
TJBA 2022

# Plano de Continuidade de TIC

Conservação e ininterrupção dos sistemas essenciais de TIC do Tribunal de Justiça do Estado da Bahia

# Sumário

| Histórico de versões | | |
|---|---|---|
| **Versão** | **Descrição** | **Responsável(eis)** |
| 1.0 | Criação da primeira versão do PCTIC | Adson Bispo<br>Viviane Batista |
| 1.0 | Aprovação | Henrique Roma |
| 1.1 | Revisão | Adson Bispo<br>Viviane Batista |
| 1.2 | Revisão Plano Consultoria e equipe TJBA | Plano Consultoria |
| | | |
| | | |
| | | |

| Histórico de alteração e exclusão | | |
|---|---|---|
| **Data** | **Inclusão/Alteração** | **Modificado por** |
| xx/xx/22 | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

## Registro de acionamento do PCTIC

| | | | | |
|---|---|---|---|---|
| | Data/Hora início | _____/____/____ ____:____ | Data/Hora fim | _____/____/____ ____:____ |
| Descrição | | | | |
| Resultado | | | | |

| | | | | |
|---|---|---|---|---|
| | Data/Hora início | _____/____/____ ____:____ | Data/Hora fim | _____/____/____ ____:____ |
| Descrição | | | | |
| Resultado | | | | |

| | | | | |
|---|---|---|---|---|
| | Data/Hora início | _____/____/____ ____:____ | Data/Hora fim | _____/____/____ ____:____ |
| Descrição | | | | |

| | |
|---|---|
| Resultado | |

## 1. Apresentação

O presente documento tem por objeto apresentar o Plano de Continuidade da SETIM do Tribunal de Justiça da Bahia - TJBA. A elaboração desse Plano é uma iniciativa para atendimento ao Guia da Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário – ENTIC-JUD 2021-2026 do CNJ e a Resolução nº 396, de 7 de junho de 2021.

O plano de continuidade de serviços de TIC (PCTIC) é elaborado internamente, em conjunto com as áreas técnicas. Tem como objetivo traçar estratégias e planos de ação que garantam o funcionamento e a disponibilidade dos serviços essenciais da organização durante as mais diversas situações de falha.

O plano é um documento macro com as diretrizes, e contém as premissas básicas a serem cumpridas durante eventos de crise, incluindo a parada dos principais serviços relacionados à prestação de serviços.

Anexo ao plano há uma matriz de riscos, com os respectivos Plano de Recuperação de Desastres – PRD, Plano de Administração de Crises - PCA, Plano de Continuidade Operacional - PCO, mapeando as ações correspondentes no caso de uma ocorrência de algum incidente disruptivo.

## 2. Justificativa e Objetivo - PCTIC

Uma vez que falhas nos serviços de TIC impactam diretamente a continuidade da prestação da justiça, almeja-se com este plano prover medidas de proteção rápidas e eficazes para os processos críticos de TIC relacionados aos sistemas essenciais em casos de incidentes graves ou desastres. O plano de continuidade atuará como resposta aos resultados da Análise de Impacto nos Negócios e Análise de Riscos.

## 3. Escopo

O Plano de Continuidade de TIC (PCTIC) abrange as estratégias necessárias à continuidade dos serviços de TI essenciais: contingência, continuidade e recuperação. Está voltado a conceder continuidade aos processos definidos como críticos para a TI do TJBA e serviços essenciais judiciais.

Este plano pode ser executado tanto no âmbito da SETIM, isoladamente, ou como parte de um Plano de Continuidade de Negócio (PCN) do TJBA.
A figura abaixo representa todos os processos envolvidos na Gestão de Continuidade de Negócios (GCN), e a área demarcada em vermelho representa o escopo principal deste plano.

