PRESIDÊNCIA DA REPÚBLICA
Gabinete de Segurança Institucional
Comitê Nacional de Cibersegurança

Ata da 8ª Reunião Ordinária (RO-004-25)

Em 17 de dezembro de 2025, das 14h30 às 17h30, reuniu-se no Palácio do Planalto, 4º Andar, Sala 96, o Pleno do Comitê Nacional de Cibersegurança (CNCiber) para sua Oitava Reunião Ordinária (RO-004-25).

1. PROCEDIMENTOS

1.1 Verificação do Quórum

Às 14h30 o Presidente do CNCiber abriu a RO-004-25 do CNCiber.

Em atendimento ao disposto no Decreto 11.856, de 26 de dezembro de 2023, que instituiu o CNCiber, procedeu-se, em primeira chamada, a verificação do quórum para a reunião. Constatou-se a presença de titulares e/ou suplentes de 20 das 25 instituições que compõem o CNCiber, cumprindo a disposição do Decreto 11.856 quanto ao quórum para reuniões do CNCiber.

1.2 Aprovação da Ata da RO-003-25

Procedeu-se, em seguida, à aprovação da ata da RO-003-25.

A referida ata fora aprovada *ad referendum* pelo Presidente do CNCiber após o envio da minuta aos membros e decorrido o prazo de manifestações em contrário, sem que nenhuma fosse registrada.

O Presidente, então, solicitou aos membros que confirmassem a referenda feita com relação à ata, a qual foi aprovada por unanimidade.

1.3 Aprovação da Pauta da RO-004-25

Procedeu-se, então, à aprovação da pauta previamente enviada aos participantes, acrescida de um item (3A) e com a subdivisão do item 5 em dois (5A e 5B) por sugestão do GSI, ficando a pauta final conforme transcrita a seguir.

1. *Verificação do quórum.*
2. *Aprovação da ata da RO-003-25.*
3. *Aprovação da pauta da RO-004-25.*

3A. Informe sobre o Marco Legal da Cibersegurança em tramitação no Senado.

4. *Deliberação sobre a conclusão dos trabalhos do GTT Lei Geral e encerramento do GTT.*

5A. Deliberação sobre o encaminhamento da proposta de Lei Geral da Cibersegurança, conforme apresentada pelo GSI e aperfeiçoada pelo GTT Lei Geral.

5B. Deliberação sobre o encaminhamento de proposta da ANATEL como Autoridade Nacional de Cibersegurança (ANCiber), conforme proposta apresentada pelo GSI.

6. *Deliberação sobre o encaminhamento de proposta de uma Agência Nacional de Cibersegurança (ANCiber) na modalidade agência reguladora (autarquia especial) para assumir a função de autoridade nacional de cibersegurança.*
7. *Deliberação sobre o encaminhamento de proposta de uma Autoridade Nacional de Cibersegurança (ANCiber) como autarquia não especial para assumir a função de autoridade nacional de cibersegurança.*

8. *Deliberação 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.*
9. *Deliberação sobre a conclusão dos trabalhos, encerramento e propostas do GTT SEICs.*
10. *Informe sobre o andamento dos trabalhos do GTT Cibereducação-Estratégias.*
11. *Informe sobre o andamento dos trabalhos do GTT P-Ciber-Estruturante.*
12. *Informe sobre o andamento dos trabalhos do GTT Maturidade.*
13. *Deliberação sobre o calendário de reuniões do CNCiber para 2026:*
    - *13.1. RO-001-26 – 18/03/26*
    - *13.2. RO-002-26 – 17/06/26*
    - *13.3. RO-003-26 – 16/09/26*
    - *13.4. RO-004-26 – 16/12/26*

A pauta foi aprovada por unanimidade.

1.4 Informe sobre o Marco Legal da Cibersegurança em tramitação no Senado.

O Presidente do CNCiber informou ao pleno que na quarta-feira (10/12/25) a Comissão de Constituição e Justiça (CCJ) do Senado aprovou por unanimidade o relatório do Sen. Hamilton Mourão sobre o PL 4.572, que estabelece o Marco Legal da Cibersegurança.

Em seguida solicitou à SE-CNCiber uma breve explanação sobre o referido Marco Legal, sua compatibilidade com a proposta de lei Geral da Cibersegurança em deliberação nesta RO-004-25, e sobre os próximos passos da tramitação.

O SE-CNCiber informou ao Plenário entender que os projetos de Lei são bastante complementares. Explicou que o Marco é subdividido em 4 grandes seções.

a) A primeira trata da terminologia para o contexto da regulamentação proposta.
b) A segunda trata do objeto da regulação, limitada à cibersegurança e à ciber-resiliência do setor público apenas, o que é bem mais restrito que a proposta do CNCiber.
c) A terceira estabelece o Programa Nacional de Segurança e Resiliência Digital e corresponde a 60% do texto do Marco Legal, de adesão voluntária, que pode ser adaptado com facilidade para ser integrado ao projeto de Lei Geral do CNCiber.
d) Já a quarta seção estabelece um ponto bastante relevante quanto ao financiamento da autoridade nacional de cibersegurança, tema não tratado pelo texto do CNCiber, sendo também facilmente adaptável.

Por conseguinte, os dois textos poderiam facilmente ser considerados complementares, e unificados em uma proposta única, ainda durante a tramitação na Comissão de Ciência e Tecnologia (CCT) do Senado, onde tramita em caráter terminativo (sem depender de aprovação no Plenário) naquela casa legislativa, evitando que as alterações sejam feitas na Câmara fazendo com que o projeto tenha que retornar ao Senado para nova aprovação.

O representante do MGI informou que a proposta do Senado já está circulando entre os Ministérios, que já foram instados a se manifestarem sobre ela, o que poderia dificultar a coordenação da redação dos textos. O SE-CNCiber informou que o CNCiber tem ciência disso, e que já há conversações entre a CC, a SRI e o GSI para, assim que aprovado o texto proposto pelo CNCiber, possam ser iniciadas as tratativas com o Senado. O representante do MJSP informou que seu Ministério também o foi, já tendo elaborado uma análise técnica e conversado com alguns Senadores. Informou também que entende que o Marco do Senado pode ser melhorado com elementos da proposta do CNCiber, e que concorda que o melhor seria que essa interlocução se desse ainda no Senado e reiterou que ouviu

dos Senadores que qualquer contribuição será bem-vinda.

O Presidente informou que essa percepção foi a razão da sugestão de separação da pauta do projeto da Lei Geral do CNCiber e da questão da ANATEL, sugerida pelo GSI.

1.5 Deliberação sobre a conclusão dos trabalhos do GTT Lei Geral e encerramento do GTT.

O Presidente observou que o GTT Lei Geral foi criado na RO-003-25 e integrado por 19 das 25 instituições do CNCiber, mas que houve interações também com o MRE, de forma que um total de 20 das 25 instituições do CNCiber tiveram participação direta no aperfeiçoamento do texto em deliberação.

O representante da ANATEL, um dos coordenadores do GTT, apresentou o relatório dos trabalhos do grupo. Informou que houve uma participação ativa de praticamente todos os membros do GTT. Informou que houve um trabalho de nivelamento com posterior detalhamento

O representante do MGI, o outro coordenador do GTT, observou que o projeto de Lei Geral é bastante completo, mas que entende que a integração deste com o texto do Senado não lhe parece tão fácil. Observou também que no tocante à proposta de uso do FNSP, embora importante, deve ser um tema polêmico posto que esses recursos são muito disputados.

Foi esclarecido pelo Presidente que, separadamente do anteprojeto de Lei Geral da Cibersegurança, as 3 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 4 propostas distintas, seriam encaminhadas à CREDEN, mas que cada uma delas seria votada individualmente para registro de seus apoios institucionais.

Apresentado o relatório do GTT Lei Geral, foi aprovado por unanimidade e o GTT foi encerrado.

1.6 Deliberação sobre o encaminhamento da proposta de Lei Geral da Cibersegurança, conforme apresentada pelo GSI e aperfeiçoada pelo GTT Lei Geral.

Passou-se à discussão do encaminhamento do Anteprojeto de Lei Geral da Cibersegurança elaborado pelo GSI e pela SAJ e aperfeiçoado pelo GTT Lei Geral. O Presidente informou que se tratava do texto que trata genericamente de uma Autoridade Nacional de Cibersegurança, adaptável a diferentes modelos de órgão de governança, retirando-se o Capítulo VI da proposta original, que trata da designação do órgão a exercer a função de Autoridade Nacional de Cibersegurança.

O representante do Banco Central observou que a legislação nacional sobre a regulação de setor financeiro é bastante específica sobre as prerrogativas do Bacen e do Conselho Monetário Nacional, e informou que a instituição entende que seriam necessários pequenos ajustes no texto, mas que esses seriam bastante pontuais, de forma a evitar a sobreposição de competências. Particular atenção mereceria o Art. 24, Inciso I, que trata da possibilidade de a ANCiber sancionar instituições financeiras por descumprimento de normas gerais sem que o regulador setorial fosse notificado da infração.

O representante da ANATEL reiterou que o texto foi elaborado com grande cautela sobre o a preservação das competências setoriais, mas que eventuais alterações poderiam vir a ser discutidas.

Após um rápido debate sobre o tema, envolvendo os representantes do BACEN, da ANATEL, da FGV, da CONEXIS-BRASSCOM e a SE-CNCiber, o representante do BACEN observou que de fato as alterações deverão ser pontuais, podendo ser discutidas posteriormente e que não inviabilizariam a aprovação do encaminhamento da proposta de texto apresentada pelo GTT Lei Geral.

O representante do MD observou que gostaria de propor pequenos ajustes nas definições constantes

do Art. 2º do Projeto de Lei Geral, em particular no tocante a um aumento do escopo da definição de Ciberespaço e um ajuste nas definições de ISAC.

O SE-CNCiber observou que sempre se pode melhorar os textos, mas que é bom lembrar que o texto passará por uma revisão na SAJ e na SAG (Casa Civil) e depois nas negociações com o Congresso. O representante da ANATEL observou que as discussões quanto às definições foram justamente as que demandaram mais tempo, e que a decisão do GTT foi de se apoiar o máximo possível naquelas definições que já haviam sido consensuadas com a SAJ, reduzindo o risco de alterações substanciais no texto.

O representante do CGI observou que o entendimento daquele comitê foi no sentido de registrado num parecer em que inseriram diversas considerações e que não elencavam preferências quanto ao órgão de governança, e que gostaria que o parecer do CGI, já enviado à SE-CNCiber, fosse apensado à ata da RO-004-25.

O representante do MGI, o outro coordenador do GTT, informou que no relatório do GTT o MGI fez constar um conjunto de 4 observações. Na revisão desta Ata, o representante do MGI solicitou que o relatório do GTT Lei Geral constasse como anexo, registrando os argumentos e contra-argumentos apresentados.

Ao final das considerações, o encaminhamento do texto foi posto em deliberação, sendo aprovado por unanimidade.

1.7 Deliberação sobre o encaminhamento da proposta da ANATEL como Autoridade Nacional de Cibersegurança (ANCiber), conforme proposta apresentada pelo GSI.

O Presidente colocou em deliberação a proposta de indicação da Agência Nacional de Telecomunicações (ANATEL) para atuar como autoridade nacional de cibersegurança.

A seguir, o Presidente franqueou a palavra àqueles que quisessem argumentar favorável ou desfavoravelmente à proposição.

O representante da FGV observou que sempre entendeu ser “a melhor alternativa na mesa”, uma vez que, junto ao Banco Central, é a única reguladora que já dedica esforço à cibersegurança do seu setor, tem disponibilidade orçamentária e de pessoal, sendo mais rapidamente efetiva do que a criação de uma nova agência/autoridade. Observou que a criação da ANPD mostra claramente a dificuldade de criação de um novo órgão até se tornar um órgão efetivo. Recomendou que se aproveite a oportunidade para se reformar a organização da ANATEL, de forma a melhorar sua autonomia e independência.

O representante do MCom observou que o ideal seria a criação de um órgão novo, específico, mas que diante dessa impossibilidade entende que a ANATEL é a melhor alternativa. Observou que a dificuldade de autonomia e independência decorre da Lei das Agências. Reiterou que a ANATEL tem ampla expertise na temática da cibersegurança, e que essa expertise tem que ser aproveitada.

O representante da ASSESPRO observou que sua instituição também se preocupa com a capacidade da ANATEL se adequar para tratar desse novo tema, posto que a cibersegurança é um “outro bicho” quando comparada à temática das telecomunicações. Na impossibilidade de se ter uma ANCiber “pura”, eles não seriam contrários à ANATEL assumir essa função, mas que seria necessário repensar a estrutura da ANATEL para tratar esse “bicho” que é a cibersegurança. Registrou também a preocupação com a grande concentração de mercado das grandes empresas de telecomunicações e de potencial influência dessas na cibersegurança.

O representante do MJSP lembrou que a primeira atividade do GTT Governança foi no sentido de

examinar o que havia órgãos de governança em termos internacionais. Que pouquíssimos países uniram órgãos de Telecom e de cibersegurança. Registrou que entende que a proposta de se usar a ANATEL como autoridade nacional de cibersegurança parece que vem muito mais da necessidade urgente de se ter um órgão do que de ser a melhor opção técnica. Que a ANATEL tem competências unicamente setoriais e que a cibersegurança é necessariamente transversal a 18 setores. Assim, a ANATEL não seria uma solução interessante para a cibersegurança e em conversas com Senadores observou que eles também seriam contrários.

O representante da ANATEL registrou que a ANATEL tem 28 anos de história, vindo de um setor de telecomunicações pré agência bastante arcaico, tendo sido a primeira experiência no Brasil, e que ao longo desse tempo levou banda larga e Internet para todo o País, e cada vez mais a segurança se aproxima do setor. Que a ANATEL vem fazendo entregas representativas para o País, tendo um know-how expressivo para o País. Que concorda que a cibersegurança é "um outro bicho" que vai demandar adaptação da ANATEL, mas que a atividade será mais de coordenação com reguladores de outros setores do que a de regulador direto. Que o CNCiber e o Sistema Nacional serão as estruturas que orientarão a ANATEL nessa temática. Que a ANATEL, assumindo a função de autoridade nacional de cibersegurança terá que promover uma mudança de regimento interno, o que demanda análise de impacto regulatório, audiência pública, tomada de subsídios, todo um processo normativo com participação social. Registrou que, como observado, tem uma estrutura capilar, tem orçamento protegido, não contingenciável, que tem uma estrutura central e 27 delegacias estaduais, um maturidade capaz de dar celeridade à incorporação de novas competências e desafios. Registrou ainda que desde 2012 a ANATEL já trata de segurança de infraestruturas críticas e que Telecom é um dos setores mais atingidos em cibersegurança, envolvendo cabos submarinos, 5G e 6G, satélites e diversos outros temas. Que desafios haverá, mas a ANATEL tem maturidade para absorvê-los.

A suplente da CONEXIS-BRASSCOM registrou a importância de se considerar o mundo real e o mundo ideal. Que a Casa Civil indicou que a criação de um órgão novo no atual momento fiscal seria muito difícil. Que a experiência da ANPD mostra que experimentação nessa temática é um problema, pois 5 anos depois de criada como autoridade a ANPD agora é transformada em Agência, mas ainda com 80% da legislação pendente de regulamentação pela "falta de braço" para atuar. Que todos no CNCiber vivem a angústia do desafio da cibersegurança e da constatação de que não dispomos de 5 anos para se criar uma agência e esperar que ela tenha robustez para tratar de seus assuntos. Entende ser importante registrar isso para que se compreenda a urgência do momento para se trabalhar com o que temos e que é uma testemunha do que a ANATEL é capaz de fazer com sua robusta experiência. Que compartilha do entendimento de que se está falando de uma "nova ANATEL", sendo necessário separar as duas temáticas e a existência de uma carreira específica, com pessoas com um "mindset" de cibersegurança. Que é necessário se estabelecer os contornos da nova tarefa e um amadurecimento da compreensão do que abarca essa nova competência.

O representante da CONEXIS-BRASSCOM registrou a importância de se atentar para a importância do fato de que a ANATEL tem, assegurada pelo TCU, a disponibilidade orçamenta=ária não contingenciável, fator primordial para a implementação dessa competência.

O representante do IPCD comentou que a preferência de sua instituição seria por uma ANCiber "puro-sangue", mas que na impossibilidade de criação desse órgão a indicação da ANATEL seria uma opção aceitável.

O SE-CNCiber registrou que a representação da FIESP, impossibilitada de participar da RO-004-25, encaminhou antecipadamente, por escrito, seu voto favorável à indicação da ANATEL como órgão de governança da cibersegurança.

O representante do MGI registrou que fez constar do relatório do GTT Lei Geral um conjunto de observações, mas que gostaria de destacar uma delas. Registrou que levar a competência de cibersegurança para a ANATEL deixando a parte da segurança da informação com o GSI poderia gerar um problema com os gestores de segurança da informação, pois criaria duas figuras diferentes olhando para o mesmo gestor de segurança, que receberia orientações de dois órgãos, algo que ele vê com preocupação. Registrou que alguns argumentam que isso ocorre apenas com o setor público, mas que esse setor é muito atacado.

