procedimentos de recuperação física e lógica;
  - e testes periódicos de restauração.

- **Capacidade operacional / sobrecarga (2 riscos)**

  Afetam continuidade por gerar filas de backlog, estouro de SLA e degradação do atendimento, especialmente em períodos de crise, quando a carga de incidentes cresce. Isso impacta o Service Desk (interno e externo) diretamente.

- **Riscos de IA (1 risco)**

  Inclui risco associado a governança/uso de IA e efeitos sobre credibilidade e conformidade. Embora nem sempre gere indisponibilidade imediata, pode exigir suspensão de funcionalidades, revalidações e ajustes de processo que afetam continuidade “funcional” do serviço.

Este plano foi desenvolvido para ser acionado quando da ocorrência de cenários de desastres que apresentam risco à continuidade dos serviços essenciais. A relação a seguir apresenta as principais ameaças e cenários que podem levar à descontinuidade dos Serviços da SETIM e ao acionamento deste plano.

Relação Executiva Consolidada de Ameaças à Continuidade dos Serviços de TIC da SETIM

- **Perda de Pessoas-Chave e Fragilidade da Capacidade Operacional**

  Descrição executiva: A saída, afastamento ou rotatividade de servidores e colaboradores críticos, associada à alta dependência de fornecedores e à falta de reposição ou transferência adequada de conhecimento, pode reduzir significativamente a capacidade da SETIM de operar, manter e recuperar serviços essenciais de TIC.

  Efeito sobre a continuidade: Atrasos na solução de incidentes, Dependência excessiva de terceiros, Risco de paralisação prolongada de sistemas judiciais essenciais.

- **Falhas Graves de Infraestrutura Física e Tecnológica**

  Descrição executiva: Incêndios, panes elétricas, falhas estruturais, defeitos em equipamentos críticos, indisponibilidade de componentes ou impossibilidade de reposição rápida podem interromper de forma abrupta os serviços de TIC.

  Efeito sobre a continuidade: Interrupção total ou parcial dos sistemas do TJBA, Indisponibilidade prolongada de serviços ao cidadão e às unidades judiciais, Risco de perda de dados e atrasos processuais relevantes.

- **Ataques Cibernéticos e Uso Indevido de Sistemas**

  Descrição executiva: Ataques cibernéticos, como ransomware, exploração de vulnerabilidades conhecidas ou avançadas, acessos indevidos e ações mal-intencionadas podem comprometer a disponibilidade, integridade e confiabilidade dos serviços digitais.

  Efeito para a continuidade: Paralisação de sistemas críticos, Bloqueio de acesso a informações essenciais, Necessidade de suspensão de serviços para contenção e recuperação.

- **Vulnerabilidades Técnicas e Fragilidade de Sistemas Legados**

  Descrição executiva: Sistemas desatualizados, falhas de configuração, ausência de correções de segurança e uso de tecnologias obsoletas aumentam a probabilidade de falhas operacionais e incidentes de segurança.

  Efeito sobre a continuidade: Interrupções recorrentes de serviços; Instabilidade operacional; Maior exposição a ataques e falhas críticas.

- **Crescimento Desordenado e Sobrecarga de Demandas**

  Descrição executiva: O aumento acelerado de demandas digitais, projetos extraordinários e picos de uso acima do previsto, sem planejamento adequado ou reforço proporcional de recursos, pode sobrecarregar a infraestrutura e as equipes.

  Efeito sobre a continuidade: Degradação do desempenho dos sistemas; Quedas de serviços em momentos críticos; Comprometimento da capacidade de resposta da SETIM.

- **Fragilidades na Gestão de Fornecedores e Contratações**

  Descrição executiva: Atrasos licitatórios, falhas contratuais, descontinuidade de contratos, falência ou incapacidade financeira de fornecedores, bem como baixa competitividade em licitações, podem interromper serviços essenciais de TIC.

  Efeito sobre a continuidade: Interrupção de serviços terceirizados críticos; Impossibilidade de manutenção ou suporte técnico; Risco de paralisação de soluções essenciais ao TJBA.

- **Falhas Operacionais, Erros Humanos e Processos Inadequados**

  Descrição executiva: Erros, esquecimentos, ações inadequadas, falhas de procedimento e ambientes de teste divergentes da realidade produtiva aumentam a probabilidade de incidentes operacionais relevantes.

  Efeito sobre a continuidade: Indisponibilidade inesperada de sistemas; Incidentes recorrentes e retrabalho; Redução da confiabilidade dos serviços de TIC.

- **Descontinuidade ou Fragilidade de Planos, Políticas e Governança**

  Descrição executiva: A inexistência, desatualização ou descumprimento de planos, políticas e diretrizes de TIC enfraquece a capacidade institucional de prevenir, responder e recuperar-se de incidentes relevantes.

  Efeito sobre a continuidade: Respostas improvisadas a crises; Recuperação mais lenta dos serviços; Aumento do impacto de incidentes sobre o negócio.

- **Não Conformidade Legal, Regulatória e Institucional**

  Descrição executiva: Descumprimentos normativos, falhas documentais, impugnações, interferências externas e inconsistências legais podem paralisar contratações, projetos e serviços de TIC.

  Efeito sobre a continuidade: Suspensão de serviços e contratos; Atrasos estratégicos; Comprometimento da capacidade institucional do TJBA.

- **Perda, Vazamento ou Indisponibilidade de Informações**

  Descrição executiva: Perda, roubo, dano físico ou má gestão de documentos, dados e mídias de armazenamento, associada a controle inadequado de versões e acessos, pode inviabilizar atividades críticas.

  Efeito sobre a continuidade: Paralisação de processos judiciais e administrativos; Dificuldade de recuperação de informações essenciais; Risco de danos institucionais e operacionais relevantes.

Com base no BIA e no registro de riscos existente no plano de gestão de riscos de 2026, conclui-se que os riscos de continuidade mais relevantes se concentram em: conectividade/rede, infraestrutura de datacenter/DR, processos operacionais (mudanças/ITSM/catálogos), contratos/fornecedores, e ciberataques disruptivos.

Para que esses riscos de continuidade possam ser endereçados adequadamente é importante que exista:

- priorização de planos e testes de continuidade;
- runbooks de recuperação por cenário de risco;
- exercícios de mesa (tabletop) integrados às coordenações envolvidas; e
- evolução da cobertura de monitoramento e escalonamento para mitigar tempo de detecção e resposta.

9. Invocação e lista de acionamentos do Plano

Esse Plano será acionado quando da ocorrência de algum dos cenários de desastres, a insurgência ou ocorrência de um risco desconhecido, ou caso uma vulnerabilidade tenha grande possibilidade de ser explorada.

O plano também poderá ser invocado em casos de testes ou por determinação do COMITÊ DE DR em conjunto com a alta administração do TJBA.

Os integrantes da EQUIPE DE COMUNICAÇÃO serão responsáveis por acionar os contatos e partes interessadas, prioritariamente por telefone, ou pessoalmente caso seja possível.

