PODER JUDICIÁRIO DO ESTADO DO ACRE TRIBUNAL DE JUSTIÇA

Maio de 2024

**PLANO DE CONTINUIDADE DE SERVIÇOS ESSENCIAIS DE TIC**

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

PRESIDENTE

Desembargadora Regina Ferrari

VICE-PRESIDENTE

Desembargador Luís Camolez

CORREGEDOR GERAL DE JUSTIÇA

Desembargador Elson Mendes

COMITÊ GESTOR DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO RESOLUÇÃO Nº 291/2023

**Histórico de Alterações**

|  |  |  |  |
| --- | --- | --- | --- |
| **Data** | **Versão** | **Descrição** | **Responsáveis** |
| 01.03.2024 | 1 | Criação da 1ª versão PCTIC | Raquel Cunha da Conceição |
| 01.03.2024 | 1 | Criação da 1ª versão PCTIC | Elson Correia de Oliveira Neto |
| 01.03.2024 | 1 | Elaboração da 1ª versão PCTIC | Elinara Bras FerreiraElson Correia de Oliveira Neto |
| 01.03.2024 | 1 | Revisão da 1ª versão PCTIC | Ronimar Ferreira de MatosLucas Bezerra Felix |
| 01.03.2024 | 1 | Aprovação da 1ª versão PCTIC | CGESTCGTICCOCRI |
| 27.05.2024 | 2 | Revisão para publicação no portal G2TIC | GESEGAssessoria de Governança |

SUMÁRIO

[1. INTRODUÇÃO 5](#_Toc167711276)

[2. OBJETIVO 5](#_Toc167711277)

[3. JUSTIFICATIVA / MOTIVAÇÃO 5](#_Toc167711278)

[4. ESCOPO 6](#_Toc167711279)

[5. CONCEITOS E DEFINIÇÕES 6](#_Toc167711280)

[6. PROBABILIDADE 8](#_Toc167711281)

[7. SERVIÇOS ESSENCIAIS DO TJAC 8](#_Toc167711282)

[7.1. SERVIÇOS ESSENCIAIS DE INFRAESTRUTURA 10](#_Toc167711283)

[7.2. SERVIÇOS ESSENCIAIS DE SEGURANÇA DA INFORMAÇÃO 10](#_Toc167711284)

[8. PAPÉIS E RESPONSABILIDADES 11](#_Toc167711285)

[9. FLUXOGRAMA DE GERENCIAMENTO DE DESASTRES 12](#_Toc167711286)

[10. PLANO DE CONTINUIDADE 13](#_Toc167711287)

[10.1. PAC – Programa de Administração de Crise 13](#_Toc167711288)

[10.2. PCO - Plano de Continuidade Operacional 15](#_Toc167711289)

[10.3. PRD – Plano de Recuperação de Desastres 17](#_Toc167711290)

[11. MATRIZ DE TESTES 19](#_Toc167711291)

[12. CONCLUSÃO 20](#_Toc167711292)

**APRESENTAÇÃO**

O presente documento tem por objeto apresentar o Plano de Continuidade de Serviços da Diretoria de Tecnologia da Informação (DITEC) do Tribunal de Justiça do Estado do Acre.

A elaboração desse Plano é uma iniciativa para atendimento a Resolução 370/2021 do CNJ, SEÇÃO III - Art 36, que estabelece o Plano de Continuidade de Negócios ou Serviços Essenciais de TIC.

# ****INTRODUÇÃO****

Este Plano de Continuidade de Negócios, de Tecnologia da Informação (TI), consiste em estabelecer as estratégias e procedimentos de caráter preventivo e de recuperação para garantir a execução das atividades do Poder Judiciário, que utilizam recursos tecnológicos, com o objetivo de minimizar as interrupções.

