SENADO FEDERAL
GABINETE SENADOR NELSINHO TRAD

SENADO FEDERAL

COMISSÃO DE RELAÇÕES EXTERIORES E DE DEFESA NACIONAL

RELATÓRIO DE ANÁLISE DO DECRETO Nº 12.573 DE 4 DE AGOSTO DE 2025, QUE INSTITUI A NOVA ESTRATÉGIA NACIONAL DE CIBERSEGURANÇA (E-CIBER)

RELATOR: SENADOR NELSINHO TRAD

Brasília, 6 de dezembro de 2025

Senado Federal – Anexo II – Ala Senador Afonso Arinos – Gabinete 6 – CEP 70165-900 – Brasília DF
Telefone: +55 (61) 3303-9050 – E-mail: sen.fabianocontarato@senado.leg.br

SUMÁRIO

SENADO FEDERAL
Gabinete do Senador NELSINHO TRAD

O Decreto nº 12.573, de 4 de agosto de 2025, institui a nova Estratégia Nacional de Cibersegurança (E-Ciber), destacando a importância da segurança e defesa cibernética no Brasil. A Política Nacional de Cibersegurança (PNCiber), estabelecida pelo Decreto nº 11.856, de 26 de dezembro de 2023, visa promover o desenvolvimento de tecnologias nacionais, garantir a confidencialidade e integridade dos dados, fortalecer a resiliência das organizações, combater crimes cibernéticos e desenvolver a educação e capacitação em segurança cibernética. O presente documento analisa essa normativa, bem como aborda a criação de uma estrutura institucional robusta, a avaliação do Tribunal de Contas da União (TCU) sobre o assunto, a ausência ainda do Plano Nacional de Cibersegurança, ações legislativas e a necessidade de uma abordagem integrada e coordenada para enfrentar as ameaças cibernéticas, propondo mudanças significativas na política pública para garantir a segurança digital do país.

1. Introdução

A segurança e a defesa cibernética têm sido objeto de avaliações de políticas públicas pela Comissão de Relações Exteriores e de Defesa Nacional, que, dentre seus objetivos, de acordo com a Resolução do Senado Federal n° 44, de 2013, está o de adequar os dispositivos normativos em vigor.

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 Comissão Parlamentar de Inquérito (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, resultou na criação dessa 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 Espiridião 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.

Em termos normativos e institucionais, devemos destacar a criação do Comitê Gestor da Internet do Brasil (CGI.br), em 1995 e aperfeiçoado em 2003 (Decreto nº 4.829/2003); do Centro de Atendimento a Incidentes de Segurança (Cais) em 1997; do Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br); o Decreto nº 3.505, de 2000, que instituiu a Política de Segurança da Informação, revogado pelo Decreto nº 9.637, de 2018 (alterado, por sua vez, pelos Decretos nº 9.832, de 2019, nº 10.631, de 2021; nº 10.641, de 2021; nº 10.849, de 2021; e nº 11.856, de 2023, e revogado pelo Decreto nº 12.572, de 2025); o Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos, em 2004 (Ctir Gov); o Estatuto NIC.br (Núcleo de Informação e Coordenação do Ponto BR) em 2005; a Lei de Acesso à Informação (Lei nº 12.527, de 2011); o Núcleo de Segurança e Credenciamento (Decreto nº 7.845, de 14 de novembro de 2012); o Marco Civil da Internet (Lei nº 12.965, de 2014); a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709, de 2018); a competência do GSI em matéria de segurança cibernética (Lei nº 13.844, de 2019); o Decreto nº 10.222, de 2020, que aprovou a Estratégia Nacional de Segurança Cibernética, válida para o quadriênio 2020-2023, e foi revogado pelo Decreto nº 12.573, de 4 de agosto de 2025; a Rede Federal de Gestão de Incidentes Cibernéticos - Regic (Decreto nº 10.748, de 2021); o Centro Integrado de

Segurança Cibernética - Cisc (Portaria SGD/MGI nº 852, de 28 de março de 2023); e o Decreto nº 11.856, de 2023, instituiu a Política Nacional de Cibersegurança e o Comitê Nacional de Cibersegurança.

2. Política Nacional de Cibersegurança

A Política Nacional de Cibersegurança – PNCiber foi estabelecida pelo Decreto nº 11.856, de 26 de dezembro de 2023, cujo art. 2º estabelece os princípios fundamentais que orientam as ações do Estado brasileiro na área de segurança digital. Em primeiro lugar, destaca-se a soberania nacional e a priorização dos interesses do país como pilares essenciais para a formulação e execução de políticas cibernéticas.

Outro princípio relevante é a garantia dos direitos fundamentais, com ênfase na liberdade de expressão, na proteção de dados pessoais, na preservação da privacidade e no acesso à informação. Esses direitos devem ser resguardados mesmo diante de medidas voltadas à segurança cibernética.

A prevenção de incidentes e ataques cibernéticos é também um foco central, especialmente aqueles que possam comprometer infraestruturas críticas e serviços essenciais à população. Para isso, é fundamental fortalecer a resiliência das organizações públicas e privadas, garantindo que estejam preparadas para enfrentar e se recuperar de tais ameaças.

Além disso, a PNCiber valoriza a educação e o desenvolvimento tecnológico voltado à segurança cibernética, reconhecendo a importância da capacitação e da inovação nesse campo. A cooperação entre órgãos e entidades, tanto públicas quanto privadas, é incentivada como forma de promover uma atuação coordenada e eficaz. Por fim, ressalta-se a relevância da cooperação técnica internacional, reconhecendo que os desafios cibernéticos transcendem fronteiras e exigem esforços conjuntos entre nações.

Já os objetivos da PNCiber são: promover o desenvolvimento de produtos, serviços e tecnologias de caráter nacional destinados à segurança cibernética; garantir a confidencialidade, integridade, autenticidade e disponibilidade das soluções e dos dados utilizados para o processamento, o armazenamento e a transmissão eletrônica ou digital de informações; fortalecer a atuação diligente nos ciberespaços, especialmente das crianças, dos adolescentes e dos idosos; contribuir para o combate aos crimes cibernéticos e às demais ações maliciosas nos ciberespaços; estimular a adoção de medidas de proteção cibernética e de gestão de riscos para prevenir, evitar, mitigar, diminuir e neutralizar vulnerabilidades, incidentes e ataques cibernéticos e seus impactos; incrementar a resiliência das organizações públicas e privadas a incidentes e ataques cibernéticos; desenvolver a educação e a capacitação técnico-profissional em segurança cibernética na sociedade; fomentar as atividades de pesquisa científica, de desenvolvimento tecnológico e de inovação relacionadas à segurança cibernética; incrementar a atuação coordenada e o intercâmbio de informações de segurança cibernética entre União, Estados, Distrito Federal e municípios, os Poderes Executivo, Legislativo e Judiciário, o setor privado e a sociedade em geral; desenvolver mecanismos de regulação, fiscalização e controle destinados a aprimorar a segurança e a resiliência cibernéticas nacionais;

implementar estratégias de colaboração para desenvolver a cooperação internacional em segurança cibernética.