Setor/Unidade	Número/Contato	Local
DRH	Gabinete: 3372-1649 Secretaria: 3372-166	Sala 103 Do Anexo I
Corregedoria	3372-5094	Sala 312 Do Anexo I
Assessoria Da Presidência	3372-5077	Sala 303-S Do Tribunal De Justiça
Secretaria De TIC	3372-5621 / 5123	Sala 303-N Do Tribunal De Justiça
ASCOM	3483-3731	Sala 312 - Edifício Advogado Pedro Milton de Brito – Anexo II
Secretaria De Administração	3372-5213	Salas 309/311-N Do Tribunal De Justiça
Balcões De Justiça	3372-5077 / 5659	Sala 301-Sul Do Tribunal De Justiça

Quadro 9: Contatos de acionamentos do TJBA

Os dados sobre as equipes a serem acionados estão contidos no Quadro 10:

Equipe	Papéis e Responsabilidades	Responsável	Telefone	Contato	Setor
Comitê de DR	Avaliar o plano periodicamente e decidir pelo seu acionamento quando da ocorrência de desastres, respondendo em nível institucional pela execução do plano e demais ocorrências relacionadas. Inclui autoridades em nível institucional e tomadores de decisão da SETIM.	SCTIC	(71)3482-3705	setim@tjba.jus.br	SETIM
Equipe de Instalações	Responsável pelas instalações físicas que abrigam sistemas de TI e pela garantia que as instalações alternativas sejam mantidas adequadamente. Avalia os danos e supervisiona os reparos para o local principal no caso de a	Coordenador da CPROD/ Analista de Datacenter	3372-1519 / 3372-1524	cprod@tjba.jus.br	CPROD

Equipe	Papéis e Responsabilidades	Responsável	Telefone	Contato	Setor
	localização primária sofra da destruição ou danos. O líder desta equipe administrará e manterá o Plano de Recuperação de Desastre.				
Equipe de Redes	Avaliar os danos específicos de qualquer infraestrutura de rede e para fornecer dados e conectividade de rede de voz, incluindo WAN, LAN e quaisquer conexões de telefonia internamente dentro do TJBA ou de infraestrutura externa junto aos prestadores de serviço.	Analista de Data Center / Analista de redes / Líder técnico de redes	3372-1524 / 3372-1716	cprod@tjba.jus.br	CPROD
Equipe de Sistemas	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 TI DR conforme necessário.	CSJUD / COSIS	CSJUD - (71) 99717-6940 COSIS - (71) 99102-9289	csjud@tjba.jus.br / Cosis@tjba.jus.br	CSJUD / COSIS
Equipe de Operações	Fornecer aos funcionários as ferramentas de que necessitam para desempenhar suas funções da forma mais rápida e eficiente possível. Eles precisarão provisionar todos os funcionários do TJBA na solução de contingência e aqueles que trabalham remotamente com as ferramentas específicas à sua atuação. O líder desta equipe administrará e manterá o Plano de Continuidade Operacional.	DIN	(71) 33721555	din@tjba.jus.br	DIN
Equipe de Comunicações	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.	DIN	(71) 33721555	din@tjba.jus.br	DIN

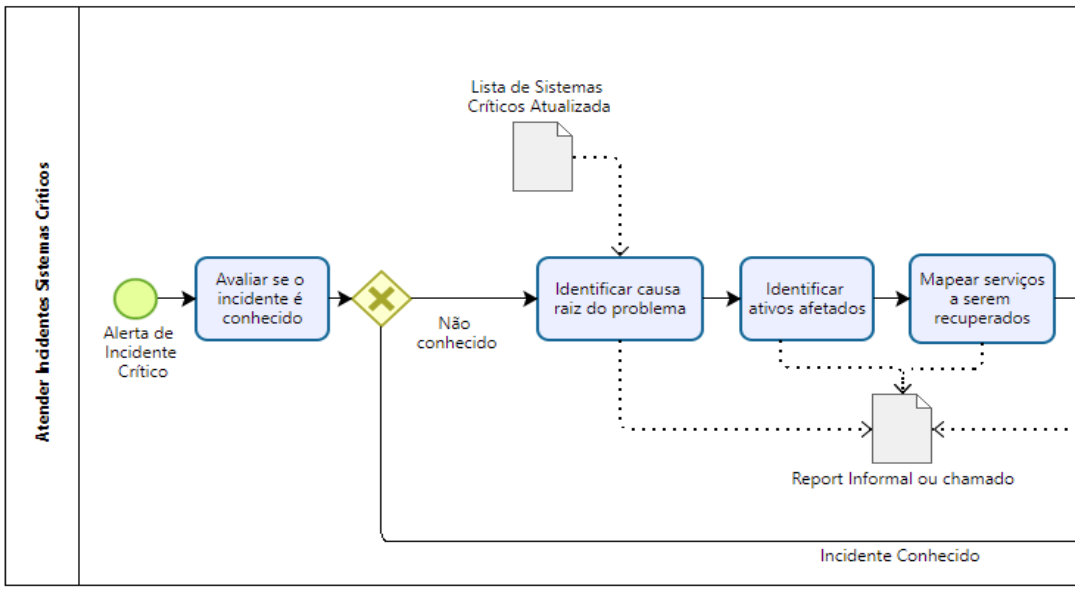
Equipe	Papéis e Responsabilidades	Responsável	Telefone	Contato	Setor
	O líder desta equipe administrará e manterá o Plano de Administração de Crise.				
Equipe de Backup	Analisar as perdas e mapear a quantidade de dados perdidos, tempo de recuperação desses dados e formular estratégia de recuperação de dados de acordo com as políticas pré-estabelecidas.	Coordenador da COTEC	(71)337215 04	cotec@tjba.jus.br	COTEC
Equipe de Segurança da Informação	Prover mecanismos de segurança no ambiente principal e alternativo. Resguardar aplicações e dados, evitando que desdobramentos de segurança afetem o acionamento da continuidade, cuja proteção estará contida na política de segurança.	Coordenador da COTEC	(71)337215 04	cotec@tjba.jus.br	COTEC

Quadro 10: Contatos de acionamentos do Plano

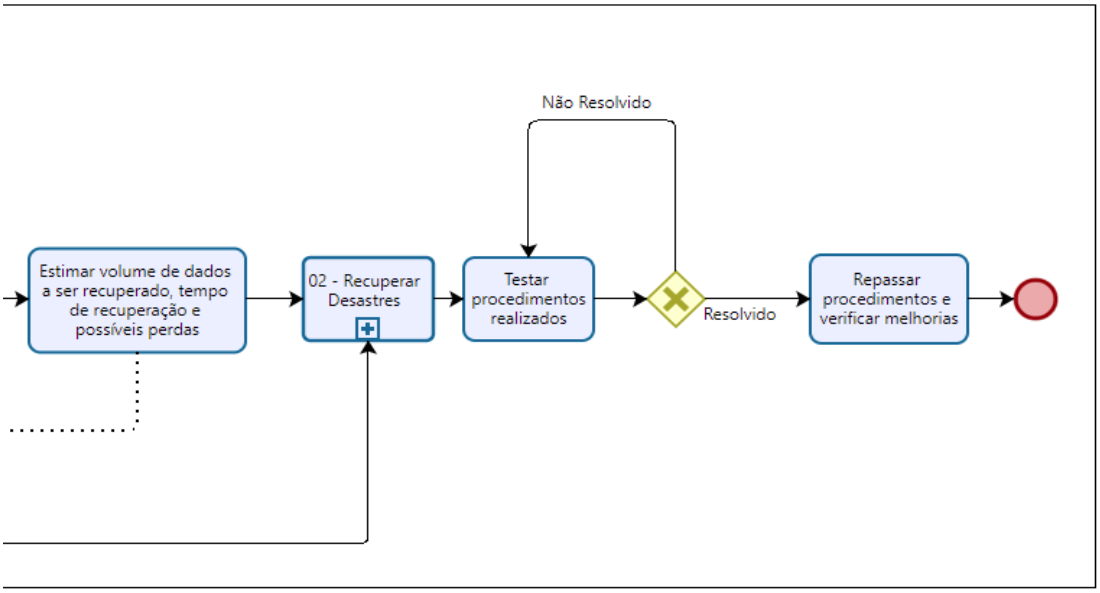
Ao acionar os contatos informar qual ponto de encontro mais próximo, local e detalhes para reunir as equipes.

