Estado do Ceará
Poder Judiciário
Tribunal de Justiça
Secretaria de Tecnologia da Informação
Gerência de Infraestrutura de TI
Coordenadoria de Segurança da Informação

Sumário

1 Objetivo 3
2 Escopo 3
3 Responsabilidades 5
4 Análise de Impacto - Serviços Essenciais 9
5 Principais Eventos de Desastres 11
6 Análise de riscos, responsáveis e procedimentos de recuperação e contingência 14
7 Aprovações 16

1 Objetivo

1.1 O Plano de Continuidade de Serviços Essenciais de Tecnologia da Informação e Comunicação (TIC) tem por finalidade descrever os procedimentos que permitam a continuidade dos serviços críticos, em especial os serviços judiciais, identificar ameaças potenciais de descontinuidade das operações de negócios para o Poder Judiciário do Estado do Ceará e os possíveis impactos.

2 Escopo

2.1 O Plano de Continuidade de TI alinha-se as estratégias necessárias à continuidade dos serviços essenciais de TI, em especial para os ativos de TI que sustentam os serviços judiciais: Compreende a contingência, continuidade e recuperação.

2.2 Direcionado a *"elaborar e aplicar processos de reposta e tratamento a incidente de segurança cibernética que contenha, entre outros, procedimentos de continuidade do serviço prestado e seu rápido restabelecimento, além de comunicação interna e externa"*, de acordo com a ENSEC-PJ, no seu Art 11, inciso III.

2.3 A continuidade dos serviços essenciais de TIC é um processo de melhoria contínua que objetiva dar maturidade ao Poder Judiciário do Estado do Ceará na identificação e avaliação dos riscos de descontinuidade na área de TIC.

2.4 As perdas potenciais (o que pode ser perdido, como perdas financeiras, de imagem etc.) e o custo, para manter as atividades parcial ou totalmente, devem ser levantados pela equipe envolvida e pela Secretaria de Tecnologia da Informação (Setin) e o resultado, inclusive as opções de alternativas deverão ser encaminhadas aos membros do Comitê de Gestão de Tecnologia da Informação e Comunicação – CGETIC e para o **Comitê de Governança da Segurança da Informação, de Crises Cibernéticas e de Proteção de Dados Pessoais – CGSICCPDP**, que após analisarem e aprovarem a definição para o assunto, devem realizar acompanhamento das ações.

2.5 Planos de Continuidade

2.5.1 .Planos de Continuidade são um conjunto de procedimentos que objetivam, no caso de ocorrência de determinado(s) incidente(s), manter as atividades em nível de funcionamento previamente estabelecido ou recuperá-las no prazo previamente estabelecido (tempo objetivado de recuperação - comumente chamado no mercado de RTO).

2.5.2 Os Planos de Continuidade podem ser elaborados visando a vários tipos de eventos ou riscos operacionais, entre os mais comuns:

2.5.2.1 Incêndio;

2.5.2.2 Inundação;

2.5.2.3 Interrupção no fornecimento de energia elétrica;

2.5.2.4 Interrupções de serviços de TIC;

2.5.2.5 atentados com artefatos de explosivos;

2.5.2.6 atos de vandalismos;

2.5.2.7 outros, a critério da administração do Poder Judiciário do Estado do Ceará ou do **CGSICCPDP**.

2.5.3 Acionamento do Plano

2.5.3.1 sempre que ocorrer um incidente que gere a descontinuidade das atividades, o gestor do processo/sistema/ativo (líder do plano) deve contatar o Gestor ou responsável pela Gestão de Continuidade para analisar o incidente, definindo se o Plano de continuidade será acionado ou não;

2.5.3.2 o responsável por acionar o plano deve acompanhar todo o processo de restabelecimento das atividades normais;

2.5.3.3 o Grupo funcional, coordenado pelo líder do grupo, deve seguir os procedimentos estabelecidos no Plano de Continuidade.

2.5.3.4 após todo e qualquer processo de ativação de Plano de Continuidade de Serviços Essenciais de TIC ou de gestão de crise, cabe registrar a descrição do incidente, o que foi bem-sucedido, o que falhou e os aprimoramentos implementados para correção das fragilidades identificadas, bem como as ações com os responsáveis e prazo para implementação, se necessário;

2.5.3.5 relatórios emitidos devem ser submetidos aos Comitês para conhecimento e adoção de medidas julgadas necessárias.

