PLANO DE AÇÃO

Implantação dos Protocolos e Manuais elencados na

Portaria nº 162/2021-CNJ

SSI

SEÇÃO DE SEGURANÇA DA INFORMAÇÃO

CPSI

COMISSÃO PERMANENTE DE SEGURANÇA DA INFORMAÇÃO

NATAL - TRE/RN

Tribunal Regional Eleitoral-RN

Tribunal Regional Eleitoral-RN

TRIBUNAL REGIONAL ELEITORAL DO RIO GRANDE DO NORTE

PLANO DE AÇÃO EM SEGURANÇA DA INFORMAÇÃO

Secretaria de Tecnologia da Informação e Eleições
Coordenadoria de Infraestrutura Tecnológica
Seção de Segurança da Informação
Natal | 2023

INTRODUÇÃO

O Conselho Nacional de Justiça (CNJ), através da Portaria nº 162 de 10/06/2021 aprovou os Protocolos e Manuais criados pela Resolução CNJ nº 396/2021, que instituiu a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ).

Os protocolos e manuais aprovados por este ato deverão ser implementados por todos os órgãos do Poder Judiciário, com exceção do Supremo Tribunal Federal.

A norma contém os seguintes protocolos (Anexos I, II e III):

I – Prevenção de Incidentes Cibernéticos do Poder Judiciário (PPINC-PJ);

II – Gerenciamento de Crises Cibernéticas do Poder Judiciário (PGCRC-PJ); e

III – Investigação de Ilícitos Cibernéticos do Poder Judiciário (PIILC-PJ).

A norma contém os seguintes manuais (Anexos IV, V, VI e VII):

I – Proteção de Infraestruturas Críticas de TIC;

II – Prevenção e Mitigação de Ameaças Cibernéticas e Confiança Digital;

III – Gestão de Identidades; e

IV – Política de Educação e Cultura em Segurança Cibernética do Poder Judiciário.

IDENTIFICAÇÃO

NOME
Plano de Ação para Implementação dos Protocolos e Manuais aprovados na Portaria nº 162/2021-CNJ no âmbito do TRE/RN

PÚBLICO-ALVO	PREVISÃO DE INÍCIO
	99/99/9999

UNIDADE ADMINISTRATIVA
Presidência
UNIDADE SOLICITANTE
Secretaria de Tecnologia da Informação e Eleições (STIE)

HISTÓRICO DE REGISTRO			
DATA	**RESPONSÁVEL**	**DESCRIÇÃO**	**VERSÃO**
04/04/2022	Seção de Segurança da Informação/COINF/STIE e Coordenadoria de Infraestrutura Tecnológica/STIE	Elaboração de documento	1.0
14/06/2023	Seção de Segurança da Informação/COINF/STIE e Coordenadoria de Infraestrutura Tecnológica/STIE	Revisão de documento	2.0

JUSTIFICATIVA

Necessidade de implementação dos Protocolos e Manuais aprovados pelo Conselho Nacional de Justiça (CNJ) através da Portaria nº 162 de 10/06/2021, criados pela Resolução CNJ nº 396/2021, que instituiu a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ), no âmbito do Poder Judiciário.

OBJETIVOS

O Plano de Ação visa a implementação dos Protocolos e Manuais aprovados pelo Conselho Nacional de Justiça (CNJ) através da Portaria nº 162 de 10/06/2021, criados pela Resolução CNJ nº 396/2021, que instituiu a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ), no âmbito do Tribunal Regional Eleitoral do Rio Grande do Norte (TRE/RN).

ALINHAMENTO ESTRATÉGICO

O Plano de Ação está alinhado quanto ao:

Plano Estratégico da Justiça Eleitoral do RN 2021-2026 (PEJERN):

- Fortalecimento da segurança da informação – Objetivo Estratégico AC3
    - Promover o fortalecimento contínuo da segurança da informação no âmbito institucional – Iniciativa AC3.1;
    - Fortalecer a segurança cibernética assegurando o alinhamento às diretrizes do Poder Judiciário – Iniciativa AC3.2;
    - Aprimorar a infraestrutura tecnológica e os serviços em nuvem – Iniciativa AC3.3;
    - Fortalecer a gestão de riscos de incidentes de TIC – Iniciativa AC3.4 ;
    - Implementar mecanismos voltados à proteção de dados pessoais – Iniciativa AC3.5.

BENEFÍCIOS ESPERADOS

Este plano tem como resultados pretendidos:

- Formalizar este plano de ação ao TRE/RN;
- Estabelecer objetivos, princípios e diretrizes de Segurança da Informação, no âmbito do TRE/RN, alinhados às recomendações constantes das normas que trata sobre o tema;
- Regulamentar as normas que dispõe sobre a Estrutura de Gestão da Segurança da Informação, no âmbito do TRE/RN;
- Sensibilizar e conscientizar os servidores sobre a Segurança da Informação;
- Aprimorar a capacidade do Poder Judiciário, no âmbito do TRE/RN, de coordenar pessoas, desenvolver recursos e aperfeiçoar processos, visando minimizar danos e agilizar o restabelecimento da condição de normalidade em caso de ocorrência de ataques cibernéticos de grande impacto.

PRIORIZAÇÃO DAS AÇÕES

Este plano está adstrito a propor à administração do TRE/RN um conjunto inicial de ações estruturantes que visam a implementação dos Protocolos e Manuais aprovados pelo Conselho Nacional de Justiça (CNJ) através da Portaria nº 162 de 10/06/2021, criados pela Resolução CNJ nº 396/2021, que instituiu a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ).

A Segurança da Informação é um tema que envolve diferentes aspectos de uma organização, desde os locais onde a informação é guardada até recursos humanos e tecnológicos.

Abrange processos de trabalho, relação com fornecedores e prestadores de serviço, uso adequado das ferramentas e serviços de tecnologia da informação, cuidados com o ambiente de trabalho e publicação de normas que regulamentem o tema.