10. Processo de acionamento do Plano

Processo de acionamento para atendimento dos Serviços Críticos da SETIM:



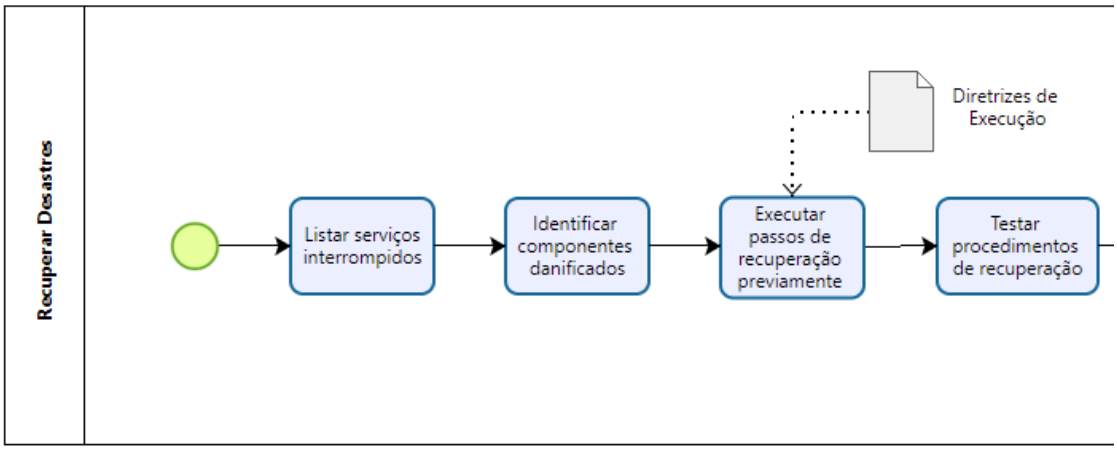
Parte A



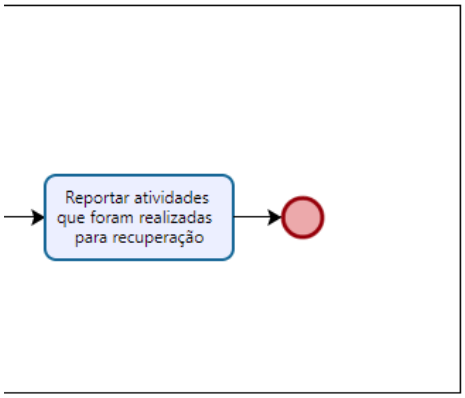
Parte B

Figura 3: Mapa do processo de atendimento dos serviços críticos de TIC

Processo de acionamento do Plano de Recuperação de Desastres:



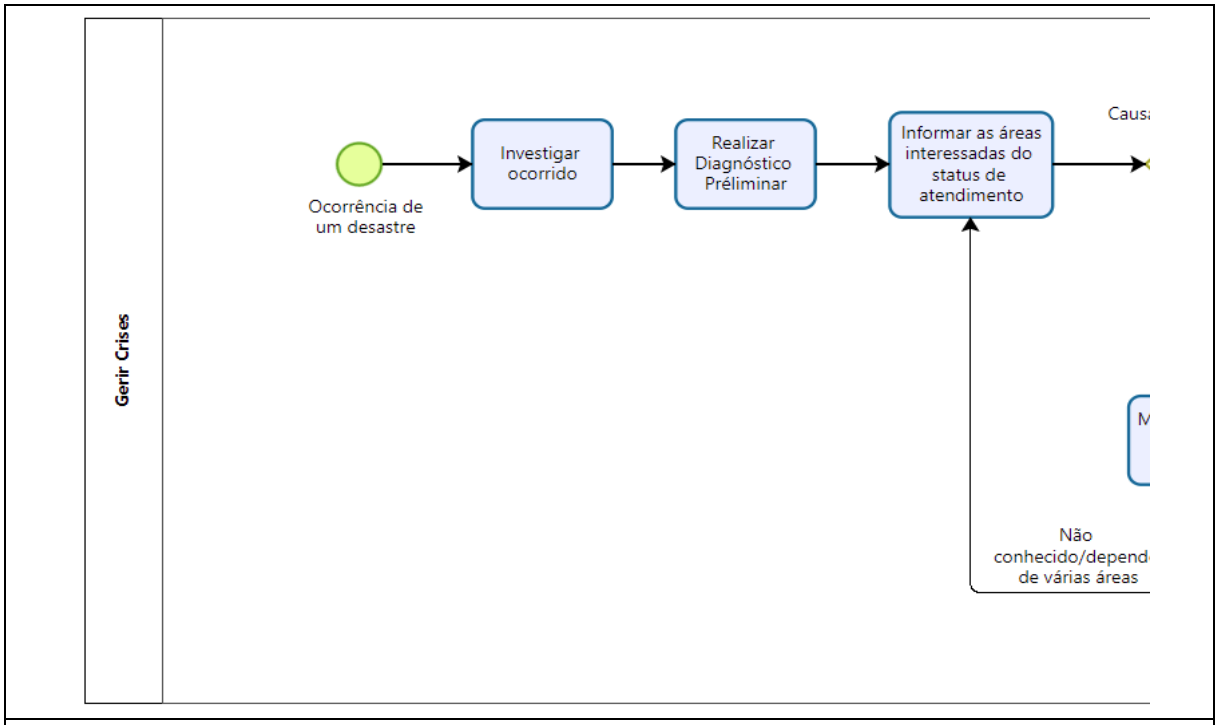
Parte A



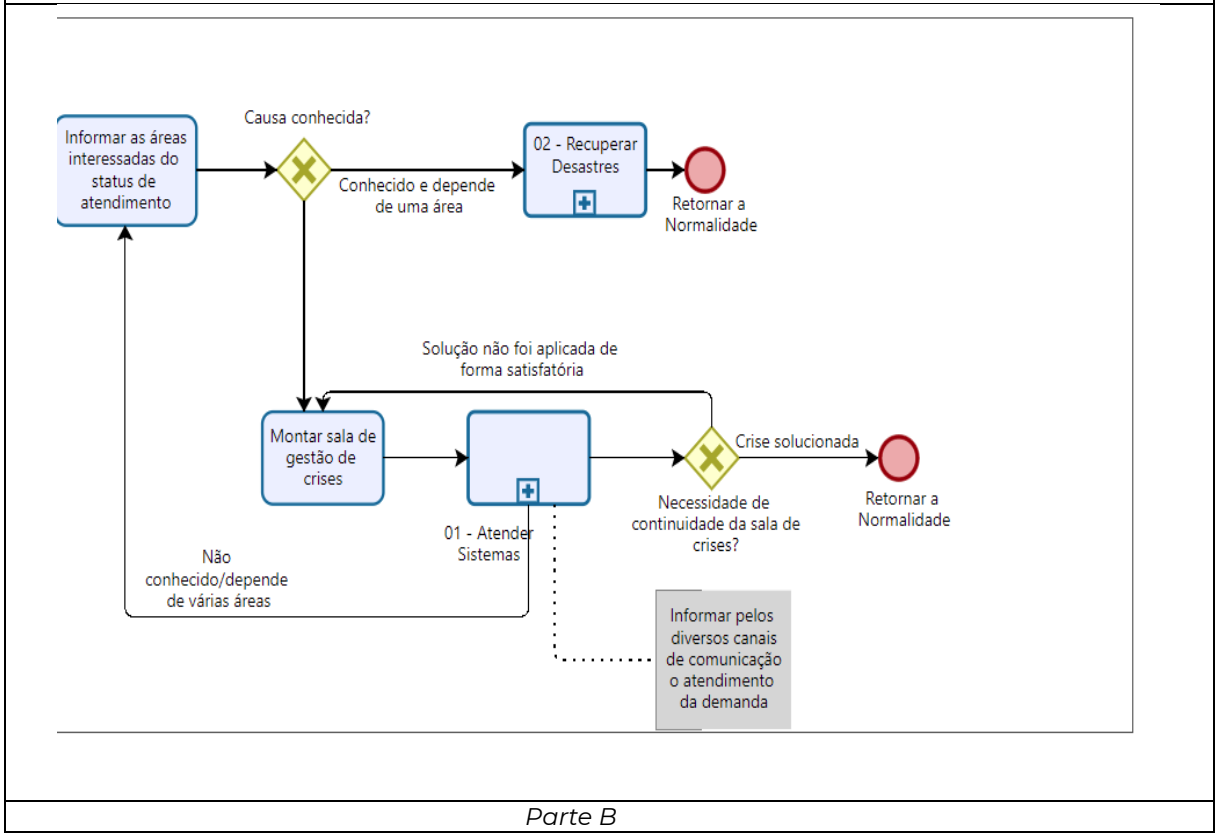
Parte B

Figura 4: Mapa de processo da ativação do PRD

Processo de acionamento do Plano de Gestão de Crises:



Parte A



Parte B

Figura 5: Mapa de processo do acionamento do PGC – (Gestão de Crises)

O Plano de Continuidade dos Serviços de TIC da SETIM integra um conjunto mais amplo de planos institucionais, que atuam de forma complementar, coordenada e hierarquizada, com o objetivo de assegurar a continuidade das atividades do Tribunal de Justiça da Bahia (TJBA) diante de eventos disruptivos de diferentes naturezas.