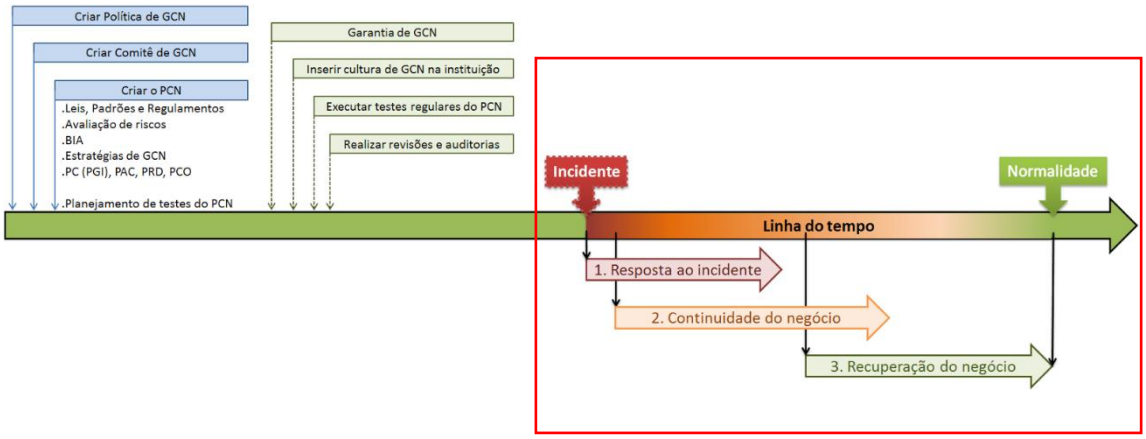


*Figura 1- Representação do Processo de Continuidade de Negócios*

## 4. Definições

**Contingência:** Situação de risco com potencial de ocorrer, inerente as atividades, serviços e equipamentos, e que ocorrendo se transformará em uma emergência. Diz respeito a uma eventualidade; possibilidade de ocorrer.

**Backup:** Cópia de um sistema completo ou de um ou mais arquivos guardados em diferentes dispositivos de armazenamento.

**Data Center:** ou Centro de Processamento de Dados, é um ambiente projetado para concentrar servidores, equipamentos de processamento e armazenamento de dados, e sistemas de ativos de rede, como switches, roteadores e outros.

**Incidente:** É o evento inesperado ou situação que altera a ordem normal das coisas, capaz de causar danos leves ou graves aos sistemas e aos equipamentos de TI do TJBA. Toda ocorrência anormal, que foge ao controle de um processo, sistema ou atividade, da qual possam resultar danos aos sistemas e/ou equipamentos de TI do TJBA.

**Serviços essenciais:** São softwares que agregam valor diretamente a sociedade e representam as atividades essenciais que o órgão executa para cumprir sua missão.

**Warm site:** Site que possui infraestrutura mínima para acomodar os computadores e componentes.

## 5. Serviços Judiciais essenciais

São os seguintes serviços essenciais, por ordem de priorização*, para o acionamento e execução do PCTIC:

| Serviço | Criticidade | RPO* | RTO* | Impacto* | | | |
|---|---|---|---|---|---|---|---|
| | | | | Financeiro | Legal | Imagem | Operacional |
| PJE | Alta | 8 horas | 8 horas | Alto | Alto | Alto | Alto |
| PROJUDI | Alta | 1 semana | N/D | N/D | Alto | Alto | Alto |
| SAIPRO | Baixa | 15 dias | 8 dias | Baixo | Baixo | Alto | Alto |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| SAJ | Alta | 1 semana | N/D | N/D | N/D | N/D | N/D |
| SCC | Baixa | 7 dias | 7 dias | Irrelevante | Baixo | Baixo | Médio |
| SELO DIGITAL | Alta | 7 dias | 8 horas | Crítico | Crítico | Crítico | Crítico |
| DAJE | Alta | 7 dias | 8 horas | Crítico | Crítico | Crítico | Crítico |
| SIGA | | | | | | | |
| Recursos Humanos | | | | | | | |
| TJMAIL | | | | | | | |
| DAJE | | | | | | | |
| Site PJBA | | | | | | | |
| E-selo | | | | | | | |
| | | | | | | | |

**RTO** – período de tempo dentro do qual os níveis mínimos dos serviços e/ou sistemas devem ser recuperados após a ocorrência de uma interrupção.

**RPO** – ponto em uma linha de tempo em que os dados devem ser recuperados após a ocorrência de uma ruptura.

Considerações:

i. Os sistemas judiciais essenciais estão detalhados nos documentos anexo do PCTIC: MAPEAMENTO DOS SISTEMAS ESSENCIAIS e MAPA PJBA.

ii. A priorização dos serviços essenciais, os níveis de impacto no negócio e tempos toleráveis de recuperação serão definidos a partir da Análise de Impacto de Negócio (AIN).

## 6. Equipes envolvidas

O PCTIC 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: Coordenação de Atendimento Técnico (COATE), Coordenação de

Sistemas (COSIS), Coordenação de sistemas Judiciais (CSJUD), Coordenação de Suporte Técnico (COTEC) e Coordenação de Produção (CPROD), lideradas pela DIN – Diretoria de Informática.

