TRIBUNAL REGIONAL ELEITORAL DA BAHIA
SECRETARIA DE TECNOLOGIA DA INFORMAÇÃO

Plano de Continuidade de Serviços de TIC

Referência:	PCS-DOC-2019-1
Versão:	1.2
Data:	16/08/2020
Autor:	Rilson Almeida
Proprietário:	Luciana Fonseca

Histórico de revisão

Versão	Data	Revisão do autor	Resumo de mudanças.
1.0	07/05/2018	Sidney Doria	Versão inicial.
1.1	09/09/2019	Rilson Almeida	1ª Revisão.
1.2	16/08/2020	Rison Almeida	2ª Revisão.

Distribuição

Nome	Cargo
Raimundo Vieira	Diretor Geral
Carla Lustosa	Secretária de Orçamento, Finanças e Contabilidade
Luciana Fonseca	Secretária de Tecnologia da Informação
Marta Gavazza	Secretária Judiciária
Maurício Amaral	Secretário de Planejamento de Estratégia e de Eleições
Robelza Rocha	Secretária de Gestão Administrativa e de Serviços
Sandra Cerqueira	Secretária de Gestão de Pessoas
Thais Habib	Secretária da Corregedoria
Victor Xavier	Secretário Especial da Presidência

Aprovação

Nome	Cargo	Data
Luciana Maria Freitas Fonseca	Secretária de Tecnologia da Informação	

Sumário

1. INTRODUÇÃO

Um Plano de Continuidade de Serviço de TIC é uma coleção de políticas, padrões, procedimentos e ferramentas através das quais uma organização poderá melhorar sua habilidade de responder a incidentes relacionados aos sistemas críticos. Também, a organização poderá melhorar sua resiliência a tais eventos, assegurando que sistemas críticos não falhem ou que falhem, mas possam ser recuperados em um tempo definido como tolerável.

Em termos normativos, este documento segue em caráter *lato* a NBR 15999, que padroniza a Gestão de Continuidade de Negócios (GCN) no Brasil e a recente normativo ABNT sobre Plano de Continuidade de Negócios, adotando em 2013 no Brasil as normas internacionais ISO 22301 e ISO 22313, formando o arcabouço brasileiro de normativas para Gestão de Continuidade de Negócios. Em caráter *strictu*, pontua-se a Norma Complementar 06/IN01/DSIC/GSIPR do Departamento de Segurança da Informação e Comunicações do Governo Federal e segue-se a Resolução CNJ nº 211/2015, em seu artigo 10º, §2º, que determina que seja estabelecido um Plano de Continuidade de Serviços críticos de TIC nos órgãos do Poder Judiciário, especialmente no que se refere aos serviços voltados à prestação jurisdicional.

Nesse contexto, é necessário definir preliminarmente junto à administração da organização quais são os sistemas críticos e quais são os tempos de retorno toleráveis para cada sistema, em caso de indisponibilidade. No Tribunal Regional Eleitoral da Bahia (TRE-BA), a Secretaria de Tecnologia da Informação (STI), o Comitê de Gestão de Tecnologia da Informação (CGesTIC), juntamente com o Comitê de Governança de Tecnologia da Informação (CGovTIC) tratam das políticas de definição, preservação e continuidade dos sistemas críticos.

Embora haja planos diversos para contingenciamento de sistemas críticos, por não estarem interconectados em um documento coeso, por não seguirem normativos oficiais e por não estarem formalmente publicados, são considerados conhecimento desestruturado e implícito.

Este documento, portanto, visa a apresentar as políticas e ações técnicas necessárias para prevenir e tratar incidentes em sistemas críticos no âmbito da Justiça Eleitoral da Bahia, através de um documento único, normatizado e formalmente publicado.

Seguindo os modelos normativos em vigor, além da introdução, este plano define na Seção 2 as Diretrizes do Programa de Continuidade de Negócios do TRE-BA. Na Seção 3 definem-se as atividades críticas do órgão. Na Seção 4 realiza-se a avaliação de riscos a que as atividades críticas estão expostas e são traçadas estratégicas de continuidade para cada atividade crítica. Apresentam-se na Seção 5 os planos de continuidade para cada serviço crítico de TIC. Por fim, na Seção 6 são apresentados os testes e as manutenções planejadas para os planos de continuidade.