Os instrumentos estabelecidos na política são a Estratégia Nacional de Segurança e o Plano Nacional de Cibersegurança. O Comitê Nacional de Cibersegurança tem por finalidade propor atualizações para o PNCiber, em relação a Estratégia Nacional de Cibersegurança, e elaborar o Plano Nacional de Cibersegurança; avaliar e propor medidas para incremento da segurança cibernética; formular proposta para o aperfeiçoamento da prevenção, detecção, análise e resposta às ameaças cibernéticas; propor medidas para o desenvolvimento da educação e segurança cibernética; promover interlocução com entes federativos; propor estratégias de colaboração para o desenvolvimento da cooperação técnica internacional; manifestar-se por solicitação do Presidente da Creden (Câmara de Relações Exteriores e Defesa Nacional) sobre assuntos relacionados à segurança cibernética.

O Comitê possui 25 (vinte e cinco) integrantes: o Gabinete de Segurança Institucional, a Controladoria-Geral da União, a Casa Civil, o Ministério do Desenvolvimento, Indústria, Comércio e Serviços; o Ministério da Fazenda, o Ministério da Defesa, o Ministério da Educação, o Ministério da Justiça e Segurança Pública, o Ministério das Comunicações, o Ministério da Ciência, Tecnologia e Inovação, o Ministério das Relações Exteriores, o Ministério de Minas e Energia, o Ministério da Gestão e da Inovação em Serviços Públicos; o Comitê Gestor da Internet, a Anatel e o Banco Central; e mais nove integrantes, sendo três de entidades da sociedade civil, três de instituições científicas e tecnológicas de inovação e três de entidades do setor empresarial, todos, logicamente, relacionados à segurança cibernética.

Os três grupos de trabalho do Comitê têm por finalidade atualizar a Estratégia Nacional de Cibersegurança, coordenado pelo Comitê Gestor da Internet no Brasil, o que foi feito; para definir os parâmetros de atuação internacional do Brasil em cibersegurança, sob coordenação do Ministério das Relações Exteriores; e um terceiro grupo, sobre governança, com a tarefa de elaboração da proposta de projeto de lei para a criação de um órgão para a governança da cibersegurança, possivelmente uma Agência Nacional de Cibersegurança ou um centro, e está a cargo do Ministério da Gestão e da Inovação em Serviços Públicos e da Anatel.

A Política Nacional de Cibersegurança foi instituída pelo Decreto nº 11.856, de 26 de dezembro de 2023, porém, a ideia original não era essa. Houve, meses antes, o debate sobre anteprojeto do Poder Executivo que pretendia instituir por lei a Política Nacional de Cibersegurança, o Sistema Nacional de Cibersegurança e a agência que regularia as atividades de cibersegurança no País.

Esse anteprojeto foi submetido a audiência pública, na manhã do dia 16 de maio de 2023, atendendo a convite do Ministro Marcos Antônio Amaro, do Gabinete de Segurança Institucional da Presidência da República (GSI), que aconteceu no auditório do Anexo I do Palácio do Planalto. Segundo o plano original, as manifestações e sugestões feitas na oportunidade seriam sistematizadas e até o mês de agosto de 2023 a proposição deveria ser enviada ao Parlamento para análise.

De acordo com a exposição de motivos desse anteprojeto, a Política Nacional pretendida seria:

> "uma proposta voltada a unificar a "colcha de retalhos" regulatória existente no país, minimizar o crescente número de incidentes que acometem o país, gerando enormes prejuízos para a sociedade brasileira, buscar diminuir o débito tecnológico nacional no setor, e ampliar a participação brasileira na cooperação internacional sobre a temática"

O modelo proposto segue, em termos gerais, a Diretiva NIS2 do Parlamento Europeu (igualmente foram considerados o documento pertinente da União Internacional de Telecomunicações - UIT/ONU; o Modelo de Maturidade da Universidade de Oxford, adotado pela OEA; o relatório do TCU de 2022 sobre a Lista de Alto Risco na Administração Pública; as recomendações do Senado Federal; o relatório da CPI da Espionagem Cibernética de 2014; a avaliação de política pública da CRE, de 2019; e proposições legislativas de ambas as casas do Congresso Nacional), com existência de um órgão central nacional, que seria a Agência Nacional de Cibersegurança, de um "ente" fiscalizador, no caso vinculado ao Gabinete de Segurança Institucional, o Comitê Nacional de Cibersegurança e um Gabinete de Gerenciamento de Cibercrises.

Outro ponto importante foi o objeto prioritário dessa política, que deixa de ser focada em infraestruturas críticas identificadas, para se dedicar a transversalidade da cibersegurança, com ênfase em serviços essenciais para o bom funcionamento da sociedade. Setores como fornecimento de água urbana; barragens; biossegurança; radiodifusão; serviços postais; telecomunicações; defesa; eletricidade; óleo e gás; financeiro; bem como transporte aéreo, aquaviário e terrestre são considerados como infraestruturas críticas, mas isso não abrangem vários outros, como justiça, saúde, educação, por exemplo. Incluir esses novos setores como infraestruturas críticas não solucionaria, pois sempre aparecerá outro. Portanto, o conceito de serviços essenciais é mais adequado.

Esse anteprojeto foi versado em 44 artigos, disposto do seguinte modo: Capítulo I - Da Política Nacional de Cibersegurança [Seção I - Disposições Gerais (Arts. 1º - 4º), Seção II - Dos Princípios (Art. 5º), Seção III Dos Objetivos (Art. 6 º), Seção IV - Das Diretrizes (Arts. 7 º - 9º), Seção V - Dos Instrumentos (Art. 10)]; Capítulo II - Do Sistema Nacional de Cibersegurança (Arts. 11-12) [Seção I - Do Comitê Nacional de Cibersegurança (Arts. 13 – 16), Seção II - Da Agência Nacional de Cibersegurança (Arts. 17-19), Seção III - Do Gabinete de Gerenciamento de Cibercrises (Art. 20-25)]; Capítulo III - Da Estratégia Nacional de Cibersegurança (Arts. 26-27); Capítulo IV - Do Plano Nacional de Cibersegurança (Arts. 28-29); Capítulo V - Da Cooperação Internacional (Art. 30); Capítulo VI - Do Ensino, Pesquisa, Desenvolvimento e Inovação Tecnológica em Cibersegurança (Arts. 31-36); Capítulo VII - Disposições Finais e Transitórias (Art. 37-44).

Do ponto de vista de construção legislativa, havia desequilíbrio no texto do anteprojeto. Apresentava capítulo com dez artigos (capítulo I) e outro com um artigo (capítulo V), além de ter capítulo dividido em seções que inicia com dois artigos "soltos" antes da Seção I, no caso o Capítulo II, o que deveria compor outra Seção, a de Disposições Gerais, tal qual o feito no Capítulo I.

Além disso, o texto se encerra com a imprópria norma de revogação genérica: *Art. 44. Revogam-se todas as disposições em contrário ao disposto nesta Lei*. De acordo com o Art. 9º da Lei Complementar nº 95, de 26 de fevereiro de 1998, a cláusula de revogação deverá enumerar, expressamente, as leis ou disposições legais revogadas.

Sobre o conteúdo do anteprojeto, o Art. 4º traz conceituações chaves, dentre as quais a da própria cibersegurança, no seu inciso XIV, que seria o

conjunto de ações voltadas à confidencialidade, integridade, autenticidade e disponibilidade de ciberativos. Sugerimos incluir a proteção às pessoas no conceito.

Por ciberativo, o inc. I do mesmo artigo conceitua como envolvendo *hardware, software ou dados utilizados para o processamento e transmissão eletrônicos de informações*.