A representante da RNP registrou que concorda com a necessidade de cuidados para a ANATEL assumir tal tarefa, que a preferência seria por uma ANCiber "puro-sangue", que o setor acadêmico é muito atacado, que a ANATEL não tem experiência com segurança nacional e segurança pública. Que tem muita preocupação com a atuação multissetorial, e assim a ANATEL não é a opção ótima, mas que estamos vivendo essa angústia de aceitar apenas o bom.

O representante do MGI reiterou sua preocupação com a divisão das responsabilidades de cibersegurança e segurança da informação. O suplente do GSI esclareceu que a tendência da regulação de cibersegurança é exigir que a alta-direção das instituições seja responsabilizada pela cibersegurança. Que hoje a regulação da cibersegurança setorial já é tratada separadamente do tratamento da segurança da informação, regulada pelo GSI.

Postos os argumentos, a proposição foi colocada em votação, recebendo **18 votos FAVORÁVEIS** e 2 votos CONTRÁRIOS. Os votos divergentes (contrários) foram do MJSP e do MGI.

1.8 Deliberação sobre o encaminhamento da proposta de uma Agência Nacional de Cibersegurança (ANCiber) na modalidade agência reguladora (autarquia especial) para assumir a função de autoridade nacional de cibersegurança.

O Presidente colocou em deliberação a proposta de indicação de criação da Agência Nacional de Cibersegurança (ANCiber), na modalidade agência reguladora, para atuar como autoridade nacional de cibersegurança.

O representante da FGV registrou que sua preferência mudou ao longo do último ano. Que originalmente entendia que um ANCiber "pura" seria a melhor opção, mas a potencial demora de 5 anos para a criação de uma Agência "puro-sangue" do zero não seria mais viável, e que o "trauma" da ANPD com a LGPD é o exemplo do que não se pode fazer com a cibersegurança. Assim, essa opção não é a sua preferência, mas a segunda opção.

O SE-CNCiber registrou que a representação da FIESP, impossibilitada de participara da RO-004-25, encaminhou antecipadamente, por escrito, seu voto preferencial pela indicação da ANCiber no modelo agência reguladora como órgão de governança da cibersegurança.

O representante do IPCD indicou que essa também é sua proposta preferencial.

Postos os argumentos, a proposição foi colocada em votação, recebendo **20 votos FAVORÁVEIS** e 0 votos CONTRÁRIOS.

1.9 Deliberação sobre o encaminhamento de proposta de uma Autoridade Nacional de Cibersegurança (ANCiber) como autarquia não especial para assumir a função de autoridade nacional de cibersegurança.

O Presidente colocou em deliberação a proposta de indicação de criação da Autoridade Nacional de Cibersegurança (ANCiber), na modalidade autarquia não-especial (modelo INMETRO ou IBAMA), para atuar como autoridade nacional de cibersegurança.

O representante da ANATEL registrou que a ANPD foi o último exemplo de uma autoridade criada nessa modelo autarquia não-especial e depois de 5 anos transformada em autarquia especial, demonstrando que essa opção não seria a mais adequada.

A representante do MRE argumentou que esse modelo não teria benefícios claros, pois teria custo similar ao dos demais modelos e alcance mais limitado.

Postos os argumentos, a proposição foi colocada em votação, recebendo **12 votos FAVORÁVEIS** e 8 votos CONTRÁRIOS. Os votos divergentes (contrários) foram do GSI, MRE, MCom, ANATEL, ASSESPRO, FGV, CONEXIS-BRASCOM e MD.

1.10 Deliberação 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.

O Presidente colocou em deliberação a proposta de indicação de criação de uma Secretaria Nacional de Cibersegurança, como entidade da administração federal direta, para atuar como autoridade nacional de cibersegurança.

A seguir, o Presidente franqueou a palavra àqueles que quisessem argumentar favoravelmente à proposição.

O representante do MGI registrou entender que é a opção mais viável pela existência da SSIC no GSI e da SGD no MGI. Argumentou que a Secretaria de Prêmios e Apostas (SPA do MF) seria um exemplo da viabilidade dessa opção.

O Presidente, então, franqueou a palavra àqueles que quisessem argumentar contrariamente à proposição.

O SE-CNCiber relatou que desde junho de 2023 o GSI apresentou a proposta de criação de uma agência reguladora para tratar do tema. Fez um breve histórico da criação da PNCiber e do CNCiber, da criação do GTT Governança em março de 2024, das discussões desse GTT até agosto, quando a opção Secretaria Forte e Secretaria Fraca foram descartadas em workshop na ENAP coordenado pelo MGI. Na ocasião as propostas selecionadas foram Agência Forte e Agência Fraca. Que em fevereiro de 2025, diante da informação de que restrições fiscais inviabilizariam a criação de uma Agência Reguladora, o GSI propôs uma adaptação do modelo de Agência Fraca na forma de uma Autoridade, uma autarquia não especial. Que em fevereiro de 2025 o MGI retomou a discussão do modelo Secretaria, mas que essa proposta não chegou a ser discutida em profundidade no GTT. Que a minuta de Decreto para instituição dessa Secretaria nunca chegou a ser discutida pelo GTT, mas que indicava que o quantitativo de pessoal dessa Secretaria seria o mesmo dimensionado pelo GSI para o modelo Autoridade, carreando assim custos similares, mas com menor alcance e menor autonomia. Registrou que o relatório do GTT Governança, aprovado na RO-001-25, registrou que 11 das 13 instituições participantes do referido GTT não apoiavam essa proposta. Considerando ainda a abstenção da Casa Civil, apenas o MGI apoiou essa alternativa. Registrou também que na RO-001-25, durante as deliberações sobre o relatório do GTT, instituições não participantes do grupo se preocuparam com o encaminhamento das alternativas como equivalentes, fazendo questão de registrarem que não o eram. Que esse modelo não teria paralelo no Brasil. Que a SPA/MF não é um paralelo adequado, pois é uma criação recente que atua num segmento muito específico e atingindo apenas algumas poucas dezenas de instituições reguladas. Que seria, assim, muito diferente de uma autoridade nacional de cibersegurança atuando transversalmente no âmbito dos 3 poderes, nos 3 níveis da Federação (União, Estado e Municípios) em quase duas dezenas de setores econômicos e regulando dezenas de milhares de instituições de portes variados. Que o TCU já apresentou ao CNCiber suas preocupações com a

necessidade de autonomia e celeridade de um órgão de governança da cibersegurança, o que não se encaixa na opção Secretaria.

O representante do MGI registrou que a proposta de Secretaria foi uma das 3 alternativas postas pelo GTT Governança.

O representante da ANATEL observou que essa opção existe, que os 3 cenários inicialmente propostos resultaram de um esforço do GTT para oferecer alternativas, mas que o que precisa ser considerado é que as alternativas oferecem capacidades distintas de entrega. Que pesa em desfavor da alternativa Secretaria é a legitimidade, em particular no tocante à normatização do setor privado. Que quando o Congresso abre mão de regular a iniciativa privada o faz delegando a uma agência reguladora essa função, posto que agências reguladoras têm que seguir um processo de participação social e transparência. Que quando se faz isso por meio de uma Secretaria o processo se complica em várias dessas bases. Que outro aspecto é o de que uma Secretaria é mais vulnerável no sentido da perenidade, posto que hoje se tem uma Secretaria e numa mudança de governo essa Secretaria pode deixar de existir, ou se tem um investimento na Secretaria e numa mudança de governo pode não haver mais esse investimento. Que, assim, embora haja alternativas distintas, cada um tem suas vantagens e desvantagens com relação à capacidade de entrega.

Postos os argumentos, a proposição foi colocada em votação, recebendo **19 votos CONTRÁRIOS** e 1 voto FAVORÁVEL. O voto divergente (favorável) foi do representante do MGI.

Na revisão desta Ata, o representante do MGI solicitou que ficasse registrado que, diferentemente do que foi apontado pela SE-CNCiber, a inclusão da alternativa “Secretaria” decorreu de solicitação da Casa Civil da Presidência da República, como membro do GTT Governança, tendo sido aceita pelo MGI e pela ANATEL e levada ao conhecimento de todo o GTT Governança. Que não houve votação no âmbito do GTT Governança para escolha entre alternativas, tendo-se optado por submeter todas as três alternativas ao Pleno do CNCiber. Ainda, que determinados argumentos registrados (como referências à efetividade da SPA/MF e a apontamentos do TCU) foram apresentados no debate pelo GSI, constituindo interpretações expostas no âmbito da discussão, registrando-se que o MGI entende que tais modelos podem, em tese, atender aos apontamentos do TCU, desde que devidamente contextualizados e aperfeiçoados para o escopo específico da governança em cibersegurança.

1.11 Ordenação preferencial das alternativas de órgão de governança da cibersegurança nacional.

Findas as deliberações sobre os 4 cenários de órgãos de governança da cibersegurança, conforme solicitações feitas em diferentes momentos da reunião, o Presidente propôs que as instituições representadas indicassem suas preferências de cenários de órgão de governança. Com a anuência dos presentes, a SE-CNCiber realizou a chamada de cada órgão representado para que indicasse suas preferências. Ao final foi feita a verificação dos registros, reproduzidos na tabela abaixo:

Instituição	ANATEL	Agência Reguladora	Autarquia Não-Especial	Secretaria
GSI	**1**	**2**	**NR**	**NR**
MCom	**1**	**2**	**NR**	**NR**
MD	**1**	**2**	**3**	**4**
MDIC	**2**	**1**	**3**	**4**

Instituição	ANATEL	Agência Reguladora	Autarquia Não-Especial	Secretaria
MF	1	2	NR	NR
MGI	NR	2	3	1
MJSP	NR	1	2	NR
MME	4	1	2	3
MRE	2	1	NR	3
BACEN	1	2	3	4
ANATEL	1	2	NR	NR
CGI	X	X	X	X
IASP	2	1	3	4
IPCD	3	1	2	NR
CPqD	2	1	4	3
FGV	1	2	NR	NR
RNP	2	1	3	NR
ASSESPRO	2	1	NR	NR
CONEXIS-BRASSCOM	1	2	3	NR
FIESP	3	1	2	NR

Legenda:

1 – Primeira preferência

2 – Segunda preferência

3 – Terceira preferência

4 – Quarta preferência

X – Sem preferência

NR – Não recomenda

1.12 Deliberação sobre a conclusão dos trabalhos do GTT SEICs e encerramento do GTT.

O presidente observou que o GTT SEICs foi instituído na RO-001-25.

O representante da ANATEL, instituição coordenadora do GTT, apresentou o relatório dos trabalhos do grupo. Informou que se buscou uma maior interação com outras agências reguladoras, mas que a resposta dessas foi pouco significativa. Que foi elaborado um material bastante robusto, mas de nível mais alto, com recomendações mais genéricas do que prescritivas.

Apresentado o relatório, foi aprovado por unanimidade e o GTT foi encerrado.

1.13 Informe sobre o andamento dos trabalhos do GTT Cibereducação-Estratégias.

A representante da RNP, integrante do GTT, fez uma explanação sobre o andamento dos trabalhos do GTT. Informou que o foco do GTT é nas melhores formas de se usar o vasto material de cibereducação disponível no Brasil. Registrou que o grupo tem discutido a questão da educação de neurodivergentes

e os impactos da IA na cibereducação. Que a conscientização será feita para os diferentes públicos prioritários nas linguagens específicas: crianças e adolescentes, neurodivergentes, idosos e público em geral. Que os temas dos materiais devem ser tratados com ênfase nesses diferentes grupos. Que a forma (meio e linguagem) de apresentar esses temas influencia sua absorção cognitiva. A representação da ANATEL informou que o GTT carece da expertise para tratar de material para certos públicos mais específicos. Por essa razão a ênfase do GTT agora está no público em geral e em crianças e adolescentes.

1.14 Informe sobre o andamento dos trabalhos do GTT P-Ciber-Estruturante.

O representante da SE-CNCiber, um dos coordenadores do GTT, fez uma explanação sobre o andamento dos trabalhos do Grupo. Informou que o GTT trabalha com 12 Iniciativas Estratégicas (IE) Estruturantes, a saber:

01) Cibereducação-Estratégias
   a. A IE foi proposta pelo próprio CNCiber, sendo objeto de um GTT específico.
02) "Programa" de Robustecimento da Cibersegurança
   a. A IE foi proposta pelo MGI e será detalhada em breve.
03) Selo Nacional [MGI]
   a. A IE foi proposta pelo MGI e será detalhada em breve, mas observa-se que difere do selo de maturidade objeto da E-Ciber, constituindo-se num selo de adesão voluntária ao programa citado no item 2.
04) Modelo de Maturidade Nacional
   a. A IE foi proposta pelo próprio CNCiber e é objeto do GTT Maturidade.
   b. No presente momento considera-se a criação de um modelo próprio que utilize elementos do CMM Oxford e do GCI da UIT.
05) Modelo de Maturidade Institucional (C2M2 + CSF + CIS) [CNCiber]
   a. A IE foi proposta pelo próprio CNCiber e é objeto do GTT Maturidade.
   b. No presente momento considera-se a criação de um modelo próprio que utilize elementos do C2M2 do USDoE, no CSF 2 do NIST e no CIS V8.
06) Lei Geral da Cibersegurança/Marco Legal da Cibersegurança
   a. A IE foi proposta pelo próprio CNCiber e foi objeto de um GTT específico, encerrado nesta RO.
   b. As próximas atividades serão de encaminhamento das propostas para compatibilização com o Marco Legal em discussão no Senado.
07) Órgão de Governança
   a. A IE foi proposta pelo próprio CNCiber e foi objeto do GTT Governança e do GTT Lei Geral.
   b. Espera-se, para breve, uma formalização do Governo quanto à opção preferencial dentre aquelas apresentadas.
08) Hotsite do P-Ciber
   a. A IE foi proposta pelo próprio CNCiber e foi objeto do GTT P-Ciber.
   b. O modelo em estudo é baseado no site do governo da Suíça, permitindo a navegação iniciada na PNCiber, passando para a E-Ciber e para o P-Ciber, apresentando os detalhes de cada item e subitem.
09) Fundos Setoriais
   a. A IE foi proposta pelo GSI, considerando que a principal dificuldade para cada ação estruturante é a obtenção de recursos financeiros.
   b. A ideia consiste em viabilizar o uso dos fundos setoriais já existentes para ações e

programas relativos à cibersegurança, com a menor alteração possível em suas regulamentações.

c. Os beneficiários dos recursos, portanto, seriam os mesmos de hoje. Apenas alterar-se-ia o escopo dos projetos para permitir seu uso em ações de cibersegurança.
d. Observou-se que recentemente houve proposta na Câmara dos Deputados para uso do FNSP que se alinha com o tema em discussão no GTT.
e. Dentre os fundos analisados destacam-se:
   i) FNSP
   ii) FUST
   iii) FUNTTEL
   iv) FDD
   v) FNDIT
   vi) FNDCT
   vii) PPI-Lei de TICs
   viii) Fundo Aeronáutico
   ix) Fundo do Exército
   x) Fundo Naval
   xi) Outros

10) Centro Coordenado Provisório
    a. A IE foi proposta pelo MGI e será detalhada em breve.
    b. Essencialmente consiste em uma conjugação de esforços do CTIR Gov (GSI) e do SISP (MGI) para atuação coordenada em prevenção e resposta a ciberincidentes até a operacionalização do CENCiber previsto na Anteprojeto da Lei Geral da Cibersegurança aprovado pelo CNCiber.
11) Fortalecimento de ISACs
    a. A IE foi proposta pelo GSI.
    b. Consiste na operacionalização das propostas do GTT ISACs e da Portaria GSI 148/2025, aumentando a capilaridade da atuação da REGIC para chegar ao setor privado.
12) Programa de Apoio PMEs
    a. A IE foi proposta pelo GSI.
    b. Consiste na operacionalização de captação de recursos e concessão de crédito para fomentar ações de cibersegurança junto a micro e pequenas empresas, em conjunto com instituições como BID, SEBRAE, BNDES, Banco do Brasil e outras

O representante do MGI, o outro coordenador do GTT, registrou que o GTT faz um trabalho interessante para juntar de 10 a 15 ações ao inventário feito pelo GTT P-Ciber.

A representante da RNP perguntou como essas iniciativas serão colocadas com relação ao tempo e os responsáveis por sua execução, ao que o representante do MGI informou que a partir de agora o GTT vai trabalhar no detalhamento das IEs na forma de um modelo 5W2H. O SE-CNCiber registrou que algumas dessas propostas não dependem exclusivamente do Executivo Federal, mas que ele pode propor, por exemplo ao Legislativo, que vai debater isso no seu tempo.