2. DIRETRIZES DO PROGRAMA DE CONTINUIDADE DE NEGÓCIOS

Da análise do planejamento estratégico de TI do TRE-BA, são extraídos os objetivos estratégicos pertinentes que norteiam este documento, a saber:

- Prover infraestrutura e portfólio adequados às atividades do Tribunal;
- Implementar gestão de riscos em TIC
- Primar pela satisfação do usuário;
- Adotar padrões tecnológicos
- Aperfeiçoar governança e gestão de TIC
- Aprimorar segurança da informação

3. SERVIÇOS CRÍTICOS

Os seguintes serviços críticos foram definidos pelo CGovTIC, com base nos objetivos estratégicos institucionais constantes no Planejamento Estratégico Institucional:

Processo de Negócio	Serviço Crítico Vinculado	Gestão	Interessados
Prestação Jurisdicional	Sistema de Acompanhamento de Documentos e Processos (SADP)	CRE SJU	TRE-BA
	Processo Judicial Eletrônico (PJe)	SJU	TRE-BA
Cadastro Eleitoral e Partidário	Cadastro de Eleitores (ELO)	CRE	Eleitores Partidos TSE Zonas Eleitorais
Tramitação Administrativa	Processo Administrativo Digital (PAD) [1]	ASSESD	TRE-BA
	Sistema Eletrônico de Informações (SEI)	COM.SEI	
Comunicação Institucional	Sítio da Internet	COMINT	Eleitores Partidos Candidatos
	Correio Eletrônico	STI	TRE-BA

1 O PAD foi substituído pelo SEI (Sistema Eletrônico de Informações) em Abril/2020

4. RISCOS ÀS ATIVIDADES CRÍTICAS

Referencial para a análise de riscos:

Probabilidades:	**Impactos:**
1 – insignificante;	**1** – insignificante;
2 – baixa;	**2** – baixo;
3 – média;	**3** – médio;
4 – alta;	**4** – alto;
5 – muito alta.	**5** – muito alto.

Matriz Probabilidade X Impacto						
		Impactos				
		1	**2**	**3**	**4**	**5**
Probabilidades	**5**	5	10	15	20	25
	4	4	8	12	16	20
	3	3	6	9	12	15
	2	2	4	6	8	10
	1	1	2	3	4	5

Resultados da probabilidade X impacto:

Risco baixo: zona verde (resultados de 1 a 5);

Risco médio: zona amarela (resultados de 6 a 12);

Risco alto: zona vermelha (resultados de 15 a 25).

Os serviços críticos possuem as seguintes dependências e riscos associados :

Serviço Críticos	**Dependência**	Indisponibilidade		
		Probabilidade	Impacto	Risco
ELO	Linha de dados com o TSE	1	5	5
	Linha de dados para Zona Eleitoral	2	2	4
	Datacenter	1	5	5
PJe	Linha de dados com o TSE	1	4	4
	Linhas de dados com as Zonas	2	2	4
	Datacenter	1	4	4
	TSE (*Datacenter*)	1	5	5
Correio Eletrônico	Linha de dados com o TSE	1	5	5
	Datacenter	1	5	5
	Aplicação	1	5	5
Sítio da Internet	TSE (*Datacenter*)	1	5	5
SADP	*Datacenter*	1	5	5
	Aplicação	1	5	1
	Banco de Dados	1	5	5
SEI	*Datacenter*	1	5	5
	Aplicação	1	5	5
	Banco de Dados	1	5	5
	Linha de dados com o TSE	1	4	4

4.1 Estratégias de Continuidade para as Atividades Críticas

Para mitigar potenciais problemas com os serviços críticos, são necessários procedimentos, que preliminarmente precisam estar associados a papéis e responsáveis indicados.

4.1.1 Papéis e Responsabilidades

Responsável: Unidade indicada para elaborar e executar o plano de continuidade do serviço.

Consultado: Unidades que deverão ser consultadas antes do início da execução do plano de continuidade.

Externo: indicação se o TRE-BA possui dependência de serviços externos, sem a gerência direta do TRE-BA.

Contrato: indicação se o TRE-BA possui dependência de contratado para a continuidade do serviço.

Serviço Crítico	Dependência	Papéis e Responsabilidades			
		Responsável	Consultado	Externo	Contrato
ELO	Linha de dados com o TSE	TSE (SESOP)	-	SIM	-
	Linha de dados com Zona Eleitoral	SEINFRA	-		Oi/Brasil Telecom
	Datacenter	SEINFRA	CCME*	SIM	Manutenção Conteiner
PJe	Linha de dados com o TSE	TSE (SESOP)	-	SIM	-
	Linhas de dados com as Zonas	SEINFRA	-	-	Oi/Brasil Telecom
	Datacenter	SEINFRA	CCME*	-	HP
	TSE (*Datacenter*)	TSE (SESOP)	-	SIM	-
Correio Eletrônico	Linha de dados com o TSE	TSE (SESOP)	-	SIM	-
	Datacenter	SEINFRA	CCME*	-	HP
	Aplicação	SEINFRA SEDESC	CCME*	-	-
Sítio da Internet	TSE (*Datacenter*)	TSE (SESOP)	-	SIM	-
SADP	*Datacenter*	SEINFRA	CCME*	-	HP
	Aplicação	SEINFRA SEDESC	CCME*	-	-
	Banco de Dados	SEINFRA SEBDA	CCME*	-	-
SEI	*Datacenter*	SEINFRA	CCME*	-	HP
	Aplicação	SEINFRA SEDESC	CCME*	-	-
	Banco de Dados	SEBDA	CCME*	-	-
	Linha de dados com o TSE	TSE (SESOP)		SIM	

*Comitê Consultivo de Mudanças Emergenciais – Processo de Gerenciamento de Mudanças

5. PLANOS DE CONTINUIDADE DOS SERVIÇOS CRÍTICOS DE TIC

São apresentados a seguir os planos de continuidade para cada serviço crítico, com ações e procedimentos correspondentes a cada cenário identificado.