Diante dessas várias linhas de ação possíveis, a CPSI, Seção de Segurança da Informação/COINF/STIE junto com a Coordenadoria de Infraestrutura Tecnológica/STI dirigiu os esforços para ações voltadas à estruturação da gestão da Segurança da Informação, com a classificação dessas necessidades, resultando na seleção de um reduzido conjunto de ações prioritárias, formado por ações estruturantes e por ações de conformidade, consideradas passíveis de execução no espaço de tempo de dois anos a partir de sua propositura.

Nele constam as ações, essas categorizadas como estratégicas, vinculados às diretrizes prioritárias definidas no plano de gestão dos dirigentes do Tribunal, alinhadas ao plano estratégico, passando a compor o portfólio institucional do biênio respectivo.

AÇÕES RECOMENDADAS

Recomenda-se à Presidência do Tribunal Regional Eleitoral do Rio Grande do Norte a implementação de ações de conformidade, ações de sensibilização e conscientização.

ACOMPANHAMENTO DAS AÇÕES

Todas as ações serão acompanhadas pela estrutura de pessoal do Sistema de Gestão da Segurança da Informação.

O Sistema de Gestão de Segurança da Informação (SGSI) do TRE/RN inclui estratégias, planos, políticas, medidas, controles, e diversos instrumentos usados para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar a segurança da informação. Estabelecido, inicialmente, junto à estrutura de Governança Corporativa de Tecnologia da Informação e Comunicação, por meio da Resolução TRE/RN n. 12/2014, consolida-se como o conjunto de instrumentos estratégicos fundamentais para que a organização possa integrar a segurança da informação às suas políticas e objetivos estratégicos.

Seu objetivo é instituir diretrizes estratégicas, responsabilidades e competências visando à estruturação da segurança da informação; promover ações necessárias à implementação e à manutenção da segurança da informação; combater atos acidentais ou intencionais de destruição, modificação, apropriação ou divulgação indevida de informações, de modo a preservar os ativos de informação e a imagem da instituição; e promover a conscientização e a capacitação de recursos humanos em segurança da informação.

No TRE/RN, a estrutura de pessoal do Sistema de Gestão da Segurança da Informação é composta pela Comissão Permanente de Segurança da Informação (CPSI), instituída por meio da Resolução TRE/RN n.º 008/2009, a Equipe de Tratamento e Respostas a Incidentes em Redes Computacionais (ETIR), instituída por meio da Portaria n.º 423/2017, o Gestor de Segurança da Informação, designado através da Portaria DG n.º 45/2017 e, pela Seção de Suporte e Segurança da Informação (SSI), vinculada à Coordenadoria de Infraestrutura Tecnológica/STIE, criada após reestruturação estabelecida pela Resolução TRE/RN n.º 19/2019.

CRONOGRAMA - PROTOCOLO DE INCIDENTES CIBERNÉTICOS DO PODER JUDICIÁRIO - PPINC-PJ (ANEXO I)

PORTARIA Nº 162/2021-CNJ				
PROTOCOLO DE INCIDENTES CIBERNÉTICOS DO PODER JUDICIÁRIO - PPINC-PJ (ANEXO I)				
Artigo/ Inciso	**Ação**	**Responsável**	**Prazo**	**Situação**
2.1.1	.identificar os Serviços Essenciais de TICma	STIE	ago/23	Finalizada
2.1.3	.consolidar o uso das ferramentas de Cibersegurança adquiridas pelo TRE de acordo com a indicação de criticidade estabelecida pelo grupo nacional de segurança	STIE	jun/23	Finalizada
2.1.4	.elaborar o Plano de Gestão e Resposta a Incidentes Cibernéticos	SSI e ETIR	ago/23	Em andamento
2.1.4	.elaborar o Plano de Comunicação de Cibersegurança	DG e STIE	dez/24	Não iniciada
2.1.4	.elaborar o Plano de Mitigação	SSI	dez/24	Não iniciada
2.1.5	.elaborar o Plano de Restauração	ETIR	jun/25	Não iniciada
3.2.1	.criar a Base de Conhecimento de Defesa	ETIR	jun/24	Não iniciada
3.2.2	.capacitar as equipes técnicas sobre segurança cibernética	EJE e STIE	jun/22	Finalizada
3.2.2	.disseminar a cultura sobre segurança cibernética	EJE e STIE	jun/22	Finalizada
3.2.4	.revisar indicadores de Segurança da Informação	SSI	dez/23	Não iniciada
3.2.5	.incluir no Plano de Capacitação institucional, ações voltadas para segurança cibernética	EJE e STIE	dez/22	Finalizada
3.2.5	.revisar, periodicamente, os instrumentos de formação, capacitação e conscientização, utilizados dentro da organização	EJE e STIE	Ação Contínua	Finalizada
3.2.6	.implementar soluções automatizadas de segurança cibernética, visando medições confiáveis, escaláveis e contínuas	STIE	Ação Contínua	Finalizada
3.2.6	.priorizar as soluções automatizadas de segurança cibernética a serem adquiridas	STIE	dez/22	Finalizada
3.2.7	.elaborar o Plano de Resiliência	ETIR	dez/24	Não iniciada

4.1	.mapear o processo de Gestão de Incidentes de Segurança	SSI	jun/23	Finalizada
5.1	.instituir a Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética (ETIR)	STIE	dez/22	Finalizada
6.1	.publicar no sítio eletrônico do órgão o funcionamento da ETIR, regulado por documento formal de constituição, devendo constar, no mínimo, os seguintes pontos: a) definição da missão; b) público-alvo; c) modelo de implementação; d) nível de autonomia; e) designação de integrantes; f) canal de comunicação de incidentes de segurança; e g) serviços prestados.	ETIR	jul/22	Finalizada
7.2	.instituir a Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética (ETIR)	ETIR	dez/22	Finalizada
7.5.1	.elaborar o Plano de Gestão e Resposta a Incidentes Cibernéticos	SSI e ETIR	ago/23	Em andamento
7.5.2	.elaborar o Plano de Gestão e Resposta a Incidentes Cibernéticos	SSI e ETIR	ago/23	Em andamento
7.5.3	.elaborar o Plano de Gestão e Resposta a Incidentes Cibernéticos	SSI e ETIR	ago/23	Em andamento
7.5.4	.elaborar o Plano de Gestão e Resposta a Incidentes Cibernéticos	SSI e ETIR	ago/23	Em andamento
7.5.5	.elaborar o Plano de Gestão e Resposta a Incidentes Cibernéticos	SSI e ETIR	ago/23	Em andamento
7.5.6	.participar dos grupos locais e nacionais de identificação e resposta a ataques cibernéticos do Poder Judiciário	.participar dos grupos locais e nacionais de identificação e resposta a ataques cibernéticos do Poder Judiciário	jul/23	Finalizada

