GRUPO II – CLASSE V – Plenário
TC 004.306/2025-2
Natureza(s): Monitoramento
Órgão/Entidade: Comitê Nacional de Cibersegurança (CNCiber) e Gabinete de Segurança Institucional da Presidência da República (GSI/PR)
Representação legal: não há

SUMÁRIO: AUDITORIA. GESTÃO DO RISCO RELACIONADO À POLÍTICA NACIONAL DE CIBERSEGURANÇA. MONITORAMENTO DE RECOMENDAÇÃO. IMPLEMENTAÇÃO DA RECOMENDAÇÃO EFETUADA. PERSISTÊNCIA DE POLÍTICA NACIONAL DE CIBERSEGURANÇA SEM ALCANCE NACIONAL. COMUNICAÇÃO AOS ÓRGÃOS ENVOLVIDOS.

RELATÓRIO

Trata-se de monitoramento com o intuito de avaliar a implementação da recomendação dirigida ao Comitê Nacional de Cibersegurança (CNCiber), com apoio do Gabinete de Segurança Institucional da Presidência da República (GSI), por meio do Acórdão 2.430/2024-Plenário, com nova redação dada pelo Acórdão 276/2025-Plenário, exarados nos autos do TC 010.387/2024-2.

2. A Unidade de Auditoria Especializada em Tecnologia da Informação assim se manifestou:

"*O monitoramento está amparado no art. 243 do Regimento Interno do Tribunal de Contas da União (RI/TCU) e no art. 4º, inciso III, da Portaria – Segecex 27/2009 (Padrões de Monitoramento), em face do disposto no art. 17, § 2º, da Resolução – TCU 315/2020.*

HISTÓRICO

1. *O monitoramento teve origem no TC 010.387/2024-2 e tem como objetivo avaliar em que medida a Política Nacional de Cibersegurança (Decreto 11.856/2023) está de acordo com as boas práticas, em especial comparada ao previsto no Referencial de Controle de Políticas Públicas do TCU.*

2. *O tema segurança da informação e segurança cibernética estava previsto na 1ª edição da Lista de Alto Risco (LAR) da Administração Pública Federal no âmbito deste Tribunal. A fim de atualizar a LAR, foram autorizadas ações de fiscalização nos temas que a integravam por meio da Portaria-TCU 81/2024. Esta fiscalização, juntamente com a do TC 010.390/2024-3, concluíram pela manutenção do tema na 2ª edição da LAR.*

3. *O Tribunal julgou a fiscalização do TC 010.387/2024-2 por meio do Acórdão 2.430/2024-TCU-Plenário, em 13/11/2024 (peça 6), ao qual foram opostos embargos de declaração pela Casa Civil requerendo a exclusão da embargante da condição de destinatária da recomendação emitida. Os embargos foram conhecidos e providos por meio do Acórdão 276/2025-TCU-Plenário, em 12/2/2025, que deu origem à seguinte recomendação (peça 7):*

> *9.1. recomendar, com fundamento na Resolução-TCU 315/2020, art. 11, I, ao* ***Comitê Nacional de Cibersegurança****, com apoio, no âmbito de suas competências, do* ***Gabinete de Segurança Institucional da Presidência da República****, que gerencie o risco consistente em uma Política Nacional de Cibersegurança sem alcance nacional e sem estrutura com autoridade e prerrogativas suficientes para coordenar a execução dessa política; e avaliar em que medida a Política Nacional*

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade e informe o código 80802595.

de Cibersegurança está de acordo com as boas práticas, em especial comparada ao previsto no Referencial de Controle de Políticas Públicas do TCU;

4. *O risco sob gestão do CNCiber, associado à recomendação, consiste em (peça 3, p. 31-32, item. 155.1):*

> *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.*

5. *O supracitado Acórdão foi comunicado ao GSI e à Casa Civil, que registraram ciência em 26/2/2025 e 27/2/2025, respectivamente (peças 131 e 132 do TC 010.387/2024-2). O CNCiber também acusou ciência dos termos do acórdão em questão, conforme peça 10.*

6. *Em 12/9/2025 a AudTI começou o monitoramento por meio de instrução inicial com proposta de diligência junto ao CNCiber para que informasse (peça 14, p.2, item 12.1):*

6.1. *as ações realizadas pelo CNCiber para atender o item 9.1 do Acórdão 276/2025-TCUPlenário; e*

6.2. *em que medida essas ações são capazes de mitigar o risco apontado na recomendação.*

7. *Em 17/9/2025 o Ministro Relator anuiu com a proposta (peça 17) e, por meio do Ofício 40029/2025-TCU/Seproc (peça 18), solicitou-se à Secretaria-Executiva do GSI[1] informações a respeito do cumprimento das deliberações em análise.*

8. *Em resposta, o CNCiber enviou os seguintes documentos (peça 31):*

8.1. *Ofício 81/2025/GAB/SE/GSI/PR (peça 22);*

8.2. *Resolução - CNCiber 13, de 8 de outubro de 2025 (peça 23);*

8.3. *Ata da 5ª Reunião Ordinária (RO-001-25), de 9 de abril de 2025 (peça 24);*

8.4. *Comparativo Entre os Modelos Propostos (peça 25);*

8.5. *Manifestação sobre a preferência dos Modelos Institucionais (Agência Reguladora, Autarquia e Secretaria) (peça 26);*

8.6. *Ata da 6ª Reunião Ordinária (RO-002-25), de 25 de junho de 2025 (peça 27);*

8.7. *Ata da 7ª Reunião Ordinária (RO-003-25), de 1º de outubro de 2025 (peça 28);*

8.8. *Manifestação CNCiber (peça 29);*

8.9. *Documento SEI 7084878 (peça 30).*

9. *A presente instrução busca monitorar a deliberação do Acórdão 276/2025-TCU-Plenário após retorno das diligências propostas na instrução de peça 14.*

---

[1] O GSI é a entidade que preside o CNCiber por meio de representante designado e, nessa forma, atua pautando medidas para incremento da segurança cibernética no País e desenvolvimento da educação em segurança cibernética no âmbito do CNCiber, conforme prevê o art. 7º, inciso I, do Decreto 11.856/2023. Uma vez que sua presidência é exercida atualmente pelo secretário executivo do GSI/PR, a diligência (peça 2, p.2, itens 10-12) foi direcionada à Secretaria-Executiva do GSI, na qualidade de presidente do Comitê.

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade e informe o código 80802595.