# ****OBJETIVO****

O Plano de Continuidade de TIC, abrange as estratégias necessárias à continuidade dos serviços de TIC essenciais: contingência, continuidade e recuperação. Está voltado a conceder continuidade aos processos definidos como críticos para a TI e serviços essenciais judiciais, de acordo com a Resolução nº 370, de 28 de janeiro de 2021, na qual estabelece a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD), em seu Art. 36, *in verbis:* “Cada órgão deverá elaborar Plano de Gestão de Continuidade de Negócios ou de Serviços no qual estabeleça estratégias e planos de ação que garantam o funcionamento dos serviços essenciais quando na ocorrência de falhas. ”

Ademais, busca alinhar-se à Política de Segurança Cibernética do Poder Judiciário, contida na Resolução 396/2021, em seu Art. 25, *in verbi*s: “São instrumentos da PSEC-PJ:

I – a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ);

II – o Protocolo de Prevenção de Incidentes Cibernéticos no âmbito do Poder Judiciário (PPINC-PJ);

 III – o Protocolo de Gerenciamento de Crises Cibernéticas no âmbito do Poder Judiciário (PGCC-PJ);”

# ****JUSTIFICATIVA / MOTIVAÇÃO****

As situações improváveis devem ser interpretadas como uma possibilidade, e a partir desta premissa, os preparativos para recuperação devem estar definidos, mesmo com aceitação de alguma degradação com o intuito de manter a continuidade das atividades em modo de contingência até que seja possível a recuperação total. Neste sentido, este documento contém os procedimentos a serem adotados pelas equipes Técnica e Administrativa desta DITEC, para assegurar a continuidade de negócios/serviços, a recuperação e resposta adequada aos incidentes.

#

# ****ESCOPO****

Este plano tem como objetivo a continuidade de negócios específicos da área de TI com foco na estrutura da rede de comunicação de dados e todos os ativos que disponibilizam os serviços de TI localizados na estrutura tanto na sede do Tribunal de Justiça, bem como, nas comarcas dos interiores.

# ****CONCEITOS E DEFINIÇÕES****

|  |  |
| --- | --- |
| **TERMO** | **CONCEITO OU DEFINIÇÃO** |
| atividade | Processo ou conjunto de processos executados pelo TJAC, que produzam ou suportem um ou mais produtos ou serviços. |
| atividade crítica | Atividade que deve ser executada de forma a garantir a consecução dos produtos e serviços fundamentais do TJAC, de tal forma que permita atingir os seus objetivos mais importantes e sensíveis ao tempo. |
| ativos de informação | Meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso. |
| continuidade dos serviços essenciais | Conjunto de práticas, procedimentos, processos, planos e ferramentas de trabalho que maximizam a possibilidade de que o órgão, dispondo de um sistema de gestão de continuidade documentado, mantenha o fornecimento dos serviços essenciais de TIC após a ocorrência de determinados cenários de desastre. |
| desastre | Evento repentino e não planejado que causa perda para todo ou parte do TJAC e gera sérios impactos em sua capacidade de entregar os serviços essenciais ou críticos por um período de tempo superior ao tempo objetivo de recuperação |
| gestão de continuidade | Processo abrangente de gestão que identifica ameaças potenciais para uma organização e os possíveis impactos nas operações de negócio, caso elas se concretizem. Este processo fornece uma estrutura para que se desenvolva uma resiliência organizacional que seja capaz de responder efetivamente e salvaguardar os interesses das partes interessadas, a reputação e a imagem do Tribunal e suas atividades de valor agregado. |
| Incidente | Qualquer evento suficientemente significante, que possa causar a interrupção do negócio |
| interrupção | Evento, previsível ou não, que cause um desvio negativo na entrega de produtos ou execução de serviços, de acordo com os objetivos do TJAC |
| Plano de Continuidade Operacional (PCO) | Documentação dos procedimentos e informações necessárias para que o Tribunal mantenha seus ativos de informação críticos e a continuidade de suas atividades críticas em um nível previamente definido, em casos de desastres |
| Programa de Administração de Crise (PAC) | Plano de ação claramente definido e documentado, para ser usado quando ocorrer um incidente que basicamente cubra as principais pessoas, recursos, serviços e outras ações que sejam necessárias para implementar o processo de gerenciamento de incidentes de TIC |
| Plano de Recuperação de Serviços de TIC - PRD | Documentação dos procedimentos e informações necessárias para que o órgão operacionalize o retorno das atividades críticas de TIC à normalidade |
| responsável pelo ativo | Indivíduo legalmente instituído por sua posição e/ou cargo, responsável primário pela viabilidade e sobrevivência dos ativos de informação |
| RTO | Recovery Time Objective: Tempo estabelecido para que um sistema seja recuperado de uma solução de continuidade |
| RPO | Recovery Point Objective: Compreende o ponto de recuperação dos dados, ou seja, uma vez recuperada a solução, qual a quantidade de dados máxima que poderá ser perdida sem que o negócio seja afetado. |
| serviços essenciais | Conjunto de ativos de informação que, por meio de integração e orquestração, entrega valor aos usuários e ao órgão, mediante recursos de TIC empregados. Os serviços essenciais estão divididos em negócio (área fim), infraestrutura e segurança da informação, (área de TIC e engenharia) |
| sistemas essenciais | Sistemas de informação do TJAC definidos como estratégicos e com alto impacto no negócio em caso de indisponibilidade. |
| criticidade | Representa o quão drástica é uma situação para o negócio do TJAC |
| impacto | Desconformidade causada por um incidente ou desastre |
| ameaça | Qualquer evento que explore vulnerabilidades ou causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização |
| solução de continuidade | Interrupção de um serviço por falha em algum de seus componentes |
| CGESTI | Comitê Gestor de Tecnologia da Informação e Comunicação |
| CGTIC | Comitê de Governança de Tecnologia da Informação e Comunicação |
| COCRI | Comitê de Crises Cibernéticas |