CRONOGRAMA - PROTOCOLO DE GERENCIAMENTO DE CRISES CIBERNÉTICAS DO PODER JUDICIÁRIO - PGCRC-PJ (ANEXO II)

PORTARIA Nº 162/2021-CNJ				
PROTOCOLO DE GERENCIAMENTO DE CRISES CIBERNÉTICAS DO PODER JUDICIÁRIO - PGCRC-PJ (ANEXO II)				
Artigo/ Inciso	**Ação**	**Responsável**	**Prazo**	**Situação**
4.1	.aprovar o Plano de Trabalho de Segurança da Informação e Proteção de Dados com cronograma de atividades em protocolo específico de Segurança Cibernética	COGESTIC	ago/23	Em andamento
4.2	.definir a Sala de Situação	STIE e DG	ago/23	Em andamento
4.2	.criar um Comitê de Crises Cibernéticas	STIE e DG	ago/23	Em andamento
4.3	.elaborar o Plano de Gestão e Resposta a Incidentes Cibernéticos	SSI e ETIR	ago/23	Em andamento
5.1	.implementar o Plano de Comunicação de Cibersegurança	DG e STIE	dez/23	Não iniciada
5.3	.elaborar o Plano de Continuidade dos Serviços Essenciais de TIC (Plano de Contingência)	COINF e COSIS	jun/23	Finalizada
5.4	.designar o responsável pela Chefia do Comitê de Crise, profissional indicado pelo Presidente do respectivo órgão do Poder Judiciário, com autoridade e autonomia para tomar decisões sobre conteúdo de comunicação a serem divulgados, bem como delegar atribuições, estabelecer metas e prazos de ações	PRES	ago/23	Não iniciada
5.9	.criar protocolo de comunicação de incidentes graves	DG e STIE	dez/23	Não iniciada
6.4	.elaborar o Relatório de Comunicação de Incidente de Segurança Cibernética, que contenha a descrição e o detalhamento da crise e o plano de ação tomado para evitar que incidentes similares ocorram novamente ou para que, em caso de ocorrência, se reduzam os danos causados	Comitê de Crise Cibernética	sob demanda	Finalizada

CRONOGRAMA- PROTOCOLO DE INVESTIGAÇÃO PARA ILÍCITOS CIBERNÉTICOS DO PODER JUDICIÁRIO - PIILC-PJ (ANEXO III)

PORTARIA Nº 162/2021-CNJ				
PROTOCOLO DE INVESTIGAÇÃO PARA ILÍCITOS CIBERNÉTICOS DO PODER JUDICIÁRIO - PIILC-PJ (ANEXO III)				
Artigo/ Inciso	**Ação**	**Responsável**	**Prazo**	**Situação**
1.1	.estabelecer os procedimentos básicos para coleta e preservação de evidências	ETIR	ago/23	Em andamento
1.1	.estabelecer os procedimentos básicos para comunicação obrigatória dos fatos penalmente relevantes ao Ministério Público e ao órgão de polícia judiciária com atribuição para o início da persecução penal	PRES, DG e STIE	jun/24	Não iniciada
2.1	.sincronizar o relógio interno dos ativos de tecnologia da informação, conforme a Hora Legal Brasileira (HLB), de acordo com o serviço oferecido e assegurado pelo Observatório Nacional (ON), de forma a garantir as configurações de: - data - hora - fuso horário	SRI	jun/22	Finalizada
2.3	.mapear o processo de Gerenciamento e Monitoramento de Logs	SRI	dez/23	Não iniciada
2.5	.aquisição de solução de *WAF (Web Application Firewall)* para atender a necessidade de proteção do perímetro das aplicações do TRE/RN, do ambiente de Rede do Tribunal [F5 BIGFIX] Solução de Firewall Camada 7 para proteção Aplicações WEB (WAF - Web Application Firewall) [NTSEC SOLUÇÕES EM TELEINFORMÁTICA]	STIE	ago/23	Em andamento
2.5	.aquisição de solução de Gerenciamento de Acessos Privilegiados (Cofre de Senhas) para dispositivos (ativos de rede, servidores físicos e virtuais e outros sistemas tecnológicos)	STIE	dez/22	Finalizada
2.5	.implantação da solução de *WAF (Web Application Firewall)*	SRI	jun/24	Não iniciada
2.5	.implantação da solução de Gerenciamento de Acessos Privilegiados (Cofre de Senhas) para dispositivos (ativos de rede, servidores físicos e virtuais e outros sistemas tecnológicos)	SRI	jun/23	Finalizada
2.8	Implantar ferramenta de Gestão de Patches e Ativos	SRI e SSI	jun/23	Finalizada