2.5.4 Gestão de Crise

2.5.4.1 os planos devem permitir estabelecer uma diretriz de comunicação a ser seguida pelas equipes em situações de crise, de modo a unificar e garantir procedimentos rápidos, precisos e eficientes a quaisquer eventos que venham a pôr em risco a imagem e reputação do Órgão.

2.5.4.2 Caso a crise afete todo o Órgão, compete as equipes (interna ou externa) aguardar ações da equipe de Comunicação do Poder Judiciário do Estado do Ceará, sem tomar a frente de uma situação junto a mídia.

2.5.4.3 Caso o acionamento do Plano de Continuidade ou a gestão de crise gere a necessidade de atendimento à imprensa, essa atribuição deve ser desempenhada de forma organizada, centralizada e por responsável ou áreas previamente definidas pela Presidência.

3 Responsabilidades

3.1 As responsabilidades objetivam gerar as condições adequadas para a efetiva implementação das diretrizes do Plano de Continuidade de Serviços essenciais de TIC na Secretaria de Tecnologia da Informação (Setin).

3.2 Alinhado à Portaria nº CNJ 162/2021, **Compete aos órgão do Poder Judiciário estabelecer um Progama de Gestão da Continuidade de Serviços, portanto, o CGSICCPDP,** "participar da elaboração do Plano de Gestão da Continuidade de Negócios que identifique as atividades críticas, avalie os riscos e defina estratégias de continuidade e planos de contingência, de forma a evitar ou mitigar as perdas em potencial.

3.3 **Compete a Setin** através dos representantes do Comitê de Gestão de Tecnologia da Informação e Comunicação – CGETIC:

3.3.1 aprovar a estratégia de continuidade e os respectivos orçamentos;

3.3.2 acompanhar o processo de implementação da estratégia de continuidade, em função dos riscos operacionais envolvidos;

3.3.3 aprovar a estratégia de continuidade para os equipamentos e sistemas que possibilitam o processamento de operações, bem como os orçamentos necessários para a efetiva implementação;

3.3.4 aprovar os planos elaborados;

3.3.5 aprovar calendário anual de testes.

3.3.6 identificar, avaliar e tratar, riscos de descontinuidade relacionados às suas atividades;

3.3.7 atender às solicitações da equipe ou consultoria referente à Gestão de Continuidade de Negócios de Serviços (GCN) e de Serviços de Essenciais de TIC;

3.3.8 no caso de incidente que gere paralisação, mesmo que momentânea, dos processos que dão suporte aos produtos e serviços fundamentais, informar à área ou responsável interno de gestão de continuidade de negócios:

3.3.8.1 a sua ocorrência;

3.3.8.2 a causa geradora do incidente;

3.3.8.3 as soluções empreendidas e os consequentes resultados;

3.3.8.4 a necessidade de adequação de sistemas, processos e(ou) pessoas e os respectivos planos de ação para a efetiva implementação.

3.3.9 se ofertados produtos e(ou) serviços, fazer a identificação dos riscos que podem paralisar as atividades, avaliando a possibilidade de perda potencial e, em uma análise de custo e benefício, empreender as ações necessárias à implementação de procedimentos (planos) específicos para continuidade dos negócios/serviços essenciais, tomando-se o cuidado de alinhar as ações de Continuidade de Negócios aos riscos operacionais identificados e avaliados;

3.3.10 manter os Planos de Continuidade de Serviços Essenciais de TIC atualizados, de forma que sejam efetivos;

3.3.11 garantir, quando aplicável, que estejam definidos, em contrato, acordos de nível de serviços que garantam o alinhamento das prestações de serviços de terceiros com as estratégias de continuidade de negócios das suas áreas;

3.3.12 manter os empregados e prestadores de serviços, que participam dos Planos de Continuidade de Serviços Essenciais de TIC, devidamente treinados, garantindo, assim, a efetividade das atividades, de acordo com os níveis previamente estabelecidos;

