PLANO DE CONTINUIDADE DE SERVIÇOS ESSENCIAIS DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

PCSETIC 2021-2026

Data: *30/06/2022*

Versão 1.0

Plano de Continuidade de Serviços Essenciais de Tecnologia da Informação e Comunicação no âmbito do Poder Judiciário do Estado do Paraná

Presidente do Tribunal de Justiça do Estado do Paraná (gestão 2021- 2022)
Desembargador José Laurindo de Souza Netto

1° Vice-Presidente
Desembargador Luiz Osório Moraes Panza

2° Vice-Presidente
Desembargadora Joeci Machado Camargo

Corregedor-Geral da Justiça
Desembargador Luiz Cezar Nicolau

Corregedor de Justiça
Desembargador Espedito Reis do Amaral

Supervisor de Tecnologia da Informação e Comunicação
Desembargador Marcelo Gobbo Dalla Dea

Comitê de Governança de Tecnologia da Informação e Comunicação do TJPR

Presidente do Comitê
Desembargador Rogério Etzel

Vice-Presidente do Comitê
Desembargador Marcelo Gobbo Dalla Déa

Juiz Auxiliar da Presidência
Dr. Anderson Ricardo Fogaça

Juíza Auxiliar da 1ª Vice-Presidência
Dra. Ângela Maria Machado Costa

Juiz Auxiliar da 2ª Vice-Presidência
Dr. Luciano Carrasco Falavinha Souza

Juiz Auxiliar da Corregedoria-Geral da Justiça
Dr. Alexandre Gomes Gonçalves

Representante da AMAPAR
Dr. Marcos Caires Luz

Secretária do Tribunal de Justiça
Mariana da Costa Turra Brandão

Diretor do Departamento de Planejamento
Vinícius Rodrigues Lopes

Diretor do Departamento de Tecnologia da Informação e Comunicação
Rafael Coninck Teigão

Servidor do Departamento de Tecnologia da Informação e Comunicação
Alessio Roman Junior

Servidor do Departamento de Tecnologia da Informação e Comunicação
Pablo Tavares

Assessor Jurídico-Administrativo da Presidência
Leonardo de Andrade Ferraz Fogaça

Servidor da Corregedoria-Geral da Justiça
Gerson Mikalixen Junior

Comitê de Gestão de Riscos do TJPR

Presidente do Comitê
Drª. Fabiane Pieruccini

Diretor do Departamento de Planejamento
Vinicius Rodrigues Lopes

Secretária do Tribunal de Justiça
Mariana da Costa Turra Brandão

Coordenador do Núcleo de Governança, Riscos e Compliance
Thiago Martini Ribeiro Pinto

Resolução nº 272/2020-OE/TJPR

Comitê de Segurança de Tecnologia da Informação e Comunicação do TJPR

Presidente do Comitê
Desembargador Marcelo Gobbo Dalla Déa

Secretária do Tribunal de Justiça
Mariana da Costa Turra Brandão

Juiz Auxiliar da Presidência
Dr. Anderson Ricardo Fogaça

Diretor do Departamento de Tecnologia da Informação e Comunicação
Rafael Coninck Teigão

Juiz Auxiliar da Corregedoria-Geral da Justiça
Dr. Alexandre Gomes Gonçalves

Portaria TJPR nº1841 e 1948/2021 (SEI!TJPR 0017196-72.2021.8.16.6000)

Comitê de Gestão de Tecnologia da Informação e Comunicação do TJPR

Alberto Heitor Molinari
Alessio Roman Junior
Cideclei Machado
Danilo Kovalechyn
Ersan Rafael Holstein
Jean Paul Bonnevialle
Carlos José Johann Kolb
Luiz Fernando Moletta Alves
Magno Mario Bayer Filho
Márcio Mortensen Wanderley
Pablo Tavares
Paulo Alfredo Ribas Toledo
Paulo Henrique Waromby
Rafael Coninck Teigão

Portaria TJPR nº4217/2021 eDJ nº 2977 em 21/05/2021 (SEI!TJPR 0033045-60.2016.8.16.6000)

Grupo de Trabalho em Segurança da Informação e Comunicação do TJPR

Lauro Andrey de Souza Bueno (líder do grupo)
Adriano Witkovski
Altimar de Souza Junior
Danilo Kovalechyn
Daniel Ferreira Caetano dos Santos
Marcio William Ebuchi
Rodrigo Daniel Campaner de Lira
Gustavo Raphael Stein

