PNCiber – Audiência Pública

Relatório da Audiência Pública
Análise das Contribuições
Transcrição da Sessão Pública

PNCiber – Relatório da Audiência Pública

Este documento apresenta a consolidação dos dados, sugestões e críticas resultantes da Audiência Pública GSI 01/2023, sobre o anteprojeto de lei proposto para a Política Nacional de Cibersegurança, realizada em 15 de junho de 2023.

1 DA PREPARAÇÃO E REALIZAÇÃO DA AUDIÊNCIA PÚBLICA

Visando dar visibilidade e transparência ao processo de elaboração do projeto de lei de iniciativa do executivo no sentido da criação de uma Política Nacional de Cibersegurança, e coletar sugestões e críticas voltadas à melhoria deste, o GSI decidiu pela realização de uma audiência pública.

1.1 Da Publicação do Aviso da AP

A publicação do aviso da Audiência Pública foi feita no dia 18 de maio de 2023, tanto no Diário Oficial da União quanto no Correio Braziliense, chamando os interessados para a audiência a ser realizada no dia 15 de junho de 2023.

Na data da publicação do Aviso da AP foi disponibilizado um arquivo pdf contendo 5 (cinco) documentos relativos ao anteprojeto de lei:

1) Apresentação do Projeto: documento que explica algumas das opções adotadas no anteprojeto;
2) Exposição de Motivos: documento que explicita a motivação, bem como a urgência e a relevância, da elaboração do projeto;
3) Anteprojeto de Lei: texto do anteprojeto base elaborado pelo GSI;
4) Anteprojeto de Decreto: texto do anteprojeto proposto para detalhar a implementação do anteprojeto de lei, regulamentando as instituições propostas:
    a. Comitê Nacional de Cibersegurança (CNCiber);
    b. Agência Nacional de Cibersegurança (ANCiber);
    c. Gabinete de Gerenciamento de Cibercrises (GGCiber).
5) Nota Técnica: documento que apresenta uma argumentação sobre os custos do projeto.

O Secretário de Segurança da Informação e Cibernética do GSI aproveitou-se de sua participação em uma audiência pública no Senado Federal no mesmo dia 18 de maio para comunicar aos presentes a publicação do aviso e o objeto da audiência futura, buscando sempre a maior visibilidade possível para o tema.

1.2 Dos Palestrantes Convidados

Foram convidados 15 (quinze) palestrantes de instituições e setores diversos de atuação, conforme tabela abaixo.

Instituição	Responsável
Gabinete de Segurança Institucional da Presidência da República	Ministro Marcos Amaro, Ministro de Estado Chefe do GSI
Senado Federal	Senador Esperidião Amin
Ministério da Relações Exteriores	Sr. Franklin Silva Netto, Conselheiro

Instituição	Responsável
Ministério da Justiça e Segurança Pública	Sra. Estela Aranha, Assessora Especial do Gabinete do Ministro
Ministério da Gestão e Inovação em Serviços Públicos	Sr. Leonardo Rodrigo Ferreira, Diretor de Departamento de Privacidade e Segurança da Informação da Secretária de Governo Digital
Autoridade Nacional de Proteção de Dados	Sr. Arthur Pereira Sabbat, Diretor
Senado Federal	Sr. Paulo Barone, Professor e Assessor do Senador Izalci Lucas
Senado Federal	Senador Rogério Carvalho
Agência Nacional de Telecomunicações	Sr. João Zanon, representando o Sr. Carlos Manoel Baigorri, Presidente
Tribunal de Contas da União	Sr. Carlos Renato Araújo Braga, Diretor da Secretaria de Fiscalização de Tecnologia da Informação
Federação das Indústrias do Estado de São Paulo	Sr. Humberto Luiz Ribeiro, Diretor do Departamento de Segurança da FIESP
Peck Advogados	Sra. Patrícia Peck Pinheiro, Advogada especializada em Direito Digital
Fundação Getúlio Vargas	Sr. Luca Belli, Professor
Confederação Nacional da Indústria	Sr. Jefferson Gomes, Diretor de Inovação e Tecnologia do Serviço Nacional de Aprendizagem Industrial
Polícia Federal	Sr. Valdemar Latance Neto, Chefe do Serviço de Análise e Inteligência Policial da Diretoria de Combate à Crimes Cibernéticos da Polícia Federal

1.3 Das Inscrições

A 5 dias da data da AP já havia sido atingido o total de assentos disponíveis no auditório, e assim foram disponibilizadas 15 (quinze) cadeiras móveis adicionais no auditório, com vistas à ampliação do número de potenciais inscritos. Ainda assim, na véspera da AP o número de inscritos já atingira o total disponível, e por questões de segurança o GSI foi obrigado a iniciar a recusa de inscrições que ainda chegavam.

