TRIBUNAL REGIONAL ELEITORAL DO RIO GRANDE DO NORTE
PLANO DE AÇÃO PARA IMPLEMENTAÇÃO DO PROTOCOLO DE INVESTIGAÇÃO PARA ILÍCITOS CIBERNÉTICOS
Resolução CNJ n.º 362/2020 - Portaria n.º 291/2020
versão 1.0

Etapas	Código da	Item da Portaria CNJ	Atividade	Descrição / Objetivo Geral	Responsável	Período	Observações	Situação
Do objetivo	1	Art. 1º e 3º	Instituir o protocolo de investigação para ilícitos cibernéticos	Estabelecer os procedimentos básicos para coleta e preservação de evidências, e comunicar os fatos penalmente relevantes ao órgão de polícia judiciária	CPSI e NSPRES	Junho/2021		
Das definições	2	Art. 4º, XIV	Definir informação sigilosa	Elaborar Plano de Classificação Documental onde encontra-se a definição de informação sigilosa que necessite ser submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado, e aquelas abrangidas pelas demais hipóteses legais de sigilo.	CPAD	Já realizado	https://www.tre-rn.jus.br/transparencia-e-prestacao-de-contas/acesso-a-informacao/arquivos_informacoes-sigilosas/classificacao-informacao-grau-de-sigilo-2019-pdf	CONCLUÍDA
	3	Art. 4º, XV	Definir e avaliar a gerencia de logs	Criar/configurar um servidor de logs centralizado, para guardar todas as informções de acesso (de rede) relevantes	SRI/COINF/STIE	Já realizado		CONCLUÍDA
	4	Art. 4º, XVIII	Definição de método de geração de resumo criptográfico	Definir e adotar um método de geração de resumo criptográfico (hash) reconhecidamente eficiente para garantir a integridade das informações guardadas	SSI/COINF/STIE	Dezembro/2021		
Dos requisitos para adequação dos ativos de informação	5	Art. 5º	Garantir que todos os ativos de informação estejam sincronizados com a Hora Legal Brasileira	Garantir o sincronismo dos registros (logs) de todos os ativos de informação, para permitir maior precisão na verificação de informações	SRI/COINF/STIE	Já realizado		CONCLUÍDA
	6	Art. 6º	Configurar os ativos de informação de forma a registrar todos os eventos relevantes de Segurança da Informação e Comunicações (SIC)	Configurar os ativos para registrar eventos tais como: I- autenticação, tanto as bem-sucedidas quanto as malsucedidas; II – acesso a recursos e dados privilegiados; e III – acesso e alteração nos registros de auditoria.	SRI/COINF/STIE	Já realizado		CONCLUÍDA
	7	Art. 8º	Levantamento dos ativos de informação que não permitem registro de eventos	Mapear e documentar os ativos de informação que não permitem os registros de eventos quanto ao tipo e formato de registros de auditoria permitidos e armazenados.	SRI/COINF/STIE, SBDS/COSIS/STIE, SDS/COSIS/STIE	Junho/2021		
	8	Art. 9º	Adequar o nível de registro dos eventos no monitoramento dos sistemas e redes de comunicação	Garantir um detalhamento mínimo das informações disponíveis para diversos eventos de segurança, de modo a garantir identificar quem acessou, o que acessou, como e quando	SRI/COINF/STIE, SBDS/COSIS/STIE, SDS/COSIS/STIE	Junho/2021		
	9	Art. 9º, V	Instituição formal de política de senhas	Elaboração e formalização de política de senhas, com previsão de modificação periódica dos critérios mínimos necessários	CPSI	Junho/2021		
	10	Art. 9º, VI	Definir arquivos e sistemas críticos	Definir quais arquivos ou sistemas críticos devem ser monitorados, para registro de acessos e modificações	COINF/STIE e COSIS/STIE	Dezembro/2021		
	11	Art. 10	Revisar os registros históricos de eventos dos servidores de hospedagem de página eletrônica	Os servidores de hospedagem de página eletrônica, bem como todo e qualquer outro ativo de informação que assim o permita, devem ser configurados para armazenar registros históricos de eventos (logs) em formato que permita a completa identificação dos fluxos de dados.Os registros devem ser armazenados pelo período mínimo de seis meses, sem prejuízo de outros prazos previstos em normativos específicos.	COSIS/STIE	Junho/2021		