EXAME TÉCNICO

Situação que levou à proposição da deliberação

10. *O processo de elaboração que resultou no Decreto 11.856/2023 (Política Nacional de Cibersegurança) iniciou-se* ***no ano de 2023*** *e teve como origem um anteprojeto de Lei encampado pelo GSI/PR (peça 33 e 34) que envolveu, entre outros esforços, a Audiência Pública da PNCiber (peça 32) e os estudos que levaram ao parecer de mérito do anteprojeto (peça 33).*

11. *A proposta de anteprojeto de lei previa a criação de uma Agência Nacional de Cibersegurança (ANCiber), que cumpriria o papel de órgão executor[2] da política pública (peça 34), e implicaria a criação (considerando o quinto ano de existência) de oitocentos cargos (peça 33, p. 10) e um orçamento anual de cerca de R$ 540 milhões (peça 33, p.14).*

12. *A Casa Civil não encaminhou o texto do anteprojeto de Lei enviado pelo GSI/PR ao Congresso Nacional, de modo que o anteprojeto não foi adiante e a política pública acabou sendo instituída por decreto federal (Decreto 11.856/2023).*

13. *No âmbito do TC 010.387/2024-2, a equipe de auditoria solicitou informações sobre o não andamento do anteprojeto de lei, contudo, com base na documentação enviada, a Casa Civil não apresentou justificativa para tal fato (peça 3, p. 25, item 117.2), impossibilitando identificar as causas da divergência entre o modelo proposto pelo GSI/PR e o atual modelo existente no Decreto 11.856/2023 (peça 3, p. 25, item 118).*

14. *Da análise das informações disponíveis, constatou-se que o papel executivo que seria desempenhado pela ANCiber está ausente no Decreto 11.856/2023,* ***pois não foi instituída instância com autoridade e prerrogativas suficientes*** *para acompanhar e cooperar junto aos atores relevantes (peça 3, p. 24, item 107).*

15. *Como o problema que a política pública visa enfrentar (ameaça cibernética) é intergovernamental, é imprescindível que a estrutura responsável pela coordenação de sua execução tenha legitimidade para atuar junto aos diversos setores da sociedade, que incluem: União (os três Poderes), Estados, Distrito Federal, Municípios, Ministério Público, Tribunais de Contas, setor privado e a sociedade civil (peça 3, p. 24, item 108).*

16. *Essa estrutura precisaria possuir mandato legal para agir nesses diversos setores, e o nível de enforcement que ela possuirá dependerá do modelo que os formuladores da política pública decidirem oportuno e conveniente (peça 3, p. 24, item 109).*

17. *A estrutura em questão deveria, ainda, possuir autoridade e prerrogativas também em sua função de liderança, quando atuar de forma a coordenar esforços descentralizados, visto que precisará cooperar com atores relevantes (p. ex.: agências reguladoras de setores críticos e agências internacionais) em ações que envolvam compartilhamento de dados, inteligência e infraestrutura (peça 3, p. 24, item. 111).*

18. *Em resumo, a atual PNCiber e, por consequência, os seus desdobramentos (instrumentos – art. 4ª do Decreto 11.856/2023), não atendem aos requisitos de uma política capaz de alcançar sua finalidade devido à:*

18.1. *abrangência do documento ser federal e não nacional, sendo que o problema é nacional, e não federal;*

18.2. *inexistência de organização ou setor encarregado com autoridade e prerrogativas suficientes para executar a política (observa-se que os decretos estabelecem o que fazer, quem*

[2] A ANCiber possuiria um papel mais abrangente (peça 71, art. 16), que incluiria atribuições de órgão responsável pela governança da PNCiber (inciso I), órgão central do SNCiber (inciso II), entidade regulatória (inciso III), órgão operacional (inciso IV) e cibereducação e capacitação (inciso V).

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade e informe o código 80802595.

aconselhará – o Comitê Nacional de Cibersegurança – CNCiber, mas não define quem executará a política).

19. *Em virtude de a PNCiber atual ser insuficiente para enfrentar o problema público identificado – a ameaça cibernética –, propôs-se que o CNCiber gerisse o risco citado no item 9.1 do Acórdão 276/2025-TCUPlenário.*

Providências adotadas pelo CNCiber com apoio do GSI/PR

20. *O GSI/PR informou que, em 9/4/2025, quando foi realizada a primeira reunião ordinária do CNCiber em 2025 (RO-001-25), o grupo de trabalho temático GTT Governança apresentou relatório em que foram apresentados ao pleno do CNCiber três modelos de governança possíveis (peça 25), cada qual com suas vantagens e desvantagens (peça 29, p.1). Os modelos discutidos pelo GTT Governança contemplavam: a) Autarquia especial (Agência Reguladora); b) Autarquia não especial (similar ao INMETRO ou IBAMA); e c) Secretaria de governo (administração federal direta).*

21. *Houve grande preocupação da maior parte dos integrantes do GTT quanto a uma possível interpretação de que os três modelos pudessem ser equivalentes. A despeito disso, boa parte dos integrantes do GTT fez questão de registrar na reunião suas preferências pelos modelos de autarquia especial e de autarquia não especial (peça 29, p.2). No tocante à elaboração de um* ***anteprojeto de lei de uma lei federal****,* ***o GTT governança optou*** *por inseri-lo na proposta relativa* ***ao modelo de autarquia não especial****. Contudo, ao final****, deliberou-se pelo encaminhamento das três propostas elaboradas para a Casa Civil****, para análise jurídica e de governo (peça 29, p.2).*

22. *Na RO-002-25, ocorrida 25/6/2025, o Presidente do CNCiber informou que as propostas continuavam sob análise jurídica e de governo da Casa Civil. O representante da Casa Civil informou que os trabalhos estavam divididos em duas frentes, com a análise jurídica sendo conduzida pela Secretaria Especial para Assuntos Jurídicos (SAEJ) e a análise de governo pela Secretaria Especial de Análise Governamental (SAG). Após a RO-002-25, a Casa Civil informou ao GSI/PR que não havia espaço para a criação de nenhum novo órgão, de nenhuma natureza, para a governança da cibersegurança nacional (peça 29, p.2).*

23. *Depois dessa reunião, o GSI/PR iniciou tratativas com a Agência Nacional de Telecomunicações - Anatel (****4ª proposta****) e a Casa Civil para buscar a elaboração de uma proposta alternativa de Lei Geral da Cibersegurança, que apontasse a Anatel como a autoridade nacional de cibersegurança, sendo convertida em Agência Nacional de Telecomunicações e Cibersegurança (peça 29, p.3).*

24. *Na RO-003-25, ocorrida em 1/10/2025 (peça 29, p.3), a Secretaria-Executiva do CNCiber (SE-CNCiber) informou ao plenário que a SAG/CC, na análise de governo, reafirmara a inviabilidade de criação qualquer tipo de órgão de governança, e que, por esse motivo, a revisão jurídica das três propostas fora interrompida. Apenas a análise jurídica da Lei Geral da Cibersegurança evoluíra, incorporada à proposta apresentada pelo GSI/PR (peça 29, p.3).*

25. *O GSI/PR registra que, nas discussões da RO-003-25, surgiram questionamentos quanto a pontos em que a redação proposta era distinta daquela originalmente apresentada pelo GTT, tendo sido explicado que esse é o processo de redação legislativa do Executivo e que um órgão de aconselhamento, como o CNCiber, apresenta propostas, que vão sendo alteradas nas diferentes instâncias do governo. Entendendo ser necessário um debate mais aprofundado sobre a proposta, foi deliberada a criação do* ***GTT Lei Geral*** *que deveria apresentar sua análise para deliberação na RO-004-25, que seria realizada em 17/12/2025 (peça 29, p.3).*

26. *Por fim, afirma que, juntamente com diversas instituições do CNCiber, o GSI/PR vem se empenhando pela proposição de uma Lei Geral da Cibersegurança e pela instituição de um órgão de governança com a maior abrangência possível. Não obstante, questões ainda não totalmente equacionadas, como a limitação do cenário fiscal, escopo de atuação da autoridade, a interrelação*

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade e informe o código 80802595.

entre os órgãos reguladores setoriais e a nova autoridade nacional de cibersegurança na busca da abrangência nacional multissetorial, e, por fim, a natureza jurídica da autoridade de governança ainda têm limitado a possibilidade de evolução célere das propostas (peça 29, p.4).