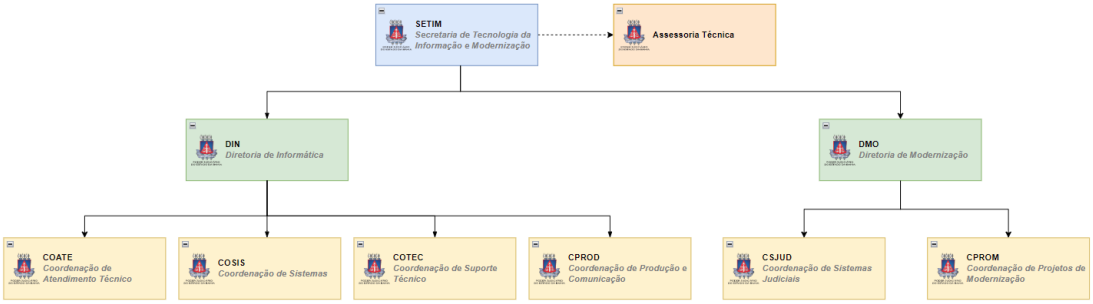


*Figura 2- Organograma SETIM*

## 7. Principais riscos

O PCTIC foi desenvolvido para ser acionado quando da ocorrência de cenários de desastres que apresentam risco à continuidade dos serviços essenciais. O quadro abaixo define estes riscos e aponta quais parâmetros para reportar as possíveis causas da ocorrência.

| Evento de desastre | Possíveis causas |
|---|---|
| 01. Interrupção de energia elétrica | . Causada por fator externo à rede elétrica do prédio ou de sua localidade com duração da interrupção superior à 12 horas.<br>. Causada por fator interno que comprometa a rede elétrica do prédio com curtos-circuitos, incêndio e infiltrações.<br>. Impossibilidade de acionar o Grupo Moto-gerador no momento de uma queda de energia. |
| 02. Falha climatização da sala cofre | Superaquecimento dos ativos devido a falha no dimensionamento de carga na sala cofre. |
| 03. Indisponibilidade de rede/circuitos | Rompimento de fibra ótica decorrente de execução de obras públicas, desastres ou acidentes. |
| 04. Falha humana | Acidente ao manusear equipamentos, ou abastecimento do tanque de combustível. |

| | |
|---|---|
| 05. Ataques internos (funcionários insatisfeitos) | Ataque aos ativos do Data Center. |
| 06. Incêndio | Incêndios que comprometam os serviços de TIC |
| 07. Desastres naturais | Terremotos, tempestades, alagamentos etc. |
| 08. Falha de hardware | Falha que necessite reposição de peça ou reparo cujo reparo ou aquisição dependa de processo licitatório. |
| 09. Ataque cibernético | Ataque virtual que comprometa o desempenho, os dados ou configuração dos serviços essenciais. |

## 8. Papéis e Responsabilidades

| 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.<br>. 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 localização primária sofra da destruição ou danos.<br>. O líder desta equipe administrará e manterá o Plano de Recuperação de Desastre. | Coordenador da CPROD/Analista de Datacenter | 3372-1519 / 3372-1524 | cprod@tjba.jus.br | CPROD |
| Equipe de Redes | . Avaliar os danos específicos de qualquer infra-estrutura 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.<br>. 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.<br>. O líder desta equipe administrará e manterá o Plano de Administração de Crise. | DIN | (71) 33721555 | din@tjba.jus.br | DIN |
| 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)33721504 | 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)33721504 | cotec@tjba.jus.br | COTEC |

## 9. Invocação do Plano

O PCTIC 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<br>Secretaria: 3372-166 | Sala 103 Do Anexo |
| Corregedoria | 3372-5094 | Sala 312 Do Anexo |
| 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 |

Considerações:

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

## 10. Macroprocessos do PCTIC

O PCTIC tem seus macroprocessos definidos nas atividades a seguir e se desmembra em planos específicos para cada área de atuação quando da ocorrência de um desastre.

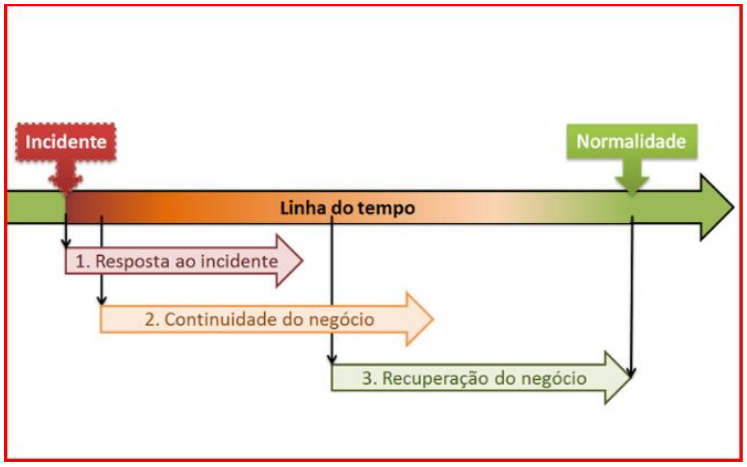


*Figura 3- Figura 1- Representação do Ciclo de GNC após ocorrência de um incidente.*