3.1	.estabelecer os procedimentos básicos para coleta e preservação de evidências durante o processo de tratamento do incidente penalmente relevante, onde deverá, sem prejuízo de outras ações, coletar e preservar: a) as mídias de armazenamento dos dispositivos afetados ou as suas respectivas imagens forenses; b) os dados voláteis armazenados nos dispositivos computacionais, como a memória principal (memória RAM); e c) todos os registros de eventos citados neste documento	ETIR	ago/23	Não iniciada
3.2	.estabelecer os procedimentos básicos para coleta e preservação de evidências nos casos de inviabilidade de preservação das mídias de armazenamento dos dispositivos afetados ou das suas respectivas imagens forenses, em razão da necessidade de pronto restabelecimento do serviço afetado, tais como: logs, configurações do sistema operacional, arquivos do sistema de informação, e outros julgados necessários, mantendo-se a estrutura de diretórios original e os "metadados" desses arquivos, como data	ETIR	ago/23	Não iniciada
3.5	.estabelecer nos procedimentos básicos de preservação de evidências ações que visem preservar os arquivos coletados, devendo-se: a) gerar arquivo que contenha a lista dos resumos criptográficos de todos os arquivos coletados b) gravar os arquivos coletados, acompanhados do arquivo com a lista dos resumos criptográficos descritos na alínea a deste subitem; e c) gerar resumo criptográfico do arquivo a que se refere a deste subitem"	ETIR	ago/23	Não iniciada
3.6	.estabelecer os procedimentos básicos para coleta de evidências durante o processo de tratamento do incidente penalmente relevante, onde todo material coletado deverá ser lacrado e custodiado pelo agente responsável pela ETIR, o qual deverá preencher Termo de Custódia dos Ativos de Informação	ETIR	ago/23	Não iniciada
3.7	.estabelecer os procedimentos básicos para coleta de evidências onde o material coletado deverá ficar à disposição da autoridade responsável pelo órgão do Poder Judiciário competente	ETIR	ago/23	Não iniciada
4.1	.estabelecer os procedimentos básicos para comunicação obrigatória dos fatos penalmente relevantes ao Ministério Público e ao órgão de polícia judiciária com atribuição para o início da persecução penal	PRES, DG e STIE	jun/24	Não iniciada
4.3	.estabelecer os procedimentos básicos para elaboração do Relatório de Comunicação de Incidente de Segurança Cibernética, descrevendo detalhadamente os eventos verificados, após a conclusão do processo de coleta e preservação das evidências do incidente penalmente relevante	ETIR	dez/23	Não iniciada
4.4	.estabelecer os procedimentos básicos para a elaboração do Relatório de Comunicação de Incidente de Segurança Cibernética, descrevendo detalhadamente os eventos verificados, após a conclusão do processo de coleta e preservação das evidências do incidente penalmente relevante, contendo as seguintes informações, sem prejuízo de outras julgadas relevantes: a) nome do responsável pela preservação dos dados do incidente, com informações de contato; b) nome do agente responsável pela ETIR e informações de contato; c) órgão comunicante com sua localização e informações de contato; d) número de controle da ocorrência; e) relato sobre o incidente que descreva o que ocorreu, como foi detectado e quais dados foram coletados e preservados; f) descrição das atividades de tratamento e resposta ao incidente e todas as providências tomadas pela ETIR, incluindo as ações de preservação e coleta, a metodologia e as ferramentas utilizadas e o local de armazenamento das informações preservadas;	ETIR	dez/23	Não iniciada

	g) resumo criptográfico dos arquivos coletados; h) Termo de Custódia dos Ativos de Informação Relacionados ao Incidente de Segurança; i) número de lacre de material físico preservado, se houver; e j) justificativa sobre a eventual inviabilidade de preservação das mídias de armazenamento dos dispositivos afetados, diante da impossibilidade de mantê-las.			
4.5	.estabelecer os procedimentos básicos para a elaboração do Relatório de Comunicação de Incidente de Segurança Cibernética, onde deverá ser acondicionado em envelope lacrado e rubricado pelo agente responsável pela ETIR, protocolado e encaminhado formalmente à autoridade responsável pelo órgão do Poder Judiciário afetado	ETIR	dez/23	Não iniciada
4.7	.estabelecer os procedimentos básicos para o encaminhamento formal, pela autoridade responsável pelo órgão do Poder Judiciário, a Comunicação de Incidente de Segurança em Redes Computacionais ao Ministério Público e ao órgão de polícia judiciária com atribuição para apurar os fatos, juntamente com o todo o material previsto neste protocolo, para fins de instrução da notícia crime	PRES	sob demanda	Não iniciada

CRONOGRAMA- MANUAL DE REFERÊNCIA - PROTEÇÃO DE INFRAESTRUTURAS CRÍTICAS DE TIC (ANEXO IV)

PORTARIA Nº 162/2021-CNJ				
MANUAL DE REFERÊNCIA - PROTEÇÃO DE INFRAESTRUTURAS CRÍTICAS DE TIC (ANEXO IV)				
Artigo/ Inciso	**Ação**	**Responsável**	**Prazo**	**Situação**
1.2	.adotar o Juízo 100% Digital visando viabilizar a execução de todos os atos processuais exclusivamente por meio eletrônico e remoto	DG e STIE	jun/23	Finalizada
1.3	.implantar no órgão os padrões mínimos visando a proteção de sua infraestrutura tecnológica	COINF e SSI	jun/23	Finalizada
1.3	.elaborar norma que trata sobre a Implantação e Gestão de Sistemas com foco na Segurança da Informação	COINF e COSIS	jul/23	Em andamento
1.3	.seguir as orientações organizacionais sobre a sua aplicação e observar a lista de controles mínimos exigidos para implantação dos padrões mínimos visando a proteção de sua infraestrutura tecnológica	COINF e SSI	jun/23	Finalizada