Portaria TJPR nº 5050/2021 eDJ nº 2998 em 23/06/2021 (SEI!TJPR 0031716-37.2021.8.16.6000)

Equipe Técnica na elaboração deste documento (servidores do DTIC)

Adriano Witkovski
Eder Sibirkin
Lauro Andrey de Souza Bueno

HISTÓRICO DE ALTERAÇÕES

Versão	Data	Autor(es)	Descrição
0.1	28/06/2022	Divisão de Gestão de Segurança de Tecnologia da Informação	Criação do Documento
0.2	-	Equipe de Apoio a Gestão e Governança de TIC e Integrantes do NGRC	
0.3	-	Equipe de Apoio a Gestão e Governança de TIC	

SUMÁRIO

TABELAS

FIGURAS

Página em branco

1. APRESENTAÇÃO

A missão do Tribunal de Justiça do Paraná está relacionada com prestação jurisdicional acessível, de qualidade e célere para toda a sociedade. No entanto, para alcançar estes objetivos são necessários meios para trilhar este percurso. A Tecnologia da Informação é essencial para suportar os processos de negócios e atividades fim.

Neste contexto, surgem os serviços essenciais de TIC que contribuem diretamente para o cumprimento da missão deste Tribunal, dando suporte as atividades judicantes. Uma vez que os serviços de TIC são fundamentais para operação do negócio, a indisponibilidade ou interrupção significativa destes serviços, tais como: desastres, incêndios, falha de hardware, falha humana, manifesta consequências que resultam no descumprimento de prazos processuais, falta de atendimento aos jurisdicionados, perda de dados e retrabalho.

Dessa forma, a elaboração de um Plano de Continuidade de Serviços Essenciais de TIC deve ser tratado como prioridade, a fim de que seja possível planejar, manter e testar procedimentos e ações para retomar a execução destes serviços.

Em consequência disso, diante de um cenário de interrupção grave ou desastre o Departamento de Tecnologia da Informação e Comunicação - DTIC terá uma direção para agir de forma adequada e organizada, executando as estratégias previamente planejadas, buscando assegurar a disponibilidade de serviços a um nível aceitável para o Tribunal.

Este documento está alinhado com o Planejamento Estratégico Institucional e Diretor do DTIC, portanto ao ciclo 2021-2026, porém será objeto de revisão periódica, pelo menos **trimestralmente**, buscando adequações à realidade do órgão, da sociedade e de mudanças do Judiciário.

Além disso, este documento contempla o Plano de Administração de Crise de Serviços Essenciais - PACSE e o Procedimentos de Recuperação de Serviços Essenciais de TIC - PRSE.

2. OBJETIVO

O presente plano tem como objetivo apresentar ações para prevenir e tratar eventos provenientes de desastres ou que impactem significativamente os Serviços Essenciais de TIC, através de um documento único, normatizado, conhecido e também:

- Conhecer o grau de exposição ao risco para eventos críticos e desastres;
- Responder de forma eficiente às interrupções graves;
- Minimizar possíveis impactos aos jurisdicionados;
- Estabelecer procedimentos e ações a serem seguidos imediatamente após a ocorrência de um desastre ou interrupção significativa;
- Estabelecer um plano de Administração de Crise - PACSE;
- Estabelecer procedimentos e ações para restaurar serviços essenciais de TIC;
- Definição de papéis e responsabilidades para executar e comandar as atividades previstas no plano;

Na ocorrência de interrupções significativas que impactem diretamente na continuidade da prestação jurisdicional no âmbito do Tribunal de Justiça do Paraná,

almeja-se com este plano prover direcionamento para ações e procedimentos, comunicação linear e rápida recuperação dos serviços essenciais de TIC;

3. ESCOPO

Este documento tem aplicabilidade para todo o Departamento de Tecnologia da Informação e Comunicação do TJPR.

O presente plano considera o(s) serviços(s) de TIC apresentado(s) na tabela abaixo como essenciais, uma vez que impactam diretamente nas atividades judicantes.

Sistemas e serviços críticos a serem tratados
Portal Institucional: Portal Institucional do Tribunal de Justiça do Paraná

O escopo deste plano se limita a eventos em caráter de desastre ou críticos que impactem significativamente nos serviços essenciais de TIC. Para eventos de menor proporção os processos de Gestão de Disponibilidade, Incidentes e Problemas são os mais adequados para o tratamento.

