TRIBUNAL REGIONAL ELEITORAL DO RIO GRANDE DO NORTE
PLANO DE AÇÃO PARA IMPLEMENTAÇÃO DO PROTOCOLO DE GERENCIAMENTO DE CRISES CIBERNÉTICAS
Resolução CNJ n.º 360/2020 - Portaria n.º 290/2020
versão 1.0

Etapas	Código	Item da Portaria	Atividade	Descrição / Objetivo Geral	Responsável	Período limite	Observações	Situação
Da Identificação da Crise Cibernética	1	Art. 6º	Definições dos pré-requisitos e parâmetros para identificação de uma crise cibernética	Relacionar possíveis danos que possam ser considerados relevantes para acionar o processo de gerenciamento de crise.	Comitê Gestor de Crises	Junho/2021		
Fases preparatória (pré-crise)	2	Art. 7º, VII	Definir o mínimo necessário para a continuídade de negócios	. Estabelecer e manter o Plano de Continuidade de Serviço de TIC(PCSTIC) e planos de recuperação que suporte a continuidade denegócio de TRE/RN . Realizar exercícios (regulares) de Análise de Impacto no Negócio (AIN) . Conduzir exercícios (de forma regular) de avaliação e gerenciamento derisco . Fornecer aconselhamento e orientação a todas as outras áreas denegócio e de TIC sobre questões relativas à continuidade e recuperação . Assegurar que os mecanismos adequados de continuidade erecuperação sejam implantados para alcançar ou superar as metasacordadas . Avaliar o impacto de todas as mudanças sobre o Plano de Continuidadede Serviço de TIC (PCSTIC) e os planos de recuperação de TIC . Assegurar que medidas proativas para melhorar a disponibilidade deserviços sejam implantadas sempre que o custo de implantação forjustificável . Negociar e acordar os contratos necessários com fornecedores para ofornecimento de recursos necessários à recuperação	COINF/STIE e COSIS/STIE	Já realizada	Portaria nº 177/2019 - GP instituiu a Gestão da Continuidade de Serviços Essenciais de TIC, no âmbito da JE/RN, incluindo Plano de Continuidade de Serviços Essenciais de TIC	CONCLUÍDO
	3	Art. 7º, IV	Avaliar continuamente os riscos a que atividades críticas estão expostas	. Instituir o processo de Gestão de Riscos da Segurança da Informação, no âmbito da Justiça Eleitoral do Rio Grande do Norte . O Processo de Gestão de Riscos da Segurança da Informação tem como objetivo principal minimizar a ocorrência de ameaças que podem interferir (negativamente) no recurso de informação utilizado pela organização para atingir os seus objetivos corporativos	SSI/COINF/STIE	Já realizada	Processo modelado e aprovado, faltando apenas a publicação da Portaria	CONCLUÍDO
	4	Art. 7º, II	definir as atividades críticas	Definir as atividades críticas que são fundamentais para a atividade finalística do órgão	Alta administração	Junho/2021		
	5	Art. 7º, III	identificar os ativos de informação críticos	Identificar os ativos de informação criticos que suportam as atividades primordiais, incluindo as pessoas, os processos, a infraestrutura e os recursos de tecnologia da informação	Comitê Gestor de Crises	Julho/2021		
	6	Art. 7º, V	Categorizar os incidentes e definir playbooks específicos	Categorizar os incidentes e estabelecer procedimentos de resposta específicos (playbooks) para cada tipo de incidente	COINF/STIE e COSIS/STIE	Dezembro/2021		

	7	Art. 7º, VI	Definir plano de contingência	Criar um plano de contingência, detalhando atividades críticas e ações necessárias para reestabelece-las.	COINF/STIE e COSIS/STIE	Já realizada	Portaria nº 177/2019 - GP instituiu a Gestão da Continuidade de Serviços Essenciais de TIC, no âmbito da JE/RN, incluindo Plano de Continuidade de Serviços Essenciais de TIC	CONCLUÍDO
	8	Art. 7º, VII	Definir cenários de simulações	Elaborar um cronograma de simulações, definindo cenários e testes para validação dos planos e procedimentos	COINF/STIE e COSIS/STIE	Dezembro/2021		
	9	Art. 8º	Criar Comitê de Crise	Criar um Comitê de Crises Cibernéticas formado por representante da Alta Administração e por representantes executivos, suportados pela Equipe de Resposta a Incidentes de Segurança Cibernética e por especialistas das áreas: I – Jurídica; II – Comunicação; III – Tecnologia da Informação; IV – Privacidade de Dados Pessoais; V – Segurança da Informação; VI – Unidades administrativas de apoio à contratação; e VII – Segurança Institucional.	Presidência	Março/2021		
	10	Art. 9º	Estruturar Plano de Gestão de Incidentes Cibernéticos, conforme ANEXO I	Elaborar um plano de gestão de incidentes ciberneticos contendo, no mínimo: Indicação do incidente cibernético, Descrição, Procedimento e Severidade	COINF/STIE e COSIS/STIE	Dezembro/2021		