# ****PROBABILIDADE****

A tabela abaixo utiliza uma escala de três pontos para definir a intensidade percebida por indivíduos envolvidos no processo e no item em questão. É importante observar que essa escala reflete a percepção dos envolvidos e, portanto, é subjetiva até certo ponto.

Dependendo do contexto analisado, os valores podem indicar uma percepção positiva, neutra ou negativa. Em situações que envolvem análise qualitativa, esses valores podem representar diferentes graus de intensidade na percepção. Por outro lado, em análises quantitativas, esses valores podem ser interpretados como probabilidades.

|  |  |
| --- | --- |
| **GRANDEZA** | **CONCEITO OU DEFINIÇÃO** |
| Alto | Representa uma grandeza muito significativa no contexto analisado, de forma a se sobressair sobre demais pontos considerados no cenário analisado. |
| Médio | Representa uma grandeza ainda significativa, embora não seja tão intensa. É, contudo, ainda bastante relevante no contexto analisado. |
| Baixo | Representa uma grandeza de pouco significado que, no entanto, ainda acarreta consequências perceptíveis no cenário analisado, embora seja de menor impacto. |

# ****SERVIÇOS ESSENCIAIS DO TJAC****

As tabelas abaixo mostram os serviços considerados essenciais no Tribunal de Justiça do Acre (TJAC), os quais estão divididos em Serviços Principais, Infraestrutura e Segurança da Informação, todos cruciais à administração. As tabelas fornecem detalhes sobre a criticidade, impacto e as expectativas de RPO (Recovery Point Objective) e RTO (Recovery Time Objective).

|  |  |  |
| --- | --- | --- |
| **SERVIÇO** | **CRITICIDADE** | **IMPACTO** |
| **FINANCEIRO** | **LEGAL** | **IMAGEM** | **OPERACIONAL** |
| Sistema SAJ | alta | baixo | alto | alto | alto |
| Sistema SEI | alta | médio | médio | médio | alto |
| Base de Usuários | alta | alto | alto | alto | alto |
| Sistema de RH | alta | médio | médio | médio | alto |
| Servidor de Arquivos | média | baixo | Médio | médio | alto |
| E-mail Corporativo | alta | baixo | Médio | alto | alto |
| Intranet | alta | baixo | Médio | médio | alto |
| Malote Digital | alta | baixo | Médio | médio | alto |
| Diário da Justiça Estadual | alta | baixo | Médio | alto | médio |
| Infraestrutura do Interior | alta | baixo | alto | médio | médio |
| Sistema Extrajud | alta | alto | alto | alto | alto |
| Sigma | média | baixo | baixo | baixo | alto |
| Sistema de portaria | média | baixo | baixo | baixo | médio |
| Sistema CPTEC | baixa | baixo | baixo | baixo | baixo |
| Sistema CODEX | baixa | baixo | Médio | médio | médio |
| Sistema SPROL | baixa | baixo | Médio | alto | médio |
| Sistema SIGEN | baixa | baixo | Médio | médio | médio |
| Sistema SIMAV | baixa | baixo | Baixo | médio | médio |