Com o objetivo de completar o conceito jurídico de ciberativo, abrangendo outros ativos não contemplados anteriormente e colocando as pessoas como foco central, sugerimos o seguinte:

Art. 4º

I - ciberativo (ou ativo cibernético): hardware, software, dados, conjunto de dados, códigos, sistemas de computação, redes de computadores ou informações utilizadas para o processamento ou transmissão eletrônicos de informações;

Igualmente o conceito de ciberexploração merecia reparos:

Atual	Proposto
XII - ciberexploração (ou exploração cibernética): conjunto de atividades voltadas ao robustecimento da consciência situacional, à produção de conhecimento de inteligência de fonte cibernética e ao levantamento de vulnerabilidades, que utiliza	XII - ciberexploração (ou exploração cibernética): conjunto de atividades voltadas ao robustecimento da consciência situacional, à produção de conhecimento de inteligência de fonte cibernética e de ameaças cibernéticas e ao levantamento de

técnicas, táticas e procedimentos semelhantes àqueles empregados nos ciberataques, diferindo deles principalmente por não buscar a produção de ciberefeitos;	vulnerabilidades, que utiliza técnicas, táticas e procedimentos semelhantes àqueles empregados nos ciberataques, diferindo deles principalmente por não buscar a produção de ciberefeitos;

As tecnologias de ciberexploração, em especial *Threat Intelligence* e *Open Source Intelligence* (OSINT) fornecem conhecimento, informações e dados sobre ameaças de segurança cibernética e outras exposições específicas de ameaças. O resultado dessa exploração tem como objetivo fornecer ou auxiliar na curadoria de informações sobre as identidades, motivações, características e métodos de ciberameaças, comumente referidos como táticas, técnicas e procedimentos. Assim, a adição do termo "produção de conhecimento de inteligência de fonte cibernética e de ameaças cibernéticas", adequa-se melhor a esta possibilidade.

Os artigos 11 e 12 definem o Sistema Nacional de Cibersegurança, com o objetivo de envolver todos os poderes da União, dos Estados, do Distrito Federal e dos Municípios, além dos Tribunais de Contas e dos Ministérios Públicos, bem assim do setor privado, das instituições de ensino e pesquisa, e dos demais agentes da sociedade. Esse sistema compõe-se do Comitê Nacional de Cibersegurança (CNCiber), da Agência Nacional de Cibersegurança, do Gabinete de Gerenciamento de Cibercrises e do Complexo Nacional de Cibersegurança.

O Comitê Nacional de Cibersegurança é órgão de assessoramento do Presidente da República sobre cibersegurança, integrado por representantes da sociedade, do setor público, do setor privado e da academia. Dentre outras funções, cabe a ele aprovar a Estratégia Nacional de Cibersegurança, o Plano Nacional de Cibersegurança e o Complexo Nacional de Cibersegurança (composto pelo conjunto de ciberativos que dão sustentação a serviços essenciais). O Gabinete de Gerenciamento de Cibercrises é órgão de assessoramento ao Presidente da República, tal qual o Comitê, mas dedicado especificamente à gestão de cibercrises.

Notamos que, na composição do Comitê, ao contrário do preconizado no anteprojeto como um todo, estão três representantes de entidades representativas das infraestruturas críticas (Art. 15, inciso XVI). O conceito de "infraestrutura crítica" foi suprimido pelo de "serviços essenciais" em todo o anteprojeto. Prudente seria adequar igualmente para a composição do Comitê, com "três representantes de entidades representativas dos serviços essenciais". Além disso, notamos a ausência de representante da Polícia Federal como membro do Comitê e do Gabinete de Cibercrises.

Igualmente, se o anteprojeto pretendia eliminar a fragmentação e a sobreposição regulatória, a exemplo dos Decretos nº 9.637/2018 (Institui a Política Nacional de Segurança da Informação), nº 10.569/2020 (Estratégia Nacional de Segurança de Infraestruturas Críticas), e da Res. CNJ 396/2021 (Institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário), seria importante incluir todas as agências reguladoras no Comitê, pois muitas delas também possuem preocupações com a segurança cibernética (Anatel, Anac, Aneel...).

A Agência Nacional de Cibersegurança seria autarquia sob regime especial, com autonomia administrativa e financeira e patrimônio próprio, vinculada ao Gabinete de Segurança Institucional da Presidência da República, com sede em Brasília.

Dentre as funções da Agência está, no Art.18, inc. VI, a de *desenvolver capacidades nacionais de prevenção, monitoramento, detecção, análise e resposta, para detectar e gerenciar ciberincidentes*. Defendemos que seria prudente alterar essa competência para *desenvolver e fomentar capacidades nacionais de prevenção, monitoramento, detecção, exploração, análise e resposta, para detectar e gerenciar ciberincidentes*.

Por fim, quanto ao tema do ensino, pesquisa, desenvolvimento e inovação tecnológica, consideramos louvável o objetivo dado ao Ministério da Educação, no Art. 32, de promover o ensino de cibersegurança na educação fundamental e média, pública e privada, com base: I – nas boas práticas de cibersegurança; II - na ética no uso da internet; III - na utilização segura de aplicativos; IV - no uso de redes sociais; e V - na proteção de dados; igualmente deveria fundar-se: VI - na intimidade e na proteção da privacidade; VII - na proteção da criança e do adolescente na internet; e VIII - nos direitos fundamentais.

Contudo, esse projeto de lei jamais foi apresentado e, em seu lugar, foi editado o **Decreto nº 11.856, de 26 de dezembro de 2023**, que institui a Política Nacional de Cibersegurança (PNCiber), composta da Estratégia Nacional de Cibersegurança e do Comitê Nacional de Cibersegurança (CNCiber).

Houve estranhamento duplo com a edição desse decreto. O primeiro, em razão de todos esperarem a submissão do anteprojeto de lei acima referido,

em que seria criada uma agência reguladora, prevista para contar com 800 (oitocentos) servidores após 5 (cinco) anos de sua instalação pelo Poder Executivo. Desse modo, o decreto regula lei inexistente, lançando dúvidas até mesmo de sua possível contrariedade ao art. 48, XI, e ao art.84, VI, "a", da Constituição Federal.

Segundo, que o Decreto revoga dois dispositivos do Decreto nº 9.637, de 26 de dezembro de 2018, que *institui a Política Nacional de Segurança da Informação,* extraindo a segurança cibernética da segurança da informação, o que é um equívoco. Este Decreto tem por finalidade assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação. Similarmente, o Decreto nº 11.856/2023, que estabelece a Política Nacional de Cibersegurança, tem por um de seus objetivos garantir a confidencialidade, a integridade, a autenticidade e a disponibilidade das soluções e dos dados utilizados para o processamento, o armazenamento e a transmissão eletrônica ou digital de informações (art. 3º, II).

Se lermos atentamente o Decreto nº 9.637/2018, notamos que a segurança da informação abrange a segurança cibernética, a defesa cibernética, a segurança física e a proteção de dados organizacionais; e as ações destinadas a assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação (art. 2º).

O Decreto nº 11.856/2023, ao revogar o inc. I, do art. 2º, e o inc. I do art. 6º do Decreto nº 9.637/2018, exclui a segurança cibernética da Política Nacional de Segurança da Informação e da Estratégia Nacional de Segurança da Informação, o que carece de sentido lógico. Um dos princípios da Política Nacional de Segurança da Informação, não revogado, é revelador desse equívoco:

> "articulação entre as ações de segurança cibernética, de defesa cibernética e de proteção de dados e ativos da informação" (art. 3º, X, do Decreto nº 9.637/2018)."