4. ABREVIAÇÕES E DEFINIÇÕES

ABREVIAÇÕES:

- **CNJ**: Conselho Nacional de Justiça
- **DTIC**: Departamento de Tecnologia da Informação e Comunicação
- **ENTIC-JUD**: Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário
- **PCSTIC**: Plano de Contratações de Solução de TIC
- **PCTIC**: Plano de Capacitação de TIC
- **PDTIC**: Plano Diretor de Tecnologia da Informação e Comunicação
- **PSI**: Política de Segurança da Informação
- **SEI**: Sistema Eletrônico de Informações
- **SIC**: Segurança da Informação e Comunicação
- **TIC**: Tecnologia da Informação e Comunicação
- **TJPR**: Tribunal de Justiça do Estado do Paraná

DEFINIÇÕES:

Avaliação do Impacto nos Negócios (BIA): Um processo que identifica e avalia os potenciais impactos (financeiro, regulatório, jurídico/contratual, reputação e assim por diante) de eventos disruptivos nas operações de negócios.

Avaliação do risco: O processo de avaliação de potenciais riscos (desastres naturais/eventos causados pelo homem) que representam uma ameaça às operações

comerciais, juntamente com sua gravidade e probabilidade de informar a estratégia de recuperação.

CGOVTIC – Comitê de Governança de Tecnologia da Informação e Comunicação: comitê responsável por apoiar e orientar as iniciativas, projetos e investimentos em Tecnologia da Informação e Comunicação, observando a estratégia institucional, dentre outros.

CGESTIC – Comitê Gestor de Tecnologia da Informação e Comunicação: comitê responsável pelos planos táticos e operacionais, análise de demandas, acompanhamento da execução de planos, estabelecimento de indicadores operacionais, dentre outros.

CSEGTI – Comitê de Segurança de Tecnologia da Informação: comitê responsável por apreciar, assessorar e aprovar a implementação das ações de segurança da informação e garantir a implementação da Política de Segurança de Tecnologia da Informação.

Equipe de Tratamento e Resposta a Incidentes - ETIR: equipe multidisciplinar criada para atuar na resolução de incidentes que afetem a continuidade do serviço no contexto de TIC.

Evento Crítico: Um incidente ou evento imprevisto que acontece inesperadamente e exige ação imediata e intervenção para minimizar potenciais perdas para as pessoas, propriedades ou rentabilidade.

Matriz de Riscos: representação formal na qual são registrados os riscos identificados, considerando as probabilidades e os impactos, de forma a permitir a definição das ações necessárias ao seu gerenciamento.

Parte interessada (Stakeholder): pessoa ou organização que pode afetar, ser afetada ou perceber-se afetada por uma decisão ou atividade.

Plano de Continuidade de Serviços Essenciais de TIC: O plano abrangente que se concentra em como sustentar as funções de negócios de uma organização durante e após uma interrupção. Normalmente inclui pessoas, processos e tecnologia. Os sistemas de TI são considerados em termos de seu suporte aos processos de negócios. Procedimentos de recuperação de desastres e planos de resposta a incidentes podem estar contidos nos planos de continuidade.

Recuperação de Serviços Essenciais de TIC: O componente técnico do BCP e foca na continuidade dos sistemas de tecnologia da informação e comunicação que suportam funções empresariais.

RPO (Objetivo de ponto de recuperação: Tempo máximo aceitável durante o qual os dados podem ser perdidos.

RTO (Recovery Time Objective, objetivo de tempo de recuperação): Tempo aceitável que o aplicativo, serviço ou processo pode estar offline.

Terceiros: Um terceiro é tipicamente uma empresa que fornece um produto/serviço auxiliar não fornecido pelo fabricante principal ao usuário final.

Teste: Procedimento para avaliação (maneira de determinar a presença, qualidade ou validade de algo).

