SENADO FEDERAL
Gabinete do Senador NELSINHO TRAD

PLANO DE TRABALHO

AVALIAÇÃO DE POLÍTICAS PÚBLICAS
(RESOLUÇÃO Nº 44, DE 2013)

Tema: Avaliação da Estrutura Institucional e da Capacidade de Resposta do Sistema Nacional de Cibersegurança (Decreto nº 12.573/2025)

Relator: **SENADOR NELSINHO TRAD**

NOVEMBRO DE 2025

I. Introdução

A segurança e a defesa cibernética têm sido objeto de avaliações de políticas públicas pela Comissão de Relações Exteriores e de Defesa Nacional.

Em 2013, o Senado Federal instaurou Comissão Parlamentar de Inquérito (CPI) destinada a "investigar a denúncia de existência de um sistema de espionagem, estruturado pelo governo dos Estados Unidos, com o objetivo de monitorar e-mails, ligações telefônicas, dados digitais, além de outras formas de captar informações privilegiadas ou protegidas pela Constituição Federal".

Na Câmara dos Deputados, em 2015, foi instaurada CPI destinada a "investigar a prática de crimes cibernéticos e seus efeitos deletérios perante a economia e a sociedade neste país".

Em 2019, a Comissão de Relações Exteriores avaliou a política sobre defesa cibernética, e, como um dos resultados, criou-se esta Subcomissão Permanente de Defesa Cibernética.

Em 25 de abril de 2024, mediante o Requerimento nº 6, de 2024, a Comissão de Relações Exteriores e Defesa Nacional (CRE) decidiu avaliar a Política Nacional de Cibersegurança, o que foi impulsionado no âmbito da Subcomissão Permanente de Defesa Cibernética, instalada no dia 14 de maio de 2024.

Em 2025, pelo Requerimento CRE nº 5, de autoria do Senador Esperidião Amin, novamente se solicita avaliação da Política Pública Nacional de

Cibersegurança, o que será concentrada na análise do Decreto nº 12.573, de 4 de agosto de 2025.

A cibersegurança tem se tornado uma questão de extrema importância no Brasil, especialmente com o aumento das ameaças cibernéticas e a crescente dependência de tecnologias digitais. Este plano de trabalho tem como objetivo analisar a recente Estratégia Nacional de Cibersegurança, com um enfoque especial no Decreto nº 12.573, e discutir a interlocução com as autoridades envolvidas na sua implementação.

II. Análise do Decreto nº 12.573

O Decreto nº 12.573, de 4 de agosto de 2025, estabelece diretrizes e objetivos para fortalecer a cibersegurança no Brasil. Entre os principais pontos do Decreto, destacam-se a criação de um sistema nacional de resposta a incidentes cibernéticos e a implementação de medidas para proteger infraestruturas críticas. No entanto, algumas lacunas foram identificadas, como a necessidade de maior clareza nas atribuições dos órgãos envolvidos e a falta de recursos adequados para a execução das ações previstas.

A Estratégia Nacional de Cibersegurança, conhecida como E-Ciber 2025, apresenta uma visão abrangente para a proteção do ciberespaço brasileiro. A estratégia é dividida em eixos temáticos que incluem a prevenção, detecção, resposta e recuperação de incidentes cibernéticos. Comparada à E-Ciber 2020, a nova estratégia traz mudanças significativas, como a inclusão de novas tecnologias emergentes e a ênfase na cooperação internacional. Essas mudanças refletem a evolução do cenário cibernético e a necessidade de uma abordagem mais integrada e dinâmica.

III. Interlocução com as Autoridades Envolvidas

A implementação da E-Ciber envolve a colaboração de diversas autoridades e órgãos governamentais. O Comitê Nacional de Cibersegurança (CNCiber) desempenha um papel central na coordenação dessas ações, sendo responsável por definir políticas e diretrizes gerais. No entanto, a coordenação entre diferentes entidades ainda enfrenta desafios, como a sobreposição de competências e a necessidade de uma comunicação mais eficaz. A colaboração com o setor privado e a sociedade civil também é essencial para o sucesso da estratégia.

O Tribunal de Contas da União (TCU) realizou uma auditoria operacional para avaliar a implementação da E-Ciber. Entre os principais pontos levantados, destacam-se a necessidade de aprimorar a governança da cibersegurança e a de aumentar a capacitação dos profissionais da área. O TCU também fez recomendações para melhorar a alocação de recursos e a eficiência das ações de resposta a incidentes. As autoridades envolvidas têm trabalhado para responder a essas recomendações, implementando medidas para fortalecer a estrutura de cibersegurança do país.

IV. Proposta

Este plano de trabalho propõe analisar os principais aspectos da Estratégia Nacional de Cibersegurança e do Decreto nº 12.573. Também examina a interlocução entre as autoridades envolvidas e suas fragilidades, como a ausência de uma agência nacional dedicada ao tema. A cibersegurança é um desafio complexo que requer uma abordagem integrada e coordenada. A

implementação eficaz da E-Ciber é fundamental para proteger o ciberespaço brasileiro e garantir a segurança das infraestruturas críticas do país e esse é o principal ponto de análise proposto.