Plano de Continuidade de Serviços de TIC

Referência:	
Versão:	1
Data:	
Autor:	
Proprietário:	

Histórico de revisão

Versão	Data	Revisão do autor	Resumo de mudanças.
1.0	28/06/2019	Paulo Cesar Rodrigues	Versão inicial.

Distribuição

Nome	Cargo
Alex Caon Fin	Diretor Geral
Jonilton Alves de Oliveira	Secretário de Administração
Wanderlan Fonseca dos Santos Júnior	Secretário de Tecnologia da Informação
Jadilson Rubens de Castro Júnior	Secretário Judiciário
Nelson Amaro Júnior	Coordenador de Orçamento e Finanças
Raimundo Marques Júnior	Coordenador de Controle Interno
Elízio Ferreiro de Melo	Coordenador de Gestão de Pessoas
Pedro José Matos de Mendonça	Coordenador de Apoio Administrativo
Hermenegildo Ataíde D'Avila	Coordenador da Corregedoria

Aprovação

Nome	Cargo	Data
Wanderlan Fonseca dos Santos Júnior	Secretário de Tecnologia da Informação	

Sumário

1.1.1	INTRODUÇÃO.....	4
2	DIRETRIZES DO PROGRAMA DE CONTINUIDADE DE NEGÓCIOS	5
3	SERVIÇOS CRÍTICOS.....	6
4	RISCOS ÀS ATIVIDADES CRÍTICAS	7
4.1	ESTRATÉGIAS DE CONTINUIDADE PARA AS ATIVIDADES CRÍTICAS.....	8
4.1.1	<i>Papéis e Responsabilidades</i>	8
5	PLANOS DE CONTINUIDADE DOS SERVIÇOS CRÍTICOS DE TIC	9
5.1	CADASTRO DE ELEITORES (ELO).....	9
5.2	PROCESSO JUDICIAL ELETRÔNICO (PJE).....	9
5.3	CORREIO ELETRÔNICO.....	9
5.4	SÍTIO DA INTERNET	9
5.5	SISTEMA ADMINISTRATIVO DE DOCUMENTOS E PROCESSOS (SADP)	10
5.6	Sistema eletrônico de Informações (SEI).....	10
6	TESTES E MANUTENÇÕES.....	10
7	PLANO CONTÍNUO DE DESENVOLVIMENTO	11

1.1.1 INTRODUÇÃO

Um Plano de Continuidade de Serviços Críticos 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, **bem como a resiliência a tais eventos**, assegurando que sistemas críticos não falhem ou, **mesmo que falhem**, 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 o 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. **(verificar se realmente a ISO 22313 cancelou a NBR 15999)**

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 de **Roraima (TRE-RR)**, a Secretaria de Tecnologia da Informação (STI), o Comitê de Gestão de Tecnologia da Informação (**CGTIC**), juntamente com o Comitê de Governança de Tecnologia da Informação e Comunicação (CGovTIC) tratam das políticas de definição, preservação e continuidade dos sistemas críticos.

Muito embora existam diversos planos para contingenciamento de sistemas críticos, por não **se encontrarem** interconectados em um documento coeso, não seguem normativos oficiais e não estarem formalmente publicados, são considerados **como de conhecimento desestruturado e implícito**, **dificultando constatar com maior celeridade e eficiência qual plano é o mais adequado para cada tipo de problema** .

Um documento compilado, normatizado e formalmente publicado visa apresentar as políticas e ações técnicas necessárias para prevenir e tratar incidentes em sistemas críticos no âmbito da Justiça Eleitoral de **Roraima**.

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-RR**. Na Seção 3 **se encontram as definições das** atividades críticas do órgão. Na Seção 4 **estão dispostas as avaliações** de riscos a que as atividades críticas estão expostas, sendo traçadas estratégias 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 TIC do TRE-RR, são extraídos os objetivos táticos 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 do Planejamento Estratégico Institucional:

Processo de Negócio	Serviço Crítico Vinculado	Gestão	Interessados
Prestação Jurisdicional	Sistema de Acompanhamento de Documentos e Processos (SADP)	SJ	TRE-RR
	Processo Judicial Eletrônico (PJe) – 1º e 2º Grau	SJ e CRE	TRE-RR
Cadastro Eleitoral e Partidário	Cadastro de Eleitores (ELO)	CRE	Eleitores Partidos TSE Zonas Eleitorais
Tramitação Administrativa	SISTEMA LETRÔNICO DE INFORMAÇÃO (SEI)	CGS	TRE-RR Publico Externo
Comunicação Institucional	Sítio da Internet	CGI	TRE-RR Publico Externo
	Correio Eletrônico	STI	TRE-RR

4 RISCOS ÀS ATIVIDADES CRÍTICAS

Referencial para a análise de riscos:

Probabilidades: 1 – insignificante; 2 – baixa; 3 – média; 4 – alta; 5 – muito alta.	Impactos: 1 – insignificante; 2 – baixo; 3 – médio; 4 – alto; 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	4	5	20
	Linha de dados para Zona Eleitoral	4	5	20
	<i>Datacenter</i>	5	5	25
PJe	Linha de dados com o TSE	4	5	20
	Linhas de dados com as Zonas	4	5	20
	<i>Datacenter</i>	5	5	25
	TSE (<i>Datacenter</i>)	1	5	5
Correio Eletrônico	Linha de dados com o TSE	4	5	20
	<i>Datacenter</i>	5	5	25
	Aplicação	3	5	15
Sítio da Internet	TSE (<i>Datacenter</i>)	1	5	5
SADP	<i>Datacenter</i>	5	5	25
	Aplicação	2	5	10
	Banco de Dados	5	5	25
SEI	<i>Datacenter</i>	5	5	25
	Aplicação	4	5	20
	Banco de Dados	5	5	25

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 Responsáveis

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-RR possui dependência de serviços externos, sem a gerência direta do próprio tribunal.