Análise

27. *Primeiramente, faz-se necessário destacar que, após envio da resposta do CNCiber, ocorreram as RO-004-25 e RO-001-26 em 17/12/2025 e 25/3/2026, respectivamente.*

28. *Em relação ao GTT Lei Geral, foi esclarecido pelo Presidente na RO-004-25 que, separadamente do anteprojeto de Lei Geral da Cibersegurança, as três opções de órgãos de governança originalmente consideradas pelo GTT Governança (Agência Reguladora específica, Autarquia não especial e Secretaria da administração direta), além da quarta opção analisada pelo GTT Lei Geral (Anatel como autoridade nacional de cibersegurança), constituindo, assim, quatro propostas distintas, seriam encaminhadas à Câmara de Relações Exteriores e Defesa Nacional do Conselho de Governo (Creden) mas que cada uma delas seria votada individualmente para registro de seus apoios institucionais (peça 35, p. 3, item 1.5).*

29. *Como deliberação relativa aos trabalhos do GTT Lei Geral, há registro de que **o texto trata genericamente de uma Autoridade Nacional de Cibersegurança** (na minuta do anteprojeto elaborado pelo GSI/PR em 2023 a ANCiber se referia a "Agência Nacional de Cibersegurança" – peça 34), sendo que o encaminhamento do texto foi posto em deliberação e aprovado por unanimidade (peça 35, p. 4). Ressalta-se que, na ata da RO-004-25, há o registro de que o texto passará por uma revisão na SAEJ e na SAG (Casa Civil) e depois nas negociações com o Congresso Nacional (peça 35, p. 4).*

30. *Após, houve deliberação sobre o encaminhamento da proposta da **Anatel** como Autoridade Nacional de Cibersegurança (ANCiber), conforme proposta apresentada pelo GSI/PR. A proposição foi colocada em votação, recebendo dezoito votos favoráveis e dois votos contrários (peça 35, p. 4-6, item 1.7).*

31. *Já no encaminhamento da proposta de criação de uma Agência Nacional de Cibersegurança na modalidade **agência reguladora (autarquia especial)** para assumir a função de autoridade nacional de cibersegurança, a proposição foi colocada em votação, recebendo vinte votos favoráveis e nenhum voto contrário (peça 35, p. 6, item 1.8).*

32. *Para o encaminhamento de proposta de uma Autoridade Nacional de Cibersegurança (ANCiber) como **autarquia não especial** para assumir a função de autoridade nacional de cibersegurança, a proposição foi colocada em votação, recebendo doze votos favoráveis e oito votos contrários (peça 35, p. 6-7, item 1.9).*

33. *Já sobre o encaminhamento de proposta de uma **Secretaria Nacional de Cibersegurança** como entidade da administração federal direta para assumir a função de autoridade nacional de cibersegurança, a proposição foi colocada em votação, recebendo dezenove votos contrários e um voto favorável (peça 35, p. 7-8, item 1.10).*

34. *Conforme ata da 9ª Reunião Ordinária - RO-001-26, ocorrida em 25 de março de 2026 (peça 36, p.2, item 1.5):*

> ***1.5 Informe sobre o Anteprojeto da Lei Geral da Cibersegurança aprovado pelo CNCiber.***
>
> *O Presidente do CNCiber informou ao pleno que **a minuta do Anteprojeto de Lei aprovada pelo CNCiber na RO-004-25 foi remetida à CC/SAEJ** logo após a reunião que o aprovou. Alguns pontos foram ajustados entre a SE-CNCiber e a SAEJ. Dias depois a SE-CNCiber e o GSI enviaram à SAEJ/CC uma proposta de um anteprojeto unificado, incorporando ao texto do Marco Legal em discussão no Senado as propostas da minuta aprovada pelo CNCiber. Informou também que foi solicitada uma reunião, entre o GSI, a CC, o MGI e a SRI para*

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade e informe o código 80802595.

verificar as alternativas de envio dos diferentes textos ao Senado antes da deliberação terminativa na CCT, mas que tal reunião ainda não ocorreu (grifou-se).

35. *Na reunião, ainda foi aprovada a proposta de dar publicidade ao anteprojeto da "Lei Geral da Cibersegurança" aprovado pelo CNCiber (peça 36, p.2, item 1.6), cuja minuta encontra-se acostada à peça 37.*

36. *Para melhor compreensão, até o momento têm-se:*

36.1. *uma proposta de **anteprojeto** da "Lei Geral da Cibersegurança" elaborada pelo CNCiber (peça 37) **com quatro propostas** (peça 25) da estrutura que assumiria o papel de Autoridade Nacional de Cibersegurança previsto nessa Lei, sendo: (i) agência reguladora; (ii) autarquia não especial; (iii) Secretaria Nacional de Cibersegurança; e (iv) Agência Nacional de Telecomunicações – Anatel.*

36.2. *a minuta do anteprojeto de Lei aprovada pelo CNCiber na RO-004-25 foi remetida à Secretaria Especial Para Assuntos Jurídicos da Casa Civil (SAEJ/CC).*

37. *Considerando que o CNCiber aprovou e encaminhou a proposta de anteprojeto de Lei Geral da Cibersegurança à Casa Civil com quatro modelos de ANCiber (parágrafos 21-23), entende-se que, dentro de suas competências legais (**Error! Reference source not found.**) o Comitê adotou as medidas que estavam ao seu alcance para gerenciar o risco consistente em uma Política Nacional de Cibersegurança sem alcance nacional e sem estrutura com autoridade e prerrogativas suficientes para coordenar a execução dessa política.*

Conclusão

38. *Ante o exposto, considera-se implementado o item 9.1 do Acórdão 276/2025-TCU-Plenário.*

DA PERSISTÊNCIA DO RISCO

39. *Primeiramente, registra-se que, de acordo com o item 63.5 do documento intitulado "Padrões de Monitoramento" do TCU, aprovado pela Portaria-Segecex 27/2009, nas situações em que ficar patente que o órgão/entidade já adotou todas as medidas cabíveis a seu alcance para o atendimento das deliberações, sem sucesso, **deve ser incluída, quando possível, proposta para outros órgãos/entidades a fim de dar efetividade às deliberações do TCU**.*

40. *Embora o CNCiber tenha executado as ações que estavam ao seu alcance para atendimento do Acórdão, verifica-se que **inexiste, ainda,** uma Política Nacional de Cibersegurança com alcance nacional e estrutura com autoridade e prerrogativas suficientes para enfrentar, de forma intergovernamental, o tema da ameaça cibernética.*

41. ***Em 2023**, o GSI/PR elaborou uma minuta de anteprojeto com prerrogativas suficientes e alcance nacional para instituir uma Política Nacional de Cibersegurança com a criação de uma Agência Nacional de Cibersegurança (peça 33 e 34), realizou audiência pública (peça 32), encaminhou à Casa Civil, mas o anteprojeto não foi para frente, sem que a Casa Civil apresentasse justificativas para tal fato (parágrafos 10-14).*