1.15 Informe sobre o andamento dos trabalhos do GTT Maturidade.

O representante da SE-CNCiber, um dos coordenadores do GTT, fez uma explanação sobre o andamento dos trabalhos do Grupo. Informou que inicialmente o GTT se debruçou no entendimento das diferenças entre modelos de maturidade e modelos de conformidade (compliance). Que a opção preferencial, dada a abrangência diversa pretendida para o modelo, seria de um modelo mais

descritivo (foco no “o quê”) mais que prescritivo (focado no “como”). Que para a maturidade nacional o GTT trabalha com elementos dos modelos de maturidade CMM de Oxford e GCI da UIT. Que para a maturidade institucional trabalha com um mix dos modelos de maturidade C2M2 do USDoE e CSF 2.0 do NIST, incorporando ainda elementos dos modelos de conformidade CIS V8, base do PPSI do MGI, e ISO 27.000, embora esse último com menor ênfase em função do entendimento de que seus elementos já estão integrados aos demais.

Em seguida, informou que o modelo nacional a ser proposto deve seguir a seguinte “lista de desejos”:

a. Hierarquia multinível, provavelmente com 3 níveis:
   i) Tema (ATIVOS, RESPOSTA, RISCOS, PESSOAL, ...)
   ii) Controle (Ativos de HW TI, Ativos de HW TO, Ativos de SW, ...)
   iii) Medida/Ação (Inventariar, Proteger, ...)
      a. Não confundir com o Método ou Procedimento (Ad Hoc, Procedural, Automatizado, ...)
      b. Observar que o Método gera Evidências Observáveis
b. Quatro Escalas
      a. Inicial, Médio, Evoluído, Avançado
c. Perfis Configuráveis
   i) Por Setor
   ii) Por Porte da Instituição
   iii) Por “Magnitude do Risco” (Probabilidade x Severidade)
d. Foco no Desenvolvimento de Capacidades
   i) Descritivo > Prescritivo
e. Institucional Alimentando o Nacional
   i) Coleta de informações por setor, ou por porte das instituições, para alimentar o processo decisório nacional

O representante do MGI, o outro coordenador do GTT, informou que essa última questão nos permitirá ter políticas públicas de cibersegurança baseadas em evidências mensuráveis.

O representante da ASSESPRO questionou se seria possível ser feito um benchmark, ou ao menos haver um “de-para” que permitisse essa comparação entre os diferentes modelos. O representante do MGI observou que o CIS é largamente utilizado em diversos lugares do mundo, e que no que for possível será adotado.

1.16 Deliberação sobre o calendário de reuniões do CNCiber para 2026.

Na deliberação sobre o calendário de reuniões de 2026, foi solicitada a alteração da primeira data, originalmente 18/03;2026, para 25/03/2026, sem observações sobre as demais datas. Outrossim, o calendário de reuniões foi aprovado como segue:

a. RO-001-26 – 25/03/26
b. RO-002-26 – 17/06/26
c. RO-003-26 – 16/09/26
d. RO-004-26 – 16/12/26

2. ENCERRAMENTO

Não havendo mais temas a tratar, a RO-004-25 foi declarada encerrada pelo Presidente.

Na revisão desta Ata, foi solicitado pelo representante do MGI que fosse reiterado o disposto no item 1.5 no sentido de que foi esclarecido pelo Presidente que, separadamente do anteprojeto de Lei Geral

da Cibersegurança, as 3 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 considerada pelo GTT Lei Geral (ANATEL como autoridade nacional de cibersegurança), constituindo assim 4 propostas distintas, seriam encaminhadas à CREDEN, cada uma das quais tendo registrado diferentes apoios institucionais. Sugeriu, também, que fossem incorporados a esta Ata, como anexos, o relatório do GTT Governança e as manifestações individuais de cada instituição participante do GTT Governança sobre os modelos de órgão de governança analisados.

3. ANEXOS

Anexei a essa ata:

1. As manifestações escritas quanto ao anteprojeto de Lei Geral da Cibersegurança e às preferências de órgão de governança enviadas anteriormente à RO-004-25 pelos representantes da FIESP, CGI e IPCD.
2. O Relatório do GTT Lei Geral aprovado pelo CNCiber.
3. O Relatório do GTT Governança aprovado pelo CNCiber.
4. As manifestações de preferência das instituições do GTT Governança quando da conclusão dos trabalhos do GTT.

MARCELO ANTONIO OSLLER MALAGUTTI

Secretário-Executivo do CNCiber

CONSELHEIRO TITULAR DO CNCIBER - SETOR EMPRESARIAL

POSICIONAMENTO – RONY VAINZOF

Ref: RO 004-25 do CNCiber que ocorrerá no dia 17/12/25 - Deliberação sobre o encaminhamento da proposta de Lei Geral da Cibersegurança e Autoridade Nacional de Cibersegurança.

Sumário

Considerandos:

- Empresas privadas e órgãos do Estado que não nasceram digitais, inevitavelmente estão em fase de digitalização e emprego de inovações tecnológicas;
- Há aumento vertiginoso na escalada e sofisticação dos ataques cibernéticos. O uso de Inteligência Artificial e algoritmos avançados aumenta tanto as capacidades defensivas quanto os riscos de exploração por agentes mal-intencionados, demandando estratégias de mitigação robustas;
- A proteção de infraestruturas críticas e de serviços essenciais deixou de ser questão apenas empresarial, tornando-se elemento central da segurança nacional e da estabilidade econômica dos países;
- A insegurança cibernética desponta como preocupação crítica a curto e longo prazo, conforme relatórios do Fórum Econômico Mundial. É pauta que vai muito além de fraudes e vazamento de dados, pois ataques cibernéticos podem paralisar organizações e países;
- Incidentes de segurança no Brasil podem ter gerado em 2024 prejuízos diretos, indiretos e induzidos de R$ 2,3 Trilhões, o que representa perda de 18% no PIB anual (INCC);
- A fragmentação de iniciativas regulatórias e normativas gera respostas lentas e ineficazes diante do volume de ameaças e complexidade de suas causas;
- A grande maioria dos incidentes de cibersegurança poderiam ser evitados com medidas básicas de proteção;
- Cibersegurança é fundamental para a sobrevivência e competitividade das empresas e nações; e

- A natureza transnacional das ameaças cibernéticas exige colaboração entre governos, empresas e organismos internacionais para aprimorar a resposta a incidentes e fortalecer a resiliência digital.

Premissas para a abordagem regulatória e para o órgão de governança:

- Marco Legal de Cibersegurança:

    - Claro, equilibrado, flexível e eficiente, capaz de alinhar as normas nacionais às melhores práticas internacionais, sem impor custos operacionais excessivos ou proibitivos, permitindo ambiente seguro, competitivo e inovador, no qual empresas possam crescer sem enfrentar obstáculos desproporcionais;
    - Abordagem baseada em risco, com maior peso normativo aos serviços essenciais e de infraestruturas críticas;
    - Excepcionar a carga regulatória para empresas de pequeno porte;
    - Incentivos econômicos e fiscais para empresas com boas práticas de governança em cibersegurança ou que desenvolvam soluções inovadoras, como redução tributária, acesso a crédito facilitado e prioridade em licitações públicas;
    - Precaução ao "importar" conceitos e regulamentações estrangeiras, garantindo a adaptação à realidade nacional; e
    - Implementação de programa nacional de conscientização em cibersegurança para empresas e cidadãos, que leve também a inclusão do tema nos currículos educacionais, desde o ensino básico até o superior.

- Autoridade Nacional de Cibersegurança:

    - Coordenar ações de cibersegurança com integração entre diferentes órgãos governamentais, setor privado e academia;
    - Poderes regulatórios claros para garantir ambiente mais equilibrado, promovendo segurança jurídica e previsibilidade, além de ser capaz de organizar, direcionar e impulsionar diferentes soluções dentro e fora do estado;
    - Evitar sobreposição de competências (*bis in idem*) com órgãos reguladores setoriais, garantindo que a regulamentação, fiscalização e sanção permaneçam no âmbito dos órgãos específicos de cada setor ou matéria;
    - Harmonizar entendimentos e diretrizes, promovendo a padronização de normas, a interoperabilidade regulatória e a cooperação entre setores;
    - Regular setores não abrangidos por reguladores específicos, prevenindo lacunas normativas e garantindo uma abordagem integrada e consistente em todo o ecossistema do país; e
    - Não impor custo econômico adicional à sociedade para a sua criação.

Conclusão:

1) **Marco Legal:** estou de acordo com o texto proposto no GTT da Lei Geral de Cibersegurança: Documento Item 5.2 - APL Geral Cibersegurança - Final.pdf

2) **Órgão Central:**

   a. As propostas do GTT anterior de "Autarquia" e "Agência Reguladora" melhor se enquadram nas premissas descritas acima;

   b. Não sendo factível no momento, por questões de orçamento, a criação de um dos órgãos supra, estou de acordo com o encaminhamento da proposta de Lei Geral da Cibersegurança com a ANATEL como Autoridade Nacional de Cibersegurança, conforme apresentada pelo GSI e aperfeiçoada pelo GTT Lei Geral, sendo importante salvaguardas para mitigar conflito de interesse.

São Paulo, 11 de dezembro de 2025.

Atenciosamente,

Rony Vainzof
Conselheiro Titular do CNCiber – Setor Empresarial

PARECER

CONTRIBUIÇÃO DO CGI.br À ANÁLISE DOS MODELOS DE GOVERNANÇA PARA A AUTORIDADE NACIONAL DE CIBERSEGURANÇA

1. INTRODUÇÃO

CONSIDERANDO que a partir das discussões no GTT Governança e, posteriormente, no GTT Lei Geral do Conselho Nacional de Cibersegurança (CNCiber) acerca da criação de um arcabouço institucional para coordenar e fortalecer as ações de Segurança Cibernética no Brasil, foram analisados quatro modelos de governança: (1) Secretaria; (2) Autarquia Especial; (3) Agência Reguladora nova; e (4) Atribuição a agência existente (ANATEL);

CONSIDERANDO o Decreto nº 12.573, de 4 de agosto de 2025, que instituiu a Estratégia Nacional de Cibersegurança (E-Ciber), estruturada em quatro eixos temáticos: proteção e conscientização; segurança e resiliência; cooperação e integração; e soberania nacional e governança;

CONSIDERANDO que tramita no Senado Federal o Projeto de Lei do Sen. Esperidião Amin, que institui o Marco Legal da Cibersegurança, cria o Programa Nacional de Segurança e Resiliência Digital e prevê a designação de autoridade nacional de cibersegurança em regulamento;

CONSIDERANDO a elaboração do Anteprojeto de Lei Geral de Cibersegurança pelo GTT Lei Geral, coordenado pelo Gabinete de Segurança Institucional (GSI) e pelo CNCiber;

CONSIDERANDO a Nota Pública do Comitê Gestor da Internet no Brasil (CGI.br), de 14 de novembro de 2025, que estabelece princípios e diretrizes fundamentais para a governança da cibersegurança nacional;

CONSIDERANDO a tradição do CGI.br de contribuir com análises técnicas fundamentadas, em linha com seu papel de espaço multissetorial e participativo para a governança da Internet no país;

CONSIDERANDO que devo contribuir da melhor forma possível, apresentando uma avaliação técnica robusta sobre os quatro modelos de governança discutidos, sobre o Anteprojeto de Lei Geral de Cibersegurança e sobre o PL em tramitação no Senado Federal, à luz dos princípios estabelecidos pelo CGI.br e da Estratégia Nacional de Cibersegurança.

2. POSICIONAMENTO INSTITUCIONAL DO CGI.br

O Comitê Gestor da Internet no Brasil, em sua Nota Pública de 14 de novembro de 2025, estabeleceu diretrizes fundamentais para o debate regulatório em torno da segurança cibernética, sem, contudo, manifestar preferência por modelo institucional específico. Essa postura reflete a natureza multissetorial do CGI.br e seu compromisso com a construção colaborativa de políticas públicas.

Alinhado a essa tradição institucional, o presente parecer **não manifestará opção pontual por nenhuma das quatro propostas de governança em debate**. Em vez disso, apresentará análise técnica fundamentada de cada modelo, identificando pontos fortes, fragilidades, aderência à E-Ciber e condições necessárias para sua eventual implementação, de modo a subsidiar a decisão que será tomada pelas instâncias competentes.

3. MARCO NORMATIVO VIGENTE E EM DISCUSSÃO

3.1. Estratégia Nacional de Cibersegurança (E-Ciber) – Decreto nº 12.573/2025

O Decreto nº 12.573, de 4 de agosto de 2025, instituiu a E-Ciber estruturada em quatro eixos temáticos que devem orientar a atuação da futura autoridade nacional de cibersegurança:

1. **Proteção e conscientização do cidadão e da sociedade:** criação de condições seguras para uso de serviços digitais, com atenção especial a grupos vulneráveis (crianças, idosos, neurodivergentes);
2. **Segurança e resiliência dos serviços essenciais e infraestruturas críticas:** instrumentos efetivos para prevenção e resposta a ciberincidentes;
3. **Cooperação e integração entre órgãos e entidades:** promoção do debate e intercâmbio de informações em âmbito nacional e internacional;
4. **Soberania nacional e governança:** proteção dos interesses brasileiros no ciberespaço e garantia de ambiente cibernético confiável.

A E-Ciber será implementada por meio do Plano Nacional de Cibersegurança, a ser proposto pelo CNCiber e aprovado pelo Ministro-Chefe do GSI. Destaca-se que o Decreto prevê ações como: criação de selo nacional de certificação; lista de alto risco de cibersegurança; mecanismo nacional de notificação de ciberincidentes; e modelo nacional de maturidade em cibersegurança.

3.2. Projeto de Lei do Senado – Marco Legal da Cibersegurança

O PL de autoria do Sen. Esperidião Amin propõe instituir o Marco Legal da Cibersegurança com abordagem distinta do Anteprojeto do CNCiber. Suas principais características são:

- **Foco na administração pública:** diferentemente do Anteprojeto que abrange setores regulados, o PL concentra-se na resiliência cibernética da administração pública direta e indireta em todos os entes federativos;
- **Autoridade designada em regulamento:** o Art. 4º remete a designação da autoridade nacional de cibersegurança a regulamento, não definindo modelo institucional na própria lei;
- **Programa de adesão voluntária:** cria o Programa Nacional de Segurança e Resiliência Digital, ao qual estados, DF, municípios e setor privado podem aderir voluntariamente;
- **Financiamento via FNSP:** vincula 3% dos recursos do Fundo Nacional de Segurança Pública e 2% das receitas de apostas de quota fixa para ações de cibersegurança;
- **Governança de cadeia de suprimentos:** estabelece obrigações detalhadas para gestão de riscos de fornecedores e parceiros tecnológicos.

Observação: A tramitação paralela do PL no Senado e do Anteprojeto no Executivo pode gerar fragmentação normativa. Recomenda-se harmonização dos instrumentos para evitar conflitos e lacunas.

4. PRINCÍPIOS ORIENTADORES PARA A AVALIAÇÃO

Com base na Nota Pública do CGI.br, na E-Ciber e nas melhores práticas internacionais, estabeleço os seguintes princípios orientadores para avaliação dos modelos:

1. **Cooperação multissetorial:** o modelo deve promover a participação colaborativa dos diferentes setores da sociedade.
2. **Não sobreposição de competências:** deve-se resguardar os papéis já consolidados de agências setoriais e autoridades competentes.
3. **Separação entre coordenação e sanção:** o Centro Nacional de Cibersegurança deve ter função coordenadora, sem funções sancionatórias.
4. **Independência dos CSIRTs:** os centros de tratamento de incidentes devem ser independentes, sem vinculação sancionatória prévia.
5. **Proporcionalidade das medidas:** máxima cautela no estabelecimento de regras para bloqueios ou medidas restritivas.
6. **Aderência à E-Ciber:** capacidade do modelo de implementar os quatro eixos estratégicos definidos no Decreto nº 12.573/2025.
7. **Proteção de direitos fundamentais:** liberdade de expressão, privacidade e proteção de dados devem ser preservados.

5. AVALIAÇÃO TÉCNICA DOS MODELOS DE GOVERNANÇA

5.1. Modelo de Secretaria

Descrição: Secretaria Nacional de Segurança Cibernética vinculada a Ministério ou diretamente à Presidência da República.

Pontos favoráveis:

- Agilidade de criação por decreto presidencial;
- Integração direta com a esfera do Poder Executivo Federal;
- Compatível com o modelo previsto no PL do Senado (autoridade designada em regulamento).

Pontos desfavoráveis:

- Dependência hierárquica e orçamentária que afeta continuidade de políticas;
- Ausência de mandatos fixos ou garantias legais de autonomia;
- Capacidade limitada de regular o setor privado.

Aderência à E-Ciber: Parcial. Pode implementar ações de conscientização e cooperação, mas enfrenta limitações para ações que exijam poder regulatório sobre infraestruturas críticas privadas.

5.2. Modelo de Autarquia Especial

Descrição: Autoridade Nacional de Cibersegurança como autarquia sob regime especial, similar ao INMETRO, com autonomia técnica e administrativa, mas sem mandatos fixos.

Pontos favoráveis:

- Maior autonomia técnica e administrativa que uma secretaria;
- Forte ênfase em coordenação com reguladores setoriais;
- Capacidade de implementar certificação e padrões mínimos previstos na E-Ciber.

Pontos desfavoráveis:

- Ausência de mandatos fixos pode fragilizar a estabilidade;
- Requer Projeto de Lei específico com tramitação no Congresso.