5.1	Implementar ferramentas de Cyber segurança definidas como prioridade 1 pelo grupo nacional de SI	COINF e COSIS	jun/23	Finalizada
5.2	.dar ciência sobre as orientações e os controles recomendados a todos os membros do órgão, sejam eles magistrados ou magistradas, servidores ou servidoras, colaboradores ou colaboradoras, fornecedores, prestadores ou prestadoras de serviços, estagiários ou estagiárias que, oficialmente, executem atividades relacionadas ao órgão	STIE	jul/22	Finalizada
5.2	.promover a divulgação da Política de Segurança da Informação, bem como ações para disseminar a cultura em segurança da informação	CPSI divulgar a PSI após a revisão	jul/23	Ação Contínua
5.2	Implantar a solução de Plataforma de Educação e Conscientização em Segurança da Informação, com simulação de Phishings	NEAD e STIE	jun/23	Finalizada
5.3	.criar a base mínima para a proteção de infraestruturas críticas de TI	STIE	jun/23	Finalizada
6.1	.instituir a nova Política de Segurança da Informação (PSI) no âmbito do Tribunal Regional Eleitoral do Rio Grande do Norte, observando como princípios norteadores a Eficiência, Ética, Impessoalidade, Legalidade, Moralidade e Publicidade	CPSI revisar PSI	jul/23	Finalizada
6.1	.promover a divulgação da Política de Segurança da Informação, bem como ações para disseminar a cultura em segurança da informação	CPSI divulgar após aprovação	jul/23	Em andamento
7.1	.implementar as soluções indicadas pelo grupo nacional de segurança cibernética como prioridade 1 para manter uma estrutura mínima de SI compatível com os outros TREs	STIE	jun/23	Finalizada
7.2	.Implementar solução de E-mail com proteção de dados e backup	SRI	dez/22	Finalizada
7.2	.implementar Solução de Backup		dez/21	Finalizada
7.3	.implementar Solução de Endpoint	SSI	dez/23	Finalizada
7.4	.direcionar e priorizar os esforços de segurança da informação a serem operacionalizados, conforme a sugestão de ordem de implantação, pela classificação por grupos, observando a sua aplicabilidade e aderência sempre validadas\adequadas para o contexto da organização	STIE	jun/22	Finalizada
7.6	.estruturar a Gestão da Segurança da Informação, no âmbito do TRE/RN	STIE	jun/22	Finalizada
7.7	.aplicar checklists, periodicamente (anualmente, pelo menos), buscando a adequação do TRE/RN ao atendimento dos requisitos mínimos estabelecidos pelo grupo nacional de segurança direcionado pelo TSE, que esses checklists tenham níveis de atendimento/maturidade, possibilitando a melhoria contínua da segurança digital de cada órgão	SSI	Ação Contínua	Finalizada

CRONOGRAMA - MANUAL DE REFERÊNCIA - PREVENÇÃO E MITIGAÇÃO DE AMEAÇAS CIBERNÉTICAS E CONFIANÇA DIGITAL (ANEXO V)

PORTARIA Nº 162/2021-CNJ				
MANUAL DE REFERÊNCIA - PREVENÇÃO E MITIGAÇÃO DE AMEAÇAS CIBERNÉTICAS E CONFIANÇA DIGITAL (ANEXO V)				
Artigo/ Inciso	**Ação**	**Responsável**	**Prazo**	**Situação**
0.1	.aprovar no plano de segurança um manual de referência para PREVENÇÃO E MITIGAÇÃO DE AMEAÇAS CIBERNÉTICAS E CONFIANÇA DIGITAL, em conformidade com o Comitê Gestor de Segurança Cibernética do Poder Judiciário (CGSCPJ)	STIE	jul/23	Finalizada
0.2	.orientar quanto a aplicação das melhores práticas de Segurança da informação	DG, STIE e EJE	dez/22 Ação contínua	Finalizada
3.1	.revisar o Sistema de Gerenciamento de Segurança da Informação (SGSI)	CPSI	dez/23	Não iniciada
4.1	.revisar o Sistema de Gerenciamento de Segurança da Informação (SGSI)	CPSI	dez/23	Não iniciada
5.1	.mapear o processo de Gestão de Riscos de Segurança da Informação	SSI	jun/23	Finalizada
7.1	.elaborar o Programa de Auditoria de sistema de gestão da segurança da informação	AUDI	dez/24	Não iniciada
11.1	.elaborar Política de Gestão de Riscos institucional	AGE	dez/24	Finalizada
11.4	.revisar o Processo de Gestão de Riscos de Segurança da Informação, observando-se as diretrizes fornecidas pela Associação Brasileira de Normas Técnicas (ABNT)	SSI	jun/23	Finalizada
12.1	.elaborar a Política Gestão de Riscos de Segurança da Informação, observando-se os seguintes princípios: a) Proteção dos valores organizacionais; b) Melhoria contínua da organização; c) Visão sistêmica; d) Qualidade e tempestividade das informações; e) Abordagem explícita da incerteza; f) Transparência;	CPSI	jun/24	Finalizada