No ambiente do TJBA, foram definidos os seguintes processos:

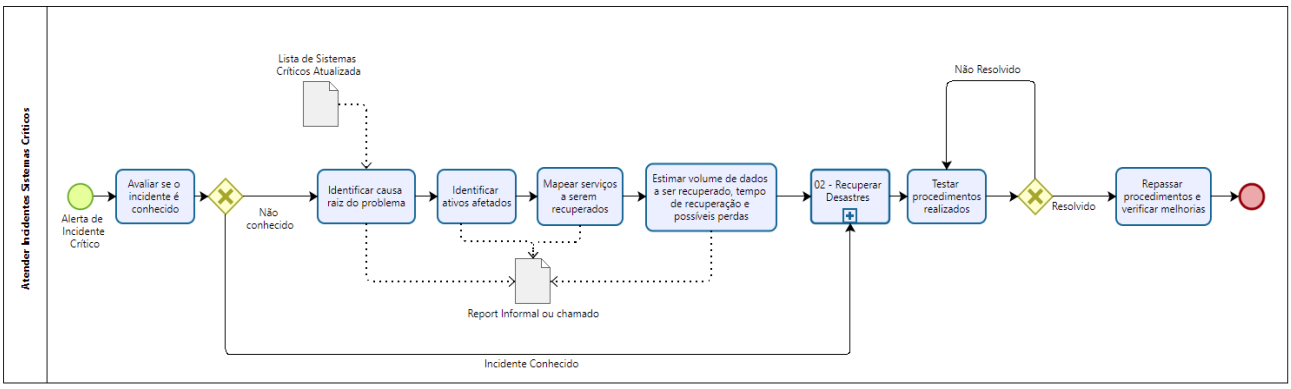


*Figura 4 - Processo de Atendimento à Sistemas Críticos*

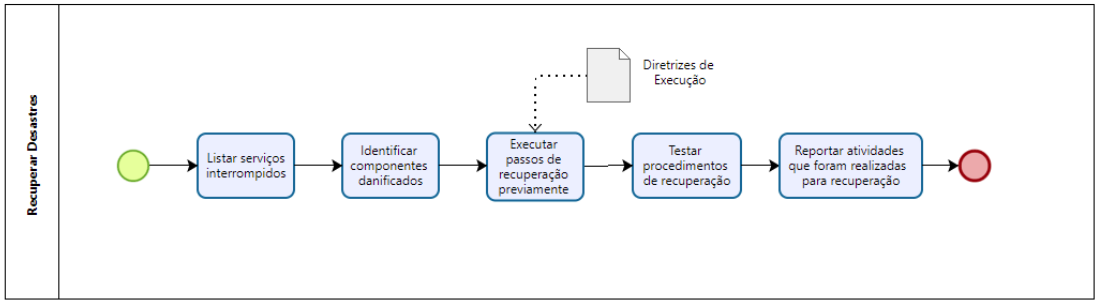


*Figura 5 - Processo de Recuperação de Desastres*

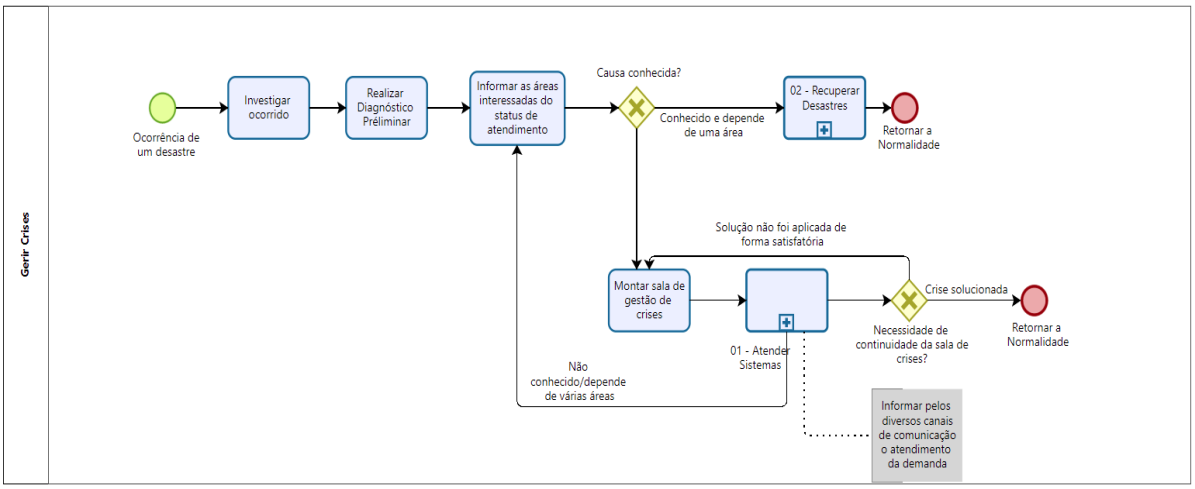


*Figura 6 - Processo de Gestão de Crises*

Os sub planos do PCTIC consistem em:

- Plano de Continuidade Operacional (PCO):
    - Garantir a continuidade dos serviços essenciais de TI críticos na ocorrência de um desastre, enquanto recupera-se o ambiente principal.

- Plano de Administração de Crise (PAC):
    - Definir atividade das equipes envolvidas e orquestrar as ações de contingência e comunicação durante e após a ocorrência de um desastre, com intuito de minimizar impactos até a superação da crise, ou seja, dar continuidade ao negócio, independente do impacto causado pelo dano.

- Plano de Recuperação de Desastre (PRD):
    - Planejar e agir para que, uma vez controlada a contingência e passada a crise, a TI do TJBA retome seus níveis originais de operação no ambiente principal.

## 11. Estratégias de continuidade

No cenário atual da TI existem duas estratégias de continuidade para os serviços essenciais judiciais, Cold Backup e Warm Site. A estratégia de warm site está sendo montada em fases sendo que a primeira aplicação essencial que está sendo migrada para a estratégia Warm Site é o PJE.

**Tipo:** Cold Backup

**Descrição:**

- Cópias de backup dos sistemas essenciais armazenadas em local alternativo: Fórum Criminal Sussuarana.
- Não possui qualquer tipo de hardware configurado no local.
- Não dispõe de conexão redundante
- Downtime médio-alto.

**Ações de contingência/recuperação:**

Mapear perda de dados e ativos, reestabelecer toda a estrutura afetada e, após o ambiente principal estar operacional, prover a recuperação dos dados em backups.

**Observações:**

As ações de contingência e recuperação são detalhadas nos sub planos a seguir.

**Tipo:** Warm Site

**Descrição:**

- Contratação de ambientes em cloud publica para funcionarem como Warm site.
- Atualmente estão sendo utilizados os provedores Amazon Web Services e Google Cloud para montagem da estratégia Warm Site, via adesão de ATA do Ministério da Economia.

- Replicação de dados (bancos de dados, arquivos, imagens de software e códigos fonte) em 'near real time' para os ambientes cloud. (fase 1)
- Montagem de imagens base (gold images) de servidores de aplicação, das aplicações essenciais (fase2)
- Montagem de imagens base (gold images) de servidores de aplicação das aplicações satélites para todas as aplicações essenciais. (fase3)
- Criação de processos de auto scaling para ativação dos ambientes quando da falha do ambiente de produção.
- Contratado link dedicado com a AWS e criadas VPNs com AWS e GCP
- Downtime: médio.

**Ações de contingência/recuperação:**

Mapear os sistemas afetados, validar fase do projeto de implantação em que se encontra os ambientes. Mapear ações necessárias a depender da fase de implantação do Warm Site. Reestabelecer toda a estrutura afetada e, após o ambiente principal estar operacional, prover a replicação reversa dos dados da nuvem para o ambiente on-premisses.

**Observações:**

As ações de contingência e recuperação são detalhadas nos sub planos a seguir.

## 12. Validação e teste de PCTIC

O PCTIC será testado e validado em reunião entre os líderes anualmente, com revisão a cada dois anos, 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.

**Tipos de testes a serem realizados:**

. 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.

**Status:**

. Programado
. Executado
. Planejado
. Agendado

| Data | Tipo | Motivo | Status |
|---|---|---|---|
| xx/xx/2022 | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

## 13. Aprovação do PCTIC

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**

**Assessoria de Segurança da Informação**

# PCO

## Plano de Continuidade Operacional

## 1. Plano de Continuidade Operacional - PCO

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

## 2. Objetivo e Escopo

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

São objetivos do PCO:

**a.** Prover meios para manter o funcionamento dos principais serviços de TI e a continuidade das operações de TI, dos sistemas essenciais.

**b.** Estabelecer procedimentos, controles e regras alternativas que possibilitem a continuidade das operações de TI durante uma crise ou cenário de desastre.