Aderência à E-Ciber: Alta. Modelo compatível com as ações de certificação (selo nacional), elaboração de lista de alto risco e modelo de maturidade. A ênfase em coordenação facilita implementação do eixo de cooperação.

5.3. Modelo de Agência Reguladora Nova

Descrição: Criação de nova Agência Nacional de Cibersegurança nos moldes das agências reguladoras brasileiras, com mandatos fixos e poder normativo amplo.

Pontos favoráveis:

- Maior autonomia com mandatos fixos e estabilidade dos dirigentes;
- Poder regulatório sólido para infraestruturas críticas;
- Alinhamento às melhores práticas internacionais (ENISA, ANSSI, CISA).

Pontos desfavoráveis:

- Maior custo e complexidade política de criação;
- Possível sobreposição com agências setoriais já consolidadas.

Aderência à E-Ciber: Plena. Modelo com capacidade integral de implementar todos os eixos da E-Ciber, incluindo regulação de serviços essenciais, certificação, cooperação internacional e desenvolvimento de soberania tecnológica.

5.4. Modelo de Atribuição à ANATEL

Descrição: Atribuição das competências de Autoridade Nacional de Cibersegurança à ANATEL, transformando-a em Agência Nacional de Telecomunicações e Cibersegurança.

Pontos favoráveis:

- Infraestrutura institucional consolidada (28 anos, presença em 27 UFs);
- Experiência em regulação de infraestrutura crítica e cibersegurança setorial desde 2019;
- Mandatos fixos e conformidade com Lei das Agências Reguladoras.

Pontos desfavoráveis:

- Potencial conflito entre regulação setorial e coordenação nacional;
- Risco de percepção de viés setorial pelos demais regulados;
- Necessidade de capacitação em novos domínios (energia, finanças, saúde).

Aderência à E-Ciber: Alta, condicionada a salvaguardas. A experiência regulatória e a estrutura existente permitem implementação célere das ações previstas, especialmente no eixo de segurança e resiliência. Requer atenção à separação estrutural para evitar subordinação da cibersegurança nacional aos interesses setoriais de telecomunicações.

5.5. Síntese Comparativa – Aderência à E-Ciber

Eixo E-Ciber	Secretaria	Autarquia	Agência Nova	ANATEL
Proteção e conscientização	Alta	Alta	Alta	Alta
Segurança e resiliência	Baixa	Média	Alta	Alta
Cooperação e integração	Média	Alta	Alta	Alta
Soberania e governança	Baixa	Média	Alta	Média-Alta
Celeridade implantação	Alta	Média	Baixa	Alta

6. AVALIAÇÃO DO ANTEPROJETO DE LEI GERAL DE CIBERSEGURANÇA

O Anteprojeto elaborado pelo GTT Lei Geral apresenta marco legal que endereça diversas das preocupações manifestadas pelo CGI.br e está alinhado com a E-Ciber:

6.1. Aspectos Positivos

1. **Preservação das competências setoriais:** assegura às autoridades setoriais o exercício pleno de suas competências, cabendo à autoridade nacional competência residual.
2. **CENCiber com função coordenadora:** atribui ao Centro Nacional competências de coordenação, sem funções sancionatórias diretas.
3. **Proteção do anonimato:** preserva o anonimato de quem comunicar vulnerabilidades.
4. **Proporcionalidade nas medidas cautelares:** bloqueios apenas em situações de risco iminente, por prazo limitado.

6.2. Pontos de Atenção

1. **Interação com o CERT.br:** O Anteprojeto não explicita a relação entre o CENCiber e o CERT.br, CSIRT de Responsabilidade Nacional já consolidado.
2. **Harmonização com PL do Senado:** A tramitação paralela pode gerar conflitos normativos. O PL foca na administração pública enquanto o Anteprojeto abrange setores regulados.
3. **Composição do CNCiber:** A concentração de representantes do Executivo federal pode desequilibrar a participação multissetorial.

7. SALVAGUARDAS E OBSERVAÇÕES DO CGI.br

Independentemente do modelo escolhido, o CGI.br recomenda que as seguintes salvaguardas sejam observadas:

1. **Preservação das competências setoriais:** As autoridades setoriais já consolidadas devem manter suas competências plenas, cabendo à autoridade nacional função residual e coordenadora.
2. **CENCiber sem funções sancionatórias:** O Centro Nacional de Cibersegurança deve ter natureza técnica e coordenadora, afastando-se funções de auditoria ou sanção para preservar a confiança e a colaboração voluntária.
3. **Independência dos CSIRTs:** Os centros de tratamento de incidentes devem ser independentes, recebendo informações sem vinculação sancionatória prévia, preservando e potencializando capacidades existentes como o CERT.br.
4. **Cautela com medidas de bloqueio:** Máxima proporcionalidade e estritos requisitos para medidas restritivas, evitando efeitos colaterais sobre a Internet.
5. **Alinhamento normativo:** Harmonização entre o Anteprojeto do Executivo e o PL em tramitação no Senado para evitar conflitos e lacunas normativas.
6. **Aderência à E-Ciber:** O modelo escolhido deve ter capacidade de implementar integralmente os quatro eixos da Estratégia Nacional de Cibersegurança.
7. **Proteção de direitos fundamentais:** Liberdade de expressão, privacidade e proteção de dados pessoais devem ser expressamente garantidos.

8. CONCLUSÃO E VOTO

Em consonância com a tradição institucional do CGI.br e com os princípios estabelecidos em sua Nota Pública de 14 de novembro de 2025, **este parecer não manifesta opção por modelo específico de governança**, apresentando, em vez disso, avaliação técnica fundamentada que subsidie a tomada de decisão das instâncias do Governo Federal.

REGISTRO que os três modelos originalmente discutidos no GTT Governança (Secretaria, Autarquia Especial e Agência Reguladora Nova) foram encaminhados ao Poder Executivo, e que o quarto modelo (atribuição de competências à ANATEL) foi incorporado posteriormente às discussões no GTT Lei Geral.

REGISTRO que todos os quatro modelos apresentam diferentes graus de aderência à Estratégia Nacional de Cibersegurança (Decreto nº 12.573/2025), conforme

demonstrado na análise comparativa, e que a escolha envolverá trade-offs entre autonomia institucional, celeridade de implementação e amplitude de coordenação.

REGISTRO a necessidade de harmonização entre o Anteprojeto de Lei Geral de Cibersegurança e o Projeto de Lei em tramitação no Senado Federal, para evitar fragmentação normativa.

VOTO pela transmissão desta contribuição técnica do CGI.br ao CNCiber e ao GSI, **com o encaminhamento dos quatro modelos de governança em análise** (Secretaria, Autarquia Especial, Agência Reguladora Nova e Atribuição à ANATEL) acompanhados das salvaguardas e observações elencadas neste parecer, cabendo às instâncias competentes do Poder Executivo e do Poder Legislativo a definição do modelo mais adequado.

REAFIRMO a disposição do CGI.br em colaborar com qualquer discussão sobre o tema, mantendo seu compromisso de atuar como espaço multissetorial e participativo para a governança da Internet no país.

Brasília, 17 de dezembro de 2025

S.M.J.

Este é o Parecer

Percival Henriques de Souza Neto

Membro Titular do CNCiber na representação do CGI.br

À Secretaria Executiva do Comitê Nacional de Cibersegurança acerca das proposta de criação de Órgão de Governança da Atividade de Cibersegurança no Brasil

São Paulo, 17 de dezembro de 2025.

Considerando a deliberação sobre o encaminhamento da proposta da Lei Geral de Cibersegurança e da criação da Autoridade Nacional de Cibersegurança e, em complemento à manifestação realizada em 26/03/2025 (1ª RO/25), apresentamos nosso posicionamento nos seguintes termos:

O Instituto Peck de Cidadania Digital (IPCD), no exercício da 3ª Representação da Sociedade Civil no Comitê Nacional de Cibersegurança (CNCiber), manifesta-se favoravelmente à proposta de criação de um órgão de governança da atividade de cibersegurança, adotando o modelo de Agência Reguladora, pelas razões a seguir expostas.

Há grande expectativa da sociedade civil quanto à criação de um órgão de governança de cibersegurança no país. Considerando os debates realizados no âmbito do GTT, entendemos que o modelo de Agência Reguladora é o mais adequado às necessidades nacionais, pois confere maior autonomia para fiscalização, regulamentação e aplicação de sanções. Esse formato permite atuação abrangente sobre os setores público e privado, garantindo mecanismos diretos de coordenação e controle.

Subsidiariamente, reconhecemos que o modelo de Autoridade Nacional também se mostra aplicável. Embora disponha de autonomia parcial, sua competência alcança igualmente os setores público e privado, sem necessidade de articulação adicional para atuação junto ao setor privado.

Por fim, caso haja restrições orçamentárias que inviabilizem a criação de um novo órgão, consideramos viável a proposta de ampliar as atribuições da Anatel para que também responda como Autoridade Nacional de Cibersegurança, desde que sejam promovidas alterações na estrutura de governança da agência, incluindo a criação de um conselho consultivo independente, a fim de mitigar riscos de conflito de interesses entre as atividades de telecomunicações e cibersegurança.

Patrícia Peck
Presidente do IPCD
Membro Titular do CNCiber

Presidência da República

Comitê Nacional de Cibersegurança (CNCiber)

GTT Lei Geral - Relatório

Brasília – Dez/2025

COMITÊ NACIONAL DE CIBERSEGURANÇA
CNCiber

SUMÁRIO

GTT Lei Geral – Relatório

Este documento apresenta a consolidação das atividades realizadas pelo GTT Lei Geral, criado pela Resolução CNCiber 013, de 8 de outubro de 2025, para aperfeiçoamento da proposta de Lei Geral de Cibersegurança apresentada pelo GSI ao CNCiber na RO-003-25. Referida proposta, baseada nos trabalhos do GTT Governança, encerrado quando da RO-001-25, estabelecia princípios, deveres e competências para organizar a atividade de cibersegurança nacional, e designava a Agência Nacional de Telecomunicações como Autoridade Nacional de Cibersegurança (ANCiber).

O GTT foi integrado por representantes de 19 das 25 instituições que integram o CNCiber, abaixo relacionadas:

I - Ministério da Gestão e da Inovação em Serviços Públicos, que o coordenou;

II - Agência Nacional de Telecomunicações, que o coordenou;

III - Gabinete de Segurança Institucional da Presidência da República;

IV - Casa Civil da Presidência da República;

V - Controladoria-Geral da União;

VI - Ministério das Comunicações;

VII - Ministério da Ciência, Tecnologia e Inovação;

VIII - Ministério do Desenvolvimento, Indústria, Comércio e Serviços;

IX - Ministério da Defesa;

X - Ministério da Justiça e Segurança Pública;

XI - Banco Central do Brasil;

XII - Comitê Gestor da Internet no Brasil - CGI.Br;

XIII - Instituto dos Advogados de São Paulo - IASP (setor sociedade civil);

XIV - Instituto Peck de Cidadania Digital - IPCD (setor sociedade civil);

XV - Fundação Getúlio Vargas - FGV (setor ciência, tecnologia e inovação);

XVI - Centro de Pesquisas e Desenvolvimento em Telecomunicações - CPqD (setor ciência, tecnologia e inovação);

XVII - Confederação das Associações das Empresas Brasileiras de Tecnologia da Informação -ASSESPRO (setor empresarial);

XVIII - Federação das Indústrias do Estado de São Paulo - FIESP (setor empresarial); e

XIX - Conexis/Brasscom (setor empresarial).

1 DA METODOLOGIA DE TRABALHO

Foram agendadas reuniões semanais, nas manhãs de sexta-feira, para debates sobre os temas. Variando entre 16 e 30 participantes em cada reunião, estima-se que o total de horas despendidas somente em deliberações tenha superado 360 pessoas.hora, não consideradas as diversas reuniões bilaterais realizadas pelos diferentes membros com o MGI, a ANATEL e o GSI, o que demonstra o elevado nível de engajamento dos participantes do GTT.

Os trabalhos foram realizados de forma participativa, onde todos os presentes puderam expor suas perspectivas e opinar, buscando-se o consenso. Após reuniões iniciais de exposição de comentários gerais sobre o anteprojeto e retomada das conclusões dos trabalhos realizados no GTT Governança, a fim de subsidiar os trabalhos no novo GTT, adotou-se um modelo de relatoria para os primeiros capítulos, no qual os integrantes do GTT enviaram suas propostas sobre os temas em debate antecipadamente e a ANATEL, MGI e GSI consolidaram essas propostas num texto único, já com respectiva avaliação e sugestão de (não) aceitação (total ou parcial), seguida de debate e deliberação do GTT.

A proposta original foi apresentada pelo GSI, e em seguida dividiu-se as deliberações em 3 módulos.

No primeiro módulo foram discutidos os Capítulos I a III do Anteprojeto de Lei, que estabelecem Objeto, Definições, Princípios, Objetivos, Direitos, âmbito de Aplicação, Gestão de Riscos, Medidas de Cibersegurança e Deveres dos Agentes de Cibersegurança.

Considerando o exíguo prazo para finalização dos trabalhos e o recebimento de muitas contribuições para o primeiro módulo, a revisão dos módulos seguintes foi proposta e conduzida pela Anatel, MGI e GSI.

No segundo módulo foram debatidos o Capítulo IV, que estabelece a Governança da Cibersegurança Nacional em diversas seções: Sistema Nacional de Cibersegurança – SNCiber, Autoridade Nacional de Cibersegurança, Autoridades Setoriais de Cibersegurança, demais integrantes do SNCiber, Conselho Nacional de Cibersegurança – CNCiber, e Centro Nacional de Cibersegurança – CENCiber) e o Capítulo V, que estabelece as Sanções Administrativas.

Por fim, foram debatidos o Capítulo VI, que estabelece as alterações da Lei Geral de Telecomunicações (LGT), Lei nº 9.472, de16 de julho de 1997 e leis correlatas para instituir a Agência Nacional de Telecomunicações (ANATEL) como Autoridade Nacional de Cibersegurança, transformando-a em Agência Nacional de Telecomunicações e Cibersegurança, e o Capítulo VII, que

estabelece Disposições Finais e Transitórias para a transição da ANATEL para incorporação das novas funções e adequação dos agentes de cibersegurança às novas regras.

2 DOS RESULTADOS

2.1 Da Lei Geral da Cibersegurança incluindo o "Cenário Anatel"

Em observância ao primeiro objetivo do GTT foi elaborada uma versão completa do Anteprojeto de Lei Geral da Cibersegurança incluindo os Capítulos VI e VII para contemplar a designação da ANATEL como Autoridade Nacional de Cibersegurança.

2.2 Da Lei Geral da Cibersegurança adaptável aos 3 "cenários" debatidos pelo GTT Governança entre março de 2024 e março de 2025

Foi elaborada uma versão limitada aos Capítulos I a V e VII do cenário anterior, que em tese podem ser adaptados aos 3 cenários originalmente analisados pelo GTT Governança que, em cada caso, demandariam implementações substancialmente diferentes no tocante aos capítulos VI e VII, conforme explica-se a seguir:

2.2.1 Cenário Agência Reguladora

2.2.1.1 Inclusão na Lei das Agências Reguladoras (Lei 13.848, de 25 de junho de 2019)

A adaptação do Capítulo VI do Anteprojeto da Lei Geral da Cibersegurança para a criação de uma Agência Nacional de Cibersegurança (ANCiber), pela mera inclusão dessa agência no rol listado no Art. 2º da Lei 13.848, bastaria para estabelecer uma robusta estrutura de governança desse órgão, no tocante aos pontos que se seguem:

- Autonomia administrativa;
- Práticas de gestão de riscos e programas anticorrupção;
- Vedação de imposição de sanções desproporcionais;
- Necessidade de Análise de Impacto Regulatório (AIR);
- Composição da diretoria (5 diretores);
- Obrigatoriedade de decisões de natureza regulatória na forma colegiada;
- Delimitação do Regimento Interno
- Publicidade das deliberações;
- Iniciativas que demandam consulta ou audiência pública;
- Controle externo pelo Congresso Nacional e pelo Tribunal de Contas da União;
- Plano de Comunicação para informação e educação de seu público;

- Plano de Gestão anual;
- Obrigatoriedade de Ouvidoria e Procuradoria;
- Interação e articulação com agências reguladoras federais e órgãos de defesa da concorrência; e
- Interação com agências reguladoras estaduais, distritais e municipais.

2.2.1.2 Outras determinações necessárias

Seria ainda necessária a adaptação dos Capítulos VI e VII para constituição de diversos pontos já presentes na estrutura da ANATEL que a criação de uma nova agência necessitaria prever:

- Composição do quadro de pessoal;
- Determinações orçamentárias e financeiras;
- Sede e foro;
- Previsão de unidades descentralizadas;

Destaca-se que no cenário de criação de nova Agência Reguladora, diversos elementos constantes da respectiva entrega do GTT Governança poderiam ser aproveitados e combinados ao marco legal de cibersegurança constante do Anteprojeto da Lei Geral da Cibersegurança.