	g) Dinamismo e interatividade; h) Alinhamento à gestão de riscos corporativos; i) Integração.			
13.1	.Mapear o processo de Gestão de Riscos de Segurança da Informação, observando-se as seguintes diretrizes: a) Ser parte integrante dos processos organizacionais de Tecnologia da Informação e Comunicação (TIC); b) Ser parte da tomada de decisões; c) Ser sistemático, estruturado e oportuno; d) Ser baseado nas melhores informações disponíveis; e) Considerar fatores humanos e culturais; f) Ser transparente e inclusivo; g) Ser dinâmico, interativo e capaz de reagir às mudanças tempestivamente; h) Contribuir para a melhoria contínua da organização.	SSI	jun/23 revisado	Finalizada
14.1	.elaborar a Política de Gestão de Riscos de Segurança da Informação, observando-se como objetivos: a) apoiar as unidades organizacionais no que tange aos riscos de segurança da informação em tecnologia da informação da organização; b) aprimorar o processo de tomada de decisão, com o propósito de incorporar a visão de riscos em conformidade com as melhores práticas; c) melhorar a alocação de recursos; d) aprimorar os controles internos; e) alinhar a tolerância a risco à estratégia adotada; f) resguardar a Administração Superior e os demais gestores da organização quanto à tomada de decisão e à prestação de contas; g) identificar, avaliar e reagir às oportunidades e ameaças; e h) melhorar a eficiência operacional por meio do gerenciamento de riscos proativos	CPSI	jun/24	Finalizada
15.1	.estabelecer uma estrutura de gestão de riscos de segurança da informação identificando pelo menos: a) a unidade dirigente de TIC do órgão; e b) os gestores de riscos	CPSI	jun/24	Não iniciada
15.2	.elaborar a Política de Gestão de Riscos de Segurança da Informação e definir como gestores de riscos, em seus respectivos âmbitos e escopos de atuação, os titulares das unidades responsáveis pelos serviços	CPSI	dez/24	Não iniciada
15.4	.elaborar a Política de Gestão de Riscos de Segurança da Informação e definir a gestão de riscos de segurança da informação de forma que seja de responsabilidade compartilhada de magistrados e magistradas, servidores e servidoras, estagiários e estagiárias, e prestadores e prestadoras de serviço, embora determinem-se papéis e responsabilidades específicas	CPSI	dez/24	Não iniciada
16.1	.aprovar a Política de Gestão de Riscos de Segurança da Informação e decidir sobre prioridades de atuação	Comitê de Governança de Tecnologia da Informação	dez/24	Não iniciada
17.1	.revisar a Política de Segurança da Informação (PSI) no âmbito da Justiça Eleitoral, observando-se que compete à unidade dirigente de TIC do órgão: I. disseminar a política de gestão de riscos de segurança da informação em suas unidades subordinadas; II. monitorar, avaliar, revisar e propor alterações na política de gestão de riscos de segurança da informação; III. monitorar o tratamento dos riscos; e IV. analisar e encaminhar o Relatório de Riscos de Segurança da Informação não tratados ao CGSI"	STIE	jul/23	Finalizada

18.1	.revisar Bienalmente a Política de Segurança da Informação (PSI) no âmbito da Justiça Eleitoral, observando-se que compete à unidade responsável pela Gestão de Segurança da Informação de TIC do TRE/RN as seguintes competências: I. propor as atualizações necessárias à presente política; II. monitorar o processo de gestão de riscos de segurança da informação	CPSI	jul/25	Finalizada
19.1	.determinar aos gestores de risco as seguintes competências: I. realizar a escolha dos processos de trabalho que devam ter os riscos gerenciados e tratados, tendo em vista a dimensão dos prejuízos que possam causar	DG e STIE	dez/24	Não iniciada
21.1.I	.estabelecimento de inventário de sistemas, serviços e ativos de Tecnologia da Informação e Comunicação do órgão que serão submetidos, periodicamente, à análise de segurança, buscando-se identificar vulnerabilidades técnicas que possam vir a comprometer os dados, os objetivos de negócio e/ou afetar a imagem institucional do órgão	SSI	jun/23	Finalizada
22.2	.indicar servidor da SSI para participar de grupo nacional de segurança da informação	SSI	jun/22	Finalizada
26.1	.revisar o Plano de Continuidade de Serviços Essenciais de TIC	STIE, COINF e COSIS	jun/23	Finalizada
32.1	.implantar solução de Gestão de Patches e Ativos	COINF	jun/23	Finalizada
34.1.a	.implantar a solução de Hiper Convergência e Alta Disponibilidade com site de backup em local divergente do datacenter principal	SRI	dez/22	Finalizada
34.1.b	.implantar a solução de Endpoint	SRI	jun/23	Finalizada
34.4.f	.implantar as soluções de: - Endpoint - Gestão de Patches e Ativos - Solução de Auditoria e Segurança para o *AD (Active Directory)* - Solução de Gerenciamento de Acessos Privilegiados para dispositivos (ativos de rede, servidores físicos e virtuais e outros sistemas tecnológicos)	SSI, SRI e SMI	jun/23	Finalizada
34.1.h	,implementar rotinas de monitoramento com a ferramenta utilizada para a análise de vulnerabilidades (*TENABLE.SC*)	SSI	dez/22	Finalizada
34.1.i	,implementar rotinas de monitoramento com as ferramentas utilizadas para a análise de vulnerabilidades (*TENABLE.SC*), Auditoria e Segurança para o *AD (Active Directory)* (*TENABLE.AD*) e *Endpoint* (*TREND*)	SSI e SRI	dez/23	Finalizada
34.1.f	.mapear o processo de Gerenciamento de Vulnerabilidades	SSI	jun/23	Finalizada

CRONOGRAMA - MANUAL DE REFERÊNCIA - GESTÃO DE IDENTIDADE E DE CONTROLE DE ACESSOS (ANEXO VI)

PORTARIA Nº 162/2021-CNJ				
MANUAL DE REFERÊNCIA - GESTÃO DE IDENTIDADE E DE CONTROLE DE ACESSOS (ANEXO VI)				
Artigo/ Inciso	**Ação**	**Responsável**	**Prazo**	**Situação**
1.1	.aprovar a criação de Manual de Referência - Gestão de Identidade e de Controle de Acessos	STIE	ago/23	Em andamento
1.2	.implantar a solução de Gerenciamento de Acessos Privilegiados	COINF e COSIS	jun/23	Finalizada
1.3	.definir na Política de Gestão de Identidades e de Controle de Acessos as responsabilidades dos titulares de contas individuais quanto à proteção de suas contas e ao uso adequado de suas autorizações, bem como aos operadores responsáveis pelo Gerenciamento de Identidade e Acesso para sistemas de informação	SSI e SRI	jun/22	Finalizada

CRONOGRAMA - MANUAL DE REFERÊNCIA - GESTÃO DE IDENTIDADE E DE CONTROLE DE ACESSOS (ANEXO VI)