3.3.13 estabelecer anualmente, cronograma de testes dos planos, realizando-os e formalizando o resultado, com apontamento do que deu certo e das necessidades de aprimoramento, com o consequente plano de ação, especificando responsáveis pela execução e prazo;

3.3.14 providenciar que as atividades relacionadas aos produtos e serviços mantidas sejam analisadas, com base no custo e benefício, e se conveniente, seja(m) implementado(s) plano(s) específicos que mantenham as atividades nos níveis desejados;

3.3.15 comunicar, imediatamente, à área ou responsável interno de gestão de continuidade de negócios qualquer alteração no cenário de negócio da área que requeira manutenção nos planos definidos para continuidade dos processos de negócio;

3.3.16 treinar os colaboradores objetivando à capacitação dos profissionais envolvidos na gestão de continuidade dos Serviços Essenciais de TIC, bem como orientar sobre os conceitos e as metodologias aplicáveis;

3.3.17 Criar cronograma e relatórios anuais de testes;

3.3.18 considerar, nas definições de estratégia de contingência de serviços Essenciais de TIC, as necessidades dos responsáveis pelos processos/serviços críticos de negócio que utilizam os recursos;

3.3.18.1 propor a estratégia de contingência de serviços Essenciais de TIC para os equipamentos e sistemas que possibilitam o processamento de operações, bem como os orçamentos necessários para a efetiva;

3.3.18.2 implementação, especificando, de forma clara e concisa para que haja o entendimento pelas pessoas que não são especialistas em tecnologia da informação:

3.3.18.2.1 os ativos (hardware e software) que suportam processos de negócios identificados como críticos e aplicados questionários Análise de Impacto nos negócios;

3.3.18.2.2 arranjos de contingência existentes;

3.3.18.2.3 propor soluções futuras de TI;

3.3.18.2.4 custo e prazo de implementação;

3.3.18.2.5 implementar planos de recuperação de desastre, visando a recuperar os ativos de TI dentro dos prazos definidos (tempos objetivados de recuperação) nos processos de negócios considerados

3.4 Grupos Funcionais

3.4.1 Grupos funcionais são constituídos pelos servidores/empregados designados para realizar os procedimentos de contingência descritos nos planos.

3.4.2 Componentes: líder e membros designados no respectivo plano.

3.4.3 Coordenador: líder do processo citado no plano.

3.4.4 Compete ao Grupo Operacional:

3.4.4.1 antes da contingência:

3.4.4.1.1 propor os procedimentos que mantenham as atividades de negócio em nível previamente definido;

3.4.4.1.2 realizar testes periódicos dos planos de serviços Essenciais de TIC, para garantir a sua efetividade, bem como treinar os empregados envolvidos.

3.4.4.2 durante a contingência:

3.4.4.2.1 acionar o Plano de Continuidade de Serviços Essenciais de TIC e, concomitantemente, o gestor responsável pelo respectivo plano;

3.4.4.2.2 avisar o representante do Grupo da respectiva área o acionamento de contingência;

3.4.4.2.3 empreender as ações necessárias à execução do plano;

3.4.4.2.4 caso não haja procedimentos de contingência descritos para o incidente identificado, ou não seja possível, por qualquer razão, acionar o plano, comunicar imediatamente e informar, se possível, sugestões de recuperação da atividade e(ou) de gestão de crise;

3.4.4.2.5 manter-se, em caso de não funcionamento do plano, em sobreaviso para executar as orientações do gestor de crise.

3.4.4.3 depois da contingência:

3.4.4.3.1 registrar, em relatório específico, a descrição do incidente e as soluções de contorno aplicadas;

3.4.4.3.2 verificar o que motivou o incidente/crise, emitindo e encaminhando ao gestor responsável as causas e as ações de aprimoramentos implementadas ou a implementar, para elaboração de relatório;

3.4.4.3.3 caso seja necessário, implementar procedimentos de aprimoramento dos respectivos planos

4 Análise de Impacto - Serviços Essenciais

Este plano é aplicado aos sistemas abaixo.