Ao todo foram confirmadas 145 (cento e quarenta e cinco) inscrições, de pessoas representando 94 (noventa e quatro) instituições e “cidadãos”.

1.4 Da Presença Efetiva

No dia da AP estiveram presentes ao local um total de 88 (oitenta e oito) participantes, ou 61% (sessenta e um por cento) do total de inscritos.

Esse percentual mostra que teria sido possível acatar vários dos pedidos de inscrição recusados devido à capacidade limite do auditório, mas a ausência de uma base histórica de informações de outras audiências públicas não nos permitiu projetar isso antecipadamente.

1.5 Da Participação Remota

Dado o grande número de inscrições, e a limitação de espaço físico do auditório, decidiu-se por viabilizar a participação remota. Para tanto, foi solicitada a transmissão em tempo real da Audiência Pública por um dos canais da Empresa Brasil de Comunicação (EBC) no Youtube, o que facultaria o acompanhamento daqueles impossibilitados de estarem presentes. Adicionalmente, facultou-se o envio das sugestões e críticas por meio de um formulário disponibilizado no site da Secretaria de Segurança da Informação e Cibernética do GSI, o qual poderia ser preenchido e enviado por e-mail até as 23h59 minutos do dia da audiência.

O link com a gravação (https://www.youtube.com/watch?v=RXf5Xn1vjdg) continua disponível, e em 14/07/2023 já acumulava cerca de 3.900 (três mil e novecentas) visualizações.

De sua parte, a página da Secretaria de Segurança da Informação e Cibernética contendo os documentos da Audiência Pública, na mesma data, registrava mais de 2.500 (dois mil e quinhentos) acessos.

A transcrição do áudio da audiência encontra-se no ANEXO II do presente relatório.

2 DA CONTRIBUIÇÕES APRESENTADAS

2.1 Do Quantitativo de Contribuições Apresentadas

Foi apresentado um total de 281 (duzentas e oitenta e uma) contribuições ao anteprojeto de lei, propostas por 63 (sessenta e três) autores de 38 (trinta e oito) instituições (com "cidadão" computado como uma destas).

Considerando-se o número de autores e instituições contribuintes relativamente aos inscritos temos o que segue:

Grupo	Inscritos	Autores	Razão
Pessoas	145	63	43%
Instituições	94	38	40%

2.2 Dos Pareceres do GSI Quanto às Contribuições

Cada uma das contribuições apresentadas foi analisada e respondida individualmente, e o relatório dessa análise constitui o ANEXO I do presente relatório. Cumpre ressaltar que a ordenação das contribuições foi feita por "Tipo de Parecer", conforme apresentado adiante.