2.2.2 Cenário "Autarquia Não-Especial"

Seria necessária a adaptação dos Capítulos VI e VII para detalharem todos os pontos descritos nos itens 2.2.1.1 e 2.2.1.2, com aproveitamento e combinação da respectiva entrega do GTT Governança ao marco legal de cibersegurança constante do Anteprojeto da Lei Geral da Cibersegurança

2.2.3 Cenário "Secretaria"

Por fim, com relação ao último cenário explorado pelo GTT Governança, seria necessária a adaptação dos Capítulos VI e VII para detalharem todos os pontos descritos nos itens 2.2.1.1 e 2.2.1.2.

Ainda, seria necessário o detalhamento da forma de relacionamento dessa Secretaria, integrante da administração direta, com os diferentes setores representados pelo conjunto de serviços essenciais.

3 NOTAS E OBSERVAÇÕES

3.1 Observações do Ministério da Gestão e Inovação em Serviços Públicos

Na última reunião do GTT Lei Geral o MGI trouxe aos integrantes do grupo as seguintes preocupações, transcritas já com as ponderações feitas em seguida pela Anatel e GSI.

3.1.1 Conflito entre Regulação e Cooperação:

3.1.1.1 Observação

Como reguladora, a ANCiber/Anatel fiscaliza as operadoras, mas dependeria delas para implementar medidas críticas de defesa digital, criando um conflito entre impor regras, fiscalizar, sancionar e cooperar (Capítulo V, Seção III, Art. 17, I) (Capítulo V, Seção I, Art. 13, I). Além disso, uma falha das operadoras poderia ser interpretada como falha da própria "agência de cibersegurança", gerando pressão política e institucional incompatível com seu papel atual.

3.1.1.2 Considerações

Foi esclarecido que a Agência continuará com competências para o setor de telecomunicações, portanto, com poder normativo e sancionador, que viabiliza a adoção de medidas pelas empresas de telecomunicações que forem entendidas como necessárias para a segurança nacional, desde que, obviamente, seguindo o rito normativo legal. Quanto a possível falha das operadoras impactar na imagem da Agência, ponderou-se que em cibersegurança sempre se considera que não é se seremos atacados, mas quando. É importante destacar que o risco maior para a reputação institucional não é coordenar e falhar — é não coordenar e deixar o país exposto.

Ademais, esse eventual conflito estaria presente em qualquer entidade criada ou designada, visto que "impor regras, fiscalizar, sancionar e cooperar" faz parte do modelo amplamente discutido e amadurecido, conforme os trabalhos do GTT Governança, não se tratando de novidade do cenário Anatel.

3.1.2 Mudança Abrupta de Escopo e Competências:

3.1.2.1 Observação

Outro ponto crucial é que essa atribuição representaria uma mudança drástica de escopo. A Anatel passaria de uma função regulatória setorial para uma missão transversal (Capítulo I, Seção IV , Art.6, I,II e III), que exige coordenação com setores como energia, saúde, defesa, finanças e órgãos de inteligência (Seção II Art.2 Parágrafo único). Essa transição não é apenas uma ampliação de responsabilidades, mas uma alteração profunda no tipo de trabalho, nas competências técnicas e até na base normativa que sustenta sua atuação, o que pode demandar nova jurisprudência ou marcos regulatórios.

3.1.2.2 Considerações

Foi observado que em grande medida os potenciais problemas já foram mitigados pelo fato de que a regulação setorial da Anatel para cibersegurança é a mais madura e abrangente dentre as Agências reguladoras nacionais. Além disso, o anteprojeto de Lei prevê que haverá um intervalo de tempo para adaptação da estrutura da ANATEL para os novos encargos, bem como para adaptação dos agentes de cibersegurança para o novo regulador. Adicionalmente, o Anteprojeto prevê a possibilidade de requisição imediata de até 60 servidores públicos de outros órgãos e a contratação temporária de até outros 60 servidores, totalizando 120 servidores, quase a metade do total de posições vagas na ANATEL e previsto para a complementação do quadro para as novas funções.

Ademais, a ANATEL contará com o apoio técnico do GSI, que inclusive deverá ceder o CTIR Gov para constituir o núcleo do novo CENCiber, o coração operacional da nova estrutura. Portanto, a preocupação não se constitui um risco não previsto e previamente mitigado.

Por fim, mister destacar que uma nova Agência teria desafio muito superior, vez que não conta sequer com infraestrutura, meios e processos, visto que a criação de novos marcos regulatórios, como mencionado, será inerente à criação/designação de qualquer entidade, com uma necessária curva de aprendizado e de adaptação.

3.1.3 Absorção de Riscos e Percepções Equivocadas:

3.1.3.1 Observação

Por fim, ao absorver competências de cibersegurança, a agência também absorveria riscos que não são inerentes ao seu escopo atual. Esse duplo papel pode gerar percepções equivocadas: problemas típicos do setor de telecomunicações podem ser vistos como falhas de segurança nacional (ou da agência de cibersegurança) (Capítulo VI, Art. 27, XXXIII), e vulnerabilidades digitais podem ser interpretadas como falhas regulatórias. Essa sobreposição comprometeria tanto a eficácia da fiscalização quanto a efetividade da cooperação necessária para enfrentar ameaças digitais.

3.1.3.2 Considerações

Desde ao menos 2013 o setor de telecomunicações sempre se constituiu no que se tratou como infraestruturas críticas, e assim conexo a questões de segurança nacional. Ainda, a ANATEL é considerada uma agência de Estado, tendo inclusive prerrogativa de representação internacional do Brasil, em coordenação com o MRE, em foros que tratam da temática da cibersegurança.

Por fim, observou-se que ANATEL assumirá a atividade operacional da cibersegurança, mas que a coordenação do CNCiber e do SNCiber, elementos do nível político-estratégico, continuará, nos

moldes do Anteprojeto de Lei, sob a responsabilidade do GSI, como o é atualmente. Outrossim não se vislumbra como relevante o risco apontado.

3.1.4 Cibersegurança x Segurança da Informação: Risco de Abordagem Limitada:

3.1.4.1 Observação

Embora cibersegurança e segurança da informação sejam conceitos distintos, a separação completa de responsabilidades entre órgãos pode gerar conflitos e lacunas. No modelo sugerido, a ANCiber/Anatel assumiria apenas a cibersegurança (Capítulo VI, Art. 27,XXXIII), enquanto a segurança da informação continuaria sob a alçada do GSI, que hoje define normas e diretrizes por meio do/apoiado pelo CGSI (Comitê Gestor da Segurança da Informação). Essa divisão cria um arranjo no mínimo contraditório: quem "regula, fiscaliza e coordena" a cibersegurança (Seção II – Art. 15) não teria ingerência sobre as políticas mais amplas de segurança da informação, que orientam práticas e governança. Essa cisão pode comprometer a coerência normativa e operacional, gerando sobreposição, lacunas e potenciais conflitos de governança. Em vez de propor absorção total, é necessário questionar se esse modelo fragmentado é sustentável e como garantir integração efetiva entre as duas esferas.

3.1.4.2 Considerações

Foi observado que desde a publicação da PNCiber em 26 de dezembro de 2023 essa separação entre Cibersegurança e Segurança da Informação já existe, tendo sido a opção adotada não apenas pelo Brasil, mas ainda pela quase totalidade do rol de nações que apresentam os mais elevados níveis de cibersegurança na atualidade.

Ainda, o GSI continuará exercendo as presidências do CNCiber e do CGSI, e assim mantendo o condão de compatibilizar, no âmbito político-estratégico, as duas áreas. Adicionalmente, o GSI continuará sendo, legalmente, o órgão regulador da Segurança da Informação no âmbito da Administração Pública Federal.

3.2 Observações da Confederação Assespro

3.2.1.1 Observações

A Confederação Assespro manifestou especial preocupação quanto à inclusão das funções de Regulação de Cibersegurança na atual estrutura da Anatel, pelos seguintes motivos:

a) A Agência possui toda a sua estrutura orientada à regulação do setor de telecomunicações, um mercado altamente consolidado e concentrado em poucas empresas. Assim, o modo de operação institucional da Anatel, incluindo a escolha de diretores, superintendentes e demais quadros técnicos, está historicamente alinhado e influenciado por esse setor específico.

b) As empresas de telecomunicações, especialmente as de grande porte, competem diretamente com outras empresas do mercado de TIC, seja utilizando seus próprios CNPJs de telecom, seja por meio de subsidiárias ou companhias pertencentes à mesma holding.

c) As empresas do setor exercem influência significativa sobre temas e decisões regulatórias, considerando seu tamanho, capilaridade nacional e representatividade econômica.

Diante disso, entende que a incorporação de novas atribuições relacionadas à cibersegurança pela Anatel, sem o devido equilíbrio na governança, pode comprometer o desempenho dessa nova função e gerar impactos negativos para o mercado de TIC como um todo.

3.2.1.2 Considerações

Informou-se que, em verdade, o mercado brasileiro de provimento de serviços de banda larga fixa, que é quem fornece conectividade a empresas e órgãos de governo, é benchmark internacional em concorrência, com mais de 16.000 empresas outorgadas nacionalmente, onde as pequenas prestadoras detêm mais de 60% do *marketshare* nacional. Ademais, a regulação do tema ciber acarretará na realização de consultas públicas e participação social, que trarão oportunidade para calibração das novas regulamentações.

Com relação à influência para a direção, os membros do Conselho Diretor são indicados pelo Presidente da República e por ele nomeados, após aprovação pelo Senado Federal, com mandatos fixos escalados, permitindo que a curto prazo haja representação temática na composição do Conselho. Quanto aos demais cargos, a composição é majoritária de servidores de carreira, que passará a contemplar necessariamente servidores com habilitação e conhecimentos específicos de cibersegurança. Dessa forma, a curto e médio prazo haverá a estabilização e o reflexo nos quadros da ampliação das competências.

Ademais, tem-se um modelo de coordenação, onde a Agência estará trabalhando o tema considerando competências setoriais que são mantidas. E, por fim, foi definido modelo de governança com Conselho Nacional de Cibersegurança, entre outros.

Outra consideração relevante apontada foi a de diretores de agências reguladoras integram um conselho, para os quais os processos são sorteados, e não exercem influência direta nas superintendências e departamentos.

3.3 Da motivação para o cenário Anatel

Na Reunião Ordinária RO-003-25 do Comitê Nacional de Cibersegurança o GSI apresentou a motivação de ter trabalhado, junto com a Secretaria de Assuntos Jurídicos da Casa Civil, em um cenário de atribuir a competência de cibersegurança nacional à Anatel.

Informou que, como reiteradamente comentado nas reuniões do CNCiber pela Casa Civil, o contexto fiscal brasileiro impõe dificuldades à criação de uma nova Agência ou Autarquia, opções largamente preferenciais apontadas pelos membros do GTT Governança (segundo documentos do GTT Governança, dos 13 membros desse GTT apenas o MGI entendeu que o cenário Secretaria seria aplicável ao contexto). Informou também que esse cenário de se aproveitar uma estrutura de Agência já existente traz benefícios, como o menor tempo necessário para a implantação da nova capacidade de autoridade nacional de cibersegurança, vez que a Anatel já dispõe de sede, servidores, estrutura em 27 Unidades da Federação, infraestrutura e processos bem delimitados, atendendo aos requisitos da Lei Geral de Telecomunicações e também da Lei das Agências.

Já experiente em 28 anos de execução dos processos de regulamentação, com realização de agenda regulatória, audiências públicas, consultas públicas, tomada de subsídios, análise de impacto regulatório, além de ter as reuniões do Conselho Diretor públicas e com agenda previamente disponibilizada.

A Agência atualmente já detém processo de certificação de equipamentos com ampla rede de laboratórios credenciados, o que é um ativo importante para o tema de cibersegurança. Ademais, já regulamenta oficialmente o setor de telecomunicações, como infraestrutura crítica, desde 2015, e a segurança cibernética desde 2019.

Adicionalmente, a Agência entende ser possível o acréscimo de pessoal vez que têm um quantitativo de servidores aprovados em Lei que ainda não foi atingido, e que esse contingente poderia ser atribuído às funções de cibersegurança.

Também é importante destacar que a Agência é organizada por processos, de forma que uma nova competência pode ser absorvida de forma orgânica, aproveitando-se do *know how* das equipes de normatização e fiscalização, o que reduz o tempo de atuação.

4 CONCLUSÃO

O GTT Lei Geral concluiu que o Anteprojeto ora proposto apresenta marco legal de cibersegurança consistente e que endereça as necessidades do país, podendo ser encaminhado para apreciação das instâncias superiores buscando seu envio ao Congresso Nacional para tramitação com a maior brevidade possível, por tratar de matéria urgente e relevante para o País.

Comitê Nacional de Cibersegurança (CNCiber)

Grupo de Trabalho Temático de Governança (GTT-2)

Relatório Final da Coordenação sobre os trabalhos do GTT Governança

Data de Submissão: 24 de março de 2025.

Brasília- DF - Março de 2025

1. Introdução

A elaboração deste relatório final é o resultado dos trabalhos desenvolvidos no âmbito do GTT Governança do **CNCiber**, instituído pela **Resolução CNCiber nº 3**, de 25 **de março de 2024**, para elaboração de proposta de Projeto de Lei para criação de órgão para a governança da cibersegurança nacional.

O GTT Governança foi instituído com prazo de 6 meses para conclusão dos trabalhos, sendo suas atividades ampliadas por igual período, consoante decisão do Plenário do CNCiber em sua terceira reunião ordinária. Dessa forma, o prazo para conclusão dos trabalhos passou a ser 31 de março de 2025.

O fortalecimento da segurança cibernética tornou-se essencial diante do cenário de crescente complexidade e sofisticação das ameaças cibernéticas, intensificadas pela rápida transformação digital dos serviços públicos e privados, pela expansão da conectividade e pelas tecnologias emergentes. A ausência de um modelo centralizado de governança nacional tem gerado lacunas na coordenação, na resposta a incidentes, na definição de responsabilidades e na articulação entre os setores público e privado.

Para enfrentar esse desafio, o CNCiber criou o GTT, cuja coordenação dos trabalhos foi atribuída ao **Ministério da Gestão e da Inovação em Serviços Públicos** e à **Agência Nacional de Telecomunicações (Anatel)**, com a participação de representantes de diversos órgãos governamentais, entidades do setor privado, da sociedade civil e da academia. A saber: Ministério da Gestão e da Inovação em Serviços Públicos (MGI) -coordenação, Agência Nacional de Telecomunicações (Anatel) - coordenação, Casa Civil da Presidência da República, Controladoria-Geral da União (CGU), Ministério das Comunicações, Ministério da Defesa, Ministério da Justiça e Segurança Pública, Comitê Gestor da Internet no Brasil (CGI.br), Centro de Tecnologia e Sociedade da Fundação Getúlio Vagas Direito Rio, Federação das Industriais do Estado de São Paulo, Instituto Peck de Cidadania Digital, Confederação das Associações das Empresas Brasileiras de Tecnologia da Informação - ASSESPRO), e Instituto dos Advogados de São Paulo.

Objetivos principais:

- Diagnosticar o cenário atual da cibersegurança no Brasil, incluindo desafios, oportunidades e lacunas de governança;
- Analisar modelos internacionais de governança em cibersegurança para identificar melhores práticas e adaptar ao contexto nacional;
- Propor modelos de governança em cibersegurança que contemplem aspectos estratégicos, táticos e operacionais; e

- Estabelecer diretrizes para a criação de um órgão nacional de cibersegurança, com competências definidas, sistema estruturante, previsões orçamentárias e estruturas organizacionais.

2. Histórico das Atividades Desenvolvidas

2.1. Reuniões Realizadas

Durante o período de vigência dos trabalhos, foram realizadas 33 reuniões virtuais para debater o diagnóstico dos problemas, desafios e oportunidades para o país e a estruturação de propostas de modelo de governança nacional de cibersegurança.

Os encontros foram organizados da seguinte forma:

- Abril de 2024 – Início dos trabalhos com apresentação dos objetivos e primeiros debates com vistas ao diagnóstico da cibersegurança no país.
- Maio a agosto - Ciclo de reuniões quinzenais para amadurecimento do diagnóstico, identificação das necessidades, definição de competências, estruturas e alternativas para o modelo de governança.
- Agosto a dezembro de 2024 – Ciclo de reuniões semanais para definição de competências, sistema e alternativas para os modelos de governança.
- Janeiro a março de 2025 – Ciclo final de reuniões semanais para consolidação e aprimoramento das propostas de modelos institucionais e elaboração do relatório final.

2.2. Workshops

- **Workshop realizado em 23 de agosto de 2024**, organizado pelo MGI na Escola Nacional de Administração Pública (ENAP) com a participação presencial dos participantes do GTT, com o objetivo de explorar diferentes cenários para a configuração da(s) proposta(s) de estrutura institucional de governança em cibersegurança.

Durante o seminário, foram avaliados três cenários principais:

1. **Administração Direta** – Capacidade executiva concentrada no órgão, com vínculo direto à administração pública.
2. **Administração Indireta** – Capacidade executiva vinculada a um órgão supervisor, com maior autonomia operacional.
3. **Modelo Híbrido** – Combinação de características dos modelos direto e indireto, com descentralização operacional e capacidade regulatória.