42. *Nota-se que o ciclo de tentativa atual (parágrafos 35-37) de dar andamento ao anteprojeto de Lei se assemelha ao que ocorreu em 2023:*

42.1. *o GSI/PR, no âmbito do CNCiber, elabora proposta de anteprojeto de lei;*

42.2. *a minuta é tornada pública;*

42.3. *a minuta é enviada para a Casa Civil;*

42.4. *o anteprojeto não é encaminhado ao Congresso Nacional pelo Presidente da República.*

43. *O atual ciclo teve como marco o encaminhamento das três propostas à Casa Civil, conforme deliberado na RO-001-25, de abril de 2025 (parágrafos 21). Um ano após, ainda não há perspectiva de*

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade e informe o código 80802595.

o anteprojeto ser encaminhado ao Congresso Nacional. Dessa forma, o que foi feito até o momento não ataca a causa do risco.

44. *Considera-se, portanto, que enquanto o Poder Executivo Federal não encaminhar o projeto de Lei ao Congresso Nacional, a causa do risco persistirá (ausência de PNCiber com alcance nacional).*

45. *Nesse sentido, persiste o risco que foi inserido na LAR[3]:*

> *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.*

46. *No atual cenário, o CNCiber possui, entre outras, as competências de propor atualizações para a PNCiber, a Estratégia Nacional de Cibersegurança e o Plano Nacional de Cibersegurança, e manifestar-se, por solicitação do Presidente da Câmara de Relações Exteriores e Defesa Nacional do Conselho de Governo (Creden), sobre assuntos relacionados à segurança cibernética. Verifica-se que sua atuação tem natureza consultiva, propositiva e de assessoramento, conforme Decreto 11.856/2023, arts. 5º e 6º.*

47. *Por sua vez a Creden, conforme Decreto 12.853/2026, é órgão de assessoramento ao Presidente da República nas áreas de relações exteriores e defesa nacional.*

48. *O GSI/PR é a entidade que preside o CNCiber por meio de representante designado. Segundo a Lei 14.600/2023, compete ao GSI/PR assistir diretamente o Presidente da República no desempenho de suas atribuições, especialmente quanto a assuntos militares e de segurança.*

49. *Já a Casa Civil, nos termos do 3º da Lei 14.600/2023, assiste diretamente o Presidente da República no desempenho de suas atribuições e, no que diz respeito à instituição de uma PNCiber nacional, sua atuação alcança apenas a coordenação e o monitoramento das ações governamentais, conforme voto condutor do Acórdão 276/2025-TCU-Plenário (peça 8, p. 2, item 8).*

50. *Verifica-se, portanto, que nenhuma dessas organizações do Poder Executivo Federal tem prerrogativa ou legitimidade para encaminhar o projeto de Lei ao Congresso Nacional. Esses órgãos possuem atribuições de assessoramento e formulação técnica, porém, não detêm competência para iniciar o processo legislativo necessário à instituição de PNCiber nacional.*

51. *Por outro lado, sob o viés de soberania digital e governança do tema segurança cibernética, são responsáveis o Congresso Nacional e a Presidência da República, já que são os responsáveis pelos normativos de maior hierarquia no disciplinamento do tema.*

52. *À luz da Constituição Federal (CF) de 1988, art. 84, inciso III, compete privativamente ao Presidente da República iniciar o processo legislativo, na forma e nos casos previstos na Constituição.*

53. *Além disso, segundo consta na CF, art. 61, § 1º, inciso II, alínea "a", são de iniciativa privativa do Presidente da República as leis que disponham sobre a "criação de cargos, funções ou*

---

[3] Tribunal de Contas da União. Lista de alto risco da Administração Pública federal. https://sites.tcu.gov.br/listadealtorisco/seguranca_da_informacao_e_seguranca_cibernetica.html

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade e informe o código 80802595.

empregos públicos na administração direta e autárquica ou aumento de sua remuneração". Já de acordo com o mesmo artigo, § 1º, inciso II, alínea "e" da Constituição Federal, cabe exclusivamente ao Presidente da República a iniciativa de leis que disponham sobre a criação e extinção de Ministérios e órgãos da administração pública direta, autárquica e fundacional.

54. *Considerando as limitações de competências normativas do CNCiber, Creden, GSI/PR e Casa Civil na proposição de projetos de lei ao Congresso Nacional (parágrafos 46-49) (**Error! Reference source not found.**), entende-se que **o envio do anteprojeto de lei pela Presidência da República** é condição necessária para dar início ao processo legislativo.*

55. *Sendo assim, deve ser feita proposta de recomendação à Presidência para que envide esforços no sentido de se articular com o Congresso Nacional para a instituição de uma política nacional compatível com o problema que visa enfrentar (ameaça cibernética).*

56. *Do exame de todo esse contexto, a AudTI propõe[4] **recomendar à Presidência da República** que defina a criação de uma Política Nacional de Cibersegurança com alcance nacional e mecanismos suficientes de enforcement, inclusive com a previsão de uma Autoridade Nacional de Cibersegurança, necessária para a coordenação da execução da política, informando, ainda, que tal definição deve ser feita mediante proposta de anteprojeto de Lei, não sendo suficiente, para tanto, a edição de Decreto do Poder Executivo, e que o risco descrito no parágrafo 44 será mantido na Lista de Alto Risco do TCU, podendo ser mitigado com envio ao Congresso Nacional da proposta de anteprojeto de Lei Geral da Cibersegurança formulada pelo CNCiber (peça 37).*

COMENTÁRIOS DOS GESTORES

57. *Esta seção visa atender ao disposto nas Normas de Auditoria do TCU, itens 144 a 148. Também atende ao disposto nos arts. 14 e 15 da Resolução - TCU 315, de 2020, no sentido de oportunizar aos destinatários das deliberações a apresentação de comentários sobre as propostas da equipe de auditoria, solicitando, em prazo compatível, informações quanto às consequências práticas da implementação das medidas aventadas e eventuais alternativas.*

58. *A Casa Civil enviou documentos contendo comentários sobre a proposta de encaminhamento, conforme peças 45 a 47.*

59. *Em síntese, os comentários **requereram a alteração do sujeito da recomendação, da Presidência da República para o GSI,** órgão responsável por submeter eventual proposta de proposição legislativa à Casa Civil, nos termos do Decreto 12.002/2024.*

60. *A tabela a seguir contempla os argumentos da Casa Civil para modificar a redação da proposta de encaminhamento formulada pela AudTI e as respectivas análises:*

Tópico	***Resumo do Argumento do Gestor***	***Referência***	***Análise da AudTI***
1. Ineficácia da proposta	*Impossibilidade de processamento da proposta aprovada pelo CNCiber, uma vez que não houve o indispensável referendo por parte do Ministro de Estado do Gabinete de Segurança Institucional (GSI), conforme previsto no artigo 46 do Decreto 12.002/2024.* *O rito necessário para o encaminhamento formal, pelo GSI, de proposta de Projeto de Lei Geral da*	*Nota SAJ 372/2026 (peça 47), itens 7-8* *SEI/PR - 7605368 – Despacho (peça 46)*	***A equipe não acolheu as justificativas.*** *A análise do contexto atual demonstra que existe um ciclo que se assemelha ao que já ocorreu no passado: o GSI/PR, no âmbito do CNCiber, elabora proposta de anteprojeto de lei; a minuta é tornada pública; a minuta é enviada para a Casa Civil; o anteprojeto não é encaminhado ao Congresso Nacional pelo Presidente da República (parágrafos 41-44).* *Esse histórico de idas e vindas sem uma solução concreta demonstra que direcionar a recomendação a órgãos de assessoramento ou de coordenação e monitoramento da ação governamental apenas perpetuará o risco descrito na seção 0.*

[4] Redação da proposta ajustada após comentários dos gestores.