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

Serviço Críticos	Dependência	Papéis e Responsabilidades			
		Responsável	Consultado	Externo	Contrato
ELO	Linha de dados com o TSE	TSE (SESOP)	-	SIM	-
	Linha de dados com Zona Eleitoral	SSO	-		Rádio
	<i>Datacenter</i>	SSO	CCME*	SIM	-
PJe	Linha de dados com o TSE	TSE (SESOP)	-	SIM	-
	Linhas de dados com as Zonas	SSO	-	-	Rádio
	<i>Datacenter</i>	SSO	CCME*	-	HP
	TSE (<i>Datacenter</i>)	TSE (SESOP)	-	SIM	-
Correio Eletrônico	Linha de dados com o TSE	TSE (SESOP)	-	SIM	-
	<i>Datacenter</i>	SSO	CCME*	-	HP
	Aplicação	SSO SAD	CCME*	-	-
Sítio da Internet	TSE (<i>Datacenter</i>)	TSE (SESOP)	-	SIM	-
SADP	<i>Datacenter</i>	SSO	CCME*	-	HP
	Aplicação	SSO SAD	CCME*	-	-
	Banco de Dados	SSO SAD	CCME*	-	-
SEI	<i>Datacenter</i>	SSO	CCME*	-	HP
	Aplicação	SSO SAD	CCME*	-	-
	Banco de Dados	SAD	CCME*	-	-

*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 CPS 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	SSO	Monitoramento	Chamado ao TSE
Linha de Dados para Zona Eleitoral Indisponível	SSO	Monitoramento	Chamado à Contratada
<i>Datacenter</i> Indisponível	SSO	Monitoramento	Chamado ao TSE

5.2 Processo Judicial Eletrônico (PJe)

Cenário	Responsável	Ação Preventiva	Ação Corretiva
Linha de Dados com o TSE Indisponível	SSO	Monitoramento	Chamado ao TSE
Linha de Dados para Zona Eleitoral Indisponível	SSO	Monitoramento	Chamado à Oi
<i>Datacenter</i> Indisponível	SSO	Monitoramento	Chamado à SSO
TSE (<i>Datacenter</i>)	TSE (SESOP)	Monitoramento	Chamado ao TSE

5.3 Correio Eletrônico

Cenário	Responsável	Ação Preventiva	Ação Corretiva
Linha de Dados com o TSE Indisponível	SSO	Monitoramento	Chamado ao TSE
<i>Datacenter</i> Indisponível	SSO	Monitoramento	Chamado à SSO
Aplicação Indisponível	SSO	Monitoramento	Manutenção Corretiva

5.4 Sítio da Internet

Cenário	Responsável	Ação Preventiva	Ação Corretiva
TSE (<i>Datacenter</i>)	TSE (SESOP)	Monitoramento	Chamado ao TSE

5.5 Sistema de Acompanhamento de Documentos e Processos (SADP)

Cenário	Responsável	Ação Preventiva	Ação Corretiva
Datacenter Indisponível	SSO	Monitoramento	Chamado ao TSE
Aplicação Indisponível	SSO	Monitoramento	Manutenção Corretiva
Banco de Dados	SAD	Monitoramento	Manutenção Corretiva

5.6 Sistema Eletrônico de Informações (SEI)

Cenário	Responsável	Ação Preventiva	Ação Corretiva
Datacenter Indisponível	SSO	Monitoramento	Chamado à SSO
Aplicação Indisponível	SSO	Monitoramento	Manutenção Corretiva
Banco de Dados	SAD	Monitoramento	Manutenção Corretiva

6 TESTES E MANUTENÇÕES

Cada unidade responsável deverá elaborar e publicar plano anual de testes detalhado, no mês de dezembro do ano anterior à sua realização, seguindo a tabela de periodicidade abaixo.

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

Após os testes, 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
Linha de Dados com o TSE	Testes de desempenho e de acionamento da redundância	Semestral	SSO TSE (SESOP)
Linha de Dados para Zona Eleitoral	Testes de desempenho e de acionamento da redundância	Semestral	SSO
Datacenter	Testes de desempenho e de acionamento da redundância	Anual	SSO

Banco de dados	Testes de desempenho e de acionamento da redundância.	Semestral	SAD SSO
	Testes de restauração de cópia de segurança (parcial e total)	Semestral	SAD SSO

7 PLANO CONTÍNUO DE DESENVOLVIMENTO

Para a correta elaboração e manutenção do plano de continuidade dos serviços críticos de TIC, devem ser inseridos 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 COBIT para o gerenciamento de continuidade.