Os principais pontos discutidos foram:

- **Administração Direta:** Risco de sobreposição de competências com órgãos setoriais, necessidade de autonomia e estabilidade para garantir continuidade; ausência de carreira própria A configuração permitiria maior controle estratégico, rápida implementação por decreto e maior alinhamento com a política de governo.
- **Administração Indireta:** Maior autonomia funcional e orçamentária, ausência de subordinação hierárquica, podendo envolver criação de novas carreiras. Risco de sobreposição com órgãos reguladores precisaria ser endereçado
- **Modelo Híbrido:** Flexibilidade para adaptação de competências e manutenção da capacidade operacional nos órgãos setoriais, com desafios na definição clara de responsabilidades.

O seminário consolidou elementos estratégicos, táticos e operacionais que **subsidiaram as discussões nos meses subsequentes do GTT**. Foram elaborados diversos documentos em preparação ao *workshop*, os quais contaram com a contribuição dos participantes e acompanham o relatório no Anexo VI.

2.3. Apresentações Temáticas

As apresentações temáticas foram realizadas com o objetivo de fornecer subsídios técnicos e estratégicos para a definição do modelo de governança em cibersegurança. Os debates permitiram o alinhamento de expectativas, a troca de experiências com modelos internacionais e a análise de diferentes abordagens para a estruturação do órgão nacional de cibersegurança.

- **Cullen International – Junho de 2024:** Apresentação das melhores práticas internacionais de governança em cibersegurança, com ênfase na integração de capacidades operacionais, modelos de resposta a incidentes e frameworks regulatórios utilizados em países da **América do Norte** e **Europa**.
- **Banco Mundial – Julho de 2024:** Apresentação das conclusões preliminares sobre o cenário internacional de governança em cibersegurança, com destaque para modelos adotados em países da **União Europeia**, **Ásia** e **América Latina**.
- **Gabinete de Segurança Institucional (GSI):**
    - **Maio de 2024** – Apresentação do Projeto de Lei proposto em 2023, detalhando as competências e a estrutura sugerida para o órgão nacional de cibersegurança.

- **Janeiro de 2025** – Apresentação de uma proposta alternativa, com a para instituição de autarquia, com foco em serviços essenciais e infraestrutura crítica.
- **Março de 2025** – Apresentação de uma proposta consolidada para criação de uma **autoridade (modelo de autarquia do Decreto-lei nº 200/67)**, incluindo um **Marco Regulatório** para garantir autonomia e poder de fiscalização.

As apresentações colaboraram diretamente para o refinamento das propostas, fornecendo subsídios técnicos, estratégicos e operacionais que foram incorporados aos modelos finais de governança em cibersegurança apresentado neste relatório.

3. Produtos Elaborados

Com base nas análises realizadas, nos debates conduzidos ao longo das reuniões e nos subsídios técnicos e estratégicos apresentados durante o seminário e as apresentações temáticas, bem como as discussões do Plenário do CNCiber, o GTT desenvolveu três propostas institucionais para a criação de um órgão de governança nacional em cibersegurança.

As propostas foram formuladas considerando diferentes níveis de autonomia, capacidade regulatória e operacional, além de modelos de governança adotados em outros países e das particularidades do contexto brasileiro.

À guisa de um breve histórico, após os estudos e reflexões durante os primeiros cinco meses de trabalho do GTT, bem como do workshop presencial, uma votação realizada direcionou os participantes a trabalharem como o modelo de administração indireta, mais especificamente de Agência Reguladora. Considerando as discussões e apontamentos do plenário do CNCiber, relatados na Ata da quarta reunião ordinária, realizada em 4 de dezembro de 2024, o GTT passou a trabalhar com propostas de modelos institucionais diferenciados, quais seja autarquia (não especial) e secretaria (administração direta), também incorporando às propostas marco legal de cibersegurança, uma das lacunas previamente apontadas.

As três propostas foram desenhadas para prover alternativas que ofereçam diferentes níveis de abrangência, autonomia e competências,, considerando os limites administrativos e jurídicos de cada modelo. Cada modelo oferece soluções específicas para os desafios de governança em cibersegurança, com diferentes graus de controle, flexibilidade e capacidade de execução.

3.1. Proposta 1 – Agência Reguladora (Agência Nacional de Cibersegurança - ANCiber)

Essa proposta prevê a criação de uma **Agência Reguladora** com poder regulatório pleno e autonomia administrativa, orçamentária e operacional, além de carreira própria O modelo é baseado em exemplos de sucesso de outras agências reguladoras no Brasil, como a **ANATEL**, **ANEEL**, **ANAC**, **ANVISA, etc**.

- **Instituição:** Projeto de Lei
- **Alcance:** Nacional (setor público e privado)
- **Competências:** Plenas (51)
- **Efetivo:** 440 servidores (progressivo) – carreira própria
- **Custo total:** R$ 325 milhões (ano 6)
- **Diretoria:** Diretoria colegiada com mandatos fixos (5 anos), sabatina pelo Senado.
- **Poder Regulatório:** Fiscalização e normatização sobre cibersegurança em setores público e privado
- **Modelo Similar:** ANATEL, ANEEL, ANAC, ANVISA, etc.

3.2. Proposta 2 – Órgão Ministerial (Secretaria Nacional de Cibersegurança - SNCiber)

Essa proposta prevê a criação de uma **Secretaria Nacional** vinculada à estrutura do Executivo, com foco em coordenação estratégica e capacidade limitada de fiscalização. Esse modelo permite maior alinhamento com a política de governo, mas apresenta limitações para regulação, fiscalização e controle (restritos à Administração Pública Federal).

- **Instituição:** Decreto
- **Alcance:** Restrito à Administração Pública Federal (APF)
- **Competências:** Limitadas (26)
- **Efetivo:** 33 servidores (progressivo)
- **Custo total:** R$ 24,4 milhões (ano 6)
- **Nomeação:** Nomeação e exoneração pelo Ministro de Estado
- **Poder Regulatório:** Normatização e coordenação no âmbito da administração pública federal
- **Modelo Similar:** SSIC/GSI e SGD/MGI

3.3. Proposta 3 – Autarquia (não especial) – Autoridade Nacional de Cibersegurança (ANCiber)

Essa proposta prevê a criação de uma **Autarquia**, com autonomia operacional e administrativa, focada nos serviços essenciais e na infraestrutura crítica. O modelo é baseado em entidades como o **INMETRO, ITI, e ICMBio**[1]

- **Instituição:** Projeto de Lei
- **Alcance:** Nacional (setor público e privado – foco em serviços essenciais e infraestrutura crítica)
- **Competências:** Plenas (51)
- **Efetivo:** 330 servidores (progressivo) – aproveitamento de carreiras em criação/existentes
- **Custo total:** R$ 244 milhões (ano 6)
- **Nomeação:** Nomeação e exoneração pelo Presidente da República
- **Poder Regulatório:** Normatização e fiscalização com foco em serviços essenciais e infraestruturas críticas.
- **Modelo Similar:** INMETRO, ITI, ICMBio ~ANPD.

3.4 Tabela Comparativa dos Modelos Propostos

Uma análise comparativa detalhada das três propostas, destacando as principais diferenças em termos de estrutura, poder regulatório, foco e custos, está disponível no Anexo IV deste relatório. Essa comparação permite uma visão clara das vantagens e limitações de cada modelo, subsidiando a tomada de decisão para a implementação do órgão nacional de governança em cibersegurança.

4. Parecer Conclusivo

Após uma análise detalhada do cenário de cibersegurança no Brasil, das experiências internacionais e das propostas apresentadas, o **GTT Governança** conclui que a criação de uma instituição responsável pela governança nacional em cibersegurança é essencial para fortalecer a capacidade de resposta a incidentes, garantir a segurança dos serviços essenciais e das infraestruturas críticas e promover a proteção de dados no ambiente digital.

4.1. Diagnóstico e Justificativa

Os trabalhos desenvolvidos pelo GTT, incluindo a análise dos modelos internacionais, o seminário com participantes e as apresentações temáticas,

[1] A ANPD é uma autarquia especial com diretores com mandato fixo e sabatinados pelo Congresso Nacional, não podendo ser livremente exonerados. Embora não seja Agência Reguladora, é uma autarquia especial.

confirmaram a existência de lacunas importantes na governança da cibersegurança no Brasil.

As propostas elaboradas pelo GTT foram desenvolvidas para buscar endereçarr essa lacuna, oferecendo diferentes modelos de estruturação com distintos níveis de autonomia, capacidade regulatória e operacional, além de fornecer alternativas para instituição do marco legal de cibersegurança, também apontado como uma importante ausência no arcabouço jurídico brasileiro.

Cabe ressaltar que é possível trabalhar com a mescla das propostas, por exemplo considerando o marco legal mais abrangente contido na proposta 3 de autoridade acrescido da proposta 1 de agência reguladora ou idealizar a criação da secretaria ministerial por projeto de lei, aprovando-se em conjunto o marco legal de cibersegurança mencionado anteriormente.

4.2. Avaliação das Propostas

O GTT elaborou **três propostas** de modelos institucionais para a criação de uma instituição nacional de governança em cibersegurança, considerando diferentes níveis de autonomia, capacidade regulatória e operacional. As três propostas foram construídas com base nas melhores práticas internacionais, nas particularidades do contexto brasileiro e nos subsídios técnicos obtidos ao longo dos trabalhos.

As propostas oferecem alternativas estratégicas para fortalecer a governança em cibersegurança no Brasil, cada uma com vantagens e limitações, que devem ser avaliadas pelo **CNCiber** e por outras instâncias de governo no contexto político, econômico e social vigente.

4.2.1 Proposta 1 – Agência Reguladora (ANCiber)

Modelo baseado em agências reguladoras já consolidadas no Brasil, com poder regulatório pleno e autonomia administrativa, orçamentária e operacional.

Vantagens:

- Capacidade plena de normatização e fiscalização sobre os setores público e privado.
- Maior autonomia de todos os modelos, garantindo o tratamento do tema como de estado, não de governo.
- Modelo consolidado e reconhecido no Brasil, facilitando a implementação.
- Capacidade de resposta rápida e eficiente a incidentes cibernéticos.
- Poder para impor sanções e medidas corretivas em casos de não conformidade.

- Carreira própria.

Limitações:

- Complexidade na aprovação legislativa, exigindo tramitação no Congresso Nacional.
- Maior custo de implementação e manutenção em comparação com os outros modelos.
- Risco de sobreposição de competências com órgãos setoriais já existentes.

4.1.2 Proposta 2 – Secretaria Ministerial (SNCiber)

Modelo de implementação rápida, baseado em decreto presidencial, com estrutura enxuta e capacidade limitada de regulamentação e fiscalização, focada na Administração Pública Federal. Eventualmente pode depender de Medida Provisória/Projeto de Lei para garantir que o Ministério ou órgão com status de Ministério tenha as competências necessárias que permitam a criação da secretaria no seu âmbito.

Vantagens:

- Fácil implementação por meio de decreto, sem necessidade de aprovação legislativa.
- Estrutura de baixo custo e maior agilidade para ajustes estratégicos.
- Alinhamento direto com a política de governo e as prioridades estratégicas.
- Capacidade de articulação rápida com outros órgãos governamentais.
- Possibilidade de transformação de estruturas existentes no governo.

Limitações:

- Poder regulatório limitado ao setor público, sem alcance direto ao setor privado.
- Sem abrangência nacional – apenas pode articular com estados, municípios, distrito federal e demais poderes.
- Menor autonomia operacional e orçamentária em comparação com uma agência reguladora.
- Sem carreira própria – dificuldade de atrair e reter profissionais.
- Risco de falta de continuidade em cenários de mudanças de governo.
- Compete com as demais prioridades ministeriais.

Proposta 3 – Autoridade (autarquia sem regime especial)

Modelo que combina autonomia operacional e administrativa, com foco em serviços essenciais e infraestrutura crítica, seguindo o exemplo de autarquias como o **INMETRO** e a **ANPD**.

Vantagens:

- Autonomia para definição de políticas e execução de medidas de proteção cibernética.
- Foco em serviços essenciais e infraestrutura crítica, com maior estabilidade institucional.
- Flexibilidade operacional e capacidade de adaptação ao cenário cibernético em evolução.
- Modelo jurídico consolidado, com segurança para contratação e gestão de recursos.

Limitações:

- Necessidade de aprovação legislativa, com maior tempo para implementação.
- Menor autonomia em comparação com Agência Reguladora.
- Menor previsibilidade considerando livre nomeação e exoneração de dirigentes.
- Sem carreira própria, utilizando carreiras em criação ou existentes.
- Custos de implementação e manutenção mais elevados em comparação com o modelo de secretaria.
- Limitação na atuação direta sobre serviços não essenciais ou fora do escopo de infraestrutura crítica.

4.3. Recomendação de Encaminhamento

- O GTT Governança **submete as três propostas** para análise e deliberação pelo CNCiber e outras instâncias de governo, considerando o contexto político, econômico e social vigente.

4.4. Flexibilidade e Adaptação

Conforme ressaltado anteriormente, as três propostas permitem ajustes e adaptações O modelo final poderá:

- Adotar uma abordagem escalonada, iniciando com uma secretaria e evoluindo para uma agência reguladora ou autoridade e/ou/
- Incorporar elementos híbridos das três propostas, combinando marco legal mais abrangente com quaisquer dos modelos institucionais; e
- Definir um plano de transição para garantir continuidade operacional e segurança durante o processo de implementação.

4.5. Conclusão

As propostas apresentadas pelo GTT Governança oferecem alternativas viáveis para fortalecer, em diferentes níveis, a governança em cibersegurança no Brasil, cada uma com pontos fortes e limitações específicas.

Independentemente do modelo institucional, o GTT Governança destaca que a criação de um órgão centralizado é essencial para:

- **Viabilizar uma coordenação não fragmentada**, abrangendo setores público e privado, incluindo todos os entes da federação e poderes da união.
- **Ampliar a capacidade de prevenção, detecção e resposta** a incidentes de segurança cibernética de maneira rápida e estruturada.
- **Fortalecer a proteção dos serviços essenciais e infraestruturas críticas, bem como dedados estratégicos do país**, reduzindo vulnerabilidades e impactos em setores essenciais.
- **Promover uma integração eficaz entre os setores público e privado**, assegurando respostas integradas e estratégias alinhadas para o enfrentamento de ameaças cibernéticas.
- **Elevar o nível de maturidade em cibersegurança** e posicionar o Brasil como referência em segurança digital no cenário global.

Durante o processo de avaliação das propostas, alguns membros do GTT Governança registraram formalmente suas preferências e justificativas, refletindo diferentes visões sobre o modelo ideal para a governança em cibersegurança. Essas manifestações foram consolidadas no **Anexo V**, oferecendo uma visão adicional sobre os fatores estratégicos, operacionais e regulatórios considerados. A diversidade de opiniões fortalece o processo de decisão, enriquecendo a análise estratégica e contribuindo para um resultado mais alinhado com os desafios e demandas de cibersegurança no Brasil.

5. Anexos

Anexo I – Proposta de Agência Reguladora - (Agência Nacional de Cibersegurança - ANCiber)

Este anexo apresenta a minuta de Projeto de Lei que dispõe sobre a promoção de cibersegurança, a instituição do Conselho Nacional de Cibersegurança (CNCiber) e a criação do Sistema Nacional de Cibersegurança (SNCiber) e da Agência Nacional de Cibersegurança (ANCiber).

Anexo II – Proposta de secretaria ministerial - Secretaria Nacional de Cibersegurança (SNCiber)

Este anexo apresenta a minuta de decreto para a criação da Secretaria Nacional de Cibersegurança, incluindo competências, e estrutura organizacional preliminar,

estimativa de custos e textos de subsídio (Lei e decretos que precisarão ser avaliados e eventualmente alterados consoante decisão do governo sobre alocação da secretaria).

Anexo III – Proposta de Autarquia (sem regime especial) – Autoridade Nacional de Cibersegurança – ANCiber

Este anexo apresenta a minuta de Projeto de Lei que estabelece a Lei Geral de Cibersegurança, estipulando princípios, garantias, direitos e deveres para a promoção do cibersegurança no Brasil e determinando as diretrizes para atuação da União, dos Estados, do Distrito Federal e dos Municípios em relação à matéria, com a instituição do Conselho Nacional de Cibersegurança (CNCiber), do Sistema Nacional de Cibersegurança (SNCiber), a criação da Autoridade Nacional de Cibersegurança (ANCiber).

Anexo IV – Análise Comparativa das Propostas

Este anexo contém uma análise comparativa detalhada das três propostas desenvolvidas pelo GTT Governança, destacando diferenças em termos de estrutura, poder regulatório, alcance, orçamento e capacidade operacional. A tabela comparativa oferece uma visão clara dos pontos fortes e limitações de cada modelo, facilitando a tomada de decisão.

Anexo V – Votos Individuais dos Membros

Este anexo reúne os registros das manifestações individuais dos membros do GTT Governança sobre as propostas apresentadas, incluindo justificativas técnicas e estratégicas para as preferências declaradas. Os votos refletem a diversidade de visões e prioridades estratégicas dos participantes, oferecendo subsídios adicionais para a decisão final.