Além disso, a Estratégia Nacional de Segurança da Informação (Decreto nº 10.222/2020) é formada por esse conceito integrador e envolve a segurança cibernética, a defesa cibernética, a segurança das infraestruturas críticas, a segurança da informação sigilosa e a proteção contra vazamento de dados. Essa estratégia, inclusive, é intitulada Estratégia Nacional de Segurança Cibernética (E-ciber).

A governança do setor, diferentemente do prometido pelo anteprojeto de lei citado[1], de "unificar a 'colcha de retalhos' regulatória existente no país", ao invés de integrar, auxilia para desintegrar as relações da segurança da informação, segurança cibernética, defesa cibernética e proteção de dados pessoais

Conforme o anteprojeto, segurança da informação envolve as ações que objetivam assegurar a confidencialidade, a integridade, a autenticidade e a disponibilidade das informações; cibersegurança (ou segurança cibernética) é o conjunto de ações voltadas à confidencialidade, integridade, autenticidade e disponibilidade de ciberativos; e, ciberdefesa (ou defesa cibernética), as ações coordenadas pelo Ministério da Defesa com a finalidade de: a) assegurar a cibersegurança de ciberativos de interesse da defesa nacional; e b) buscar superioridade no domínio cibernético sobre os ciberativos do oponente.

[1] Minuta do projeto de lei que institui a Política Nacional de Cibersegurança (PNCiber) e o Sistema Nacional de Cibersegurança (SNCIber). Disponível em: <https://www.gov.br/gsi/pt-br/ssic/audiencia-publica/PNCiberAudienciaPublicaProjetoBase.pdf> Acesso em; 23/02/2024.

Ademais, a Cibersegurança e a ciberdefesa no Brasil são estruturadas em nível **político** (segurança cibernética, aos cuidados da Presidência da República / GSI), **estratégico** (defesa cibernética, sob responsabilidade do Ministério da Defesa, Estado-Maior Conjunto das Forças Armadas e dos Comandos das Forças), **operacional** (guerra cibernética, cuidada pelo comando operacional ativado) e **tático** (guerra cibernética, encarregado pela Força Conjunta de Guerra Cibernética ou um Destacamento Conjunto de Guerra Cibernética).

Observemos que são conceitos e estruturas necessariamente interligados e que merecem governança e regulação igualmente integradas, o que o Decreto nº 11.856/2023 não entregou.

Consciente dessa realidade, o próprio CNCiber, composto por integrantes do poder executivo federal, do Comitê Gestor da Internet, da sociedade civil, de instituições científicas e do setor empresarial, instituiu os seguintes grupos de trabalho para melhorar o sistema: GTT-1: Grupo de Trabalho Temático para atualização da Estratégia Nacional de Cibersegurança – e-Ciber; 2 - Grupo de Trabalho Temático para Elaboração de Proposta de Projeto de Lei para criação de Órgão para a Governança da Cibersegurança Nacional; 3 - Grupo de Trabalho Temático para Definição de Parâmetros de Atuação Internacional do Brasil em Cibersegurança.

3. Estratégia Nacional de Cibersegurança

O Decreto nº 10.222, de 2020, aprovou pela primeira vez a Estratégia Nacional de Segurança Cibernética, cuja denominação foi alterada pelo Decreto nº 12.573, de 2025, para Cibersegurança, ambas abreviadas como E-Ciber. De acordo com o art. 2º, inciso VII, da E-Ciber 2025, cibersegurança é o conjunto de

ferramentas, salvaguardas, diretrizes, abordagens de gestão de riscos, ações, treinamentos, melhores práticas, garantias e tecnologias, entre outras medidas usadas para proteger o ciberespaço e os ciberativos (*hardwares*, *softwares*, redes, dispositivos, aplicações, serviços, sistemas e dados utilizados para processar, armazenar ou transmitir informações por meio eletrônico ou digital) do usuário e da organização.

A E-Ciber 2025 estabeleceu quatro eixos temáticos, nomeadamente a (a) proteção e conscientização do cidadão e da sociedade; (b) segurança e resiliência dos serviços essenciais e das infraestruturas críticas; (c) cooperação e integração entre os órgãos e entidades, públicas e privadas; e (d) soberania nacional e governança. A E-Ciber 2020 dividia de modo diferente, entre os Eixos de Proteção e Segurança (governança da segurança cibernética nacional; universo conectado e seguro: prevenção e mitigação de ameaças cibernéticas; e proteção estratégica) e os Eixos Transformadores (dimensão normativa; dimensão internacional e parcerias estratégicas; pesquisa, desenvolvimento e inovação; e educação). Já os objetivos da E-Ciber 2025 são aqueles da Política Nacional de Cibersegurança – PNCiber, já citados.

A PNCiber envolve, justamente, a E-Ciber e o Plano Nacional de Cibersegurança, sendo este o meio de estabelecer ações estratégicas específicas para implementar os quatro eixos da E-Ciber 2025.

A E-Ciber 2025, de modo mais estruturado que a E-Ciber 2020, definiu o que seriam ciberativos, ciberameaça, cibercrime, ciberefeito, ciberincidente, ciberofensa, cibersegurança, ciberdefesa, ciber-risco, tecnologia da informação e tecnologia operacional.

Quanto ao Eixo 1 (proteção e conscientização do cidadão e da sociedade), o objetivo principal é garantir condições seguras para o uso dos serviços digitais, com atenção especial às pessoas em situação de vulnerabilidade, como crianças e adolescentes, idosos e pessoas neurodivergentes. Essa abordagem reconhece que a inclusão digital deve vir acompanhada de medidas que assegurem a segurança e a autonomia dos usuários mais suscetíveis a riscos no ambiente virtual.

Para alcançar esse objetivo, a E-Ciber 2025 estabelece uma série de ações estratégicas. Entre elas estão o incentivo à atuação segura no ciberespaço e à expansão de serviços de apoio às vítimas de crimes digitais. Também se destaca a promoção de mecanismos de identificação e autenticação de usuários, respeitando a privacidade, e o estímulo à capacitação de professores e gestores em temas de cibersegurança. A estratégia prevê ainda a inclusão desses temas nos currículos escolares de todos os níveis, bem como a participação ativa em fóruns acadêmicos e técnicos.

Além disso, há ações voltadas ao setor produtivo, como a orientação a microempresas e startups na gestão de riscos e na recuperação pós-incidentes, e a avaliação de modelos flexíveis de conformidade em cibersegurança para órgãos públicos. O E-Ciber 2025 também promove o desenvolvimento de planos de contingência institucionais, testes de segurança, e ações multissetoriais para prevenir e combater cibercrimes e fraudes digitais. Por fim, destaca-se a divulgação de instrumentos internacionais como a Convenção sobre o Crime Cibernético (promulgada pelo Decreto nº 11.491, de 12 de abril de 2023), o fortalecimento dos canais de denúncia e a capacitação dos órgãos de persecução

penal para enfrentar os desafios do cibercrime (crimes praticados contra ou por meio de ciberativos) com maior eficácia

Sobre o Eixo 2, pertinente à segurança e resiliência dos serviços essenciais e das infraestruturas críticas, a finalidade é garantir que a sociedade disponha de instrumentos eficazes para prevenir e responder a ciberincidentes (ciberofensa combinada ao ciberefeito real ou potencial resultante da ciberofensa; a considerar ciberofensa como ações adotadas no ciberespaço em oposição a ciberativo e ciberefeito como dano, permanente ou temporário, indisponibilidade ou limitação da operação, total ou parcial, ou mudança de comportamento de ciberativo ou não, resultante de ciberofensa) que possam comprometer serviços fundamentais, como energia, saúde, comunicações e transporte. Essa abordagem reconhece que a continuidade e a confiabilidade desses serviços são vitais para o funcionamento do país e para a proteção da população.