5. REFERÊNCIAS NORMATIVOS

ID	Documento	Descrição
RN01	CNJ - Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD), no período de 2021-2026.	Dispõe sobre a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD), no período de 2021-2026. Resolução nº 370 do CNJ, 28/01/2021.
RN02	CNJ - Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ)	Dispõe sobre a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ). Resolução nº 396 do CNJ, 07/06/2021.
RN03	Política de Segurança de Tecnologia da Informação do TJPR.	Dispõe sobre a Política de Segurança de Tecnologia da Informação, no âmbito do Poder Judiciário do Estado do Paraná, e estabelece competências administrativas aos seus órgãos integrantes. Objetiva instituir responsabilidades e diretrizes corporativas para a proteção dos ativos de Tecnologia da Informação e a prevenção de responsabilidade legal para todas as autoridades judiciais, servidores e usuários do Poder Judiciário do Estado do Paraná. Documento 0964880 no SEI!TJPR 0063818-25.2015.8.16.6000. Decreto Judiciário nº 631/2016 publicado no diário da justiça nº 1827 em 23/06/2016.
RN04	Política de Gestão de Riscos do TJPR.	Dispõe sobre a Política de Gestão de Riscos e institui o Comitê de Gestão de Riscos do Poder Judiciário do Estado do Paraná. Resolução nº 272/2020 - OE do TJPR, 14/09/2020.
RN05	Manual de Gestão de Riscos do TJPR.	Documento que apresenta, resumidamente, os principais conceitos, princípios e atores da gestão de riscos, possibilitando que qualquer pessoa possa compreender e gerir os riscos nos processos de trabalho em que atue. SEI!TJPR 0021241-22.2021.8.16.6000. Decreto Judiciário nº 461/2021 publicado no diário da justiça nº 3030 em 06/08/2021.

ID	Documento	Descrição
RN06	Política de Proteção aos Dados Pessoais, conforme a Lei nº 13.709/2018 (LGPD).	Estabelece medidas para o processo de adequação à Lei Geral de Proteção de Dados Pessoais a serem adotadas pelos tribunais.
RN07	Comitê de Segurança de Tecnologia da Informação (CSEGTI) do TJPR.	Instituir o Comitê de Segurança de Tecnologia da Informação e a Política de Segurança de TI. Decreto Judiciário nº 631/2016, em 23/06/2016.
RN08	Comitê Gestor de Tecnologia da Informação e Comunicação (CGESTIC) do TJPR.	Institui o Comitê Gestor de Tecnologia da Informação e Comunicação (CGESTIC), no âmbito do Tribunal de Justiça do Estado do Paraná. Decreto Judiciário nº 506 do TJPR, em 22/08/2019.
RN09	Comitê de Governança de Tecnologia da Informação e Comunicação (CGOVTIC)	Institui o Comitê de Governança de Tecnologia da Informação e Comunicação e define suas diretrizes no âmbito do Tribunal de Justiça do Estado do Paraná. Decreto Judiciário nº 361 do TJPR, em 04/06/2019.
RN10	NS - Norma de Continuidade de Serviços Essenciais de Tecnologia da Informação e Comunicação no âmbito do Tribunal de Justiça do Estado do Paraná.	Instrução Normativa que institui a Norma de Continuidade de Serviços Essenciais de Tecnologia da Informação e Comunicação no âmbito do Tribunal de Justiça do Estado do Paraná.
RN11	ABNT NBR ISO/IEC 31000:2018	ABNT NBR ISO/IEC 31000:2018 – Gestão de riscos – Diretrizes.
RN12	ABNT NBR ISO/IEC 27005:2019	ABNT NBR ISO/IEC 27005:2019 - Tecnologia da informação - Técnicas de segurança - Gestão de riscos de segurança da informação.
RN13	ABNT NBR ISO/IEC 22301:2013	ABNT NBR ISO/IEC 22301:2013 – Sistema de Gestão de Continuidade de Negócio (SGCN).

Tabela 1 - Documentos de Referência para elaborar o PCSETIC do TJPR

6. RESPONSABILIDADES

Considerando que o tratamento de eventos de desastres ou impactos significativos continuidade de Serviços Essenciais de TIC necessitam de atuação multidisciplinar de vários perfis, esta seção define as responsabilidades para execução deste plano.

Comitê de Segurança de Tecnologia da Informação - CSEGTI

- deliberar sobre Plano de Continuidade de Serviços de TIC e o Plano de Administração de Crise;

- apreciar as informações e os relatórios de testes ou acionamentos dos Planos de Continuidade de TIC;

Comitê de Governança de Tecnologia da Informação e Comunicação - CGOVTIC

- aprovar a classificação dos Serviços Essenciais de TIC, conforme princípios e diretrizes que orientem a forma de utilização da Tecnologia da Informação;

Comitê de Gestão de Tecnologia da Informação e Comunicação - CGESTIC

- classificar os serviços essenciais de TIC com base nos objetivos estratégicos institucionais apresentados no Planejamento Estratégico Institucional - PEI;
- revisar a elaboração, implementação, cenários e resultados de testes e atualização dos planos;
- propor melhorias na implantação de novos instrumentos relativos à Continuidade de Serviços Essenciais de TIC;

