PLANO DE AÇÃO Nº 0609619 / 2023 - PRESI/DG/STI/ASPGOVTI

Plano de Ação: Implementação da Prevenção e Mitigação de Ameaças Cibernéticas e Confiança Digital

Plano de Ação 2023-2024

IMPLEMENTAÇÃO DOS ITENS DO MANUAL DE PREVENÇÃO E MITIGAÇÃO DE AMEAÇAS

1. APRESENTAÇÃO

Em resposta aos recentes episódios de ameaças cibernética sofridas por entes da Administração Pública, foi instituído o Comitê Gestor de Segurança Cibernética do Poder Judiciário, com o objetivo de apoiar os órgão do Judiciário com a implementação de padrões mínimos para proteção de sua infraestrutura tecnológica.

2. PADRÕES MÍNIMOS DE GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO

A gestão de riscos em âmbito corporativo é essencial para a boa governança, uma vez que fornece garantia razoável para que os objetivos organizacionais sejam alcançados. A integração da gestão de riscos à governança corporativa é apontada em diversos modelos de melhores práticas.

3. OBJETIVO GERAL

Implementação dos itens do Manual de Prevenção e Mitigação de Ameaças Cibernéticas e Confiança Digital, constantes do anexo V, da Portaria CNJ n. 162/2021.

4. REFERÊNCIA NORMATIVA

- Resolução CNJ no 370/2021, que institui a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD);
- Portaria CNJ n. 242/2020, que institui o Comitê de Segurança Cibernética do Poder Judiciário;
- Portaria CNJ n. 249/2020, que designa os integrantes do Comitê de Segurança Cibernética do Poder Judiciário (CSCPJ);

- Portaria TRE/AC n. 165/2023, que institui o Protocolo Protocolo de Prevenção de Incidentes Cibernéticos;
- Portaria TRE/AC n. 163/2023, que institui o Protocolo de Investigação para Ilícitos Cibernéticos;
- Portaria TRE/AC n. 156/2023, que institui o Protocolo Protocolo de Gerenciamento de Crises Cibernéticas;
- Recomendações constantes da norma técnica ABNT NBR ISO/IEC 27005:2019 – Gestão de Riscos de Segurança da Informação;
- MITRE ATT&CK , modelos e metodologia de ameaças;
- Norma ABNT NBR ISO/IEC 27000:2018, oferece visão geral dos sistemas de gerenciamento de segurança da informação e os termos e definições comumente usados na família de normas ISO/IEC 27001;
- Norma ABNT NBR ISO/IEC 27001:2013, especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão da segurança da informação dentro do contexto da organização;
- Norma ABNT/NBR ISO/IEC 27005:2019, fornece diretrizes para o processo de gestão de riscos de segurança da informação;
- Norma ABNT NBR ISO/IEC 27007:2018, Fornece diretrizes sobre como gerenciar um programa de auditoria de sistemas de gestão da segurança da informação (SGSI), sobre como executar as auditorias e sobre a competência dos auditores de SGSI6, em complemento às diretrizes descritas na norma ABNT NBR ISO/IEC 19011:2018;
- Norma ABNT NBR ISO/IEC 19011:2018, fornece orientação sobre a auditoria de sistemas de gestão, incluindo os princípios de auditoria, a gestão de um programa de auditoria e a condução de auditoria de sistemas de gestão, como também orientação sobre a avaliação de competência de pessoas envolvidas no processo de auditoria.
- Norma Complementar no 11/IN01/DSIC/GSIPR, de 2012, Estabelece diretrizes para avaliação de conformidade nos aspectos relativos à Segurança da Informação e Comunicações (SIC) nos órgãos ou entidades da Administração Pública Federal, direta e indireta (APF);
- NIST SP 800-160 Vol. 2, abordagem de Engenharia de Segurança de Sistemas;
- Resolução CNJ no 309/2020, aprova as Diretrizes Técnicas das Atividades de Auditoria Interna Governamental do Poder Judiciário (DIRAUD-Jud) e dá outras providências.

5. CAMPO DE APLICAÇÃO

- Tribunal Regional Eleitoral e Zonas Eleitorais do Estado do Acre.