Para alcançar esse objetivo, o E-Ciber 2025 estabelece um conjunto abrangente de ações. Entre elas, destaca-se o estímulo às entidades reguladoras para que promovam a gestão de riscos e adotem medidas de proteção específicas em seus setores. Também são previstas ações como o desenvolvimento de mecanismos de regulação e fiscalização, a adoção de alertas de risco na prestação de serviços digitais e a criação de uma lista nacional de alto risco em cibersegurança, que servirá como base para decisões estratégicas.

Outras medidas incluem o incentivo à adoção de padrões mínimos de segurança para dados sensíveis, a criação de um selo nacional de certificação de ciberativos e o estímulo ao uso de seguros contra ciberincidentes. O decreto também promove a realização de exercícios e simulações regulares para testar a resiliência dos serviços, o aprimoramento contínuo das normas de cibersegurança,

o fortalecimento da interoperabilidade de dados e canais digitais, e o incentivo às empresas brasileiras para que contratem produtos e serviços que sigam padrões mínimos de segurança. Essas ações visam consolidar uma infraestrutura digital robusta, confiável e preparada para enfrentar ameaças cibernéticas complexas.

O Eixo 3, sobre cooperação e integração entre órgãos e entidades, públicas e privadas, tem por escopo central promover o debate e o intercâmbio de informações sobre cibersegurança em níveis nacional e internacional, reconhecendo que a proteção no ciberespaço exige articulação multissetorial e colaboração contínua entre diferentes atores.

Para alcançar esse objetivo, o E-Ciber 2025 estabelece diversas ações estratégicas. Entre elas, destaca-se o estímulo à criação de equipes especializadas em prevenção e resposta a incidentes, centros de análise e compartilhamento de informações, e laboratórios dedicados à pesquisa em cibersegurança. Também é incentivada a criação de um mecanismo nacional para notificação de ciberincidentes, que permitirá maior agilidade e coordenação na resposta a ameaças.

Outro ponto importante é o fortalecimento da cooperação entre instituições acadêmicas e agências nacionais e internacionais, com foco em desenvolver ações conjuntas de cibersegurança e ciberdefesa, compartilhar experiências, divulgar vulnerabilidades de forma coordenada e combater crimes digitais. O E-Ciber 2025 ainda prevê apoio à capacitação dos países vizinhos em iniciativas bilaterais ou multilaterais, além de incentivar a participação ativa do Brasil em fóruns e organizações internacionais dedicadas ao tema. Essas medidas visam consolidar uma rede colaborativa capaz de enfrentar os desafios crescentes da segurança digital.

Já o Eixo 4, sobre soberania nacional e governança, busca proteger os interesses da sociedade brasileira no ciberespaço e garantir um ambiente digital confiável que favoreça o crescimento econômico e tecnológico do país. Para isso, estabelece ações estratégicas que envolvem a atualização e implementação da Política Nacional de Cibersegurança, a criação de um modelo nacional de maturidade para avaliar e orientar o setor, e a formação de profissionais em escala compatível com as demandas nacionais.

Além disso, busca-se reduzir o débito tecnológico em áreas emergentes por meio de políticas afirmativas, fomentar a avaliação contínua da conformidade em produtos e serviços de cibersegurança, e estimular o uso de sistemas seguros para troca de informações. O decreto também incentiva o setor privado a desenvolver soluções voltadas especialmente para microempresas e startups, promove parcerias com institutos de pesquisa para ampliar a inovação tecnológica, e apoia a criação de linhas de pesquisa e bolsas de estudo para formar especialistas e professores na área. Por fim, reforça o estímulo ao desenvolvimento de tecnologias nacionais que fortaleçam a cibersegurança no Brasil.

4. Plano Nacional de Cibersegurança

O Plano Nacional de Cibersegurança é um instrumento estratégico fundamental para a implementação coordenada da política pública de proteção digital no Brasil e, ao lado do E-Ciber 2025, comporá a PNCiber.

Ele será elaborado pelo Comitê Nacional de Cibersegurança, conforme previsto no Decreto nº 11.856/2023, e submetido à aprovação do Ministro Chefe do Gabinete de Segurança Institucional da Presidência da República. Essa estrutura garante que o plano seja formulado por um colegiado

técnico e multissetorial, mas validado por uma autoridade central, reforçando sua legitimidade e alinhamento com os interesses nacionais.

O conteúdo do plano será composto por três elementos essenciais: as iniciativas estratégicas específicas, que detalham as ações concretas a serem executadas; o cronograma de execução, que organiza essas ações no tempo e permite o acompanhamento de sua implementação; e a governança das atividades, que define os responsáveis, os mecanismos de coordenação e os critérios de avaliação. Essa abordagem assegura clareza, previsibilidade e responsabilidade na condução da Estratégia Nacional de Cibersegurança.

Além disso, a publicação do plano dependerá da anuência dos órgãos e entidades públicas que integram o Comitê Nacional de Cibersegurança, conforme o artigo 7º do Decreto nº 11.856/2023. Isso significa que o plano será fruto de consenso institucional, envolvendo representantes de diferentes setores do Estado, o que fortalece sua legitimidade e viabilidade.

Na 7ª Reunião Ordinária do Comitê Nacional de Cibersegurança (CNCiber) ocorrida em 1º de outubro de 2025, no Palácio do Planalto, sob a presidência do Gabinete de Segurança Institucional (GSI), relatou-se que a criação de um órgão de governança da cibersegurança foi considerada inviável pela Casa Civil, em razão das restrições fiscais do país. O Tribunal de Contas da União - TCU, contudo, demonstrou preocupação com a falta de avanços nesse tema, destacando a importância de uma estrutura de governança diante do aumento dos ciberincidentes em 2025.

A Secretaria-Executiva do CNCiber apresentou informações sobre o Marco Legal da Cibersegurança proposto pela Frente Parlamentar de Apoio à

Cibersegurança (FrenCyber), em tramitação no Senado Federal, ressaltando sua complementaridade com a proposta do GSI, especialmente quanto à criação de um fundo para custeio de uma futura autoridade nacional. Em seguida, o GSI apresentou sua proposta de Lei Geral de Cibersegurança, que prevê a transformação da ANATEL em Autoridade Nacional de Cibersegurança, a criação do Sistema Nacional de Cibersegurança (SNCiber) e o aproveitamento de 250 vagas existentes para criação de uma nova carreira de especialistas na área. Após debates, decidiu-se pela criação do GTT Lei Geral da Cibersegurança, com duração de dois meses, para aprofundar a análise do anteprojeto.