Para todos os planos, o nível de resposta é mitigação do incidente e a COSUP deve ser informada das indisponibilidades e prazos de retorno, para notificar adequadamente os usuários.

Os planos de contingência descritos aqui devem ser revisados em caso de mudança na composição dos sistemas críticos ou falha em algum teste da Seção 6.

5.1 Cadastro de Eleitores (ELO)

Cenário	Responsável	Ação Preventiva	Ação Corretiva
Linha de Dados com o TSE Indisponível	SEINFRA	Monitoramento Link secundário	Chamado ao TSE
Linha de Dados para Zona Eleitoral Indisponível	SEINFRA	Monitoramento Link secundário	Chamado à Oi/Brasil Telecom
***Datacenter* Indisponível**	SEINFRA	Monitoramento Redundância	Chamado SEMAC / Contratada manutenção Conteiner

5.2 Processo Judicial Eletrônico (PJe)

Cenário	Responsável	Ação Preventiva	Ação Corretiva
Linha de Dados com o TSE Indisponível	SEINFRA	Monitoramento Link secundário	Chamado ao TSE
Linha de Dados para Zona Eleitoral Indisponível	SEINFRA	Monitoramento Link secundário	Chamado à Oi/Brasil Telecom
***Datacenter* Indisponível**	SEINFRA	Monitoramento Redundância	Chamado SEMAC / Contratada manutenção Conteiner
TSE (*Datacenter*)	TSE (SESOP)	Monitoramento	Chamado ao TSE

5.3 Correio Eletrônico

Cenário	Responsável	Ação Preventiva	Ação Corretiva
Linha de Dados com o TSE Indisponível	SEINFRA	Monitoramento	Chamado ao TSE
***Datacenter* Indisponível**	SEINFRA	Monitoramento	Chamado SEMAC / Contratada manutenção Conteiner

Aplicação Indisponível	SEINFRA	Monitoramento	Manutenção Corretiva

5.4 Sítio da Internet

Cenário	Responsável	Ação Preventiva	Ação Corretiva
TSE (*Datacenter*)	TSE (SESOP)	Monitoramento	Chamado ao TSE

5.5 Sistema de Acompanhamento de Documentos e Processos (SADP)

Cenário	Responsável	Ação Preventiva	Ação Corretiva
***Datacenter* Indisponível**	SEINFRA	Monitoramento	Chamado SEMAC / Contratada manutenção Conteiner
Aplicação Indisponível	SEINFRA	Monitoramento	Manutenção Corretiva
Banco de Dados Indisponível	SEBDA	Monitoramento	Manutenção Corretiva Acionar SEINFRA (problemas c/backup)

5.6 Sistema Eletrônico de Informações (SEI)

Cenário	Responsável	Ação Preventiva	Ação Corretiva
***Datacenter* Indisponível**	SEINFRA	Monitoramento	Chamado SEMAC / Contratada manutenção Conteiner
Aplicação Indisponível	SEINFRA	Monitoramento	Manutenção Corretiva
Banco de Dados Indisponível	SEBDA	Monitoramento	Manutenção Corretiva Acionar SEINFRA (problemas c/ backup)
Linha de Dados com o TSE Indisponível	SEINFRA	Monitoramento Link secundário	Chamado ao TSE

6. TESTES E MANUTENÇÕES

Cada unidade responsável deverá elaborar e publicar plano de testes anual detalhado a cada mês de Dezembro do ano anterior à sua realização, seguindo a tabela de periodicidade abaixo.

Para cada um dos testes abaixo, cria-se uma condição de falha e mitigação. **Durante cada teste todos os sistemas críticos devem ter seu funcionamento aferido.**

Após cada teste, deve ser produzido e publicado um relatório com as ações realizadas, resultados obtidos e oportunidades de melhoria.

Os planos de contingência devem ser revistos no caso de alguma falha nos testes.

Cenário	Teste	Periodicidade	Unidade Responsável
Datacenter	Testes de desempenho e de acionamento da redundância	Anual	SEINFRA
Banco de Dados	Testes de restauração de cópia de segurança (parcial e total)	Anual	SEBDA SEINFRA

7. PLANO CONTÍNUO DE DESENVOLVIMENTO

Para a correta elaboração e manutenção do plano de continuidade dos serviços críticos de TIC, devem ser inseridos, de acordo com a necessidade, treinamentos específicos no plano anual de capacitação de TIC, visando às seguintes competências técnicas e gerenciais:

- Conscientização das equipes internas, apresentando as regras, as responsabilidades, os níveis de serviço mínimos e os procedimentos dos planos de continuidade;
- Soluções técnicas de continuidade de serviços de TIC;
- Processos para o gerenciamento de continuidade.