**c.** Estabelecer uma equipe para cada plano PCO, PRD e PAC.

**d.** Definir os formulários, checklists e relatórios a serem entregues pelas equipes ao executar a contingência.

## 3. Equipes 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

## 4. Gestão

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

## 5. Execução do Plano

### a. 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.

### b. 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 | | | ☐ |

**c. Contingência de 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 | | | ☐ |

## 6. Encerramento do PCO

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

Informar à Equipe de Comunicação o retorno das atividades.

# PAC

Plano de Administração de Crises

## 1. Plano de Administração de Crises - PAC

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

## 2. Objetivo

O objetivo deste plano é garantir a comunicação, gerenciar as crises e viabilizar uma compreensão linear a todos os envolvidos das ações antes, durante e após a ocorrência de uma catástrofe.
São objetivos específicos do PAC:

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

## 3. Execução do Plano

As figuras abaixo representam respectivamente, o diagrama de atividades a serem desempenhadas na execução do Plano de Administração de Crises PAC e as Comunicações necessárias a serem realizadas em caso de desastre.

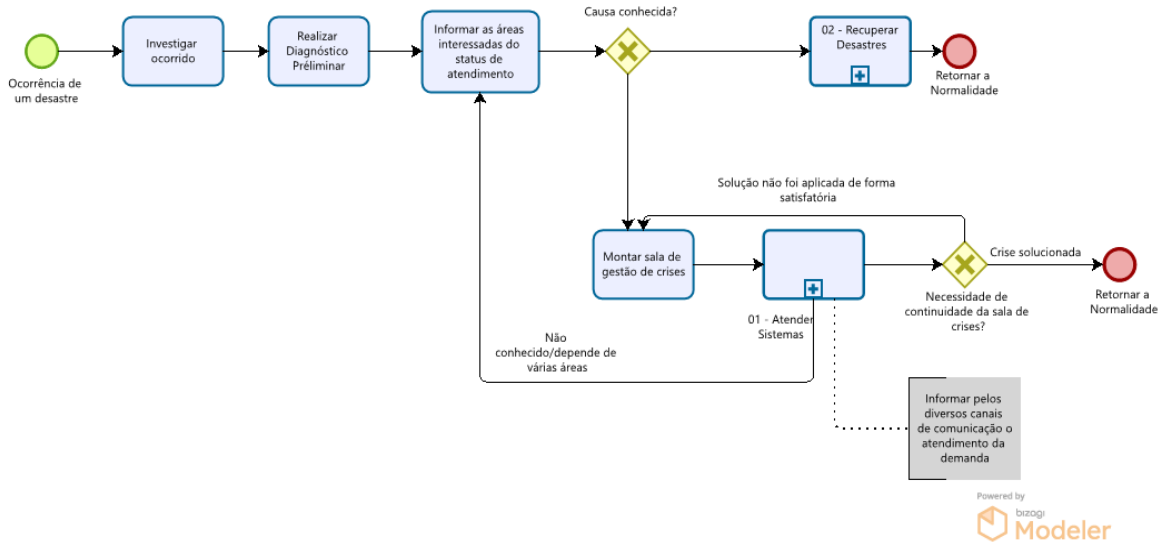


*Figura 7 - Processo 01 - Atender Sistemas Críticos*

Após ocorrência de um desastre se faz necessário a investigação do ocorrido e a realização de um diagnostico preliminar, após realizado essas atividades deverá ser repassadas as informações do andamento dos atendimentos e a avaliação de necessidade de criação de uma sala de gestão de crises, garantindo melhor agilidade, resposta e recuperação do desastre até a retomada a normalidade das operações.