O plenário também deliberou sobre o encerramento dos trabalhos do GTT P-Ciber, responsável pela elaboração do Plano de Cibersegurança (P-Ciber). O grupo relatou dificuldades decorrentes do calendário orçamentário e optou por um documento descritivo das iniciativas em andamento, sem metas quantitativas. A publicação do plano foi aprovada, assim como a criação de um novo GTT P-Ciber Estruturante, para propor ações de longo prazo.

Contudo, até a elaboração deste trabalho, o referido Plano não foi apresentado.

5. Avaliação do Tribunal de Contas da União

O Tribunal de Contas da União (TCU), por meio de Auditoria Operacional realizada junto ao Gabinete de Segurança Institucional da Presidência da República (GSI) e à Casa Civil da Presidência da República, no âmbito do processo TC 010.387/2024-2, sob relatoria do Ministro Benjamin Zymler, avaliou o grau de conformidade da Política Nacional de Cibersegurança (PNCiber) em relação às boas práticas e aos parâmetros definidos no Referencial de Controle de Políticas Públicas do TCU.

O objetivo da auditoria foi examinar a adequação do modelo da PNCiber para o enfrentamento das ameaças cibernéticas e dos riscos delas decorrentes para o Estado brasileiro. Observou-se que a superfície de ataque nacional apresenta tendência de crescimento e se encontra entre as mais vulneráveis do mundo, sem que haja, até o momento, uma estrutura organizacional centralizada e eficaz para o enfrentamento desses desafios.

Com vistas à consecução dos objetivos, a auditoria estabeleceu as seguintes questões de avaliação:

- Em que medida são necessárias proteções cibernéticas ao ambiente digital sob a governabilidade do Brasil?

- Em que medida as ações previstas na Política Nacional de Segurança da Informação (PNSI), relacionadas à segurança cibernética e executadas entre dezembro de 2018 e dezembro de 2023 (período compreendido entre a publicação da PNSI e da PNCiber), contribuíram para a segurança do ambiente digital sob responsabilidade do Estado brasileiro?

- Em que medida a Política Nacional de Cibersegurança (PNCiber) foi formulada em conformidade com as boas práticas e com o Referencial de Controle de Políticas Públicas do TCU?

- Quais riscos o país enfrenta caso os objetivos de segurança cibernética estabelecidos pelo Estado brasileiro não sejam alcançados?

A auditoria ressaltou que o Gabinete de Segurança Institucional da Presidência da República (GSI/PR) é o órgão responsável pela coordenação e

supervisão das ações de segurança cibernética no âmbito da administração pública federal. Entretanto, constatou-se que o Brasil ainda não dispõe de autoridade central ou norma federal abrangente que discipline a matéria além da esfera do Poder Executivo, o que evidencia a falta de priorização da segurança cibernética no Estado brasileiro.

Em decorrência desse cenário, têm sido observados ataques cibernéticos exitosos contra organizações públicas, empresas privadas e cidadãos, ocasionando danos relevantes à confidencialidade, integridade e disponibilidade de informações e sistemas. Esses ataques geram impactos negativos sobre a soberania digital, a confiança no ambiente digital e o processo de transformação digital do país, além de provocarem prejuízos financeiros, danos à imagem institucional e interrupção de serviços essenciais.

Entre as principais modalidades de ataque identificadas, destacam-se o ransomware, que consiste em malware destinado a sequestrar dados de sistemas ou dispositivos, exigindo pagamento para sua liberação, e o phishing, técnica de engenharia social que induz o usuário a fornecer informações sensíveis ou a realizar ações que possibilitem o acesso indevido a contas, equipamentos ou redes.

Urge o fortalecimento da soberania digital, de modo a capacitar o Estado brasileiro para controlar e proteger suas infraestruturas críticas, redes eletrônicas, bancos de dados e sistemas de informação que sustentam a própria governança pública.

Em sentido preocupante, observa-se o aumento da frequência e da gravidade dos ataques cibernéticos direcionados a tribunais, empresas, ministérios

e unidades administrativas, os quais têm causado expressivos prejuízos financeiros e comprometido a eficiência do serviço público.

O cenário atual demonstra a necessidade de investimentos estruturantes na área, como a criação de uma Agência Nacional de Segurança Cibernética, que possibilite coordenação técnica e integração institucional. Ressalta-se que os recursos empregados nessa estrutura retornariam rapidamente, considerando-se os prejuízos recorrentes ocasionados pelos incidentes cibernéticos.

O Tribunal de Contas da União (TCU) apontou fragilidades significativas no Sistema de Administração dos Recursos de Tecnologia da Informação (Sisp), destacando que os órgãos integrantes não implementam, de forma satisfatória, o conjunto básico de medidas de segurança cibernética. Ademais, verificou-se a inexistência de uma entidade responsável pela consolidação e compartilhamento de dados entre os órgãos públicos e o setor privado, o que dificulta o gerenciamento de riscos e a adoção de medidas coordenadas de prevenção.

Quanto aos efeitos do Decreto nº 11.856, de 2023, que instituiu a Política Nacional de Cibersegurança (PNCiber), o TCU identificou dois fatores limitadores da efetividade da política pública: a) o caráter preparatório da atual PNCiber; e b) as restrições de origem na formulação da política.

Nesse contexto, constatou-se que o Comitê Nacional de Cibersegurança (CNCiber) não dispõe de competência para coordenar e executar políticas públicas, atuando de forma mais próxima a um grupo de trabalho consultivo do que a um órgão operacional. Assim, o CNCiber apresenta natureza

transitória e preparatória, voltada à construção de um marco legal futuro. Paralelamente, a política pública carece de alcance nacional e de estrutura executiva consolidada, o que limita sua efetividade.

Por ter sido instituída por decreto, a PNCiber restringe-se ao âmbito do Poder Executivo Federal, sem a capilaridade necessária para enfrentar uma ameaça de natureza multidimensional, multissetorial e transnacional, como é o caso da cibernética. Entre os principais riscos decorrentes dessa limitação, destacam-se:

- baixa competitividade nacional em produtos, serviços e tecnologias de segurança cibernética;
- vulnerabilidade acentuada de usuários, especialmente crianças, adolescentes e idosos, em razão da ausência de conscientização adequada sobre riscos digitais;
- baixa resiliência das organizações públicas e privadas, ampliando a probabilidade de sucesso e o impacto de ataques como o ransomware;
- estagnação da inovação e fuga de talentos especializados;
- inexistência de diretrizes claras para que instituições de ensino alinhem suas atividades às demandas nacionais em segurança cibernética; e
- ausência de orçamento nacional específico destinado à segurança cibernética.

Considerando que o problema da segurança cibernética afeta todos os níveis do setor público, do setor privado e da sociedade civil, é imperativo que a política pública voltada ao seu enfrentamento — a Política Nacional de

Cibersegurança (PNCiber) — seja intergovernamental, articulada e coordenada de forma integrada.

Tal característica somente seria plenamente alcançada por meio de lei federal, capaz de instituir uma estrutura de coordenação nacional com cargos, funções e atribuições específicas. De acordo com o Tribunal de Contas da União (TCU), o anteprojeto de lei originalmente proposto para a PNCiber contemplava essa estrutura coordenadora, ao prever os seguintes instrumentos: I – o Sistema Nacional de Cibersegurança; II – a Estratégia Nacional de Cibersegurança; III – o Plano Nacional de Cibersegurança; IV – a cooperação internacional; e V – o ensino, a pesquisa, o desenvolvimento e a inovação tecnológica em cibersegurança.