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade e informe o código 80802595.

	Cibersegurança para análise da Casa Civil ainda não foi completamente cumprido, de modo que a proposta ainda está em fase de análise preliminar no interior daquele órgão, não estando disponível para análise formal desta SAG. *Por essa razão, sugere-se que seja requisitada alteração do sujeito da recomendação, da "Presidência da República" para o GSI, órgão responsável por submeter eventual proposta de proposição legislativa à Casa Civil, o que deve ser realizado nos termos do disposto pelo já citado Decreto 12.002, de 22 de abril de 2024.*		*A proposta de encaminhamento formulada pela AudTI não trata de atribuições operacionais ou executórias. Portanto, não há que se falar em alterar o sujeito da recomendação para o GSI, uma vez que essa proposição não foca em trâmites procedimentais e formalidades internas (Decreto 12.002/2024), desviando a atenção do atual empecilho para tratamento do risco, que é a falta de direcionamento e fixação de prazo pela Presidência da República para que as instâncias inferiores lhe apresentem proposta para encaminhamento legislativo.* *Dessa forma, a proposta de recomendação deve ser direcionada à Presidência da República, pois esta é a única instância que possui governança e autoridade sobre todas as partes envolvidas no processo, além de ter poder de decisão final e de articulação política.*
2. Pactuação prévia com outros Ministérios	*Um anteprojeto com essas características institucionais demandaria pactuação prévia com o Ministério da Gestão e da Inovação em Serviços Públicos (MGI) e Ministério do Planejamento e Orçamento (MPO).* *Com isso em mente, não se faz possível que seja a Presidência da República o sujeito genérico da recomendação, quando as providências necessárias para o regular prosseguimento da matéria são incumbidas, por força de norma, ao GSI. Consequentemente, o direcionamento da deliberação deve recair especificamente sobre o referido Gabinete, visto ser este o órgão público formalmente responsável por sanar as pendências procedimentais e conduzir as pactuações prévias exigidas para a maturação do anteprojeto*	*Nota SAJ 372/2026 (peça 47), itens 9-11* *SEI/PR - 7605368 - Despacho (peça 47) p. 1, III*	***A equipe não acolheu as justificativas.*** *A inclusão de mais um ator no processo torna ainda mais necessário que a recomendação seja feita a quem tem governança sobre todos.* *Casa Civil, GSI, CNCiber, MGI e MPO não detêm competência constitucional para iniciar o processo legislativo.* *A criação de órgãos públicos e a alteração da estrutura regimental do governo federal são competências privativas do Presidente da República, conforme o art. 84, III, c/c o art. 61, § 1º, II, "a" e "e", da Constituição Federal [5].* *A proposta de recomendação da AudTI apenas orienta que a Presidência da República inicie o processo de formulação de uma Política Nacional de Cibersegurança (CF, art. 84, inciso III[6]), permitindo que a pactuação com o MGI e MPO possa ser realizada durante o trâmite legislativo, sem que isso impeça o envio inicial do anteprojeto ao Congresso Nacional*
3. Competência Legislativa e Separação de Poderes	*A iniciativa legislativa para criar órgãos públicos e estruturar a administração é prerrogativa exclusiva do Presidente da República, conforme a Constituição*	*Nota SAJ 372/2026 (peça 47), itens 12-15*	***A equipe acolheu parcialmente as justificativas e fez ajustes no texto da instrução.*** *Das quatro propostas apresentadas pelo CNCiber, três preveem a criação de estruturas e cargos, e uma atribuições para uma estrutura existente (Anatel).*

[5] § 1º São de iniciativa privativa do Presidente da República as leis que: II - disponham sobre: a) criação de cargos, funções ou empregos públicos na administração direta e autárquica ou aumento de sua remuneração; e) criação e extinção de Ministérios e órgãos da administração pública, observado o disposto no art. 84, VI;

[6] Art. 84. Compete privativamente ao Presidente da República: III - iniciar o processo legislativo, na forma e nos casos previstos nesta Constituição;

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade e informe o código 80802595.

	Federal. O TCU não pode impor essa obrigação ao Executivo. *A recomendação do TCU para envio de anteprojeto de lei invade a esfera de competência do Executivo, desrespeitando o princípio constitucional da separação de poderes.* *Base legal:* *Art. 84, III, c/c o art. 61, § 1º, II, "a" e "e", da Constituição Federal.* *Princípio da separação dos Poderes (Constituição Federal de 1988).*		*O intuito da proposta formulada pela AudTI não é recomendar a criação de cargos e estrutura, mas a atribuição da responsabilidade pela execução política a uma autoridade nacional definida em Lei.* *Cabe à Presidência a discricionariedade de escolher a forma que melhor entender para implementar essa autoridade.* *Portanto, para que esta discricionariedade fique clara, a proposta de encaminhamento será ajustada para:* *recomendar, com fundamento no art. 11 da Resolução-TCU 315/2020, à Presidência da República que defina a criação de uma Política Nacional de Cibersegurança com alcance nacional e mecanismos suficientes de enforcement, inclusive com a previsão de uma ~~estrutura que assumirá o papel~~ Autoridade Nacional de Cibersegurança, necessária para a coordenação da execução da política, informando, ainda, que tal definição deve ser feita mediante proposta de anteprojeto de Lei, não sendo suficiente, para tanto, a edição de Decreto do Poder Executivo, e que o risco descrito abaixo será mantido na Lista de Alto Risco do TCU, podendo ser mitigado com envio ao Congresso Nacional da proposta de anteprojeto de Lei Geral da Cibersegurança formulada pelo CNCiber:* *Essa nova redação visa dar melhor clareza no sentido de que não configura ingerência na prerrogativa legislativa do Presidente e nem viola a separação de poderes, mas sim se trata de uma orientação do controle externo para que o Executivo tome medidas concretas para enfrentar os riscos cibernéticos, que já foram classificados como de alto impacto pelo TCU, assegurando a efetividade de políticas públicas essenciais à soberania digital.*
4. Controle Externo Limitado ***Estratégia de Gestão por Decretos***	*À luz do art. 20 da Lei de Introdução às Normas do Direito Brasileiro (Lindb), as decisões nas esferas administrativa e controladora devem, obrigatoriamente, motivar-se com base nas consequências práticas da imposição de novos deveres.* *O enfretamento das ameaças cibernéticas por meio de decretos presidenciais, como os Decretos 11.856/2023, 12.572/2025 e 12.573/2025, reflete uma estratégia legítima de gestão diante da amplitude da agenda nacional e das inevitáveis restrições orçamentárias* *Base legal:* *Art. 20 e Art. 22 da LINDB[7]; Limites da auditoria operacional.*	*Nota SAJ 372/2026 (peça 47), itens 16-17*	***A equipe não acolheu as justificativas.*** *O art. 20 da LINDB exige que decisões administrativas considerem as consequências práticas. A recomendação do TCU está alinhada a essa diretriz, pois busca mitigar os impactos de ataques cibernéticos, que já causaram prejuízos significativos à soberania digital.* *O TC 010.387/2024-2 (Auditoria na Política Nacional de Cibersegurança – PNCiber) demonstrou que o Estado brasileiro não possui autoridade responsável para orientar a atividade cibernética do país em âmbito nacional, de forma que os esforços empregados no âmbito do poder executivo federal são insuficientes para alcançar todo o país.* *Além disso, o TC 010.390/2024-3 (Auditoria de Controles de Segurança da Informação nas organizações do Sistema de Administração dos Recursos de Tecnologia da Informação - Sisp) evidenciou que as atividades de segurança cibernética no país estão insuficientes, como ocorre, por exemplo, nas 254 organizações do Sisp que não implementam completamente o conjunto básico de medidas de segurança de defesa cibernética esperado de uma*