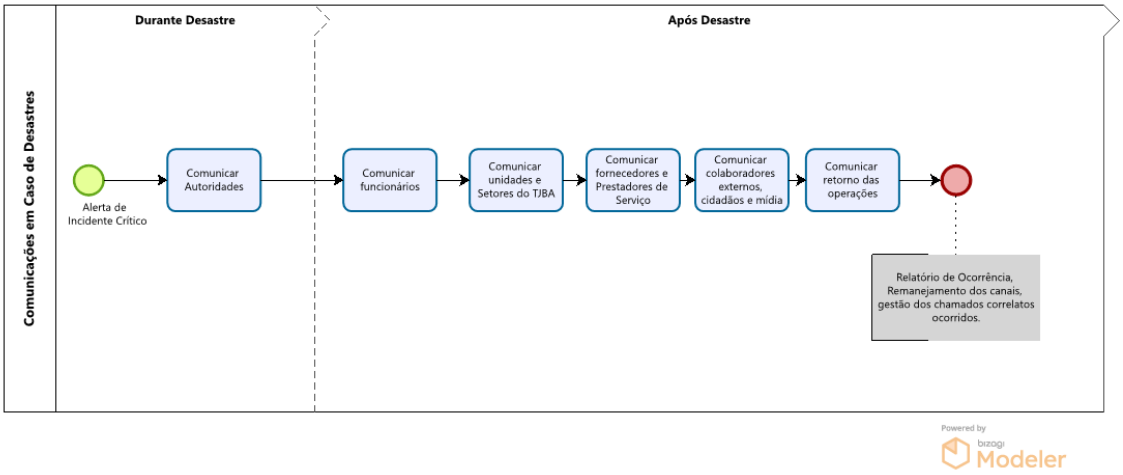


*Figura 8 - Processo de comunicação em caso de desastres*

**a. Comunicação na ocorrência de um Desastre**

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

A comunicação com cada parte ocorrerá da seguinte forma:

**a.1 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 | _____/____/____ ____:____ | |

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

**b. 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.

**b.1 Comunicação com os funcionários**

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

**b.2 Comunicar unidades e setores do TJBA**

- Acionar diretamente as unidades afetadas pelo desastre e fornecer contato
- Natureza, impacto e abrangência da catástrofe
- Ações de contingência em andamento
- Processos/sistemas e serviços cobertos pelo plano de continuidade (serviços essenciais)

| Setor/ Unidade | Número/contato | Data/Hora do contato | Local |
|---|---|---|---|

| | | | |
|---|---|---|---|
| DRH | Gabinete: 3372-1649<br>Secretaria: 3372-166 | _____/____/____<br>____:____ | Sala 103 do Anexo |
| Corregedoria | 3372-5094 | _____/____/____<br>____:____ | Sala 312 do Anexo |
| Assessoria da Presidência AEP II | 3372-5077 | _____/____/____<br>____:____ | Sala 303-S do Tribunal de Justiça |
| Secretaria de TIC | 3372-5077/ 5123 | _____/____/____<br>____:____ | Sala 303-N do Tribunal de Justiça |
| ASCOM | Recepção: 3483-3731 | _____/____/____<br>____:____ | Sala 312 - Edifício Advogado Pedro Milton de Brito – Anexo II |
| Secretaria de Administração | 3372-5123 | _____/____/____<br>____:____ | Sala 309/311-N do Tribunal de Justiça |
| Balcões de Justiça | 3372-5077/ 5659 | _____/____/____<br>____:____ | Sala 303-S do Tribunal de Justiça |

### b.3 Comunicar fornecedores e Prestadores de serviço

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

| | |
|---|---|
| **Empresa:** OI<br>**Contato:** | **Pessoa/Contato:** _____<br>**Data/Hora Acionamento:**<br>_____/_____/_____ ____:____:____ |
| **Empresa:** CEMIG<br>**Contato:** | **Pessoa/Contato:** _____<br>**Data/Hora Acionamento:**<br>_____/_____/_____ ____:____:____ |
| **Empresa:** PRODEB<br>**Contato:** | **Pessoa/Contato:** _____<br>**Data/Hora Acionamento:**<br>_____/_____/_____ ____:____:____ |

### b.4 Colaboradores externos, cidadãos e mídia

A equipe de comunicação, em consonância com a Assessoria de Comunicação do TJBA, deverá fornecer informações pertinentes aos colaboradores externos: Advogados, cidadãos e outros órgãos.

- Validar a situação passada de acordo com o cenário
- Buscar publicar em meios oficiais e de ampla divulgação, com aval do comitê de continuidade e institucional, informações sobre o ocorrido.

| NOME DA EMPRESA | RESPONSÁVEL | TELEFONE | Objeto do Contrato | PAPEL | Coordenação |
|---|---|---|---|---|---|
| Solutis | Geisa Correia | (71) 98732-4130 | Desenvolvimento de Sistemas | Preposta | COSIS/CSJUD |
| Qintess | Débora Freitas | (71) 99147-2657 | Suporte Especializado em Sistemas | Preposta | COSIS/CSJUD |
| Aceco TI LTDA. | Danilo Nogueira Rocha | (71) 99939-6728 | Sala Cofre | Preposta | CPROD |

| | | | | | |
|---|---|---|---|---|---|
| Unentel Soluções Tecnológicas LTDA. | Marcelo Simões / Claudio / Joeva | (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. | Cléber Bramante/Leonardo Bernardino/Divaldo | (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 | Patrícia Leite | (71)98366-2213 | Suporte a usuários nos níveis 1 e 2. | Preposta | COATE |
| OI S.A | Andrea Menezes/ Fernanda Mota | (71)98807-2855 / (71)98845-0115 | Circuitos de comunicação de dados (links) | Preposta | CPROD |
| EDS | Rodrigo Leite | +55 (81) 99345-3808 | Ambientes Cloud | Preposto | COTEC |
| Hepta | Hugo Dias | (021 71) 98857-9768 | Suporte ambiente infra N3 | Preposto | COTEC |

**c. Comunicar retorno das operações**

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

## 4. Encerramento do PAC

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

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

# PRD

Plano de Recuperação de Desastres

## 1. Plano De Recuperação de Desastres - PRD

Este plano descreve os cenários de inoperância e seus respectivos procedimentos planejados, definindo as atividades prioritárias para reestabelecer o nível de operação dos serviços no ambiente afetado dentro de um prazo tolerável.