Enquanto o Plano de Continuidade dos Serviços da SETIM concentra-se na manutenção e recuperação dos serviços de TIC sob sua responsabilidade, outros planos possuem abrangência institucional maior ou foco específico em aspectos operacionais, estratégicos ou de gestão de crises, sendo acionados conforme a natureza, a gravidade e o impacto do evento.

Plano de Continuidade Operacional (PCO)

O Plano de Continuidade Operacional (PCO) tem como objetivo assegurar a continuidade das operações essenciais do TJBA, mesmo em cenários de indisponibilidade significativa de infraestrutura, pessoas, sistemas ou instalações, independentemente da causa do evento, não se restringindo especificamente aos recursos de TIC.

O PCO atua no nível institucional e operacional do negócio, definindo:

- Processos críticos do TJBA;
- Formas alternativas de execução das atividades essenciais;
- Prioridades operacionais enquanto perdurar a situação de contingência.

Relação com o Plano de Continuidade dos Serviços da SETIM: O Plano de Continuidade dos Serviços de TIC da SETIM suporta o PCO, garantindo que os serviços tecnológicos necessários à continuidade das operações judiciais e administrativas estejam disponíveis dentro dos limites de RTO e RPO definidos pela BIA/AIN. Assim, o PCO, define o que precisa continuar funcionando no TJBA enquanto o PCTIC da SETIM define como os serviços de TIC necessários a essa continuidade serão mantidos ou recuperados.

Plano de Administração de Crises (PAC)

O Plano de Administração de Crises (PAC) estabelece a estrutura de governança, os papéis, as responsabilidades e os fluxos de comunicação para a gestão coordenada de situações de crise institucional que possam afetar o TJBA e tem como finalidade:

- Coordenar as decisões estratégicas durante eventos de alto impacto;
- Orquestrar a atuação integrada das áreas envolvidas;
- Garantir comunicação clara, tempestiva e institucional com partes interessadas internas e externas;
- Minimizar impactos institucionais, legais, operacionais e reputacionais.

Relação com o Plano da SETIM: Durante uma crise, o Plano de Continuidade dos Serviços de TIC da SETIM opera sob a governança do PAC, fornecendo:

- Informações técnicas sobre impacto, indisponibilidade e tempo estimado de recuperação;
- Execução das ações de contingência e recuperação tecnológica;
- Subsídios para a tomada de decisão estratégica e para a comunicação institucional.

O PAC não executa ações técnicas, mas coordena e direciona os planos operacionais, incluindo os planos de continuidade e recuperação de TIC.

Plano de Recuperação de Desastre (PRD)

O Plano de Recuperação de Desastre (PRD) tem como objetivo ajudar a restabelecer os serviços de TIC do TJBA ao seu estado normal de operação, no ambiente principal, após a contenção do evento disruptivo e a superação da fase crítica da crise, o PRD atua principalmente no nível tático e operacional da TIC, abrangendo:

- Recuperação de ambientes tecnológicos afetados;
- Restauração definitiva de sistemas, dados e infraestrutura;
- Retorno controlado da operação do ambiente alternativo para o ambiente principal.

Relação com o Plano da SETIM: O PRD complementa o Plano de Continuidade dos Serviços da SETIM ao tratar do pós-crise, enquanto o plano de continuidade dos serviços trata da manutenção temporária dos serviços essenciais durante a indisponibilidade do ambiente principal. Considerando a atuação integrada, temos:

- O Plano de Continuidade assegura a continuação dos serviços críticos;
- O PRD assegura a restauração plena e sustentável da operação normal.

Plano	Foco Principal	Momento de Atuação	Abrangência
Plano de Continuidade dos Serviços da SETIM	Manter e recuperar serviços essenciais de TIC	Durante o incidente	Serviços de TIC da SETIM
PCO – Continuidade Operacional	Continuidade das operações do TJBA	Durante o incidente	Institucional
PAC – Administração de Crises	Governança, decisão e comunicação	Durante e após o incidente	Institucional
PRD – Recuperação de Desastre	Retorno à operação normal	Pós-crise	institucional

Quadro 11: Visão integrada dos Planos de Continuidade

O Plano de Continuidade dos Serviços de TIC da SETIM integra um sistema institucional de gestão da continuidade, no qual a manutenção dos serviços tecnológicos essenciais é condição necessária para a continuidade das operações do TJBA, sob a coordenação da governança de crises e com posterior recuperação plena por meio do Plano de Recuperação de Desastre

11. Estratégias de Continuidade dos Serviços de TIC

As estratégias de continuidade dos serviços de TIC da SETIM foram definidas com base na criticidade dos serviços ao funcionamento do Poder Judiciário, nos impactos potenciais à atividade jurisdicional e administrativa do TJBA e na capacidade institucional de resposta e recuperação diante de eventos disruptivos.

Considera-se que a indisponibilidade prolongada de determinados sistemas pode resultar em descontinuidade das atividades judiciais, atraso na prestação jurisdicional e prejuízos institucionais relevantes. Dessa forma, foram estabelecidas estratégias graduais de continuidade, compatíveis com o nível de criticidade de cada serviço essencial.

No cenário atual, a SETIM adota duas estratégias principais de continuidade para os serviços de TIC considerados essenciais: Cold Backup e Warm Site, aplicadas de forma diferenciada conforme o impacto esperado da interrupção de cada serviço.

11.1. Estratégia de Continuidade – Cold Backup

Essa estratégia deve ser aplicada aos serviços de TIC importantes, porém, de menor criticidade ou com maior tolerância à indisponibilidade.

A estratégia de Cold Backup é adotada para serviços de TIC cuja interrupção, embora relevante, não compromete de forma imediata e irreversível as os serviços de TIC prestados externamente e/ou os serviços essenciais da função do TJBA.

Essa estratégia baseia-se na preservação de dados e ativos digitais críticos para posterior restauração, sem a manutenção prévia de infraestrutura tecnológica alternativa pronta para ativação imediata.

As principais características dessa estratégia são:

- Existência de cópias de segurança dos sistemas e dados essenciais, armazenadas em local alternativo (Fórum Criminal de Sussuarana);
- Ausência de infraestrutura computacional previamente configurada no local alternativo;
- Inexistência de conectividade redundante ativa;
- Tempo de recuperação médio a elevado, compatível com a criticidade dos serviços enquadrados nessa estratégia.

Ações de Contingência e de Recuperação de Desastres dessa estratégia, em caso de incidentes relevantes, incluem ações como:

- Identificação da extensão da perda de dados, sistemas e ativos afetados;
- Restabelecimento da infraestrutura tecnológica no ambiente principal ou alternativo;
- Recuperação dos dados a partir das cópias de backup disponíveis;
- Retomada gradual dos serviços, conforme priorização definida nos subplanos específicos.

Os procedimentos detalhados de resposta e recuperação associados a esta estratégia devem ser descritos nos procedimentos operacionais de continuidade correspondentes.

11.2 Estratégia de Continuidade – Warm Site

Essa estratégia deve ser aplicada aos serviços de alta criticidade, com baixo nível de tolerância à indisponibilidade.