Anexo VI – Estudos e documentos elaborados para subsidiar os trabalhos do GTT

Manifestação sobre a preferência dos Modelos Institucionais (Agência Reguladora, Autarquia e Secretaria)

Agência Nacional de Telecomunicações (Anatel) – Representantes Gustavo Santana Borges (Titular) e Suzana Silva Rodrigues (Suplente)

Considerando as propostas de modelos institucionais para a criação de uma instituição nacional para a governança nacional de cibersegurança, a Agência Nacional de Telecomunicações reitera que o modelo de Agência de Reguladora é o mais adequado para promover e priorizar cibersegurança como um assunto de estado, sendo pilar habilitador e fundamental para a transformação digital e, por consequência, para o desenvolvimento do país e bem-estar da população brasileira.

O modelo de Agência Reguladora confere autonomia funcional, decisória, administrativa e financeira; e carreira própria e dedicada, necessárias para que os enormes desafios de promoção de cibersegurança em toda sociedade e, necessariamente, abarcando setores público e privado e todos os entes da federação e poderes, possam ser endereçados através da coordenação; regulação; e acompanhamento e controle, em um sistema que preserva e reforça a atuação setorial, ao ressalvar as competências e a atuação próprias dos demais dos demais órgãos, a exemplo da ANATEL, de forma coordenada e harmonizada no tema.

Ainda, o arcabouço legal das Agências prevê uma série de garantias a seu processo decisório, como a definição de ritos normativos - que incluem a elaboração de análises de impacto regulatório prévias -, a participação popular obrigatória - por meio da realização de amplo debate social na forma de audiências e consultas públicas -, e o estabelecimento de mandatos fixos para seus dirigentes, que confere legitimidade e estabilidade a suas decisões. A maior previsibilidade setorial decorrente de tal modelo reflete-se em novos investimentos para o país, atributo essencial em um setor tecnológico de ponta.

É importante reforçar que o modelo de agência reguladora, embora represente um desafio orçamentário à primeira vista, precisa ser observado de maneira mais sistêmica, pois a digitalização de todos os setores da economia, vivenciada por todos os países, depende de um ambiente digital confiável e seguro. A Agência certamente contribuiria para o desenvolvimento desse ambiente.

A alternativa de criação de uma autoridade (autarquia não especial), embora represente avanço em termos institucionais de governança, ainda padece de desafios que podem impactar a sua implementação e efetividade, pois a menor autonomia pode acarretar falta de previsibilidade para os agentes regulados. Já o modelo de secretaria, embora possa representar um ganho mais imediato de capacidade mais para o país em relação a atual organização, trata-se de um ganho que não corresponde ao tamanho do desafio da cibersegurança para os países.

Por fim, a Agência manifesta preocupação com eventual prerrogativa de requisição de servidores, a qual pode impactar severamente órgãos e entidades que já sofrem com déficit nos seus quadros de pessoal.

Ministério da Gestão e Inovação em Serviços Públicos (MGI) – Representante Leonardo Rodrigo Ferreira

Conforme as discussões conduzidas no Grupo de Trabalho Temático (GTT 2) do Conselho Nacional de Segurança Cibernética (CNCiber), foram apresentadas três propostas para a estruturação da governança da segurança cibernética no Brasil:

1. Secretaria Nacional de Segurança Cibernética (vinculada a um Ministério ou à Presidência);
2. Autarquia Especial (modelo similar ao INMETRO);
3. Agência Reguladora (com autonomia decisória e poder normativo amplo).

Após análise criteriosa das três alternativas, considerando o contexto econômico desafiador, a urgência para o fortalecimento da capacidade de coordenação executiva e a necessidade de integração com as competências e órgãos já existentes na estrutura governamental de segurança cibernética, o **Ministério da Gestão e da Inovação em Serviços Públicos (MGI)** se posiciona a favor da possibilidade de criação de uma **Secretaria Nacional de Segurança Cibernética** como a melhor solução para o cenário atual.

A proposta da Secretaria apresenta vantagens estratégicas significativas, tais como:

✅ Agilidade de criação – A criação de uma Secretaria pode ser viabilizada por meio de decreto presidencial, com trâmites simplificados em comparação à criação de uma autarquia ou agência reguladora, permitindo uma resposta mais rápida às crescentes ameaças cibernéticas.

✅ Integração direta com o Poder Executivo – A inserção da Secretaria na estrutura governamental facilita a coordenação com outros órgãos federais, estaduais e municipais, potencializando sinergias institucionais já estabelecidas (Por exemplo, Coordenação Executiva em Cibersegurança por meio da Rede GOV.BR, reforçada pela Estratégia Nacional de Governo Digital, prevista na Lei nº 14.129/2021 e no Decreto nº 12.069/2024, com Estados e Municípios.

✅ Implantação progressiva – A criação de uma Secretaria como estrutura de Governança de Cibersegurança Nacional daria espaço para uma possível evolução para estruturas mais complexas ao longo dos anos.

✅Sinergias com estruturas atuais - A implantação de uma Secretaria traria de forma imediata maior capacidade de articulação com estruturas já exitentes em Cibersegurança como PF, ABIN, MGI, ANATEL GSI e outras.

✅ Menor custo político e financeiro – A implementação de uma Secretaria envolve menor complexidade política e orçamentária inicial, garantindo um processo de implementação mais rápido e eficiente.

O modelo de Agência Reguladora oferece maior estabilidade e capacidade regulatória de longo prazo, mas os custos financeiros elevados, a complexidade de criação e a necessidade de tramitação legislativa tornam esta alternativa menos viável no curto prazo.

O modelo de Autarquia Especial, embora ofereça maior autonomia técnica e administrativa, enfrenta desafios semelhantes aos das agências reguladoras em termos de custos financeiros elevados, complexidade de criação e necessidade de tramitação legislativa, o que torna esta alternativa menos viável que uma Secretaria.

Diante da necessidade de resposta imediata para fortalecer a segurança cibernética nacional e garantir continuidade nas ações estratégicas, a criação de uma Secretaria emerge como a alternativa mais eficaz para responder à urgência dos riscos cibernéticos, sem comprometer a viabilidade política e econômica do processo.

Comitê Gestor da Internet no Brasil (CGI.br) - Representante Percival Henriques se Souza Neto

1. INTRODUÇÃO

CONSIDERANDO que a partir das discussões no GTT 2 do Conselho Nacional de Segurança Cibernética (CNCiber) acerca da criação de um arcabouço institucional para coordenar e fortalecer as ações de Segurança Cibernética no Brasil, foram apresentadas três propostas de modelo de governança:

1. Secretaria (inserida na estrutura de um Ministério ou da Presidência);

2. Autarquia Especial (em formato semelhante ao INMETRO;

3. Agência Reguladora (com mandatos fixos, autonomia decisória e poder regulatório amplo).

CONSIDERANDO que devo contribuir da melhor forma possível, com um parecer expondo, de forma comparativa, os prós e contras de cada modelo, levando em conta experiências internacionais, melhores práticas setoriais, o cenário atual da Segurança Cibernética global, bem como os riscos postos para a economia e a soberania nacionais. Recomendando ao final qual modelo, no meu entendimento, melhor atende à realidade brasileira.

2. CONTEXTO INTERNACIONAL E MELHORES PRÁTICAS

A segurança cibernética vem sendo tratada, em diversos países, por meio de estruturas dotadas de coordenação centralizada, mas com bom grau de autonomia técnica para emitir normas e fiscalizar sua aplicação. Alguns exemplos de destaque:

• ENISA (União Europeia): atua como agência europeia para Segurança Cibernética, apoiando Estados-membros na implementação de normas e boas práticas, com forte ênfase em pesquisa e coordenação.

• CISA(Estados Unidos): órgão do Departamento de Segurança Interna (DHS), dotado de amplos poderes de coordenação e resposta a incidentes, mas ainda assim com autonomia para emitir diretrizes de Segurança Cibernética, inclusive para infraestruturas críticas.

• ANSSI (França): agência nacional ligada ao Primeiro-Ministro, com competências de regulação técnica e coordenação de incidentes.

Em geral, observa-se a busca por estruturas que combinem autoridade técnica, capacidade de regulação e poder de coordenação, sobretudo em setores críticos (energia, telecomunicações, financeiro etc.). Também há uma tendência de fortalecimento de estruturas mais independentes do ciclo político, de modo a conferir estabilidade e continuidade às políticas de Segurança Cibernética.

3. ANÁLISE DOS MODELOS

3.1. Modelo de Secretaria

Proposta que altera a estrutura já existente de governo, criando, por decreto, uma

Secretaria Nacional de Segurança Cibernética, vinculada a um Ministério (ou diretamente à Presidência) para editar normas, promover articulação e coordenar ações de Segurança Cibernética.

Prós

• Agilidade de criação: pode ser feita por meio de decreto presidencial, com trâmites legislativos reduzidos.

• Integração direta: insere-se de forma orgânica na esfera do Poder Executivo Federal, facilitando contato com outros órgãos da alta administração.

• Menor custo político inicial: evita debates legislativos mais extensos, já que não requer lei específica para instituir nova autarquia ou agência.

Contras

• Dependência hierárquica e orçamentária: a Secretaria pode ficar vulnerável a mudanças de governo ou reorganizações administrativas, afetando a continuidade de políticas de longo prazo.

• Menor estabilidade: sem mandatos fixos ou garantias legais de autonomia, há risco de descontinuidade a cada troca de ministro ou de governo.

• Escopo potencialmente limitado: embora possa editar normas para a Administração Pública Federal, a capacidade de regular o setor privado ou coordenar estados e municípios depende de portarias ou convênios menos robustos em termos legais.

Diante de experiências internacionais, observa-se que estruturas meramente governamentais – sem mandato técnico independente – frequentemente enfrentam dificuldades para impor padrões mínimos a setores estratégicos, sobretudo onde haja agências reguladoras já consolidadas.

3.2. Modelo de Autarquia Especial

Inspirado em um formato próximo ao do INMETRO, conforme o projeto que a denomina “Autoridade Nacional de Segurança Cibernética”. Trata-se de uma autarquia “sob regime

especial”: nomeação presidencial dos diretores, porém sem mandatos fixos (ou seja, diretores podem ser substituídos a qualquer momento).

Apresenta, ainda, autonomia técnica e administrativa e quadro de pessoal próprio, com foco prioritário em Serviços Essenciais e Infraestruturas Críticas.

Prós

• Maior autonomia técnica e administrativa do que uma secretaria, ainda que não tanto quanto uma agência típica com mandatos fixos.

• Menor custo político do que uma agência reguladora tradicional, pois não exige necessariamente a tramitação legislativa de igual complexidade (a depender da formatação).

• Forte ênfase em coordenação com reguladores setoriais já existentes, mantendo a competência residual em temas gerais de Segurança Cibernética.

• Escalonamento do quadro funcional previsto: de 330 profissionais em até 6 anos, com redução de custos em relação à proposta de agência (que previa 440 profissionais).

Contras

• Ausência de mandatos fixos pode fragilizar a estabilidade da liderança, pois os diretores continuam expostos a substituições políticas.

• Menor robustez na interlocução internacional, se comparada a uma agência com maior amplitude regulatória (embora não seja um impeditivo).

• Complexidade de criação: requer Projeto de Lei específico, com tramitação no Congresso, o que pode retardar o início efetivo das atividades, embora menos do que um projeto de agência reguladora integral.

Na perspectiva de comparações internacionais, algumas autoridades de Segurança Cibernética contam com mandatos fixos para seus dirigentes, o que reforça independência decisória. Entretanto, se houver garantias de autonomia orçamentária e apoio governamental, este modelo de autarquia pode ser suficiente para garantir a coordenação nacional.

3.3. Modelo de Agência Reguladora

Proposta de criação de uma agência nos moldes tradicionais brasileiros (ex.: ANATEL, ANEEL, ANP, etc.), com mandatos fixos e mais rígidos, quadro robusto (inicialmente projetado em 440 servidores) e poder normativo amplo sobre setores público e privado na área de Segurança Cibernética.

Prós

• Maior autonomia: mandatos fixos e estabilidade dos dirigentes reduzem pressões políticas e asseguram continuidade.

• Poder regulatório sólido: possibilidade de expedir normas técnicas e sanções com maior legitimidade e menor contestação.

• Alinhamento às melhores práticas internacionais: a maior parte das agências de Segurança Cibernética internacionais de referência (ENISA, ANSSI, etc.) opera com alto grau de independência e pessoal dedicado.

• Amplitude de atuação: abrange a regulação integral, garantindo obrigatoriedade de implementação de padrões mínimos por todos os entes públicos e operadores críticos do setor privado.

Contras

• Maior custo e complexidade política: criação de uma agência reguladora exige lei específica mais detalhada, tramitação legislativa potencialmente longa e alto engajamento do Congresso.

• Investimento financeiro maior: projeção de até 440 servidores, implicando custo de implantação (acumulado em seis anos) superior ao modelo de autarquia.

• Possível sobreposição com agências setoriais já consolidadas: seria necessária uma coordenação fina para evitar conflitos de competência.

A agência reguladora é o modelo que, em tese, garante a independência decisória e a robustez regulatória de longo prazo, mas exige um processo legislativo e político mais complexo.

4. RISCOS E URGÊNCIA DO TEMA

A Segurança Cibernética tornou-se um fator de estabilidade econômica e soberania nacional. Estima-se que prejuízos vinculados a incidentes cibernéticos possam chegar a dezenas de bilhões de reais ao ano no contexto brasileiro, sem contar impactos reputacionais, políticos e sociais. Nesse sentido, a governança de Segurança Cibernética não pode ser frágil: precisa de mandato, recursos e suporte de alto nível para coordenar esforços em todos os entes federativos e no setor privado.

5. CONCLUSÃO: PRÓS/CONTRAS EM SÍNTESE

Modelo	Principais Vantagens	Principais Desvantagens
Secretaria	Simplicidade, agilidade de criação, menor custo político inicial	Baixa autonomia, sujeita a mudanças políticas, limitada capacidade regulatória
Autarquia	Autonomia administrativa e técnica intermediária, custos menores que agência	Sem mandatos fixos, ainda exposta a interferências políticas, requer lei específica
Agência	Alta independência, mandatos fixos, poder regulatório sólido e amplo	Maior complexidade de criação, custo político e financeiro mais elevado

6. MEU PARECER

Considerando:

• A necessidade de celeridade, mas também de estabilidade e continuidade na política de Segurança Cibernética;

• A conveniência de um arcabouço legal que dê segurança jurídica às ações, mas sem onerar excessivamente o Estado;

• A experiência internacional, que aponta para estruturas com independência técnica (mandato) e amplitude na coordenação com setores público e privado;

• A importância de minimizar riscos de descontinuidade a cada novo governo, essencial para que as políticas de Segurança Cibernética tenham horizonte de planejamento de médio e longo prazo;

VOTO pela adoção do modelo de Autarquia Especial, conforme a proposta que cria a "Autoridade Nacional de Segurança Cibernética (ANCiber)" no padrão INMETRO. Entendo que tal formato:

1. Equilibra a necessidade de autonomia técnica e administrativa com a viabilidade político-institucional, reduzindo entraves que uma agência reguladora tradicional poderia enfrentar no Congresso;

2. Permite maior flexibilidade de ajustes e diálogo com as agências setoriais existentes, evitando sobreposição de competências;

3. Mantém custos de implantação comparativamente menores do que a proposta de agência reguladora (pois prevê cerca de 330 servidores ao longo de 6 anos, em vez de 440).

4. Facilita a tramitação legislativa em relação a uma agência clássica, embora ainda exija aprovação de Projeto de Lei;

5. Cria um órgão com competência residual e capacidade regulatória nacional sobre Segurança Cibernética, em coordenação com reguladores setoriais e demais atores.

RESSALTO que, para a robustez desse modelo, recomenda-se que o texto final do PL preveja salvaguardas de autonomia, condições mínimas para estabilidade da alta direção (mesmo que sem mandatos fixos, ao menos com critérios e prazos claros para exoneração), além de mecanismos de financiamento e controle social adequados.

Em face ao cenário global e às demandas de soberania e desenvolvimento tecnológico, REAFIRMO que a AUTARQUIA ESPECIAL apresenta um caminho viável, que equilibra a urgência do tema com a complexidade de seu enfrentamento e implementação.