Diretor do Departamento de Tecnologia da Informação e Comunicação - DTIC

- definir a composição e instituir o Comitê de acionamento do Plano de Continuidade de TIC;

Divisão de Segurança de Tecnologia da Informação - DSEG

- elaborar o Plano de Continuidade de Serviços Essenciais de TIC e o Plano de Administração de Crise;
- elaborar e atualizar os modelos de documentos utilizados na Gestão de Continuidade de Serviços Essenciais de TIC;
- gerir os documentos que compõem os planos de continuidade de TIC;
- apoiar na elaboração dos Procedimentos de Recuperação de Serviços de TIC;
- assessorar o Comitê de acionamento de Continuidade de TIC na tomada de decisões a respeito de situações decorrentes de interrupções graves e desastres;
- manter os registros e histórico dos incidentes e dos acionamentos dos planos e os seus resultados;
- prover informações para o Comitê de Segurança de Tecnologia da Informação - CSEGTI a respeito dos resultados dos testes ou acionamento dos planos de continuidade de TIC;
- garantir que estrutura documental dos Planos de Continuidade de Serviços Essenciais de TIC, Plano de Administração de Crise e Procedimentos de Recuperação de Serviços Essenciais de TIC esteja disponível em ambiente alternativo.

Equipe de Tratamento e Resposta a Incidentes - ETIR

- contribuir para a elaboração do Plano de Continuidade, Plano de Administração de Crise e os Procedimentos de Recuperação de Serviços Essenciais de TIC;

- receber, analisar, tratar e responder às notificações relacionadas aos incidentes que acionaram o Plano de Continuidade de Serviços Essenciais de TIC;
- elaborar relatórios de tratamento sobre os incidentes ocorridos;

Gestor técnico do Serviço Essencial de TIC

- apoiar na elaboração e manutenção nos Planos de Continuidade e de Administração de Crise;
- elaborar e manter o Procedimento de Recuperação de Serviços Essenciais de TIC;
- definir o tempo máximo para retorno operacional (RTO) do serviço essencial de TIC após a ocorrência de um desastre, quando não houver regulamentação específica;

Comitê de Acionamento do Plano de Continuidade de Continuidade de TIC

- acionar o Plano de Continuidade de Serviços de TIC, Plano de Administração de Crise e o Procedimentos de Recuperação de Serviços Essenciais de TI;
- deliberar ações não contempladas nos Procedimentos de Recuperação para garantir a continuidade dos serviços, com posterior avaliação pelo Comitê de Segurança de Tecnologia da Informação;

7. AVALIAÇÃO DE RISCO

Os principais riscos e ameaças que impactam na continuidade dos serviços essenciais de TIC devem ser identificados e gerenciados, com objetivo de prevenir e mitigar os seus efeitos em virtude da sua manifestação.

Para os riscos e as ameaças identificadas neste plano não se esgota aqui todas as possibilidades de ocorrência. Porém, espera-se apresentar um mapeamento inicial que, aderente ao **Plano de Gestão de Risco de TIC,** deverá ser continuamente melhorado com foco em sua maturidade.

7.1. PRINCIPAIS RISCOS

O plano deverá ser ativado sempre que houver a ocorrência de um evento em caráter de desastre, evento crítico que afete ou tornem os serviços essenciais do TIC indisponíveis, ou caso exista uma vulnerabilidade altamente relevante, comprometendo assim a capacidade de execução operacional dos serviços.

Para este plano são considerados eventos de desastres ou críticos, baseados nas orientações do Gartner que norteiam as avaliações mínimas de riscos no contexto da continuidade de serviços essenciais de TIC:

- Interrupção de Energia Elétrica;
- Falha de Climatização em data center;
- Falha Humana;
- Ataques Internos;
- Incêndio;
- Desastres Naturais;

- Falha de Hardware;
- Ataque Cibernético;
- Falha de Conectividade;
- Ruptura Contratual;

A tabela abaixo apresenta uma visão dos principais riscos e ameaças inicialmente identificadas para continuidade dos serviços essenciais de TIC.