A estratégia de Warm Site é adotada para os serviços de TIC classificados como altamente críticos ao funcionamento do TJBA, cuja indisponibilidade pode provocar impacto direto na atividade jurisdicional, no atendimento ao cidadão e na continuidade do negócio institucional.

Essa estratégia está sendo implantada de forma gradual e evolutiva, priorizando inicialmente as aplicações judiciais essenciais, com destaque para o Processo Judicial Eletrônico (PJe).

As principais características da estratégia incluem:

- Utilização de ambientes em nuvem pública como sítio alternativo de operação (Amazon Web Services – AWS e Google Cloud Platform – GCP), por meio de adesão à Ata de Registro de Preços do Ministério da Economia;
- Replicação contínua ou quase em tempo real de dados críticos (bancos de dados, arquivos, imagens de software e códigos-fonte), correspondente à Fase 1 da estratégia;
- Preparação de imagens base padronizadas (gold images) para servidores de aplicação das soluções essenciais (Fase 2);
- Preparação de imagens base para aplicações satélites e sistemas de apoio às aplicações essenciais (Fase 3);
- Implementação progressiva de mecanismos de ativação sob demanda e escalabilidade automática, permitindo a rápida disponibilização dos ambientes alternativos em caso de falha do ambiente principal;
- Existência de conectividade dedicada e túneis seguros (VPNs) entre o ambiente on-premises e os ambientes em nuvem;
- Tempo de indisponibilidade reduzido, compatível com a criticidade dos serviços protegidos por esta estratégia.

Ações de Contingência e de Recuperação de Desastres dessa estratégia, em caso de evento disruptivo, incluem ações como:

- Identificação dos sistemas impactados e da criticidade associada;
- Verificação do estágio de implantação do Warm Site aplicável a cada sistema;
- Ativação do ambiente alternativo conforme os recursos disponíveis em cada fase da estratégia;
- Operação temporária dos serviços no ambiente de contingência;
- Após a estabilização do ambiente principal, execução da replicação reversa dos dados do ambiente em nuvem para o ambiente on-premises;
- Retorno controlado à operação normal.

Os procedimentos operacionais detalhados, critérios de acionamento e responsabilidades encontram-se descritos nos procedimentos operacionais específicos de continuidade e recuperação.

A adoção combinada das estratégias de Cold Backup e Warm Site permite à SETIM equilibrar custo, complexidade e nível de proteção, assegurando que os serviços mais críticos ao TJBA disponham de mecanismos mais robustos de continuidade, enquanto os serviços com maior tolerância à indisponibilidade sejam protegidos de forma proporcional ao seu impacto no negócio.

12. Relação de Criticidade, RTO, RPO e Estratégias de Continuidade

Os valores de RTO e RPO abaixo refletem a criticidade dos serviços da SETIM já apurada até o momento, podendo ser refinados conforme evolução da BIA por serviço específico.

Nível de Criticidade do Serviço	Impacto ao Negócio do TJBA	RTO (Tempo Máximo de Recuperação)	RPO (Perda Máxima de Dados Aceitável)	Estratégia de Continuidade Adotada	Exemplos de Serviços
Crítico Essencial	Interrupção provoca paralisação imediata da atividade jurisdicional ou prejuízo institucional relevante	Até 4 horas	Até 15 minutos	**Warm Site em Nuvem (Alta Prioridade)** com replicação quase em tempo real e ativação sob demanda	PJe, sistemas judiciais centrais, autenticação corporativa
Crítico Relevante	Impacto significativo na prestação jurisdicional ou administrativa, com tolerância limitada	Até 8 horas	Até 1 hora	**Warm Site em Nuvem (Parcial / Faseada)** com imagens base e replicação periódica	Sistemas de apoio ao PJe, sistemas administrativos críticos
Importante	Impacto operacional relevante, porém sem paralisação imediata do negócio	Até 24 horas	Até 24 horas	**Cold Backup Estruturado** com restauração priorizada	Sistemas administrativos não judiciais, portais internos
Suporte / Não Crítico	Impacto baixo ou tolerável por período prolongado	Acima de 48 horas	Acima de 48 horas	**Cold Backup Convencional**	Sistemas de apoio secundário, soluções departamentais

Quadro 12: Relação de criticidade dos serviços SETIM com RTO, POR e Estratégias

A definição das estratégias de continuidade dos serviços de TIC da SETIM está diretamente vinculada aos resultados da Análise de Impacto no Negócio (BIA), que identifica:

- Processos institucionais críticos do TJBA;
- Dependência desses processos em relação aos serviços de TIC;
- Impactos operacionais, institucionais, legais e reputacionais decorrentes da indisponibilidade dos sistemas;
- Tolerância máxima à interrupção (RTO) e à perda de dados (RPO).

A partir da BIA, os serviços de TIC foram classificados em níveis de criticidade, permitindo:

- A priorização objetiva dos serviços essenciais;
- A definição de estratégias de continuidade proporcionais ao impacto;
- O direcionamento de investimentos e esforços para os serviços com maior risco de descontinuidade do negócio.

A estratégia de Warm Site é aplicada prioritariamente aos serviços classificados como Críticos Essenciais e Críticos Relevantes, enquanto a estratégia de Cold Backup é utilizada para serviços com maior tolerância à indisponibilidade, conforme definido na BIA.

12.1. Governança da Continuidade de Serviços de TIC

A governança do Plano de Continuidade de Serviços da SETIM assegura que as estratégias definidas:

- Estejam alinhadas aos objetivos estratégicos do TJBA;
- Sejam periodicamente revisadas à luz de mudanças tecnológicas, organizacionais e regulatórias;
- Considerem a evolução da criticidade dos serviços e dos riscos associados.

No âmbito da governança, cabem à SETIM as seguintes responsabilidades principais:

- Manter atualizada a classificação de criticidade dos serviços, com base na BIA;
- Revisar periodicamente os RTOs e RPOs, considerando mudanças de demanda, capacidade e arquitetura;
- Garantir que os subplanos de contingência e recuperação estejam alinhados às estratégias (Cold Backup ou Warm Site);
- Monitorar contratos, fornecedores e ambientes tecnológicos que suportam as estratégias de continuidade;
- Promover testes periódicos e exercícios de continuidade, especialmente para os serviços protegidos por Warm Site.

A governança também prevê a integração do Plano de Continuidade com a gestão de riscos corporativos, assegurando que eventos de TIC sejam tratados como riscos institucionais capazes de afetar diretamente a continuidade do negócio do TJBA.

A criticidade dos serviços de TIC, os parâmetros de recuperação (RTO e RPO) e as estratégias de continuidade adotadas pela SETIM estão fundamentados na Análise de Impacto no Negócio e integrados à governança institucional, assegurando uma resposta proporcional, planejada e eficaz a eventos que possam comprometer a continuidade das atividades do TJBA.

13. Validação e teste de PCTIC

Este plano será testado, revisado e validado em reunião entre os líderes, minimamente uma vez ao ano 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 tipos de testes a serem realizados são:

- **Teste de mesa**: Testar os algoritmos para validar se existe algum erro de lógica.
- **Caminho percorrido**: Assegurar que cada integrante de processo crítico se familiarize com o PCTIC.
- **Simulação**: Simular uma situação real de interrupção.