PORTARIA Nº 162/2021-CNJ				
MANUAL DE REFERÊNCIA - GESTÃO DE IDENTIDADE E DE CONTROLE DE ACESSOS (ANEXO VI)				
Artigo/ Inciso	**Ação**	**Responsável**	**Prazo**	**Situação**
1.1	.aprovar a criação de Manual de Referência - Gestão de Identidade e de Controle de Acessos	STIE	ago/23	Em andamento
1.2	.implantar a solução de Gerenciamento de Acessos Privilegiados	COINF e COSIS	jun/23	Finalizada
1.3	.definir na Política de Gestão de Identidades e de Controle de Acessos as responsabilidades dos titulares de contas individuais quanto à proteção de suas contas e ao uso adequado de suas autorizações, bem como aos operadores responsáveis pelo Gerenciamento de Identidade e Acesso para sistemas de informação	SSI e SRI	jun/22	Finalizada
2.1.1	.adotar as diretrizes de práticas recomendadas para segurança cibernética do *Center for Internet Security Critical Security Controls for Effective Cyber Defense20*	STIE	dez/23	Não iniciada
2.3.1	.especificar os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão da segurança da informação dentro do contexto da organização	STIE	Ação Contínua	Ação Contínua
3.1	.dar publicidade a Política de Gestão de Identidades e de Controle de Acessos	STIE	ago/23	Não iniciada
3.2	.estabelecer, em normativo próprio, o regramento do órgão, considerando as boas práticas de segurança da informação e em observância às seguintes diretrizes: -definição de padrão de identidade do órgão, que contemple, no mínimo, os critérios para padronização de nome de usuário e de conta de e-mail -consideração do princípio de privilégio mínimo e de segregação de funções, visando a evitar acessos indevidos e reduzir os riscos de vazamento de informações; -estabelecimento de processo e de responsáveis por solicitação, gerenciamento e revogação de contas de acesso, preferencialmente de forma automática - utilização de login único para acesso a serviços de diretório corporativo e para acesso aos sistemas, com o objetivo de uniformizar e garantir a experiência única de interação e evitar a criação de contas e autorizações locais -adoção de modelo de controle de acesso, preferencialmente utilizando controle de acesso baseado em funções (RBAC) em que as credenciais recebam os privilégios de acesso conforme os papéis e as responsabilidades executadas pelos usuários -criação de processos de verificação de identidade nas interações entre sistemas,	STIE	jun/22	Finalizada

	internos ou externos, com vinculação das credenciais aos usuários e às suas autorizações -registro de trilhas de auditoria que vise ao registro dos acessos a sistema de informação, quais operações foram realizadas e em qual período -definição de requisitos de tamanho, reutilização, critérios de complexidade e período de expiração de senhas -empenho pela adoção de múltiplo fator de autenticação -busca pela unificação de plataformas de autenticação, autorização e autenticação (AAA) -estabelecimento de regras quanto ao acesso remoto e forma de disponibilização de sistemas e serviços na internet -gestão de credenciais privilegiadas e restrição ao uso de credenciais genéricas e de uso compartilhado -rastreabilidade de acessos e ações executadas por administradores de TI -utilização de mecanismos seguros de criptografia para o armazenamento e trânsito de credenciais de acesso -segregação de redes conforme o grupo dos serviços, sistemas ou usuários -controle do acesso físico aos ativos de tecnologia da informação e comunicação (TIC) -implementação de controles de acesso proporcionais à classificação da informação -monitoração dos acessos e tentativas de acesso para identificação de ataques			
4.1	.adotar o método de criação de conta, em um repositório central, com autenticação federada	COINF e COSIS	dez/23	Finalizada
4.2	. remover ou limitar o uso de contas compartilhadas	COINF e COSIS	jun/23	Finalizada
4.4	.limitar o uso de privilégios em contas com autorizações privilegiadas e desencorajar ou vetar o uso direto de contas compartilhadas com privilégios	COINF e COSIS	jun/23	Finalizada
6.1	.revisar a norma de controle de acessos aos sistemas informatizados	SRI	jul/23	Finalizada
6.1	.aquisição de solução de Gerenciamento de Acessos Privilegiados (Cofre de Senhas) para dispositivos (ativos de rede, servidores físicos e virtuais e outros sistemas tecnológicos)	STIE	dez/22	Finalizada
6.1	.implantação da solução de Gerenciamento de Acessos Privilegiados (Cofre de Senhas) para dispositivos (ativos de rede, servidores físicos e virtuais e outros sistemas tecnológicos)	SRI	dez/22	Finalizada
6.2	.instituir regras para a gestão de identidade e de controle de acessos físico e lógico ao ambiente cibernético do TRE/RN	COGESTIC	jul/23	Finalizada
6.2	.dar ciência às unidades envolvidas na concessão de autorizações da política de autorização da norma que trata sobre o controle de acesso aos sistemas informatizados	COGESTIC	jul/23	Finalizada
6.3.2.1	.exigir que as funções de aprovador administrativo e de aprovador técnico não sejam exercidas pela mesma pessoa ou, quando for o caso, que o custodiante de dados não desempenhe nenhuma dessas funções	COINF e COSIS	jul/23	Finalizada
6.3.4.1	.projetar e implantar soluções para possibilitar sistemas e aplicativos com remoção das autorizações e contas de uma pessoa nos momentos apropriados	COINF e COSIS	junho/22	Finalizada
7.1	.garantir na Política de Gestão de Identidades e de Controle de Acessos que os usuários devam: -criar senhas que estejam em conformidade com os critérios de senhas seguras estabelecidos pelo órgão -não compartilhar senhas relacionadas a algum sistema corporativo com qualquer outra pessoa -não reutilizar senhas relacionadas a qualquer sistema corporativo em contas pessoais -alterar imediatamente as senhas e notificar o gestor do sistema apropriado e/ou área de segurança da informação se houver motivos para acreditar que uma senha foi divulgada, acessada ou utilizada indevidamente por uma pessoa não autorizada	STIE	jul/23	Finalizada