### **7.1. SERVIÇOS ESSENCIAIS DE INFRAESTRUTURA**

|  |  |  |
| --- | --- | --- |
| **SERVIÇO** | **CRITICIDADE** | **IMPACTO** |
| **FINANCEIRO** | **LEGAL** | **IMAGEM** | **OPERACIONAL** |
| Ambiente Container | alta | baixo | baixo | alto | alto |
| Servidor de Aplicação | alta | baixo | baixo | alto | alto |
| Serviços de Rede  | alta | baixo | baixo | alto | alto |
| Serviços de Storage | alta | baixo | baixo | alto | alto |
| Serviços de Computadores/Servidores | alta | baixo | baixo | alto | alto |
| Serviços de Monitoramento | alta | baixo | baixo | alto | alto |
| Datacenter | alta | baixo | baixo | alto | alto |
| Comunicação de Dados | alta | baixo | baixo | alto | alto |

### **7.2. SERVIÇOS ESSENCIAIS DE SEGURANÇA DA INFORMAÇÃO**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **SERVIÇO** | **CRITICIDADE** | **IMPACTO FINANCEIRO** | **IMPACTO LEGAL** | **IMPACTO IMAGEM** | **IMPACTO OPERACIONAL** |
| Firewall | alta | baixo | médio | alto | alto |
| Segurança de Endpoint | alta | baixo | médio | alto | alto |

# ****PAPÉIS E RESPONSABILIDADES****

|  |  |
| --- | --- |
| **EQUIPE** | **RESPONSABILIDADE** |
| Comitê de Crises Cibernéticas - COCRI | 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. Incluir autoridades em nível institucional e tomadores de decisão da DITEC - Diretoria de Tecnologia da Informação e ComunicaçãoResponsável 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.O líder desta equipe administrará e manterá o Plano de Administração de Crise. |
| Gerência de Segurança da Informação | O líder desta equipe administrará e manterá o Plano de Recuperação de Desastre |
| Gerência de Segurança da Informação (Infraestrutura, aplicações, backup) | Responsável pelas instalações físicas que abrigam sistemas de TIC e pela garantia que as instalações de alternativa são mantidas adequadamente.Avalia os danos e supervisiona os reparos.Fornecer infraestrutura de servidor físico e virtuais necessária para que a TI execute suas operações e processos essenciais durante um desastre.Garantir que as aplicações essenciais funcionem como exigido para atender aos objetivos de negócios em caso de e durante um desastre.Eles serão os principais responsáveis por assegurar e validar o desempenho das aplicações essenciais e podem ajudar outras equipes de TIC conforme necessário.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.O líder desta equipe irá liderar os PCO relacionados a estes itens. |
| Gerência de Segurança da Informação (Banco de Dados) | Responsável pelas configurações e manutenções dos ambientes de bancos de dados, incluindo execução e recuperação dos backups.> O líder desta equipe irá liderar os PCO relacionados exclusivamente a bancos de dados. |
| Gerência de Segurança da Informação (Serviço de Infraestrutura de Redes) | Avaliar os danos específicos de qualquer infraestrutura de rede e para fornecer dados e conectividade de rede, incluindo WAN, LAN ou de infraestrutura externa junto aos prestadores de serviço.> O líder desta equipe irá liderar os PCO relacionados exclusivamente à comunicação de dados. |
| Gerência de Segurança da Informação (Segurança da Informação) | Responsável por ativos que provêm o controle de acesso a sistemas e a comunicação de dados.> O líder desta equipe irá liderar os PCO relacionados exclusivamente à segurança da informação |

# ****FLUXOGRAMA DE GERENCIAMENTO DE DESASTRES****

****

# ****PLANO DE CONTINUIDADE****

### **10.1. PAC – Programa de Administração de Crise**

|  |  |  |
| --- | --- | --- |
| **Versão** | **Descrição** | **Responsáveis** |
| 1 | Criação da 1ª versão PCTIC | Raquel Cunha da Conceição |
|  | Criação da 1ª versão PCTIC | Elson Correia de Oliveira Neto |
|  |  | **Elaboração** |
|  | Criação da 1ª versão PCTIC | Elinara Bras Ferreira |
|  | Criação da 1ª versão PCTIC | Elson Correia de Oliveira Neto |
|  |  | **Revisão** |
|  | Revisão da 1ª versão PCTIC | Ronimar Ferreira de Matos |
|  | Revisão da 1ª versão PCTIC | Lucas Bezerra Felix |
|  | Aprovação da 1ª versão PCTIC | **Aprovação** |
|  |  | CGEST |
|  |  | CGTIC |
|  |  | COCRI |

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

**OBJETIVOS**

Minimizar os efeitos adversos de uma crise de TIC, tanto em termos financeiros quanto de reputação da organização.