Os testes previstos no âmbito do Plano de Continuidade dos Serviços de TIC do TJBA serão registrados, acompanhados e controlados por meio dos seguintes status, que indicam a situação de cada teste ao longo do seu ciclo de vida:

- **Planejado**: Status atribuído aos testes que foram definidos no Plano de Continuidade, na BIA ou no plano anual de testes, com objetivo, escopo e tipo de teste estabelecidos, porém sem data, equipe ou recursos formalmente definidos.
  Indica que o teste está previsto estrategicamente, é necessário para validação da continuidade e que ainda depende de detalhamento operacional.
- **Programado**: Status atribuído aos testes que, além de planejados, já possuem definição preliminar de período de realização, tipo de teste, ambientes envolvidos e responsáveis principais, mas ainda não tiveram data e agenda formalmente confirmadas.
  Indica que o teste já foi priorizado, está inserido no planejamento operacional e aguarda consolidação de agenda e recursos.
- **Agendado**: Status atribuído aos testes que possuem data, horário, equipes, ambientes e recursos formalmente definidos e comunicados, estando prontos para execução conforme o cronograma estabelecido.
  Indica que o teste tem agenda confirmada, envolve áreas e equipes notificadas e está autorizado para execução.
- **Executado**: Status atribuído aos testes que foram efetivamente realizados, conforme o escopo aprovado, independentemente do resultado obtido (sucesso total, sucesso parcial ou falha).
  Indica que o teste foi conduzido conforme o planejamento, possui registro de evidências e deve gerar relatório de resultados, lições aprendidas e eventuais planos de ação.

Observação Importante para Governança: O status ***Executado*** não implica, necessariamente, que o teste tenha sido bem-sucedido, mas apenas que foi realizado, a avaliação de efetividade e maturidade dos controles é tratada nos relatórios de teste e nos planos de melhoria contínua.

Esses status permitem que exista a rastreabilidade completa do ciclo de vida dos testes, a transparência para governança, auditoria e órgãos de controle e a avaliação contínua da maturidade da continuidade de serviços do TJBA.

Data	Tipo	Motivo	Status
xx/xx/2026			

Quadro 13: Registro dos testes efetuados nos planos

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

<Inserir assinatura digital para todas diretorias e coordenações abaixo>

DIN - Diretoria de Informática

DMO - Diretoria de Modernização

COSIS - Coordenação de Sistemas de Informação

CSJUD - Coordenação de Sistemas Judiciais

COATE - Coordenação de Atendimento Técnico

CPROD - Coordenação de Produção e Comunicação

COTEC - Coordenação de Suporte Técnico

CPROM – Coordenação de Projetos de Modernização

ASI - Assessoria de Segurança da Informação

14. Integração com Plano de Continuidade Operacional - Visão TIC

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

É escopo deste plano garantir ações de continuidade operacional durante e depois da ocorrência de uma crise ou cenário de desastre tratando-se apenas das ações de contingência relacionadas com a estratégia de continuidade dos serviços de TIC.

Objetivos pretendidos com essa visão do PCO:

- Prover meios para manter o funcionamento dos principais serviços e a continuidade das operações, envolvendo os sistemas essenciais.
- Estabelecer procedimentos, controles e regras alternativas que possibilitem a continuidade das operações durante uma crise ou cenário de desastre.
- Estabelecer equipes para atuar em cada plano específico PCO, PRD e PAC.
- Definir os formulários, checklists e relatórios a serem entregues pelas equipes ao executar as ações e atividades planejadas.

Equipes SETIM envolvidas:

- DIN - Diretoria de Informática
- DMO - Diretoria de Modernização
- COSIS - Coordenação de Sistemas de Informação
- CSJUD - Coordenação de Sistemas Judiciais
- COATE - Coordenação de Atendimento Técnico
- CPROD - Coordenação de Produção e Comunicação
- COTEC - Coordenação de Suporte Técnico

Gestão: A COTEC é a unidade responsável por implementar, manter e melhorar a integração com o PCO e toda documentação inerente ao desdobramento desse plano.

Execução do Plano:

- Avaliação de Impacto de Desastre

  Identificada a ocorrência de um incidente ou crise o Líder da Equipe de Operação e Backup deve verificar a dimensão do impacto, extensão e possíveis desdobramentos do ocorrido.

  O documento Anexo I “AVALIAÇÃO DE IMPACTO DE DESASTRE” deve ser preenchido e submetido ao COMITÊ DE DR para avaliação e decisão sobre o acionamento do plano e início das ações de contingência.

  Divulgar a informação a todas as equipes envolvidas.

- Acionamento do Plano

  Dado o aval pelo COMITÊ DE DR acionamento do plano a EQUIPE DE OPERAÇÕES convocará reunião de emergência com os líderes do PRD e PAC com o intuito de:

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

  Contingência de Cold Backup: Devem ser adotadas as seguintes ações de contingência e continuidade por processo ou serviço essencial:

ID	Instrução	Duração	Observação	Resultado
1.	Verificar status da aplicação de backup e estimar impacto de perda dados (janela)			☐
2.	Identificar fitas cujos dados em questão foram afetados			☐
3.	Mapear blocos a serem recuperados			☐
4.	Estimar volume de dados a serem recuperados, tempo de recuperação dos dados e possíveis perdas operacionais			☐
5.	Atestar retorno do funcionamento do ambiente principal com Líder do PRD			☐
6.	Teste de aplicação de backup após desastre			☐
7.	Validar policies implementadas			☐
8.	Prover recovery dos dados às aplicações			☐

Quadro 14: Ações de contingência de Cold Backup

- Ativação das ações relacionadas ao Warm Site

  Devem ser adotadas as seguintes ações de contingência e continuidade por processo ou serviço essencial:

NUVEM				
ID	**Instrução**	**Duração**	**Observação**	**Resultado**
1.	Validar fase em que se encontrar a implementação do WarmSite: dados, aplicações ou satélites.			☐
2.	Caso concluída a fase 1, criar ambiente de aplicação para aplicações principais e satélites, realizar deploy da aplicação e disponibilizar o ambiente			☐
3.	Caso concluída a fase 2, ativar ambiente de DR para aplicações principais e realizar deploy das aplicações satélite, disponibilizar o ambiente			☐
4.	Caso concluída a fase 3, ativar ambiente de DR para aplicações principais e satélite. Disponibilizar o ambiente			☐

Quadro 15: Ações de contingência e continuidade por processo ou serviço essencial

- Encerramento do plano

  Uma vez validado o funcionamento do retorno das operações essenciais e estabilidade dos recursos de TIC envolvidos, deverá ser emitido um parecer ao comitê relatando as atividades realizadas neste plano e informar à Equipe de Comunicação o retorno das atividades.

15. Integração com Plano de Gerenciamento de Crises - Visão TIC

O objetivo deste plano é garantir que exista a comunicação e a integração com as estruturas institucionais do TJBA para gerenciar as crises e viabilizar uma compreensão linear a todos os envolvidos das ações antes, durante e após a ocorrência de uma crise.

Objetivos pretendidos com esta visão do Plano:

- Garantir a segurança à vida das pessoas;
- Minimizar transtornos sobre os desdobramentos de incidente e estimular o esforço em conjunto para superação da crise.
- Orientar os funcionários e demais colaboradores com informações e procedimentos de conduta.
- Informar a sociedade em tempo e com esclarecimentos condizentes com o ocorrido.

Execução do Plano:

As figuras a seguir representam, o diagrama de atividades a serem desempenhadas na execução do Plano e as Comunicações necessárias a serem realizadas em caso de crise.