4.1 Informações coletadas através do questionário – Análise de Impacto.

4.2 São os seguintes os serviços essenciais, para acionamento e execução do PCSETIC

Serviço/Sistema	**RPO***	**RTO****	**Impacto**			**Histórico de descontinuidade**	
			Financeiro	**Legal**	**Imagem**	**Tempo mais longo de interrupção**	**Causa da Interrupção**
DJE	6 horas	60 min	Superior	Médio	Critico (Severo)	08/09/21 13:08 a 08/09/21 20:07 -> 419 min com o serviço indisponível; 3 dias sem possibilidade de fazer publicações no DJE do SAJ.	Queda de energia no Datacenter, devido a falha no gerador. Devido ao incêndio no prédio do TJCE, a energia da concessionária foi desligada e o gerador do datacenter funcionou initerruptamente por cerca de 2 dias. Mesmo estando revisado, o gerador não suportou o regime de operação e desligou por aquecimento.

MALOTE DIGITAL	60 min	4h	Irrelevante	***	Médio	24 horas	Erro no Sistema
PJE	30 min	60 min	Crítico (severo)	Crítico (severo)	Crítico(severo)	18/10/2020 00:14 a 18/10/2020 09:05 531min (domingo)->	Indisponibilidade link ETICE entre TJCe e Fórum, o banco Oracle caiu.
						12/09/2020 07:50 a 12/09/2020 12:05 255min (sabado)->	Queda link da ETICE
PORTAL-ESAJ	60 min	59 min	Alto	***	Médio	7 dias(21/07 a 28/07/2016)	Erro no Sistema
PROJUDI	60 min	4h	Irrelevante	***	Médio	24 horas	Erro no Sistema
SOLUÇÃO SAJ-SG	60 min /Backup mais recente	60 min, aceitável 24 horas (1 dia)	Superior	Crítico. Causa descontinuidade temporária do negócio.	Severo	Sim. Do período de março de 2022 a março/2023 tivemos o maior tempo de interrupção do SAJ SG informado abaixo: 06/05;2022 às 19:00 às 09/05/2022 23:59 – 4619 minutos	Essa interrupção decorreu devido à realização da Cópia do TJCEGAS.
SOLUÇÃO SAJ-PG	60 min	60 min	Superior	Crítico (severo)	Crítico(severo)	Sim. 11/02/2022 21:11 às 14/02/2022 10:50 – 3.699 minutos	Essa interrupção decorreu devido a um problema no banco de dados, onde a tablespace INDSG5CE foi apagada por erro humano;
SPROC	60 min	4h	Irrelevante	Crítico	Médio	***	***

*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.

***Não informado na análise de impacto

Serviço/Sistema	**Dependem de informações de outros processos/áreas internas**	**Dependem de informações de outros processos/empresas/áreas externas**	**Geram informações para outros processos/áreas internas**	**Geram informações para outros processos/áreas externas**
DJE	Sim.	Sim..	Sim.	Sim.
MALOTE DIGITAL	Sim. Active Directory (AD)	Sim. Informações vindas do Malote Digital instalado dos outros órgãos do poder judiciário.	Não	Sim. Malote Digital instalado dos outros órgãos do poder judiciário.
PJE	Sim.	Sim.	Sim.	Sim.
PORTAL-ESAJ	Sim. Sistema processual SAJ alimentado pelas varas e setores do Poder Judiciário.	Sim. Informações oriundas das unidades judiciárias e administrativas do Poder Judiciário.	Sim. Para as unidades judiciárias e administrativas do Poder Judiciário, jurisdicionados.	Sim. Para os jurisdicionados e unidades judiciárias do Poder Judiciário Estadual.
PROJUDI	Sim. RH, Infraestrutura	Não	Sim. SCPU e Sistemas Estatisticos (SGEC e SEI).	Sim. BNMP do CNJ, Arquimedes da Procuradoria, SAJ, PUSH
SOLUÇÃO SAJ-SG	Sim.	Sim.	Sim.	Sim.
SOLUÇÃO SAJ-PG	Sim.	Sim.	Sim.	Sim.
SPROC	Sim. SCPA, RH, Tabelas corporativas	Sim. BNMP do CNJ.	Não informado	Sim. BNMP do CNJ, Arquimedes da Procuradoria, SAJ, PUSH.

5 Principais Eventos de Desastres

5.1 PCSETIC foi desenvolvido pra ser acionado em situações de desastres que apresentem riscos de descontinuidade de serviços essenciais.