## 2. Objetivo e Escopo

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

São objetivos PRD:

**a.** Avaliar danos aos ativos e conexões do datacenter e prover meios para sua recuperação.

**b.** Evitar desdobramentos de outros incidentes na facilidade principal.

**c.** Reestabelecer o datacenter dentro do prazo tolerável

## 3. Execução do Plano

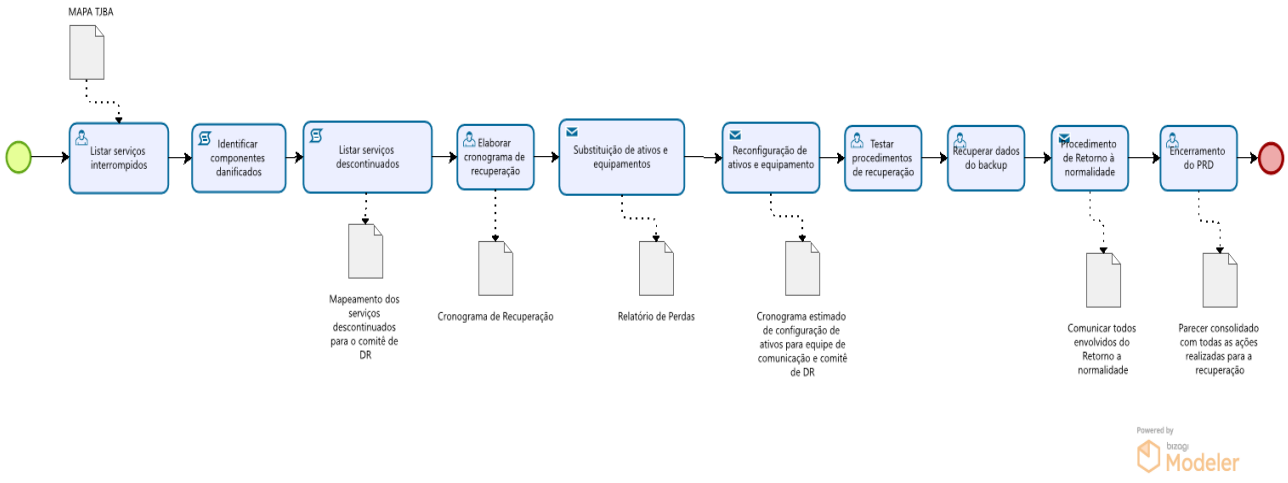


*Figura 9 - Processo 02 - Recuperar Desastres*

### a. Listar Serviços Interrompidos

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.

**b. Identificar componentes danificados**

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.

**c. Listar serviços descontinuados**

A equipe do PRD deverá mapear quais serviços foram descontinuados contendo as informações de perda de ativo e de conexão com intuito de levar ao conhecimento do Comitê de DR. O relatório deverá abranger todos os componentes necessários à plena operação da aplicação como servidores, máquinas virtuais, banco de dados, firewall, storage, routers e switches, bem como respectivas configurações de proxy, DNS, rotas, V etc.

**d. Elaborar cronograma de recuperação**

O líder do PRD após o mapeamento das perdas e impactos elaborará um breve cronograma de recuperação das aplicações levando em consideração:

- A priorização dos serviços essenciais, ou de acordo com determinação de nível institucional.
- O RTO definido para cada serviço essencial.
- A força de trabalho disponível.

**d.1. Substituição de ativos e equipamentos**

Em caso de perda de ativos, deverá ser imediatamente informado ao comitê de DR a necessidade de aquisição de ativos perdidos que não puderem ser recuperados. A equipe irá mensurar quanto tempo a aquisição irá impactar o RTO de cada serviço comunicando ao 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 [b.3].

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

**d.2. Reconfiguração de ativos e equipamentos**

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.

### d.3. Testar procedimentos de recuperação

Os testes têm por objetivo assegurar a eficiência e a efetividade do PCN 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. | | | | ☐ |

**d.4. Recuperar dados do backup**

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

## 4. Procedimento de Retorno à normalidade

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

## 5. Encerramento do PRD

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