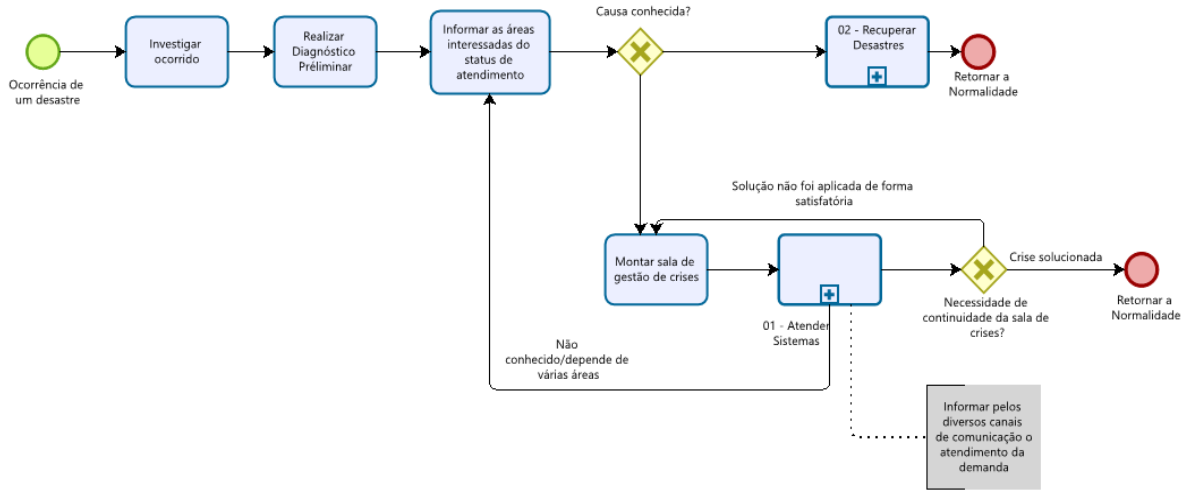


Figura 6: Mapa do Processo de Atender Recursos Críticos

Após ocorrência de uma crise, pode ser necessário realizar a apuração do ocorrido e a realização de um entendimento preliminar, após realizadas essas atividades as informações do andamento, dos atendimentos e a avaliação de necessidade de ativação da sala de gestão de crises, precisam ser informadas para assegurar mais

agilidade, resposta e chance de sucesso no tratamento da crise até a normalidade das operações.

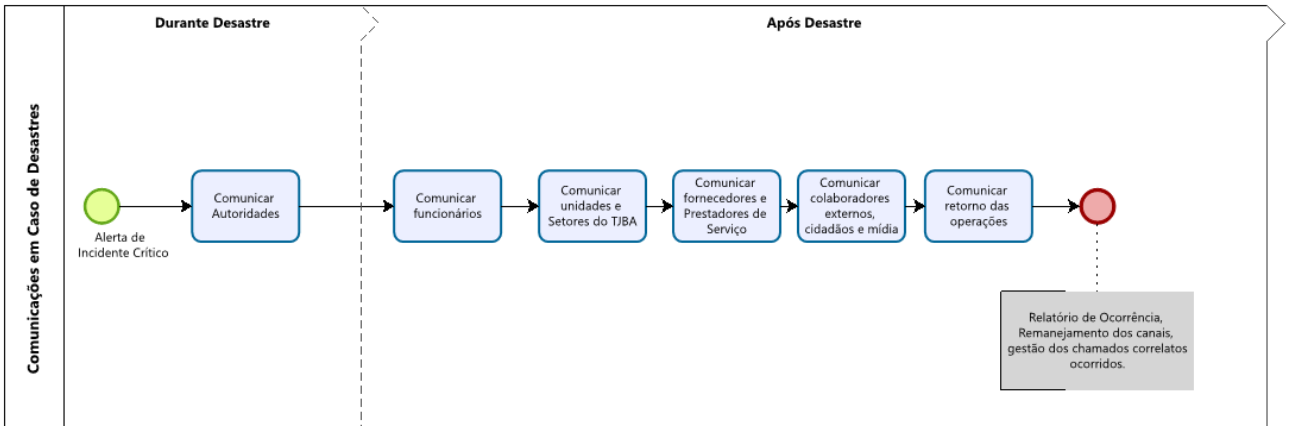


Figura 7: Mapa do Processo de comunicação de desastres

Comunicação da 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 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	Número	Data/Hora do registro	Nº ocorrência
Polícia	190	_____/_____/_____ _____:_____	
Bombeiros	193	_____/_____/_____ _____:_____	
SAMU	192	_____/_____/_____ _____:_____	
ANPD	https://www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca	_____/_____/_____ _____:_____	
DSIC/CTIR	https://www.gov.br/gsi/pt-br/assuntos/dsi	_____/_____/_____ _____:_____	

Quadro 16: Contatos com Autoridades

Em casos de incidentes cibernéticos, deverão ser seguidas as diretrizes estabelecidas nos seguintes documentos:

- Protocolo de Prevenção de Incidentes Cibernéticos do Poder Judiciário (PPINC-PJ)

- ANEXO I – Protocolo – Prevenção de incidentes cibernéticos do Poder Judiciário

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 reestabelecimento dos serviços inativos.

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

Números de Contato a serem disponibilizados:

- Telefone: (71) 3372-7508 ou 3320-6636
- Contatos de E-mail: cprod@tjba.jus.br, cotec@tjba.jus.br
- Central de Serviços (Service Desk): 0800 0718522/ (71) 3324-7400

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

As informações a serem dadas irão se referir a:

- Se é seguro para eles entrarem no ambiente afetado
- Onde eles devem ir se não puderem ter acesso ao TJBA.
- Que serviços ainda estão disponíveis para eles
- Expectativas de trabalho durante o desastre
- Comunicar unidades e setores do TJBA
- Acionar diretamente as unidades afetadas pelo desastre e fornecer contato
- Natureza, impacto e abrangência da catástrofe
- Ações em andamento
- Processos e serviços cobertos pelo plano (serviços essenciais)

Setor/ Unidade	Número/contato	Data/Hora do contato	Local
DRH	Gabinete: 3372-1649 Secretaria: 3372-166	_____/____/____ ____:____	Sala 103 do Anexo
Corregedoria	3372-5094	_____/____/____ ____:____	Sala 312 do Anexo
Assessoria da Presidência AEP II	3372-5077	_____/____/____ ____:____	Sala 303-S do Tribunal de Justiça
Secretaria de TIC	3372-5077/ 5123	_____/____/____ ____:____	Sala 303-N do Tribunal de Justiça
ASCOM	Recepção: 3483-3731	_____/____/____ ____:____	Sala 312 - Edifício Advogado Pedro

Setor/ Unidade	Número/contato	Data/Hora do contato	Local
			Milton de Brito – Anexo II
Secretaria de Administração	3372-5123	_____/____/____ ____:____	Sala 309/311-N do Tribunal de Justiça
Balcões de Justiça	3372-5077/ 5659	_____/____/____ ____:____	Sala 303-S do Tribunal de Justiça

Quadro 17: Contatos com os servidores

Contatos dos principais fornecedores de TIC	
Empresa: HP **Contato:** 0800 709 7751 ou 0800 556 405 Netsul: 0800 710 2029	**Pessoa/Contato:** _____ **Data/Hora Acionamento:** _____/_____/_____ ____:____:____
Empresa: SUN/ORACLE **Contato:** 0800 709 7751 ou 0800 556 405	**Pessoa/Contato:** _____ **Data/Hora Acionamento:** _____/_____/_____ ____:____:____
Empresa: DELL **Contato:** 0800 722 3300 / 0800 770 3811	**Pessoa/Contato:** _____ **Data/Hora Acionamento:** _____/_____/_____ ____:____:____
Empresa: CISCO **Contato:** 0800 891 4972	**Pessoa/Contato:** _____ **Data/Hora Acionamento:** _____/_____/_____ ____:____:____
Empresa: ENTERASYS **Contato:** amauri.costa@zcr.com.br	**Pessoa/Contato:** _____ **Data/Hora Acionamento:** _____/_____/_____ ____:____:____
Empresa: HITACHI **Contato:** 0800 772 1044 **Obs.:** Site ID 457020I	**Pessoa/Contato:** _____ **Data/Hora Acionamento:** _____/_____/_____ ____:____:____
Empresa: ACECO **Contato:** 0800 887 0775	**Pessoa/Contato:** _____ **Data/Hora Acionamento:** _____/_____/_____ ____:____:____
Empresa: OI **Contato:**	**Pessoa/Contato:** _____ **Data/Hora Acionamento:** _____/_____/_____ ____:____:____

Contatos dos principais fornecedores de TIC	
Empresa: CEMIG **Contato:**	**Pessoa/Contato:** _____ **Data/Hora Acionamento:** _____/_____/_____ ____:____:____
Empresa: PRODEB **Contato:**	**Pessoa/Contato:** _____ **Data/Hora Acionamento:** _____/_____/_____ ____:____:____

Quadro 18: Contatos dos principais fornecedores de TIC

A equipe de comunicação, em consonância com a Secretaria de Comunicação do TJBA, deverá fornecer informações pertinentes aos colaboradores externos, incluindo advogados, cidadãos e outros órgãos. Nessa comunicação deverá minimamente validada a situação passada de acordo com o cenário do desastre ou crise e buscar publicar em meios oficiais e de ampla divulgação, com aval do comitê de continuidade e institucional, informações sobre o ocorrido e os impactos estimados.