[7] Art. 20. Nas esferas administrativa, controladora e judicial, não se decidirá com base em valores jurídicos abstratos sem que sejam consideradas as consequências práticas da decisão.
Art. 22. Na interpretação de normas sobre gestão pública, serão considerados os obstáculos e as dificuldades reais do gestor e as exigências das políticas públicas a seu cargo, sem prejuízo dos direitos dos administrados.

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade e informe o código 80802595.

	Decretos 11.856/2023, 12.572/2025 e 12.573/2025		*organização de pequeno a médio porte e não há organização que realize a consolidação desses dados para o restante do setor público e para o setor privado* *Recentemente o TC 012.850/2025-0 (Auditoria sobre golpes digitais por meio de personificação governamental) revelou que as fraudes e os golpes digitais apresentam tendência de aumento e se consolidaram como uma atividade econômica altamente lucrativa para o crime no país, gerando prejuízos estimados, em 2024, na ordem de 100 bilhões de Reais, o que equivale a aproximadamente 0,85% do PIB nacional. Apesar da gravidade do problema, a auditoria constatou que o combate aos golpes digitais baseados em personificação governamental ainda não está devidamente incorporado à agenda governamental.* *Portanto, entende-se que a estratégia adotada pelo Poder Executivo é legítima, porém as evidências demostram que é insuficiente.*
5. Fluxo Procedimental Interno estabelecido pelo Decreto n.º 12.002/2024	*A interferência do órgão de controle no rito de elaboração legislativa desconsidera também o fluxo procedimental interno estabelecido pelo Decreto 12.002/2024, posto que o processo de confecção de atos normativos no âmbito do Poder Executivo possui ritos próprios de governança, exigindo análises técnicas, de mérito e de impacto fiscal por comitês especializados e ministérios finalísticos antes de qualquer envio ao Congresso Nacional.* *Assim, a recomendação parece pressupor a possibilidade de que se ignore as fases de amadurecimento institucional que precedem o envio de um anteprojeto de lei ao Poder Legislativo.* *Base legal:* *Decreto 12.002/2024*	*Nota SAJ 372/2026 (peça 47), itens 18-19*	***A equipe não acolheu as justificativas.*** *A AudTI não pretende com a proposta de recomendação alterar procedimento legítimo estabelecido pelo Decreto 12.002/2024.* *O monitoramento do TC 004.306/2025-2 demonstra que o Comitê Nacional de Cibersegurança (CNCiber) realizou estudos técnicos e elaborou propostas de anteprojeto de lei, que foram submetidas à Casa Civil. Há, inclusive, nos estudos, o impacto orçamentário e financeiro com a criação da Autoridade (TC 004.306/2025-2, peça 59, item não digitalizável) (peça 3, p. 24-25, item 117.1.):* **Item / Ano 1 / Ano 2 / Ano 3 / Ano 4 / Ano 5** Pessoal no Ano: 69 / 103 / 137 / 172 / 206 Pessoal Acum.: 69 / 172 / 309 / 481 / 687 Subsídios: 25.742.117,04 / 65.055.513,12 / 118.364.299,68 / 186.491.157,84 / 269.480.572,32 Funções: 17.723.097,73 / 34.955.209,32 / 48.862.362,08 / 55.466.576,88 / 55.466.576,88 ***Pessoal: 43.465.214,77 / 100.010.722,44 / 167.226.661,76 / 241.957.734,72 / 324.947.149,20*** Custeio: 28.976.809,85 / 66.673.814,96 / 111.484.441,17 / 161.305.156,48 / 216.631.432,80 ***Total: 72.442.024,62 / 166.684.537,41 / 278.711.102,93 / 403.262.891,20 / 541.578.582,00*** *Outras informações tais como impacto sobre o meio ambiente, impacto sobre outras políticas públicas, benefícios esperados e urgência contam também dos estudos que levaram ao parecer de mérito do anteprojeto (TC 004.306/2025-2, peça 68).* *Portanto, o amadurecimento institucional já teria ocorrido, e a proposta de recomendação visa apenas garantir que o processo legislativo seja iniciado* *A proposta de recomendação dirigida ao Presidente da República, no contexto da Política Nacional de Cibersegurança (PNCiber), não busca interferir na prerrogativa exclusiva do Chefe do Executivo de iniciar o processo legislativo, mas sim garantir que as competências já atribuídas à Casa Civil pelo Decreto 12.002/2024 sejam efetivamente exercidas. O Capítulo VII do referido decreto estabelece que a Casa Civil é responsável por propor e examinar propostas de atos normativos encaminhados ao Presidente da República, incluindo a análise de mérito, constitucionalidade, legalidade e impacto fiscal. Assim, a recomendação proposta é no sentido de que o Presidente demande da Casa Civil o pleno cumprimento dessas atribuições, promovendo a tramitação do anteprojeto de lei já elaborado pelo CNCiber.* *No ciclo anterior, o monitoramento realizado no âmbito*

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade e informe o código 80802595.