A ausência do Sistema Nacional de Cibersegurança no Decreto nº 11.856, de 2023, em razão de suas limitações normativas, frustrou a expectativa de adoção das boas práticas internacionais. O sistema, conforme delineado no anteprojeto, seria composto por: I – o Comitê Nacional de Cibersegurança; II – a Agência Nacional de Cibersegurança; III – o Gabinete de Gerenciamento de Cibercrises; e IV – o Complexo Nacional de Cibersegurança.

Embora o decreto tenha instituído a Estratégia Nacional de Cibersegurança e o Plano Nacional de Cibersegurança, tais instrumentos não podem ser considerados de caráter verdadeiramente “nacional”, uma vez que o decreto não possui a abrangência e a força normativa de uma lei.

No anteprojeto de lei, a Agência Nacional de Cibersegurança estava prevista como órgão executor da política pública, responsável pela

implementação e coordenação das ações. No entanto, o Decreto nº 11.856/2023 não estabeleceu estrutura equivalente.

Segundo o TCU, a estrutura institucional voltada à segurança cibernética deve dispor de autoridade e prerrogativas compatíveis com sua função de liderança, de modo a permitir a coordenação de esforços descentralizados e a cooperação com agências reguladoras de setores críticos, organizações internacionais e demais atores estratégicos em ações que envolvam compartilhamento de dados, inteligência e infraestrutura tecnológica.

A análise conduz à conclusão de que não há priorização governamental adequada para o tema. Estima-se que a criação da Agência Nacional de Cibersegurança demandaria a instituição de 687 cargos e um orçamento anual de aproximadamente R$ 540 milhões. Em contraste, o orçamento destinado à implementação das ações de segurança cibernética em 2023, no âmbito da Política Nacional de Segurança da Informação (PNSI), não ultrapassou R$ 600 mil.

Sobre as respostas às questões formuladas na Auditoria Operacional, apresentam-se as seguintes conclusões:

Questão 1 – Em que medida são necessárias as proteções cibernéticas ao ambiente digital sob a governabilidade do Brasil?

Resposta:

Constatou-se que as proteções cibernéticas são necessárias em nível de política pública nacional, devendo ser estruturadas a partir de avaliações de risco conduzidas pelo Estado brasileiro. A auditoria identificou que a ameaça

cibernética representa fator de alta relevância estratégica para o país e apresenta tendência de agravamento no cenário nacional, o que demanda atuação coordenada e permanente.

Questão 2 – Em que medida as ações previstas na PNSI, relativas à segurança cibernética, executadas entre dezembro de 2018 e dezembro de 2023 (período entre a publicação da PNSI e da PNCiber), contribuíram para tornar seguro o ambiente digital sob a governabilidade do Brasil?

Resposta:

Verificou-se que as ações previstas na Política Nacional de Segurança da Informação (PNSI) foram parcialmente executadas pelo Gabinete de Segurança Institucional da Presidência da República (GSI/PR) no período compreendido entre dezembro de 2018 e dezembro de 2023. No entanto, as limitações do modelo federal, e não nacional, da PNSI reduziram a eficácia das ações implementadas, dificultando o alcance de seus objetivos e comprometendo a segurança do ambiente digital sob a governabilidade do Brasil, conforme disposto no art. 4º do Decreto nº 9.637/2018.

Questão 3 – Em que medida a Política Nacional de Cibersegurança (PNCiber) foi formulada segundo as boas práticas, em especial comparada ao previsto no Referencial de Controle de Políticas Públicas (RCPP) do TCU?

Resposta:

O estágio de formulação da PNCiber — correspondente aos Blocos I, II e III do Referencial de Controle de Políticas Públicas (RCPP) — demonstra alinhamento parcial às boas práticas de formulação de políticas públicas. A principal fragilidade identificada refere-se à incoerência entre o modelo adotado e o problema identificado, o que compromete a efetividade da política e o alcance de seus objetivos, nos termos do art. 3º do Decreto nº 11.856/2023.

A equipe de auditoria ressalta, ainda, que a PNCiber configura ato preparatório, possivelmente voltado à futura instituição de um marco regulatório nacional em segurança cibernética, a ser desenvolvido a partir das conclusões dos trabalhos do Grupo de Trabalho Técnico nº 2 (GTT-2).

Questão 4 – A quais riscos o país está submetido ao não se alcançar os objetivos de segurança cibernética estabelecidos pelo Estado brasileiro?

Resposta:

A não consecução dos objetivos da PNCiber poderá resultar na perda de controle e soberania sobre infraestruturas críticas e dados digitais estratégicos. Tal cenário acarretaria impactos diretos sobre a soberania digital — e, por consequência, sobre a soberania nacional —, além de comprometer a confiança no ambiente digital e retardar a transformação digital no país.

Diante das constatações apresentadas, o Tribunal de Contas da União (TCU) concluiu pela necessidade de instituição de uma lei federal, de iniciativa privativa da Presidência da República, com abrangência nacional, destinada a: I – estabelecer uma política pública de segurança cibernética de caráter permanente e estruturado; e II – criar uma estrutura de coordenação nacional com autoridade suficiente em todo o território brasileiro para garantir a execução e a efetividade da política.

A recomendação do TCU foi direcionada à Casa Civil da Presidência da República e ao Gabinete de Segurança Institucional da Presidência da República (GSI/PR), com o objetivo de promover o gerenciamento adequado do risco cibernético e o fortalecimento da governança nacional sobre o tema.

> "Não há priorização do tema segurança cibernética no Estado brasileiro, o que leva a uma Política Nacional de Cibersegurança que não tem alcance Nacional e à ausência de estrutura com autoridade e prerrogativas suficientes para coordenar a execução dessa política, o que leva à insuficiência de orientação do Estado brasileiro para a atividade de segurança cibernética no país, o que leva a atividades de segurança cibernética insuficientes, as quais combinadas com ataques cibernéticos, leva ao sucesso dos ataques contra organizações e cidadãos brasileiros, o que leva a danos em diversas dimensões por perda da confidencialidade, integridade e disponibilidade de informações e sistemas (e.g., fraudes contra cidadãos, paralisação de serviços prestados à sociedade, prejuízos à imagem das organizações públicas e privadas, perdas financeiras), o que impacta negativamente a soberania digital, a confiança no ambiente digital e a aceleração da transformação digital no país."

A Casa Civil da Presidência da República interpôs embargos de declaração em face do Acórdão nº 2.430/2024 – TCU – Plenário, proferido no âmbito da Auditoria Operacional sobre a Política Nacional de Cibersegurança (PNCiber).

O referido acórdão do Tribunal de Contas da União (TCU) havia recomendado à Casa Civil, com o apoio do Gabinete de Segurança Institucional

da Presidência da República (GSI/PR), a adoção de medidas voltadas ao gerenciamento do risco decorrente da ausência de alcance nacional e da insuficiência estrutural da PNCiber para coordenar sua execução de forma efetiva.

Nos embargos apresentados, a Casa Civil alegou omissão no acórdão e sustentou que: I – não possui competência legal para gerenciar riscos ou executar políticas de segurança cibernética, atribuição que cabe a outros órgãos da Administração Pública Federal; II – o tema é tratado pelo Comitê Nacional de Cibersegurança (CNCiber), órgão responsável pela coordenação e acompanhamento da implementação da PNCiber; e III – suas competências, conforme estabelecido pela Lei nº 14.600/2023 e pelo Decreto nº 11.329/2023, restringem-se à coordenação e ao monitoramento de ações governamentais, não abrangendo a execução operacional de políticas públicas.