2.3 Da Análise das Contribuições Apresentadas

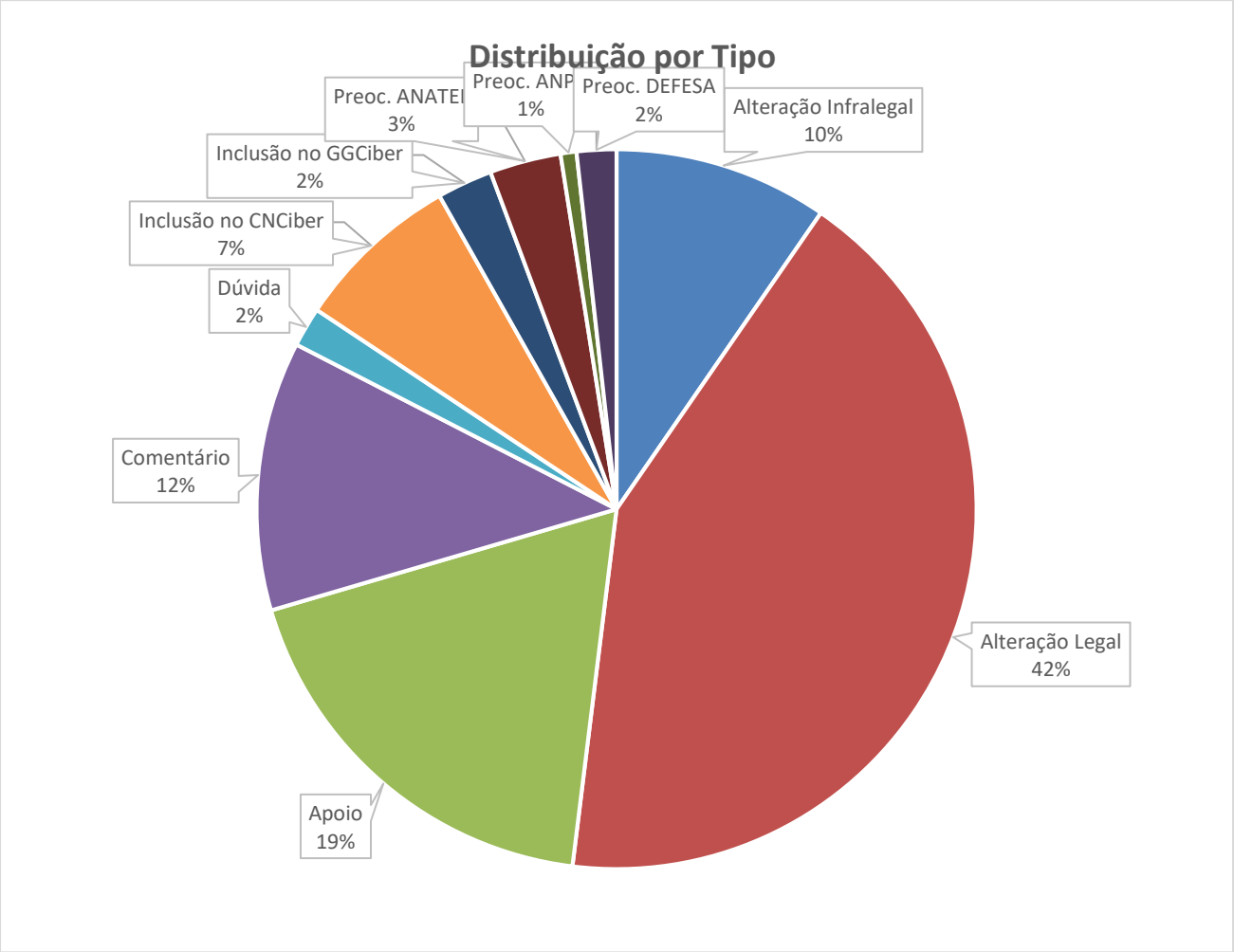
Para viabilizar a análise das contribuições de uma forma sistemática, foi adotado um conjunto de "categorias de análise".

2.3.1 Da Categorização do "Tipo de Contribuição"

Observou-se que as contribuições apresentavam uma "tipificação" que permitia agrupá-las conforme disposta na tabela abaixo:

Tipo de Contribuição	Descrição
Alteração Infra legal	Sugestão aplicável apenas em um documento de natureza infra legal, como uma resolução da ANCiber, por exemplo
Alteração Legal	Sugestão aplicável em documento de natureza legal
Apoio	Manifestação de apoio à PNCiber
Comentário	Comentário que não afeta a redação do anteprojeto
Dúvida	Pedido de esclarecimento que pode ou não ensejar uma alteração do anteprojeto
Inclusão no CNCiber	Sugestão de inclusão de instituições no Comitê Nacional de Cibersegurança
Inclusão no GGCiber	Sugestão de inclusão de instituições no Gabinete de Gestão de Cibercrises
Preoc. ANATEL	Preocupação com eventual conflito de competências com a Agência Nacional de Telecomunicações
Preoc. ANPD	Preocupação com eventual conflito de competências com a Autoridade Nacional de Proteção de Dados
Preoc. DEFESA	Preocupação com a presença do tema ciberdefesa na Política Nacional de Cibersegurança

A distribuição das contribuições de acordo com essa categorização deu-se conforme ilustra o gráfico abaixo.