ID	Evento	Causa	Consequências
R01	Ataque cibernético	1. Serviços vulneráveis e desatualizados; 2. Baixa conscientização em segurança; 3. Falta ou ineficiência de Controles de segurança;	indisponibilidade do serviço afetado incapacidade de acessar dados críticos, acesso não autorizado a dados confidenciais;
R02	Interrupção de Energia Elétrica	1. Falha no fornecimento de energia principal e secundário;	indisponibilidades de todos os serviços
R03	Desastres naturais	1. Enchentes, vendavais, Ocorrências Sísmicas.	acesso restrito ao data center
R04	Falha Humana	1. Baixa conscientização em segurança; 2. Baixa capacitação técnica;	indisponibilidade do serviço afetado; perda de dados;
R05	Falha de Conectividade	1. rompimento dos meios de comunicação; 2. mal funcionamento ou erros nas configurações de equipamentos;	indisponibilidade do serviço afetado; perda da capacidade de conexão;
R06	Falha de Hardware	1. Falha ou queima de componentes sem redundância;	indisponibilidade do serviço afetado;
R07	Incêndio	1. Sobrecarga das instalações; 2. Baixa qualidade nos componentes; 3. Baixa capacitação técnica; 4. Falta ou ineficiência de Controles de segurança contra incêndios;	destruição de equipamentos e materiais;
R08	Ataques Internos	1. Insatisfação humana; 2. Falhas de segregação de função e controles de acesso;	acesso não autorizado; roubo de informação; indisponibilidade do serviço;

R09	Falha de Climatização em data center	1. Sobrecarga das instalações; 2. Falha na manutenção dos equipamentos de refrigeração;	superaquecimento dos ativos do data center; perda de dado e ativos;
R10	Ruptura Contratual	1. Atrasos ou demora nos processos de contratação; 2. Rescisão contratual;	indisponibilidade do serviço;

Tabela 2 – Principais Riscos

8. ANÁLISE DE IMPACTO (BIA)

Análise de impacto do negócio é o processo de analisar as funções do negócio e os efeitos que interrupções significativas podem causar, quantificando os impactos da descontinuidade dos serviços essenciais de TIC, considerando os riscos reconhecidos, o tempo e ponto objetivados de recuperação (RTO e RPO), e os requisitos tecnológicos.

Portal Institucional	
Tipo	Sistema
Impacto	Alto
Descrição	Sistema que centraliza serviços e informações ao público interno e ao externo ao TJPR
RPO	01 hora
RTO	01 hora
Período crítico	Dias úteis
Requisitos tecnológicos	Conectividade de internet Servidor da aplicação Banco de dados Storage Core LAN Data center

Tabela 3 - Análise de Impacto do Serviço Essencial

9. ATIVAÇÃO DO PLANO

O **acionamento** do Plano de Continuidade será invocado por qualquer membro do ***Comitê de acionamento do Plano de Continuidade de TIC,*** obedecendo as seguintes ações:

Papéis	Responsabilidades	Ações
Comitê de acionamento do Plano de Continuidade de TIC	**Acionar** o plano de continuidade de TIC	**Notificar** os membros do Comitê de acionamento do Plano de Continuidade de TIC; **Notificar** o líder da ETIR; **Notificar** o Diretor do DTIC.

Comitê de acionamento do Plano de Continuidade de TIC	**Registrar** o início da ativação do PCSE-TIC	**Registrar** de modo manual ou eletrônico, informações como data e hora de início do incidente, horário de ativação do plano, breve descrição do ocorrido e a confirmação da ciência das equipes de apoio envolvidas.
Comitê de acionamento do Plano de Continuidade de TIC	**Garantir** que todos os contados da árvore hierárquica foram comunicados	**Comunicar,** validar e garantir que todos os contatos presentes na árvore hierárquica foram avisados.

Tabela 4 - Ativação do Plano

Para agilidade das ações de execução deste plano, as etapas, contatos e links de acesso aos demais documentos associados estarão resumidos no **Manual Execução de Continuidade de TIC**.

9.1. ÁRVORE HIERÁRQUICA DE ACIONAMENTO

Na ocorrência de um evento que impacte na continuidade dos serviços essenciais do TIC, o membro do ***Comitê de acionamento do Plano de Continuidade de TIC*** deverá comunicar os principais líderes e gestores que serão informados da situação atual, conforme quadro de comunicação abaixo:

Papel	Meio de comunicação
Líder ETIR	Telefone
Membros do Comitê de Acionamento	Telefone
Diretor DTIC	Telefone
Coordenador DTIC-CGP	Telefone
Coordenador DTIC-CSI	Telefone
Coordenador DTIC-CIN	Telefone
Coordenador DTIC-CQ	Telefone
Gestor - DPRO	E-mail ou Teams
Gestor - DSEG	E-mail ou Teams
Gestor - DCON	E-mail ou Teams
Gestor - DADOS	E-mail ou Teams
Gestor - DDEV	E-mail ou Teams
Gestor - DES	E-mail ou Teams
Gestor - DCOLAB	E-mail ou Teams
Gestor - DINFRA	E-mail ou Teams
Gestor - DSUST	E-mail ou Teams
Gestor - DAT	E-mail ou Teams
Gestor - DQA	E-mail ou Teams
Gestor - DNRI	E-mail ou Teams

NGRC	E-mail ou Teams

Tabela 5 - Árvore Hierárquica de Acionamento

9.2. EQUIPES DE APOIO

As seguintes equipes apoiarão no gerenciamento da continuidade, comunicação e restauração das operações dos serviços essenciais de TIC durante o acionamento do plano de continuidade.