Restaurar os sistemas e serviços afetados o mais rápido possível para minimizar interrupções nos negócios e recuperar a funcionalidade normal da infraestrutura de TI.

Informar a sociedade em tempo e com esclarecimentos condizentes com o ocorrido.

**ESCOPO**

Administração e gerenciamento de impactos causados por alguns desastres que venham a ocorrer.

**GESTÃO**

A gestão de crises é estruturada em três níveis de atuação: Estratégico, Tático e Operacional.

**Nível Estratégico:** É formado pelo Comitê Gestor de Tecnologia da Informação e Comunicação - CGEST. Neste nível são deliberadas as decisões estratégicas do negócio, as respostas aos incidentes de impactos críticos, a comunicação às alçadas superiores da organização;

**Nível Tático:** É formado pelos líderes das equipes, que atuam inicialmente na avaliação e resolução do incidente, que dependendo do tipo, podem convocar outras pessoas para identificação e tratamento do incidente. O nível tático tem autonomia de convocar o CGEST, quando entender que o incidente tratado atinja o cenário de crise;

**Nível Operacional:** É formado pelos analistas e especialistas do departamento. Entram em ação quando a execução do plano é ativada, reporta o status da resolução do incidente para o nível tático;

**EXECUÇÃO**

Em situações de emergência, sejam elas ocasionadas por eventos naturais ou não, é fundamental ativar este plano. A equipe de comunicação será encarregada de classificar o incidente e transmitir a informação à equipe responsável. No caso de falhas no sistema, a equipe técnica será mobilizada.

Em incidentes naturais, é crucial estabelecer comunicação com diversas áreas, especialmente aquelas diretamente impactadas, para notificá-las sobre as consequências na continuidade dos serviços e estimar o tempo necessário para a recuperação.

A equipe de comunicação assumirá a responsabilidade de contatar essas unidades afetadas e fornecer informações pertinentes a cada grupo, setor ou segmento impactado.

As unidades serão contatadas obedecendo a seguinte a classificação:

Comunicação às autoridades responsáveis, (SAMU, BOMBEIRO, POLÍCIA), caso este se trate de catástrofe, principalmente se envolver risco às pessoas, fornecendo as seguintes informações de localização, natureza, magnitude e impacto do desastre;

Comunicação as todos os envolvidos na Administração, desde os afetados aos que irão solucionar o incidente ocorrido, para que este tome ciência do que veio a afetar e ocasionar a inatividade de determinado serviço ou local;

E por fim, após o retorno das operações/serviços/locais, se faz necessário uma nova comunicação para avisar as partes acima da recuperação do desastre ocorrido.

**ENCERRAMENTO DO PAC**

Após o repasse do retorno dos serviços, ainda é necessário, compor relatório com relação das atividades executadas após a ocorrência dos desastres identificados, atualizando se necessário canais de informação, fazendo abertura, acompanhamento ou encerramento de chamados correlatos ao ocorrido.

### **10.2. PCO - Plano de Continuidade Operacional**

|  |  |  |
| --- | --- | --- |
| **Versão** | **Descrição** | **Responsáveis** |
| 1 | Criação da 1ª versão PCTIC | Raquel Cunha da Conceição |
|  | Criação da 1ª versão PCTIC | Elson Correia de Oliveira Neto |
|  |  | **Elaboração** |
|  | Criação da 1ª versão PCTIC | Elinara Bras Ferreira |
|  | Criação da 1ª versão PCTIC | Elson Correia de Oliveira Neto |
|  |  | **Revisão** |
|  | Revisão da 1ª versão PCTIC | Ronimar Ferreira de Matos |
|  | Revisão da 1ª versão PCTIC | Lucas Bezerra Felix |
|  | Aprovação da 1ª versão PCTIC | **Aprovação** |
|  |  | CGEST |
|  |  | CGTIC |
|  |  | COCRI |

O Plano de Continuidade Operacional - PCO, descreve os procedimentos de contingência em uma situação de falha ou interrupção nos ativos que sustentam esses processos em andamento na Administração

**OBJETIVOS**

Garantir a segurança da informação e dos dados críticos durante eventos de crise ou desastres, prevenindo perdas ou vazamentos de informações sensíveis.