6. FINALIDADE E METAS

Estabelecer as diretrizes estratégicas para aplicação dos controles de prevenção e mitigação de ameaças cibernéticas, buscando assegurar que as auditorias sobre segurança da informação cumpram pontos mais específicos desse tipo de auditoria, além de buscar caminhos para viabilizar auditorias cruzadas e terceirizadas.

7. PADRÕES MÍNIMOS DE GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO

Os padrões mínimos de Gestão de Riscos de Segurança são um conjunto de diretrizes que fornecem uma estrutura para a implementação de um programa de gestão de riscos eficaz. Esses padrões são geralmente baseados nas melhores práticas internacionais, conforme normas acima citadas.

8. ORÇAMENTO

As despesas relacionadas a esse plano que por ventura venham a ter gastos, serão providas com recursos provenientes do orçamento corrente do TRE-AC.

9. PLANO DE AÇÃO PARA UTILIZAÇÃO DOS CONTROLES PARA PREVENÇÃO E MITIGAÇÃO DE AMEAÇAS CIBERNÉTICAS E CONFIANÇA DIGITAL

Plano de Ação 2023-2024

Confiança digital, prevenção e mitigação de ameaças cibernéticas				
Ação 1	**(Referência - NBR 27.005:2019)**	**Setor Responsável**	**Previsão de conclusão**	**Situação**
Mapear processo de gestão de riscos de segurança da informação	• Estabelecer o Processo de Gestão de Riscos de Segurança Cibernética, chancelado pela administração superior. • Associar ao Sistema de Gestão de Segurança da Informação. • Possuir atividade de Estabelecimento de Contexto definida.	SCSEG/ (responsável) STI/ ASPGOVTI (auxiliar)	Novembro de 2023	Iniciado
	Definir subprocesso de Avaliação de Riscos que contempla atividade de Identificação, análise e avaliação de Riscos. Além dos critérios para: • Determinação do impacto/criticidade e probabilidade dos riscos de segurança cibernética estão definidos; • Aceitação de riscos de segurança cibernética estão definidos; • Atividade de Tratamento de Riscos definida; • Monitoramento e Análise Crítica definida; • Comunicação e Consulta definida • Revisado e atualizado periodicamente.	SCSEG/ (responsável) STI/ ASPGOVTI (auxiliar)	Abril de 2024	Não Iniciado

Previsões para a fiscalização da adequação dos requisitos de segurança inclusive sob contratação externa e/ou criação de rotina de auditorias cruzadas				
Ação 2	**(Referência - ISO 27007:2018)**	**Setor Responsável**	**Previsão de conclusão**	**Situação**
Atualizar plano de auditorias e procedimentos de auditoria em consonância com os controles estabelecidos pelo CNJ	Atualizar plano com os padrões mínimos recomendados no anexo I.	SCSEG/COCIN (responsáveis) STI/ ASPGOVTI (auxiliar)	Abril de 2024	Não inciado

Obs.: **Padrões mínimos recomendados para execução da Ação 2, devem seguir o cheklist do anexo I do Manual de Referência. Link < https://atos.cnj.jus.br/files/original135535202106146 0c75fd70e87f.pdf>**

Confiança digital, prevenção e mitigação de ameaças cibernéticas				
Ação 3	**(Referência - NBR 27.005:2019)**	**Setor Responsável**	**Previsão de conclusão**	**Situação**
Adotar mecanismos *(framework)* de resiliência cibernética.	Adotar mecanismos de resiliência cibernética que implementam as seguintes fases: • identificação de ameaças; • proteção de ativos; • detecção de ameaças; • recuperação e, • respostas a ameaças.	SCSEG/ (responsável) STI/ ASPGOVTI (auxiliar)	Abril de 2024	Iniciado

9. PREMISSAS E RESTRIÇÕES DO OBJETO

- Apoio da Administração, Diretoria Geral e Secretarias do Tribunal

- Disponibilidade orçamentária;

- Cumprimento dos prazos previamente fixados para realização das tarefas pelas unidades envolvidas;

- Comprometimento de todas as áreas impactadas;

Controle de versões:

Plano de Ação 2023-2025

versão preliminar 1.1

Responsável: STI/ASPGOVTI/ACSEG