5.2 O quadro abaixo identificamos alguns destes desastres:

Item	**Descrição/Tratamento de contingência**	**Contato da Área responsável pela Contingência**

01- Interrupção de energia elétrica nos Data Centers	Causada por fator externo à rede elétrica do prédio ou de sua localidade com duração da interrupção superior a 12 horas. Causada por fator interno que comprometa a rede elétrica do prédio com curto-circuitos, incêndio e infiltrações. Impossibilidade de acionar o Grupo Moto-gerador no momento de uma queda de energia. **Acionar o Plano de Continuidade DataCenters Falta Energia.odt**	
02 - Falha Climatização nos ambientes de Climatização dos Data Centers	Superaquecimento dos ativos devido a falha no dimensionamento de carga nos Data Centers	Contatos da manutenção do FCB. Caso algum problema ocorra no Data Center do FCB. – Edneudo, Supervisor – 85 986081113 – Paulo Guedes – Chefe manutenção – 85 987849817 – David – Fiscal – 996437943 Ramais: 8108 (Edneudo), 8104 (Paulo) Manutenção do TJCE – César Duarte, matrícula: 7720, telefone do plantão: 98619-8977 Caso algum problema ocorra em Ar-condicionado: Empresa AR FRIO fone 30486639 Igor – 98777-8776 Vitor – 986661259 Contrato N° 18/2019 inciso IV, V e VI; paragrafo 7 (prazos); cláusula quarta (informação da gestão do contrato – Manutenção).
03 - Falha humana	Acidente ao manusear equipamentos, ou abastecimento do tanque de combustível do Grupo Gerador.	
04 - Indisponibilidade de rede/circuitos	Rompimento de fibra ótica decorrente de execuções obras públicas, desastres ou acidentes.	Cristiano Lima de Carvalho e Andrea Antunes de Carvalho – (85) 99957-9242 Heldir Sampaio Silva – (85) 988021162
05 - Falha de hardware nos Data Centers	Falha que necessite reposição de peça, ou reparo ou substituição do equipamento cujo reparo ou aquisição dependa de processo licitatório. (Será tratado de acordo com o estabelecido nos contratos que originou a aquisição de Hardware)	
06 - Ataque cibernético	Ataques que comprometam o desempenho, os dados ou configuração dos serviços essenciais. (Será tratado como Incidente de Segurança da Informação)	
07 - Ataques internos/Danos as instalações	Ataque aos ativos do DataCenter. Será tratado de acordo com os	**Para ocorrências no FCB**

(funcionários insatisfeitos)	procedimentos e planos estabelecidos pela Assistência Militar.	- Oficial de Serviço FCB: 85 98739-2336 - Recepção do FCB: 3492-8206 **** Para ocorrências no CDI** - Oficial de Serviço TJ: 85 98778-2167 - Recepção CDI: 3207-7436 - Recepção do TJ: 3207-7432
08 - Incêndio	Será tratado de acordo com os Planos da 8ª Seção de Bombeiro Militar, estabelecido pela Assistência Militar	- Oficial de Serviço FCB: 85 98739-2336 - Recepção do FCB: 3492-8206 - Cmt da 8a Cia de Bombeiros (Maj Erle): 85 98787-8836 **** Para ocorrências no CDI** - Oficial de Serviço TJ: 85 98778-2167 - Recepção CDI: 3207-7436 - Cmt da 8a Cia de Bombeiros (Maj Erle): 85 98787-8836 - Recepção do TJ: 3207-7432
09 - Desastres Naturais	Será tratado de acordo com os Planos da 8ª Seção de Bombeiro Militar, estabelecido pela Assistência Militar	- Oficial de Serviço FCB: 85 98739-2336 - Recepção do FCB: 3492-8206 - Cmt da 8a Cia de Bombeiros (Maj Erle): 85 98787-8836 **** Para ocorrências no CDI** - Oficial de Serviço TJ: 85 98778-2167 - Recepção CDI: 3207-7436 - Cmt da 8a Cia de Bombeiros (Maj Erle): 85 98787-8836 - Recepção do TJ: 3207-7432

Os Desastres mencionados no item 5 (cinco) poderão ser modificados sempre que for identificado alguma alteração nos procedimentos e contatos, cabendo ao Serviço de Segurança da Informação comunicar ao CGETIC.