Minimizar o impacto de interrupções nos serviços de TI sobre os usuários e partes interessadas, mantendo um nível aceitável de serviço mesmo em situações adversas.

Identificar e priorizar os processos de negócio e os sistemas de TI críticos para a continuidade das operações, a fim de direcionar os esforços de recuperação e manutenção.

Assegurar a prontidão das equipes de resposta a incidentes e de recuperação de desastres, por meio de treinamentos regulares e simulações de cenários de crise.

Estabelecer métricas e indicadores de desempenho para avaliar a eficácia do plano de continuidade operacional de TI e promover melhorias contínuas.

**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.

**GESTÃO**

Ficará sob responsabilidade da Gerência de Segurança da Informação, juntamente com o Comitê de Crise - COCRI.

**EXECUÇÃO**

Uma vez identificada a necessidade de acionar o Plano de Recuperação Operacional, a equipe convocará reunião de emergência com os demais líderes, dos Planos PAC e PRD, com o intuito de coordenar os prazos, definir prioridades, repassar instruções, e ainda designar responsável técnico pelo restabelecimento do serviço e dentre outros alinhamentos necessários.

**ENCERRAMENTO DO PCO**

Após a validação do funcionamento dos sistemas e estabilidade dos mesmos, deverá ser feita a emissão de um parecer/relatório técnico, relatando as atividades realizadas, efeitos destas e resultado à equipe da DITEC, a qual repassará aos demais CGEST e COCRI.

### **10.3. PRD – Plano de Recuperação de Desastres**

|  |  |  |
| --- | --- | --- |
| **Versão** | **Descrição** | **Responsáveis** |
| 1 | Criação da 1ª versão PRD | Raquel Cunha da Conceição |
|  | Criação da 1ª versão PRD | Elson Correia de Oliveira Neto |
|  |  | **Elaboração** |
|  | Criação da 1ª versão PRD | Elinara Bras Ferreira |
|  | Criação da 1ª versão PRD | Elson Correia de Oliveira Neto |
|  |  | **Revisão** |
|  | Criação da 1ª versão PRD | Ronimar Ferreira de Matos |
|  | Criação da 1ª versão PRD | Lucas Bezerra Felix |
|  | Criação da 1ª versão PRD | **Aprovação** |
|  |  | CGEST |
|  |  | CGTIC |
|  |  | COCRI |

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

**OBJETIVOS**

O principal objetivo de um plano de recuperação de desastres de TIC é reduzir ao máximo o tempo em que os sistemas de TI ficam inativos após um desastre, permitindo uma rápida retomada das operações normais.

Minimizar os custos associados à recuperação, como perda de receita, custos de reparo de sistemas danificados e despesas com serviços de recuperação.

Visa proteger a reputação da organização, demonstrando sua capacidade de resposta eficaz a eventos adversos.

Prevenir a propagação de incidentes para outras áreas da instalação principal;

**ESCOPO**

Assegurar a retomada das operações do ambiente principal após a ocorrência de uma crise ou cenário de desastre, concentrando-se exclusivamente nos ativos, conexões e configurações desse ambiente.

**EXECUÇÃO DO PRD**

As equipes de Infraestrutura devem identificar e listar todos os ativos danificados em caso de um desastre.

A equipe de redes é responsável por identificar as interrupções de conexões e acessos gerados após o desastre, especificando se a abrangência está na rede local, na rede WAN ou com o provedor de serviços. Além disso, a equipe de redes, segurança e infraestrutura deve mapear quais serviços foram interrompidos, fornecendo informações sobre perda de ativos e desconexões, com o objetivo de informar o COCRI - Comitê de Crises.

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

* A priorização dos serviços essenciais ou determinação de nível institucional;
* O RTO definido para cada serviço essencial;
* Disponibilidade da equipe técnica.

Em caso de perda de ativos, o Comitê de Crises deve ser informado imediatamente sobre a necessidade de adquirir ativos perdidos que não possam ser recuperados. A equipe deve estimar quanto tempo a aquisição irá impactar o RTO de cada serviço e comunicar ao COCRI se há alguma solução alternativa enquanto a aquisição é realizada.