Instituto dos Advogados de São Paulo (IASP) – Representantes Juliana Abrusio (titular) e Mauro Aspis (suplente)

Na qualidade de representantes de entidade da sociedade civil do CNCiber, e diante da demanda quanto à análise dos modelos propostos para a governança da cibersegurança nacional, quais sejam, Agência Reguladora, Autoridade e Secretaria, o Instituto dos Advogados de São Paulo (IASP), através de seus representantes Juliana Abrusio (titular) e Mauro Aspis (suplente), manifesta sua opinião pela adoção do modelo de Autoridade como mais adequada. O modelo institucional da Autoridade equilibra autonomia regulatória e operacional sem os custos e entraves políticos de uma agência reguladora, além de garantir abrangência nacional, permitindo a interação com o setor privado e entes federativos. No nosso entendimento a Autoridade possui competências

normativas e fiscalizatórias suficientes, com autonomia técnica e administrativa, para estruturar e coordenar a Política Nacional de Cibersegurança, garantindo maior eficácia na supervisão do cumprimento das obrigações de cibersegurança. Além disso, sua flexibilidade administrativa e menor tempo de implementação em comparação à criação de uma nova agência reguladora tornam essa escolha mais pragmática e eficiente. Dessa forma, entende-se que o modelo da Autoridade (Autarquia não especial) atende de maneira adequada às necessidades de governança da cibersegurança, assegurando coordenação efetiva entre os setores público e privado, sem comprometer a eficiência administrativa ou a capacidade de regulação e fiscalização

Ministério da Defesa – Representante Cel. Harley de Pinho, Subchefe do Centro de Coordenação de Operações Cibernéticas do ComDCiber

O posicionamento da Defesa foi apresentado em vários momentos durante esta jornada de aprendizado e troca de conhecimentos entre todos os integrantes do GTT Governança.

A falta de maturidade de Segurança Cibernética em nosso país é latente. A importância de implementação de uma estrutura forte e com poderes regulatórios que esteja focada nos Objetivos Nacionais Permanentes (ONP) e que se preocupe 24h/7dias da semana com a Segurança Nacional não pode esperar o amanhã. A Segurança Nacional, com tudo que ela carrega a reboque tem como premissa básica guardar o bom funcionamento de todas as infraestruturas críticas que impactam desde a vida dos cidadãos até as nossas fronteiras digitais. Não estamos coordenados e sincronizados para esta missão no âmbito da Administração Pública Federal e Setor Privado.

O portfólio cognitivo de ideias apresentadas neste GTT confirmou que possuímos ilhas de modernidade na área cibernética, porém com escopos limitados as suas áreas de abrangência (Telecomunicações, Financeiro, Energia, Segurança e Defesa dentre outros).

Neste diapasão, a Defesa é de parecer pela criação de uma Agência Reguladora ou uma Autoridade de âmbito nacional que possa ser este elo que falta entre as diversas iniciativas já apresentadas.

Confederação das Associações das Empresas Brasileiras de Tecnologia da Informação (ASSESPRO) – Representante Rodrigo Jonas Fragola

Vivemos em uma era digital, onde a tecnologia permeia todos os aspectos de nossas vidas. Desde as transações bancárias e comunicações pessoais até a infraestrutura crítica que sustenta nossa sociedade, dependemos cada vez mais de sistemas digitais interconectados.

No entanto, essa crescente dependência também nos torna vulneráveis a ameaças cibernéticas cada vez mais sofisticadas e perigosas. Ataques de ransomware, roubo de dados, espionagem cibernética e sabotagem de infraestruturas críticas são apenas alguns exemplos dos riscos que enfrentamos diariamente.

Segundo dados do segundo Panorama de Ameaças para a América Latina 2024, o Brasil é segundo país com mais ataques cibernéticos no mundo. Em um período de 12 meses, foram registrados mais de 700 milhões de ataques cibernéticos no país, totalizando 1.379 por minuto, números em amplo crescimento no país. Destacase ainda que o custo médio de violação de dados em nosso país atingiu em 2024 a marca de R$ 7,44 milhões, um aumento de 11,5% ante 2023, segundo dados do Brasil extraídos do relatório "Cost of a Data Breach", divulgado pela IBM.

A recente escalada dos conflitos geopolíticos globais intensificou ainda mais a ameaça cibernética. Estados nacionais e grupos criminosos utilizam o ciberespaço para obter vantagens estratégicas e causar danos significativos. Vale ressaltar que os ataques cibernéticos também são utilizados para se obter vantagens competitivas através de roubo de informações estratégicas das empresas tais como produtos inovadores, projetos de pesquisa, lista de clientes, etc...

As várias iniciativas existentes, tanto na esfera governamental como privada ainda tem uma reduzida capacidade de colaborar entre si diante deste novo cenário. Um dos principais fatores de risco reside na complexa cadeia de fornecimento que conecta empresas privadas ao governo, onde o nó mais fraco da cadeia aumento o risco de todo o sistema de integração.

A segurança cibernética é uma responsabilidade compartilhada, e a criação de um órgão forte e independente melhora não só aspectos de segurança governamental e defesa nacional como também melhora significativamente aspectos de prevenção, contenção e investigação de incidentes cibernéticos. Estes aspectos melhoram muito o ambiente de negócios, impulsionando o desenvolvimento do setor de tecnologia da informação, gerando empregos e novas oportunidades.

Nesse sentido, acredito de suma importância que a criação de um órgão que seja capaz de coordenar as atividades já existentes relativas ao tema, atuando em sincronia e parceria com outras instituições que tem parte de sua obrigação regular escopos específicos do tema ou setores da economia, como CGI.BR, NIC.BR, ANATEL, ANPD, dentre outras.

Em relação aos modelos apresentados, entendo que o mesmo deve atender os seguintes princípios:

» Regulação e fiscalização: Estabelecer normas e padrões de segurança cibernética para empresas e órgãos governamentais, garantindo a proteção de dados e infraestruturas críticas. A geração de padrões de segurança cibernética claros e atualizados é essencial para orientar o setor público e privado na adoção de melhores práticas e tecnologias de proteção.

» Resposta a incidentes: Coordenar a resposta a ataques cibernéticos em larga escala, mobilizando recursos e expertise instalados em nosso país para mitigar danos e restaurar a normalidade.

» Inteligência e monitoramento: Coletar e analisar informações sobre ameaças cibernéticas, identificando padrões e tendências para antecipar e prevenir ataques.

» Cooperação internacional: Fortalecer a cooperação com outros países e organizações internacionais para combater o cibercrime e promover a segurança cibernética global.

» Conscientização e educação: Promover a conscientização sobre segurança cibernética entre empresas e cidadãos, capacitando-os a se protegerem contra ameaças digitais.

» Fomento à pesquisa e desenvolvimento: Incentivar a pesquisa e o desenvolvimento de tecnologias e soluções de segurança cibernética, impulsionando a inovação e a competitividade do setor.

» Autonomia Financeira e Regulatória: Garantir a independência de suas operações e a capacidade de investir em tecnologia, pessoal qualificado e infraestrutura de ponta.

Isto posto, entendo que a solução que melhor se adequa a estes requisitos é o **Modelo de Agência Reguladora**, um modelo já bem consolidado e que teria a capacidade e a autonomia necessárias para conduzir os trabalhos de forma continua e com maior abrangência, tanto no setor público quanto no privado.

O **Modelo de Autoridade** seria a segunda opção. Entretanto entendo que necessita de mais discussões e aprofundamento.

Já o **Modelo de Secretaria**, entendo que agregaria muito pouco as iniciativas já existentes, tendo limitações substanciais em relação a abrangência e capacidade de "se fazer cumprir" normas editadas por ela.

Instituto Peck Cidadania Digital – Representante Patrícia Peck

O Instituto Peck de Cidadania Digital (IPCD), na atribuição da 3ª Representação da Sociedade Civil no Comitê Nacional de Cibersegurança (CNCiber), no tocante a proposta de criação de Órgão de Governança da Atividade de Cibersegurança, objeto de estudo do presente Grupo Técnico de Trabalho (GTT), manifesta-se favoravelmente a proposta do modelo de Agência Reguladora, pelas razões a seguir expostas.

Inicialmente, destaca-se reportagem da revista Veja, de 13/05/2025, que o Brasil é o 4º maior alvo de software maliciosos nas Américas de acordo com a empresa NordVPN, com cerca de 10 milhões de tentativas de ataques cibernéticos em 2024, que poderiam resultar em situações que envolvam sequestro de dados, roubos de identidade e vazamentos.

Nesse sentido, há grande expectativa da Sociedade Civil sobre a criação de um órgão de governança de cibersegurança no país e, considerando os debates realizados no decorrer dos trabalhos do presente GTT, entendemos o modelo de Agência Reguladora como o mais adequado às necessidades do País, vez que a Agência detém maior autonomia para as finalidades de fiscalização, regulamentação e sancionatória, permitindo alcançar tanto o setor público quanto o setor privado, possuindo ainda, controle direto de coordenação e controle.

Subsidiariamente, o modelo proposto de Autoridade também se demonstra aplicável, embora possua autonomia parcial, sua competência também alcança o setor público e o setor privado, não exigindo articulação para atuação no setor privado como seria o caso do terceiro modelo proposto, qual seja, Secretaria, que não seria recomendável, ainda, por se tratar de uma estrutura limitada, com coordenação e controle indiretos, e possuir capacidade parcial de fiscalização.

Federação das Industriais do Estado de São Paulo – Representante Rony Vainzof

Considerandas:

• Empresas privadas e órgãos do Estado que não nasceram digitais, inevitavelmente estão em fase de digitalização e emprego de inovações tecnológicas;

• Há aumento vertiginoso na escalada e sofisticação dos ataques cibernéticos. O uso de Inteligência Artificial e algoritmos avançados aumenta tanto as capacidades defensivas quanto os riscos de exploração por agentes mal-intencionados, demandando estratégias de mitigação robustas;

• A proteção de infraestruturas críticas e de serviços essenciais deixou de ser questão apenas empresarial, tornando-se elemento central da segurança nacional e da estabilidade econômica dos países;

• A insegurança cibernética desponta como preocupação crítica a curto e longo prazo, conforme relatórios do Fórum Econômico Mundial. É pauta que vai muito além de fraudes e vazamento de dados, pois ataques cibernéticos podem paralisar organizações e países;

• Incidentes de segurança no Brasil podem ter gerado em 2024 prejuízos diretos, indiretos e induzidos de R$ 2,3 Trilhões, o que representa perda de 18% no PIB anual (INCC);

• A fragmentação de iniciativas regulatórias e normativas gera respostas lentas e ineficazes diante do volume de ameaças e complexidade de suas causas;

• A grande maioria dos incidentes de cibersegurança poderiam ser evitados com medidas básicas de proteção;

• Cibersegurança é fundamental para a sobrevivência e competitividade das empresas e nações; e

• A natureza transnacional das ameaças cibernéticas exige colaboração entre governos, empresas e organismos internacionais para aprimorar a resposta a incidentes e fortalecer a resiliência digital.

Premissas para a abordagem regulatória e para o órgão de governança:

• Marco Legal de Cibersegurança:

- Claro, equilibrado, flexível e eficiente, capaz de alinhar as normas nacionais às melhores práticas internacionais, sem impor custos operacionais excessivos ou proibitivos, permitindo ambiente seguro, competitivo e inovador, no qual empresas possam crescer sem enfrentar obstáculos desproporcionais;
- Abordagem baseada em risco, com maior peso normativo aos serviços essenciais e de infraestruturas críticas;
- Excepcionar a carga regulatória para empresas de pequeno porte;
- Incentivos econômicos e fiscais para empresas com boas práticas de governança em cibersegurança ou que desenvolvam soluções inovadoras, como redução tributária, acesso a crédito facilitado e prioridade em licitações públicas;

- Precaução ao “importar” conceitos e regulamentações estrangeiras, garantindo a adaptação à realidade nacional; e
- Implementação de programa nacional de conscientização em cibersegurança para empresas e cidadãos, que leve também a inclusão do tema nos currículos educacionais, desde o ensino básico até o superior.

• Entidade de coordenação nacional de cibersegurança:

- Coordenar ações de cibersegurança com integração entre diferentes órgãos governamentais, setor privado e academia;
- Poderes regulatórios claros para garantir ambiente mais equilibrado, promovendo segurança jurídica e previsibilidade, além de ser capaz de organizar, direcionar e impulsionar diferentes soluções dentro e fora do estado;
- Evitar sobreposição de competências (bis in idem) com órgãos reguladores setoriais, garantindo que a regulamentação, fiscalização e sanção permaneçam no âmbito dos órgãos específicos de cada setor ou matéria;
- Harmonizar entendimentos e diretrizes, promovendo a padronização de normas, a interoperabilidade regulatória e a cooperação entre setores;
- Regular setores não abrangidos por reguladores específicos, prevenindo lacunas normativas e garantindo uma abordagem integrada e consistente em todo o ecossistema do país; e
- Não impor custo econômico adicional à sociedade para a sua criação.

Conclusão: as propostas do GTT de “Autarquia” e “Agência Reguladora” melhor se enquadram nas premissas descritas acima.

Centro de Tecnologia e Sociedade da Fundação Getúlio Vagas Direito Rio – Representante Luca Belli

Considerando a elaboração de três propostas que contemplam entidades com características distintas para exercerem a governança em cibersegurança – agência reguladora, autarquia e secretaria – venho, por meio deste parecer, apresentar a ordem de preferência para indicação ao plenário do CNCiber pelo Centro de Tecnologia e Sociedade da FGV.

É essencial que o arranjo institucional tenha poderes regulatórios, incluindo poderes normativos, fiscalizatórios e sancionatórios, bem como tenha competência para coordenar o ambiente cibernético no que se refere à cibersegurança, promovendo a aproximação entre os diversos setores e atores evolvidos. Esses poderes são importantes diante da atual fragmentação no âmbito da cibersegurança, evidenciada, entre outros fatores, pelas disparidades nos níveis de segurança entre os órgãos e entidades dos entes federativos, decorrentes da desigualdade normativa nessa temática; pela escassez de pessoal qualificado para lidar com a pronta resposta a incidentes cibernéticos; e pela ausência de harmonização e de uma rede de cooperação efetiva entre os atores que atuam na área.

Dessa forma, é fundamental a criação de um arranjo com abrangência nacional, capaz de exercer essa coordenação sob dois aspectos: normativo e operacional. **Nesse sentido, o modelo institucional mais adequado seria o de uma agência reguladora,** pois, além

de ser um modelo gerencial já adotado em outros setores regulados economicamente, trata-se de um modelo tecnicamente mais completo para endereçar as necessidades mencionadas na área de cibersegurança.

O modelo de autarquia também se mostra uma alternativa viável para suprir tais demandas, sendo, portanto, a segunda opção mais recomendável. Ainda assim, considera-se mais vantajoso do que a simples existência de uma secretaria, que, na visão deste membro, seria menos eficiente, uma vez que não dispõe de mecanismos suficientes para promover melhorias significativas no cenário atual. A principal diferença entre agência reguladora e autarquia reside no fato de que a agência apresenta uma autonomia multifacetária – administrativa, financeira, patrimonial e, sobretudo, decisória –, o que se revela essencial para o desenvolvimento da política nacional de cibersegurança.

Ministério das Comunicações (MCom) – Representante Jordan Silva de Paiva

Inicialmente, é importante salientar que a abordagem em relação às complexas questões afetas à cibersegurança exige que a atuação do Estado se desenvolva tanto no âmbito político-estratégico quanto na dimensão regulatória.

Nesse sentido, reiteram-se os argumentos já presentes nas manifestações de representantes da sociedade civil e da Anatel, para expressar que **o modelo de governança para cibersegurança, na dimensão regulatória, precisa ser erigida a partir de uma agência reguladora.**

Acrescente-se que, diante das informações de que seria inviável a criação de uma nova agência reguladora, **mostra-se mais adequado que uma agência reguladora já existente seja a entidade responsável pelas competências descritas pelo GTT de Governança em cibersegurança do CNCiber.**

Em razão da pertinência e proximidade dos temas, **a Anatel se apresenta como a opção correta para recepcionar essa atividade**.

Destaca-se que a Anatel apresenta as seguintes vantagens, dentre outras: **alcance nacional, com presença física em todos os Estados da federação; quadro atual com mais de 1400 servidores; corpo técnico altamente qualificado, com expertise em todo o processo regulatório (regulamentação, fiscalização etc.); autonomia financeira.**

Controladoria-Geral da União (CGU) – Representante Jaíza Alves Gomes

Considerando os modelos apresentados nos trabalhos do GTT (Agência Nacional de Cibersegurança, Autoridade Nacional de Cibersegurança e Secretaria Nacional de Cibersegurança) entendemos que as agências reguladoras tem se mostrado mais adequadas para setores que exigem regulação técnica e especializada.

As agências reguladoras apresentam autonomia e independência administrativa, apresentam carreira própria e dedicada, permitindo regulação mais precisa e técnica, possuem poderes mais amplos de fiscalização e aplicação de sanções, oferecem maior

estabilidade nas políticas regulatórias e alcançam tanto o setor público quanto o setor privado.

Na impossibilidade da criação de agência reguladora, o modelo de Autoridade Nacional seria a segunda opção. A Secretaria Nacional, ainda que apresente vantagens como a agilidade de criação, fica restrita ao setor público e não conseguiria atender desafios da cibersegurança que os outros dois modelos atenderiam.

Ministério da Justiça e Segurança Pública – Representante Priscila de Castro Busnello

Consideramos que o modelo mais adequado para enfrentar o problema apresentado ao GTT, especialmente no que se refere à governança em cibersegurança, é o de agência reguladora. Esse modelo oferece a estrutura, autonomia, abrangência e atribuições necessárias para lidar com a questão de forma efetiva.

Caso a adoção desse modelo não seja viável, entendemos que, em caráter subsidiário, o modelo de autarquia poderia ser uma alternativa.

.....