			do TC 004.306/2025-2 revelou que o anteprojeto de lei, aprovado pelo CNCiber e submetido à Casa Civil, permanece paralisado, sem justificativa formal para sua não tramitação. Essa inércia compromete a implementação de uma PNCiber com alcance nacional e mecanismos de enforcement, conforme apontado no Acórdão 276/2025-TCU-Plenário, de relatoria do Ministro Benjamin Zymler. A ausência de ação por parte da Casa Civil perpetua o risco identificado na Lista de Alto Risco da Administração Pública Federal, que ameaça, em última análise, a soberania digital do país na perspectiva da segurança cibernética. *Portanto, a recomendação proposta pela AudTI não invade a discricionariedade política do Presidente, mas reforça a necessidade de que Presidência exerça governança sobre a Casa Civil, com o intuito de viabilizar o envio do anteprojeto ao Congresso Nacional.*
6. Tutela do planejamento normativo futuro do Estado	*O controle exercido pelo Tribunal de Contas deve se ater à conformidade legal, à legitimidade e à economicidade dos atos já praticados, abstendo-se de tutelar o planejamento normativo futuro do Estado.* *O direcionamento de ordens ou recomendações que moldem a iniciativa de leis ordinárias e a organização regimental de ministérios extrapola os limites constitucionais da auditoria operacional e invade a arena da discricionariedade política originária.* *A escolha da melhor estratégia regulatória, bem como o momento político adequado para a conversão de uma diretriz administrativa em projeto de lei, constitui matéria de mérito administrativo. A ingerência em tais opções por parte de órgãos de controle externo encontra óbice intransponível no princípio constitucional da separação dos Poderes.*	*Nota SAJ 372/2026 (peça 47), itens 21-25*	***A equipe não acolheu as justificativas.*** *Com a nova redação da proposta de recomendação formulada pela AudTI, há clareza que o TCU não está tutelando o planejamento normativo futuro do Estado (não molda o conteúdo do anteprojeto de lei), mas exercendo sua função constitucional de controle externo, que inclui a emissão de recomendações para mitigar riscos e aprimorar a governança pública. O art. 11 da Resolução-TCU 315/2020 autoriza o Tribunal a recomendar ações que mitiguem riscos identificados, como no caso da segurança cibernética, que foi incluída na Lista de Alto Risco da Administração Pública Federal.* *Quanto ao momento, a AudTI não fixou prazo para a recomendação ser implementada, mas informa que o Risco potencialmente alcança todos os cerca de 220 milhões de brasileiros e o PIB nacional. Portanto, a redação da proposta permite que o Poder Executivo escolha a melhor estratégia regulatória, bem como o momento político adequado para envio do projeto de lei, ao mesmo tempo que informa a gravidade, urgência e tendência do risco.* *Por fim, entende-se que a proposta de encaminhamento está alinhada ao interesse público, pois busca proteger os cidadãos e a* ***soberania digital*** *do país contra os impactos de ataques cibernéticos. A ausência de uma política robusta perpetua os riscos identificados, justificando a necessidade de ação imediata do Presidente da República, que tem governança sobre o processo e participação do processo de criação dos normativos de maior hierarquia no disciplinamento do tema.*
7. Processo Legislativo Complexo e Prioridades do Executivo	*O envio de um anteprojeto de lei não é um ato simples e burocrático, mas exige articulação política e técnica para garantir sua aprovação no Congresso Nacional.* *A definição de prioridades legislativas é prerrogativa do Presidente da República, que deve equilibrar demandas complexas e urgentes em diversas áreas estratégicas.*	*Nota SAJ 372/2026 (peça 47), itens 26-29*	***A equipe acolheu parcialmente as justificativas, mas não fez ajustes no texto da instrução.*** ***O TCU, como órgão técnico, não opina em questões políticas, como não o fez na proposta de encaminhamento formulada****.* *Neste monitoramento, a AudTI restringiu-se a identificar riscos e responsáveis pelo seu gerenciamento, no caso, a Presidência da República.* *Este é um exercício legítimo do Controle Externo: a recomendação é técnica e fundamentada, a qual orienta que o processo legislativo seja iniciado para enfrentar os riscos cibernéticos identificados, tendo em vista que a*

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade e informe o código 80802595.

			estratégia atual de enfrentamento a esses riscos por meio de Decretos regulamentares é considerada insuficiente, conforme já exposto anteriormente. *Essa abordagem não adentra questões políticas ou de articulação com o Congresso Nacional, respeita a prerrogativa do Executivo de conduzir as negociações políticas e permite que as questões de mérito e oportunidade sejam discutidas no foro apropriado, sem comprometer a urgência de se enfrentar os riscos identificados o mais rápido possível.*

61. *Diante o exposto, a AudTI reformou a proposta de encaminhamento constante da instrução preliminar (peça 38, p. 8), cuja nova redação já está refletida no parágrafo 56:*

> *recomendar, com fundamento no art. 11 da Resolução-TCU 315/2020, à Presidência da República que defina a criação de uma Política Nacional de Cibersegurança com alcance nacional e mecanismos suficientes de enforcement, inclusive com a previsão de uma ~~estrutura que assumirá o papel de~~ Autoridade Nacional de Cibersegurança, necessária para a coordenação da execução da política, informando, ainda, que tal definição deve ser feita mediante proposta de anteprojeto de Lei, não sendo suficiente, para tanto, a edição de Decreto do Poder Executivo, e que o risco descrito abaixo será mantido na Lista de Alto Risco do TCU, podendo ser mitigado com envio ao Congresso Nacional da proposta de anteprojeto de Lei Geral da Cibersegurança formulada pelo CNCiber:*

CONCLUSÃO

62. *O CNCiber implementou a recomendação no item 9.1 do Acórdão 276/2025-TCU-Plenário (parágrafo 38).*

63. *Contudo, o risco permanece, pois, apesar das ações empreendidas pelo CNCiber e pelo GSI/PR no âmbito de suas competências, a ausência de uma Política Nacional de Cibersegurança (PNCiber) com alcance nacional, acompanhada de uma autoridade com prerrogativas suficientes para sua execução, impede a efetiva orientação do Estado brasileiro para a atividade de segurança cibernética no país (parágrafos 39-56), impactando negativamente na soberania digital do país (peça 3, p. 16-18, item 3.2).*

64. *Assim, enquanto as ações necessárias para o encaminhamento do citado anteprojeto de Lei ao Congresso Nacional não forem tomadas, a causa do risco persistirá, exigindo o acompanhamento pelo TCU das ações ou omissões para gerenciar o risco descrito na LAR.*

PROPOSTA DE ENCAMINHAMENTO

65. *Ante o exposto, submetem-se os autos ao gabinete do Relator, Ministro Benjamin Zymler, propondo:*

65.1. ***recomendar**, com fundamento no art. 11 da Resolução-TCU 315/2020, **à Presidência da República** que defina a criação de uma Política Nacional de Cibersegurança com alcance nacional e mecanismos suficientes de enforcement, inclusive com a previsão de uma Autoridade Nacional de Cibersegurança, necessária para a coordenação da execução da política, informando, ainda, que tal definição deve ser feita mediante proposta de anteprojeto de Lei, não sendo suficiente, para tanto, a edição de Decreto do Poder Executivo, e que o risco descrito abaixo será mantido na Lista de Alto Risco do TCU, podendo ser mitigado com envio ao Congresso Nacional da proposta de anteprojeto de Lei Geral da Cibersegurança formulada pelo CNCiber:*

> *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*

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade e informe o código 80802595.

*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.*

65.2. *nos termos do art. 8º da Resolução - TCU 315, de 2020, fazer constar, na ata da sessão em que estes autos forem apreciados, comunicação do Relator ao colegiado no sentido **de autorizar o monitoramento da recomendação** proposta nesta instrução.*"

É o relatório.

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade e informe o código 80802595.

VOTO

Trata-se de monitoramento com o intuito de avaliar a implementação da recomendação dirigida ao Comitê Nacional de Cibersegurança (CNCiber), com apoio do Gabinete de Segurança Institucional da Presidência da República (GSI), por meio do Acórdão 2.430/2024-Plenário, com nova redação dada pelo Acórdão 276/2025-Plenário.