A equipe também deve verificar se os ativos danificados estão cobertos por garantia e se podem ser acionados através dos fornecedores. Qualquer alteração no tempo de recuperação dos serviços deve ser comunicada às equipes do PCO e PAC.

É necessário verificar se as configurações dos ativos reparados ou substituídos estão em pleno funcionamento. Se não estiverem, um cronograma estimado deve ser fornecido para configurar esses ativos, com informações transmitidas à equipe de Comunicação, pertencente ao Plano de Administração de Crises, para que sejam repassadas aos envolvidos e ao Comitê de Crises - COCRI para conhecimento.

Antes da recuperação dos dados do backup, o ambiente principal do Data Center deve ser testado para garantir que o processo de recuperação ocorra conforme o planejado.

**ENCERRAMENTO DO PRD**

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

# ****MATRIZ DE TESTES****

O Plano de Continuidade de TI pode ser acionado em casos de testes ou por determinação da própria DITEC, em conjunto com o Comitê de Segurança - COCRI. Nesse caso, periodicamente ou com a insurgência de novos fatores de risco, mudança na análise de impacto ou inclusão de um novo serviço no plano de continuidade, os líderes de cada plano (PCO, PAC e PRD) devem seguir o seguinte modelo de checklist:

|  |  |  |  |
| --- | --- | --- | --- |
| **DATA** | **TIPO** | **MOTIVO** | **STATUS** |
|  |  |  |  |

* Data: Refere-se ao dia da execução ou validação do teste;
* Tipo: o teste pode ser, de mesa, caminho percorrido, simulação, entre outros;
* Motivo: O Motivo pelo qual o teste foi necessário;
* Status: programado, executado, planejado, agendado.

# ****CONCLUSÃO****

O Plano de Continuidade de Serviços (PCS) é uma estratégia elaborada por uma organização para garantir que suas operações críticas possam ser mantidas ou retomadas em caso de interrupções ou desastres. O objetivo principal de um PCS é minimizar os impactos negativos e as consequências de eventos disruptivos, permitindo que o Tribunal de Justiça do Acre continue funcionando de forma eficaz e atenda às necessidades de seus servidores.

Em suma, o PCS é essencial para a resiliência e a sustentabilidade das operações de uma organização. Ele envolve a identificação dos processos e serviços críticos, a avaliação dos riscos e vulnerabilidades, o desenvolvimento de estratégias de mitigação, a implementação de planos de contingência e a realização de testes e exercícios para garantir a eficácia do plano.

Ao ter um PCS bem estruturado, a DITEC estará mais preparada para lidar com eventos inesperados, como falhas de sistemas, desastres naturais, ciberataques, entre outros. Alguns benefícios de um PCS adequado incluem:

1. Minimização de interrupções: O PCS ajuda a minimizar a duração e o impacto de interrupções, permitindo uma resposta rápida e eficiente em situações de crise.

2. Proteção da reputação: Ao manter as operações essenciais, mesmo em situações adversas, uma organização pode proteger sua reputação e a confiança de seus clientes, parceiros e partes interessadas.

3. Redução de perdas financeiras: Um PCS eficaz ajuda a reduzir as perdas financeiras decorrentes de interrupções nos negócios, garantindo a continuidade das receitas e a minimização dos custos relacionados à recuperação.

4. Conformidade regulatória: Na Diretoria de Tecnologia da Informação que têm regulamentações específicas e exigem a implementação de um PCS, garantindo o cumprimento de obrigações legais e regulatórias.

5. Melhoria da resiliência organizacional: O PCS promove a resiliência organizacional, permitindo que a organização se recupere rapidamente de eventos disruptivos e aprenda com essas experiências para melhorar sua capacidade de enfrentar futuros desafios.

Em resumo, um Plano de Continuidade de Serviços é uma ferramenta essencial para garantir a resiliência, a sustentabilidade e a capacidade de recuperação de uma organização diante de eventos disruptivos. Ele envolve uma abordagem estruturada para identificar riscos, implementar medidas de mitigação e garantir a continuidade das operações críticas, minimizando os impactos negativos nos serviços e nos clientes.



**TRIBUNAL DE JUSTIÇA**

**Diretoria de Tecnologia da Informação**

**www.tjac.jus.br**

Rua Tribunal de Justiça, s/n. Via Verde. 69.920-193

Rio Branco-AC | (68) 3302-0360 / 3302-0361