Equipe de Gerenciamento de Continuidade de TIC			
Nome/Função	**Funções Habituais**	**Responsabilidades**	**Contato**
Equipe de Tratamento e Resposta a Incidentes - **ETIR/TIC**	Equipe multidisciplinar do DTIC	**Realizar** avaliação quanto a dimensão do impacto, extensão e possíveis desdobramentos; **Prestar** informações ao Comitê de acionamento do Plano de Continuidade de TIC; **Dialogar** com as equipes comunicação de crise e equipes relacionadas no plano de recuperação de TIC; **Validar** retorno à normalidade do serviço ou ambiente; **Emitir** relatório sobre o incidente.	dtic-etir@tjpr.jus.br Chat Teams
Comitê de acionamento do Plano de Continuidade de TIC	Membros a serem definidos	Informar os líderes e gestores e partes interessadas;	dtic-continuidade@tjpr.jus.br

Tabela 6 - Equipe de Gerenciamento

Equipe de Comunicação de Crise de TIC			
Nome/Função	**Funções Habituais**	**Responsabilidades**	**Contato**
Comitê de acionamento do Plano de Continuidade de TIC	Membros a serem definidos	**Assumir** a liderança na comunicação com todos os grupos de stakeholders (servidores e reguladores);	dtic-continuidade @tjpr.jus.br
Lider do ETIR/TIC		**Articular** a comunicação entre as equipes de gerenciamento de continuidade de TIC e equipe de comunicação de crise;	dtic-etir@tjpr.jus.br
Assessoria de Imprensa do Gabinete do Presidente	Comunicação com a mídia	**Assumir** a liderança na comunicação com todos os grupos de mídia externos.	<inserir contato>

Tabela 7 - Equipe de Comunicação

Equipe de Recuperação de Serviços Essenciais de TIC			
Nome/Função	**Funções Habituais**	**Responsabilidades**	**Contato**
Equipe de Tratamento e Resposta a Incidentes - **ETIR/TIC**	Equipe multidisciplinar do DTIC	**Apoiar** as equipes de recuperação dos Serviços de TIC;	dtic-etir@tjpr.jus.br
Equipe de Apoio de recuperação de serviços de TIC	Funções operacionais dos serviços ou componentes	**Executar** as estratégias de recuperação de serviços ou componentes;	[diversas áreas internas do DTIC]

Tabela 8 - Equipe de Recuperação

10. PLANO DE ADMINISTRAÇÃO DE CRISE DE TIC (PACSE)

O Plano de Administração de Crise **estabelece o fluxo e modelo de comunicação entre diversas áreas e partes interessadas**, com objetivo de informá-las sobre as interrupções dos serviços essenciais de TIC, bem como as ações e estimativa do tempo de recuperação, obtidas através das informações fornecidas pela ETIR/TIC e também pelos planos de recuperação.

Além disso, o plano contempla a comunicação com usuários internos do TJPR, usuários externos e mídia, contatos com fornecedores e prestadores de serviço e contatos de emergência.

O ***Comitê de acionamento do Plano de Continuidade de TIC*** será responsável por contactar os grupos relevantes e apresentar informações pertinentes para cada grupo.

PACSE

QR Code	Plano_de_Administração_de_Crise_de_TIC_(PACSE) https://tjpr.sharepoint.com/:w:/s/DTIC-CGP-DSEG/Ee0_DbrP36lKmBeNFBKWCFMBHlQf7irBtAjzp7sPi6mgig?e=oCGDN4

11. PROCEDIMENTO DE RECUPERAÇÃO DE SERVIÇOS ESSENCIAIS DE TIC (PRSE)

O procedimento de recuperação descreve as ações e procedimentos necessários para execução das estratégias para recuperação dos serviços essenciais de TIC, bem como retorno à normalidade.