	-utilizar os privilégios associados a uma conta apenas para a finalidade para a qual foram autorizados e nada mais -valer-se de contas e autorizações privilegiadas apenas quando tal privilégio for necessário para completar uma função -fazer logoff ou utilizar bloqueio de tela que exija autenticação ao deixar um dispositivo sem supervisão			
8.4	.aplicar periodicamente *checklists* ou listas de autoverificação implementadas pela organização (no mínimo com periodicidade anual) .estabelecer os níveis de maturidade nessa avaliação	STIE	mar/23	Finalizada
8.4	.aplicar periodicamente (no mínimo com periodicidade anual) *checklists* ou listas de autoverificação implementadas pela organização	STIE	mar/23	Finalizada
8.4	.estabelecer os níveis de maturidade na avaliação realizada através de *checklists* ou listas de autoverificação implementadas pela organização, de forma a possibilitar a melhoria contínua de normativos, processos e iniciativas em segurança cibernética da organização	STIE	mar/23	Finalizada

CRONOGRAMA - MANUAL DE REFERÊNCIA - POLÍTICA DE EDUCAÇÃO E CULTURA EM SEGURANÇA CIBERNÉTICA DO PODER JUDICIÁRIO (ANEXO VII)

PORTARIA Nº 162/2021-CNJ				
MANUAL DE REFERÊNCIA - POLÍTICA DE EDUCAÇÃO E CULTURA EM SEGURANÇA CIBERNÉTICA DO PODER JUDICIÁRIO (ANEXO VII)				
Artigo/ Inciso	**Ação**	**Responsável**	**Prazo**	**Situação**
0.1	.estabelecer as diretrizes necessárias consubstanciadas em ações permanentes de capacitação, de educação, de engenharia social e de formação de cultura especializada	EJE e STIE	jun/23	Finalizada
0.1	.implantar a solução de Plataforma de Educação e Conscientização em Segurança da Informação, com simulação de Phishings	NEAD e STIE	jun/23	Finalizada
0.2	.tratar o tema de formação de cultura e de educação em segurança cibernética de forma equânime, uniforme e articulada com todos os órgão do Poder Judiciário e em conformidade com os mais atualizados paradigmas, procedimentos e padrões nacionais e internacionais	STIE	jun/22	Finalizada
0.3	.incentivar a troca de experiências e conhecimentos, com participação de servidores do TRE/RN em fóruns multisetoriais e treinamentos ofertados por outros órgãos, na área de Segurança Cibernética	NEAD, STIE e SSI	ago/23	Em andamento
0.4	.desenvolver ações educacionais, no órgão, observando a diversidade e a multiplicidade de opções de cursos; programas de treinamento; modalidades de aquisição e disseminação de conhecimentos; formação técnica e gerencial; e plataformas tecnológicas educacionais presentes no mercado educacional contemporâneo	NEAD e STIE	Ação contínua	Ação Contínua
1.2.1.a	.incluir no plano de capacitação e de contração ações voltadas para melhoria da Segurança Cibernética	NEAD e STIE	dez/22	Finalizada
1.2.1.d	.dar ciência à todo usuário da Política de Segurança da Informação	NEAD e STIE	jul/22	Finalizada
1.2.1.e	.assegurar que novos conhecimentos atinentes ao tema da segurança cibernética sejam permanentemente ofertados aos profissionais das áreas de Tecnologia da Informação e Comunicação e de Segurança da Informação, técnico, gerencial, entre outros aplicáveis	NEAD e STIE	Ação contínua	Ação Contínua

PORTARIA Nº 162/2021-CNJ				
MANUAL DE REFERÊNCIA - POLÍTICA DE EDUCAÇÃO E CULTURA EM SEGURANÇA CIBERNÉTICA DO PODER JUDICIÁRIO (ANEXO VII)				
Artigo/ Inciso	**Ação**	**Responsável**	**Prazo**	**Situação**
2.1.1	.desenvolver ações de capacitação, formação, reciclagem, fomento e conscientização em segurança cibernética, podendo incluir, entre outras: a) programas de formação; b) programas de reciclagem; c) programas de extensão educacional; d) programas de pesquisa e fomento de natureza técnica, acadêmica e científica; e) elaboração de artigos, materiais e publicações de natureza técnica, acadêmica e científica; f) programas de intercâmbio, imersão e cooperação educacional; g) ações periódicas de capacitação; h) cursos em plataformas do tipo *MOOC – Massive Open Online Courses*; i) programas de certificação especializada; j) palestras, congressos, seminários e afins; k) concursos, competições e premiações; e l) *workshops*	EJE, NEAD e STIE	Ação contínua	Ação Contínua
3.3.1	.incluir nos planejamentos anuais, através das áreas de Comunicação Social e Institucional do órgão, programas de divulgação, conscientização, informação e esclarecimentos aos seus públicos-alvo, tanto internos como externos, referentes a temas de Segurança Cibernética	ASCOM, DG e STIE	Ação contínua	Ação Contínua
4.1.a	.garantir que os programas de formação, capacitação e reciclagem devem propiciar que o órgão possua: a) profissionais de Tecnologia da Informação e Comunicação e de Segurança da Informação em seus quadros, qualificados em segurança cibernética em nível de graduação, pós-graduação ou de certificações especializadas	EJE, NEAD e STIE	dez/22	Ação Contínua
4.1.b	.garantir que os programas de formação, capacitação e reciclagem devem propiciar que o órgão possua: b) todos os usuários internos com educação básica e cultura em segurança cibernética	NEAD e STIE	dez/23	Finalizada
4.2	.apresentar ao CNJ, no início do ano seguinte, relatório que comprove a efetividade das ações realizadas no exercício anterior e o respectivo desempenho dos usuários e profissionais treinados	DG e STIE	início de cada ano	Ação Contínua

CONSIDERAÇÕES FINAIS

Considerando os benefícios decorrentes das ações aqui propostas, bem como a proteção do conjunto de dados e informações corporativas, buscando garantir a sua disponibilidade, integridade e confiabilidade e o cumprimento da Política de Segurança da Informação e Comunicação vigente, manifesta-se a expectativa de que a Administração deste Tribunal acolha este Plano de Ação em Segurança da Informação, reconheça o seu caráter estratégico e, consequentemente, priorize a implementação das ações no âmbito do Tribunal Regional Eleitoral do Rio Grande do Norte (TRE/RN).