2. A recomendação objeto de monitoramento está transcrita a seguir:

"*9.1. recomendar, com fundamento na Resolução-TCU 315/2020, art. 11, I, ao Comitê Nacional de Cibersegurança, com apoio, no âmbito de suas competências, do Gabinete de Segurança Institucional da Presidência da República, que gerencie o risco consistente em uma Política Nacional de Cibersegurança sem alcance nacional e sem estrutura com autoridade e prerrogativas suficientes para coordenar a execução dessa política; e avaliar em que medida a Política Nacional de Cibersegurança está de acordo com as boas práticas, em especial comparada ao previsto no Referencial de Controle de Políticas Públicas do TCU;*" (grifou-se).

3. A respeito, a unidade técnica informou que somente a superveniência de disciplina legal poderia estabelecer uma Política Nacional de Cibersegurança com alcance nacional, incluindo a criação de uma Agência Nacional de Cibersegurança (ANCiber), que cumpriria o papel de órgão executor da política pública.

4. Ao apreciar as ações adotadas pelos destinatários da recomendação, a unidade técnica registrou que eles elaboraram anteprojeto de lei a ser encaminhado ao Congresso Nacional. Assim, concluiu que "*dentro de suas competências legais, o Comitê adotou as medidas que estavam ao seu alcance para gerenciar o risco consistente em uma Política Nacional de Cibersegurança sem alcance nacional e sem estrutura com autoridade e prerrogativas suficientes para coordenar a execução dessa política*".

5. A respeito, a unidade instrutiva destacou que o anteprojeto de lei elaborado não foi encaminhado ao Congresso Nacional, perpetuando o risco identificado. Dessa forma, foi proposta a realização de nova recomendação, dessa vez dirigida à Presidência da República para que "*defina a criação de uma Política Nacional de Cibersegurança com alcance nacional e mecanismos suficientes de enforcement, inclusive com a previsão de uma Autoridade Nacional de Cibersegurança, necessária para a coordenação da execução da política, informando, ainda, que tal definição deve ser feita mediante proposta de anteprojeto de Lei*" (grifou-se).

6. Entretanto, entendo que expedição de nova recomendação não encontra amparo em razões de necessidade ou utilidade. O risco objeto da deliberação já foi identificado, examinado e formalmente levado ao conhecimento do Poder Executivo por meio da recomendação anteriormente proferida, circunstância que esgota a atuação pedagógica e indutora atribuída a este Tribunal nessa matéria.

7. A partir daí, cabe exclusivamente ao Poder Executivo deliberar acerca da conveniência e da oportunidade de encaminhar proposta legislativa destinada a suprir a lacuna normativa existente. Trata-se de juízo inserido no núcleo de discricionariedade administrativa e governamental, insuscetível de substituição pela vontade do órgão de controle.

8. Em outras palavras, a decisão de encaminhar, ou não, projeto de lei ao Poder Legislativo é fundamentada em critérios de oportunidade, conveniência, viabilidade e prioridades da ação estatal. Assim, não se mostra adequado que este Tribunal reitere recomendação destinada a instar a adoção de providência cuja pertinência já é conhecida pela Administração e cuja implementação depende de juízo discricionário reservado constitucionalmente ao Chefe do Poder Executivo.

9. Por certo, o risco da ausência da Política Nacional de Cibersegurança permanece. Por outro lado, a Casa Civil da Presidência da República possui papel de coordenação horizontal, monitoramento

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade e informe o código 80803113.

estratégico e integração de ações governamentais – imanente à sua importância como órgão de centro de governo - missão disposta genericamente no art. 3º, incisos I e IV, da Lei 14.600/2023" (grifou-se).

10. Assim, no presente momento processual, entendo que a medida mais adequada seja informar a Casa Civil da Presidência da República sobre o teor destes autos, para que o órgão avalie a matéria no âmbito de sua atuação como integradora das ações governamentais.

11. Por outro lado, ante o exposto, entendo que cabe considerar cumprida a recomendação constante do subitem 9.1 do Acórdão 2.430/2024-Plenário, com nova redação dada pelo Acórdão 276/2025-Plenário, e dar ciência aos órgãos envolvidos do que for decidido por este Tribunal.

Diante do exposto, voto por que o Tribunal adote o acórdão que ora submeto à deliberação deste Colegiado.

TCU, Sala das Sessões, em 21 de outubro de 2026.

BENJAMIN ZYMLER
Relator

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade e informe o código 80803113.

ACÓRDÃO Nº 2909/2026 – TCU – Plenário

1. Processo nº TC 004.306/2025-2.
2. Grupo II – Classe de Assunto: V – Monitoramento
3. Interessados/Responsáveis: não há
4. Órgão/Entidade: Gabinete de Segurança Institucional da Presidência da República.
5. Relator: Ministro Benjamin Zymler.
6. Representante do Ministério Público: não atuou.
7. Unidade Técnica: Unidade de Auditoria Especializada em Tecnologia da Informação (AudTI).
8. Representação legal: não há

9. Acórdão:

VISTOS, relatados e discutidos estes autos de monitoramento de recomendação efetuada em trabalhos de fiscalização,

ACORDAM os Ministros do Tribunal de Contas da União, reunidos em sessão do Plenário, por unanimidade, ante as razões expostas pelo relator, em:

9.1. considerar cumprida a recomendação constante do subitem 9.1 do Acórdão 2.430/2024-Plenário, com nova redação dada pelo Acórdão 276/2025-Plenário;

9.2. informar a Casa Civil da Presidência da República sobre o risco de a Política Nacional de Cibersegurança carecer de alcance nacional e de uma estrutura com autoridade e prerrogativas suficientes para coordenar a sua execução, a fim de que o órgão avalie a matéria, no momento em que entender adequado, no âmbito de sua atuação como integradora das ações governamentais; e

9.3. encaminhar cópia deste acórdão, acompanhado do relatório e do voto que o fundamentam, ao Comitê Nacional de Cibersegurança (CNCiber) e ao Gabinete de Segurança Institucional da Presidência da República (GSI/PR).

10. Ata n° 41/2026 – Plenário.
11. Data da Sessão: 21/10/2026 – Ordinária.
12. Código eletrônico para localização na página do TCU na Internet: AC-2909-41/26-P.
13. Especificação do quórum:
13.1. Ministros presentes: Walton Alencar Rodrigues (na Presidência), Benjamin Zymler (Relator), Jhonatan de Jesus, Odair Cunha e Rodrigo Pacheco.
13.2. Ministros-Substitutos convocados: Augusto Sherman Cavalcanti, Marcos Bemquerer Costa e Weder de Oliveira.
13.3. Presidente não votou (Resolução-TCU 375/2025, art. 3º).

(Assinado Eletronicamente)
WALTON ALENCAR RODRIGUES
na Presidência

(Assinado Eletronicamente)
BENJAMIN ZYMLER
Relator

Fui presente:

(Assinado Eletronicamente)
CRISTINA MACHADO DA COSTA E SILVA
Procuradora-Geral

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade e informe o código 80803759.