NOME DA EMPRESA	TELEFONE	Objeto do Contrato	PAPEL	Coordenação
Solutis	(71) 98732-4130	Desenvolvimento de Sistemas	Preposta	COSIS/CSJUD
Qintess	(71) 99147-2657	Suporte Especializado em Sistemas	Preposta	COSIS/CSJUD
Aceco TI LTDA.	(71) 99939-6728	Sala Cofre	Preposta	CPROD
Unentel Soluções Tecnológicas LTDA.	(71)98113-4621 / (71)3417-7761 / (71)98806-7578	Centrais telefônicas das demais localidades (Interior, região metropolitana de Salvador e outras unidades da capital)	Preposta	CPROD
Metodo Telecomunicacoes e Comercio LTDA.	(31)997973-3797 / (31)98619-9587 / (31)99905-6702	Centrais telefônicas: Sede e seus anexos / Fórum Rui Barbosa e seus anexos / Fórum Criminal	Preposta	CPROD
Solutis Tecnologias LTDA	(71)98366-2213	Suporte a usuários nos níveis 1 e 2.	Preposta	COATE
OI S.A	(71)98807-2855 / (71)98845-0115	Circuitos de comunicação de dados (links)	Preposta	CPROD
EDS	+55 (81) 99345-3808	Ambientes Cloud	Preposto	COTEC
Hepta	(021 71) 98857-9768	Suporte ambiente infra N3	Preposto	COTEC

Quadro 19: Empresas a serem contactadas em casos de desastres

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

Uma vez validado o funcionamento do retorno dos recursos de TIC essenciais e obtida a estabilidade operacional, a Equipe de Comunicação entrará em contato com as partes descritas neste plano provendo as informações de retorno das operações com as informações de status dos serviços essenciais.

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

16. Integração com Plano de Recuperação de Desastres - Visão TIC

É escopo deste plano garantir o retorno das operações com a utilização dos recursos originais depois da ocorrência de uma crise ou cenário de desastre tratando-se apenas dos ativos, conexões e configurações dos recursos de TIC com as operações do TJBA.

Objetivos pretendidos com esta visão do Plano:

- Avaliar danos e prover meios para recuperação dos recursos originais envolvidos no desastre.
- Evitar desdobramentos de outros incidentes decorrentes da não utilização dos recursos originais.
- Reestabelecer os recursos originais de TIC dentro dos prazos estabelecidos no BIA/AIN.

A Figura 8 mostra o mapa do processo de acionamento da recuperação de desastres:

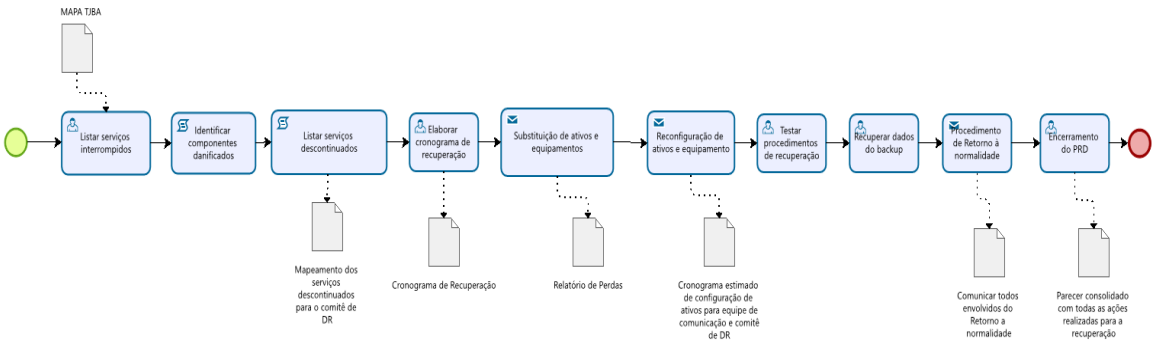


Figura 8: Mapa do processo Recuperar Desastres

Listar Serviços e Recursos de TIC Interrompidos ou afetados

As equipes de Instalação/Backup/Servidores/Rede deverão identificar e listar todos os ativos danificados da ocorrência do desastre.

As informações de cada ativos encontram-se no MAPA TJBA.

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.

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, V 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 recursos de TIC essenciais, ou de acordo com determinação de nível institucional.
- O RTO definido para cada serviço essencial.
- A força de trabalho disponível.

Em caso de perda de ativos e recursos de TIC, 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 COMITÊ DE DR se há alguma solução alternativa a ser tomada enquanto é realizada a aquisição.

A equipe de Instalações deve verificar quais ativos foram danificados estão cobertos por garantia e se poderá ser acionada neste caso através da lista de fornecedores.

As informações pertinentes à alteração do tempo de recuperação dos serviços serão passadas às equipes do PCO e PAC.

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 Comitê de DR.

Testar procedimentos de recuperação

Os testes têm por objetivo assegurar a eficiência e a efetividade do plano e deverão ser planejados e executados com periodicidade mínima anual a partir da data da sua implantação.

A responsabilidade pelo planejamento e organização dos testes, assim como pela definição dos cenários a serem contemplados é da área de Tecnologia da Informação.

Os cenários deverão ser definidos e registrados em um documento formal que deverá ser aprovado pela SETIM, e deverá ser arquivado por um período mínimo de 5 (cinco) anos.

Os testes não deverão provocar quaisquer tipos de indisponibilidade ou parada nos ambientes. As simulações deverão ser realizadas sobre cenários e ameaças contemplados no plano, devendo cobrir os riscos e ameaças com maior probabilidade de ocorrência,

Os testes incluem:

- Garantir os mesmos níveis de capacidade e disponibilidade dos serviços essenciais antes do desastre ref.: mapeamento serviços essenciais.
- Validar as configurações.

Sistema	Instrução	Duração	Observação	Resultado
1.				☐
2.				☐
3.				☐
4.				☐
5.				☐
6.				☐
7.				☐
8.				☐

Quadro 20: Relatório de testes de procedimentos de recuperação

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

Cabe ao líder da Contingência encerrar o acionamento e a execução do plano e comunicar os envolvidos no processo a situação de retorno à normalidade.

Ao término do procedimento de recovery, as informações da recuperação serão consolidadas em parecer específico informando horário de reestabelecimento de cada serviço, equipamentos adquiridos, procedimentos de recuperação realizados e fornecedores acionados.

17. MONITORAMENTO DO DESEMPENHO

O monitoramento do desempenho da Continuidade dos Serviços de TIC é feito com base em indicadores de desempenho (KPIs). No Plano de Continuidade de Serviços de TIC tem como objetivo acompanhar a capacidade da organização de manter ou restabelecer os serviços essenciais de TIC em situações de interrupção. Esses indicadores permitem avaliar a efetividade dos planos, procedimentos e recursos definidos para garantir a continuidade dos serviços críticos.

Os KPIs devem ser objetivos, mensuráveis e acompanhados periodicamente, possibilitando a identificação de falhas, a melhoria dos planos de resposta e a priorização de ações corretivas. Como referência, podem ser adotados os seguintes indicadores:

- Percentual de serviços críticos de TIC com Plano de Continuidade formalizado;
- Percentual de testes de continuidade realizados conforme o planejado;
- Tempo médio de recuperação dos serviços (RTO) em relação ao definido;
- Percentual de serviços recuperados dentro do prazo estabelecido;
- Quantidade de falhas identificadas durante testes de continuidade;
- Percentual de incidentes críticos recuperados dentro do RTO;
- Percentual de ações de melhoria decorrentes de testes e incidentes implementadas.