Ao apreciar os embargos, o relator reconheceu que as atribuições da Casa Civil são de natureza coordenadora, e não executiva, e que as ações mencionadas no acórdão estão mais adequadamente inseridas no âmbito de atuação do CNCiber.

O Gabinete de Segurança Institucional da Presidência da República (GSI/PR), por sua vez, mantém competências específicas relacionadas à segurança cibernética no âmbito da Administração Pública Federal, devendo permanecer como destinatário da decisão.

Dessa forma, o relator votou pelo acolhimento dos embargos de declaração, a fim de alterar o principal destinatário da recomendação constante do Acórdão nº 2.430/2024, substituindo a Casa Civil pelo Comitê Nacional de

Cibersegurança (CNCiber), preservando, contudo, a participação do GSI/PR nas ações recomendadas.

6. Considerações finais

A cibersegurança tornou-se um tema central para a proteção de dados, sistemas de informática e serviços essenciais. O cenário atual mostra ataques cada vez mais sofisticados, explorando falhas técnicas e humanas. Casos recentes no setor financeiro revelam prejuízos bilionários, confirmando a urgência de medidas preventivas.

As ameaças cibernéticas estão marcadas por uma crescente sofisticação e diversidade de vetores de ataque. Entre os principais riscos estão o software malicioso (malware), engenharia social, ransomware, ameaças à identidade, comprometimento de e-mail empresarial, ataques de negação de serviço (DoS/DDoS), ameaças avançadas persistentes e ameaças internas. Os principais agentes de ameaça incluem grupos criminosos, mercenários digitais e atores estatais, que buscam ganhos financeiros, espionagem e sabotagem.

Uma política efetiva de cibersegurança deve focar mais em ações preventivas do que punitivas, buscando reduzir os riscos de ocorrência de incidentes significativos. É necessário atuar tanto na eliminação de vulnerabilidades quanto na mitigação dos efeitos decorrentes de um ataque. A política deve contar com ações educativas, incentivos à autorregulação dos agentes, ações de controle e fiscalização, e, por último, sanções penais. Uma política completa precisa ter um lado voltado à defesa da soberania e outro orientado à manutenção da ordem interna (segurança pública). No contexto interno, a política de cibersegurança deve regular a atuação da administração pública, definir parâmetros mínimos de segurança cibernética para indivíduos e

empresas, e corrigir e prevenir atividades criminais contra estruturas ou pessoas localizadas em território nacional.

A legislação atual trata de crimes digitais, mas não estabelece diretrizes amplas de segurança cibernética. Decretos recentes criaram a estratégia e política nacionais, mas sua natureza infralegal limita o alcance. Importa ressaltar, nesse ponto, que o Senado não está alheio a esta lacuna.

O Projeto de Lei nº 4.752/2025, de autoria do Senador Esperidião Amin e outros, volta-se à administração pública para criar um programa nacional com financiamento estável, deixando de impor obrigações ao setor privado. Igualmente, o Senador Jaques Wagner tem defendido a proposição de um marco legal abrangente, com princípios, direitos, deveres, governança e sanções, incluindo exigências para empresas e operadores de infraestrutura crítica, mas também deixa lacunas relevantes. Sugere-se a união entre ambas as propostas para criar um marco legal mais robusto, preventivo, flexível e aplicável a todos os setores. Nenhuma das propostas analisadas, entretanto, apresentou avanços em aspectos de defesa cibernética, aprimoramentos na segurança pública e extraterritorialidade. Também lhes falta a criação de uma estrutura administrativa e de governança especializada em cibersegurança, em função de restrições no poder de iniciativa parlamentar.

O PL nº 4.752/2025, de autoria do Senador Esperidião Amin e outros, institui o Marco Legal da Cibersegurança com foco na resiliência cibernética da administração pública em todos os entes da federação. O projeto cria o Programa Nacional de Segurança e Resiliência Digital (PNSERD) e altera a legislação existente para garantir seu financiamento. As diretrizes do PL incluem a resposta coordenada a incidentes, a promoção de uma cultura de cibersegurança entre

servidores, a proteção de infraestruturas críticas e a responsabilização de gestores e agentes públicos. O projeto prevê a designação de uma "autoridade nacional de cibersegurança" para normatizar, fiscalizar e auditar, bem como estabelecer padrões mínimos de segurança. O PNSERD é voltado para a administração pública federal, com adesão voluntária de estados e municípios. O projeto destaca a governança de riscos das cadeias de suprimentos e a criação de um mecanismo de financiamento estável, destinando percentuais fixos do Fundo Nacional de Segurança Pública (FNSP) e da arrecadação de apostas esportivas para ações de cibersegurança.

Assim, destaca-se a importância de uma abordagem integrada e coordenada para enfrentar as ameaças cibernéticas. A Política Nacional de Cibersegurança (PNCiber) e a Estratégia Nacional de Cibersegurança (E-Ciber) são passos importantes, mas ainda há lacunas significativas que precisam ser abordadas para garantir a segurança cibernética no Brasil.

Desse modo, propõe-se:

Criação de uma Agência Nacional de Cibersegurança: A criação de uma agência reguladora dedicada à cibersegurança é essencial para coordenar e implementar políticas públicas de forma eficaz. Esta agência deve ter autonomia administrativa e financeira, além de autoridade suficiente para atuar em todo o território nacional.

Estabelecimento de uma Estrutura de Coordenação Nacional: É necessário instituir uma estrutura de coordenação nacional com cargos, funções e atribuições específicas para garantir a execução e a efetividade da política de segurança cibernética. Esta estrutura deve ser capaz de integrar esforços

descentralizados e cooperar com agências reguladoras de setores críticos, organizações internacionais e outros atores estratégicos

Desenvolvimento de Capacidades Nacionais: A política pública deve focar no desenvolvimento e fomento de capacidades nacionais de prevenção, monitoramento, detecção, exploração, análise e resposta a ciberincidentes. Isso inclui a promoção de pesquisa científica, desenvolvimento tecnológico e inovação na área de cibersegurança

Educação e Capacitação em Cibersegurança: É fundamental promover a educação e a capacitação técnico-profissional em segurança cibernética na sociedade. Isso inclui a inclusão de temas de cibersegurança nos currículos escolares de todos os níveis e a capacitação de professores e gestores em temas de cibersegurança

Cooperação Técnica Internacional: A cooperação técnica internacional deve ser fortalecida, reconhecendo que os desafios cibernéticos transcendem fronteiras e exigem esforços conjuntos entre nações. Isso inclui a participação ativa do Brasil em fóruns e organizações internacionais dedicadas ao tema

Regulação e Fiscalização: Desenvolver mecanismos de regulação, fiscalização e controle destinados a aprimorar a segurança e a resiliência cibernéticas nacionais. Isso inclui a criação de um selo nacional de certificação de ciberativos e o estímulo ao uso de seguros contra ciberincidentes.

Elevação do status normativo regulatório: Aguarda-se a apresentação e publicação do Plano Nacional de Segurança pelo Poder Executivo; contudo, importa que o tema da cibersegurança seja regulado por lei federal.

Essas proposições visam fortalecer a segurança cibernética no Brasil, garantindo uma abordagem mais integrada e coordenada para enfrentar as ameaças cibernéticas e proteger a soberania digital do país.