6 Análise de riscos, responsáveis e procedimentos de recuperação e contingência

6.1 Após a identificação dos sistemas/ativos críticos, foram realizados análise de impacto para cada sistema/ativo.

6.2 Nesta versão foram revisados os planos de Continuidade dos serviços essenciais de TIC para o Sistema SAJ SG, e mantidos para o Sistema SAJ PG, DJe administrativo e Pje;

Sistema/Ativo	**Solução Sistema de Automação Judicial do Primeiro Grau SAJ-PG**						
Plano de Gestão de Incidentes/recuperação							
Risco e Probabilidade	**Resposta**	**Responsável**	**Tipo de Falha**	**Ação Preventiva**	**Ação de Contingência**	**Ação de Recuperação**	**Tempo estimado Até a recuperação**
Aplicação com Erro Impeditivo (médio)	Mitigar	Gerência de Informática do Fórum Clóvis Beviláqua/Coordenadoria de Suporte Técnico e Supervisor de Suporte e Monitoramento de Sistema	Aplicação com Erro Impeditivo	Plano de Continuidade - Aplicação com Erro Impeditivo SAJ PG			
Indisponibilidade do BD (baixa)	Mitigar		Indisponibilidade do BD	Plano de Continuidade - Indisponibilidade do Banco de Dados SAJ PG			

Sistema/Ativo	**Solução Sistema de Automação Judicial do Segundo Grau SAJ-SG**						
Plano de Gestão de Incidentes/recuperação							
Risco e Probabilidade	Resposta	Responsável	Tipo de Falha	Ação Preventiva	Ação de Contingência	Ação de Recuperação	Tempo estimado Até a recuperação
Aplicação com Erro Impeditivo (médio)	Mitigar	Gerência de Sistemas da Setin/Coordenadoria de Suporte Técnico	Aplicação com Erro Impeditivo	Plano de Gestão de Incidentes: aplicação com erro impeditivo;			
Indisponibilidade do BD	Mitigar		Indisponibilidade do BD	Plano de Gestão de Incidentes: indisponibilidade de banco de dados;			

(baixa)							

Sistema/Ativo	**Processo Judicial Eletrônico - PJe**						
Plano de Gestão de Incidentes/recuperação							
Risco e Probabilidade	Resposta	Responsável	Tipo de Falha	Ação Preventiva	Ação de Contingência	Ação de Recuperação	Tempo estimado Até a recuperação
Aplicação com Erro Impeditivo (médio)	Mitigar	Gerência de Sistemas da Setin/Coordenadoria do PJE/Coordenadoria de Suporte Técnico	Aplicação com Erro Impeditivo	Plano de Continuidade – Aplicação com Erro Impeditivo – Pje.odt			
Indisponibilidade do BD (baixa)	Mitigar		Indisponibilidade do BD	Plano de Continuidade – Indisponibilidade do Banco de Dados – Pje.odt			

Sistema/Ativo	**Diário da Justiça Eletronica - DJE**						
Plano de Gestão de Incidentes/recuperação							
Risco e Probabilidade	Resposta	Responsável	Tipo de Falha	Ação Preventiva	Ação de Contingência	Ação de Recuperação	Tempo estimado Até a recuperação
Aplicação com Erro Impeditivo (médio)	Mitigar	Gerência de Sistemas da Setin/Coordenadoria de Sistemas Judiciais/Coordenadoria de Suporte Técnico	Aplicação com Erro Impeditivo	PC GI Erro Impeditivo DJE Administrativo			
Indisponibilidade do BD (baixa)	Mitigar		Indisponibilidade do BD	PC GI Indisponibilidade do BD DJE Adm			

Os Planos mencionados no item 6 (seis) poderão ser modificados sempre que for identificado alguma alteração nos procedimentos e contatos, cabendo ao Serviço de Segurança da Informação comunicar ao CGETIC as alterações necessárias.

Outros Planos poderão ser acrescentados ao item 6 (seis) com prévia autorização do CGETIC.

7 Aprovações

Coordenadoria de Segurança da Informação

Comitê de Gestão de Tecnologia da Informação e Comunicação – CGETIC

Fortaleza, 25 de abril de 2023