Este plano considera também a recuperação de componentes associados aos serviços essenciais, tais como: componentes de rede, hardware de computador, equipamentos especializados, sistemas operacionais e aplicação.

PRSE

QR Code	Procedimento de Recuperação de TIC (PRSE) https://tjpr.sharepoint.com/:w:/s/DTIC-CGP-DSEG/EZ1Qcr56SSJPpzjdACI6F58BQaEWLLgj82dklP0F6U4HsA?e=nnKEVY

12. ENCERRAMENTO DO PLANO DE CONTINUIDADE

Após validação do funcionamento de retorno dos serviços essenciais de TIC à normalidade, o ***Comitê de acionamento do Plano de Continuidade de TIC*** comunicará as partes interessadas, promovendo informações sobre o retorno operacional com as informações de status e também a declaração de encerramento do Plano de Continuidade.

13. TESTE DO PLANO DE CONTINUIDADE DE SERVIÇOS DE TIC

Com objetivo de validar os procedimentos e ações planejados deverão ser executados testes dos planos de modo integral ou parcial, podendo abranger testes de mesa e testes de simulação, visando a melhoria contínua dos procedimentos, ações, fluxo de comunicação e recuperação dos serviços essenciais de TIC.

Os testes serão agendados, informados e gerenciados pela Divisão de Gestão de Segurança de TIC e acompanhado por todas as equipes envolvidas deste plano.

13.1. CRONOGRAMA DE TESTE

A tabela a seguir descreve o cronograma de testes para validar o plano de continuidade de Serviços Essenciais de TIC do Departamento de Tecnologia da Informação e Comunicação do TJPR.

Objetivo	*Validar o teste das capacidades de comunicação do Plano de Continuidade de Serviços de TIC*
Periodicidade	*Primeiro teste sendo até 30 dias após aprovação do plano e demais testes semestralmente*
Envolvidos	*Equipe de Recuperação de TI*
Tipo de teste	*Teste de escala parcial*
Facilitador(es)	*Comitê de Acionamento, ETIR/TIC*
Detalhes (local, cenário)	*Cenário de simulação inicial: R02 - Interrupção de Energia Elétrica*
Medidas de sucesso	*Todos os envolvidos executarem as funções planejadas*

Tabela 9 - Tabela de Teste

13.2. RESULTADO DO TESTE

A tabela a seguir apresenta um modelo inicial para ser utilizada na execução dos testes do plano de continuidade de Serviços Essenciais de TIC do Departamento de Tecnologia da Informação e Comunicação do TJPR.

Data	**Resultados dos testes recentes**	**Ações e recomendações**

Tabela 10 - Resultado de Teste

14. MANUTENÇÃO E REVISÃO

A manutenção e revisão deste plano será realizada sempre que houver mudanças na classificação nos serviços essenciais de TIC, necessidade de ajustes após de testes e quando ocorrer alterações significativas nos riscos de TIC.

15. PLANO DE AÇÃO SOBRE SERVIÇOS ESSENCIAIS DE TIC

Atividades necessárias ou próximas ações para continuidade de Serviços Essenciais de TIC, a serem realizadas no período de julho de 2022 a julho de 2023:

ID	Título
1	Elaborar o Procedimento de Recuperação
2	Elaborar o Manual de Execução do Plano de Continuidade de Serviços Essenciais de TIC
3	Definir as ações para execução dos testes
4	Desenhar o processo de gestão de continuidade de serviços essenciais de TIC
5	Definir a lista de serviços essenciais de TIC
6	Realizar o processo de gestão de riscos de TIC para os sistemas e serviços essenciais de TIC estratégicos

Tabela 11 - Ações Futuras

16. CONSIDERAÇÕES FINAIS

Este plano apresenta uma direção para ação de forma estruturada e organizada, buscando a definição de responsabilidades, comunicações eficientes e lineares e procedimentos para assegurar a disponibilidade de serviços a um nível aceitável para o Tribunal.

Trata-se de uma iniciativa que entrará em ação e que proporcionará a coleta de dados através de testes e acionamentos. Após análises e feedbacks, serão propostas melhorias em busca do aperfeiçoamento contínuo deste plano.

17. ANEXOS

Plano de Administração de Crise - PACSE
Procedimento de Recuperação de Serviços Essenciais - PRSE
Processo de Gerenciamento de Continuidade de Serviços Essenciais de TIC

18. METODOLOGIA E PROCESSO DO PLANO DE CONTINUIDADE DE SERVIÇOS ESSESNCIAIS DE TIC