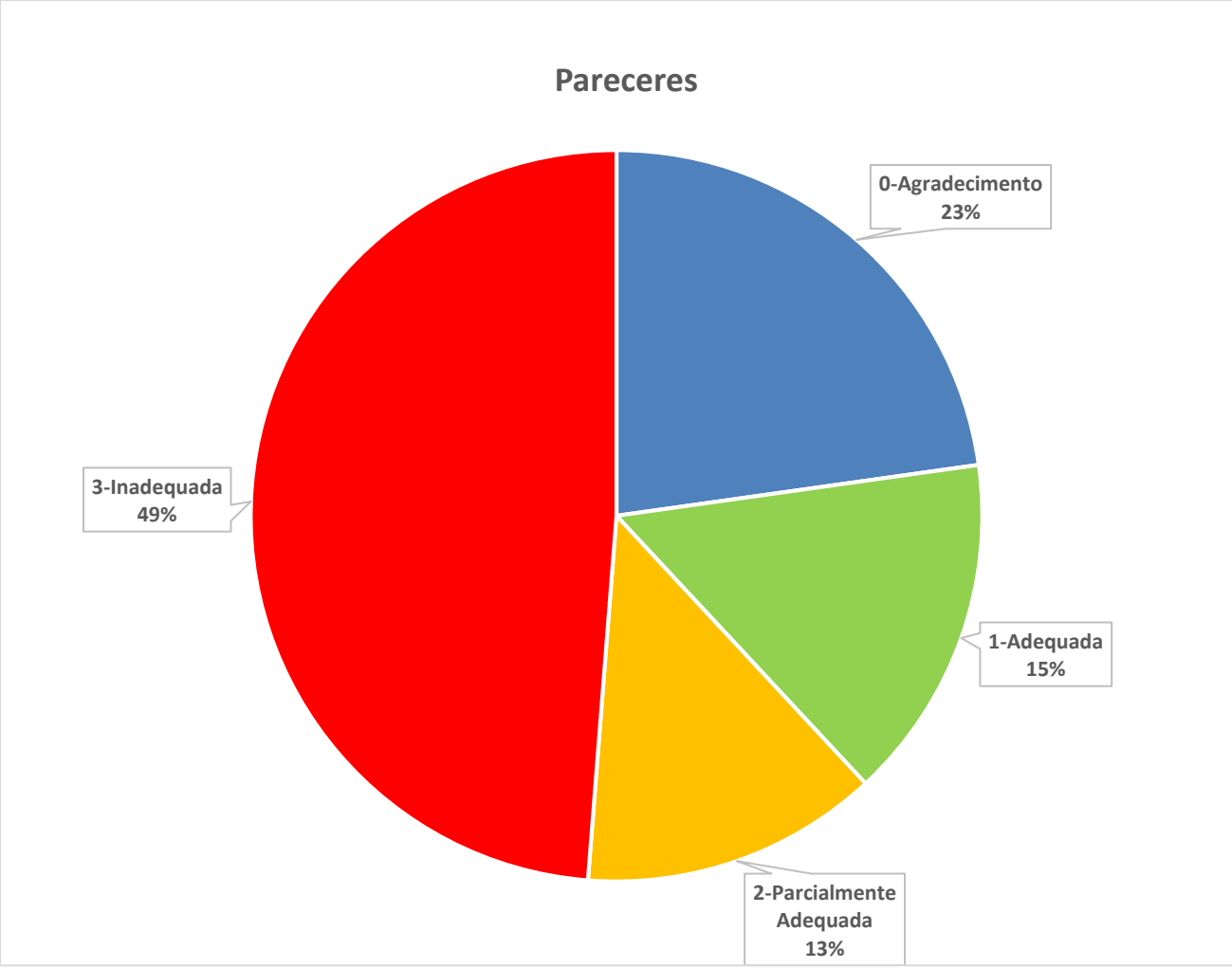


2.3.2 Da Categorização do "Tipo de Parecer"

Conforme se analisava as respostas dadas às contribuições emergia uma "categoria de análise" que permitia agrupar os pareceres dados em conforme dispõe a tabela abaixo:

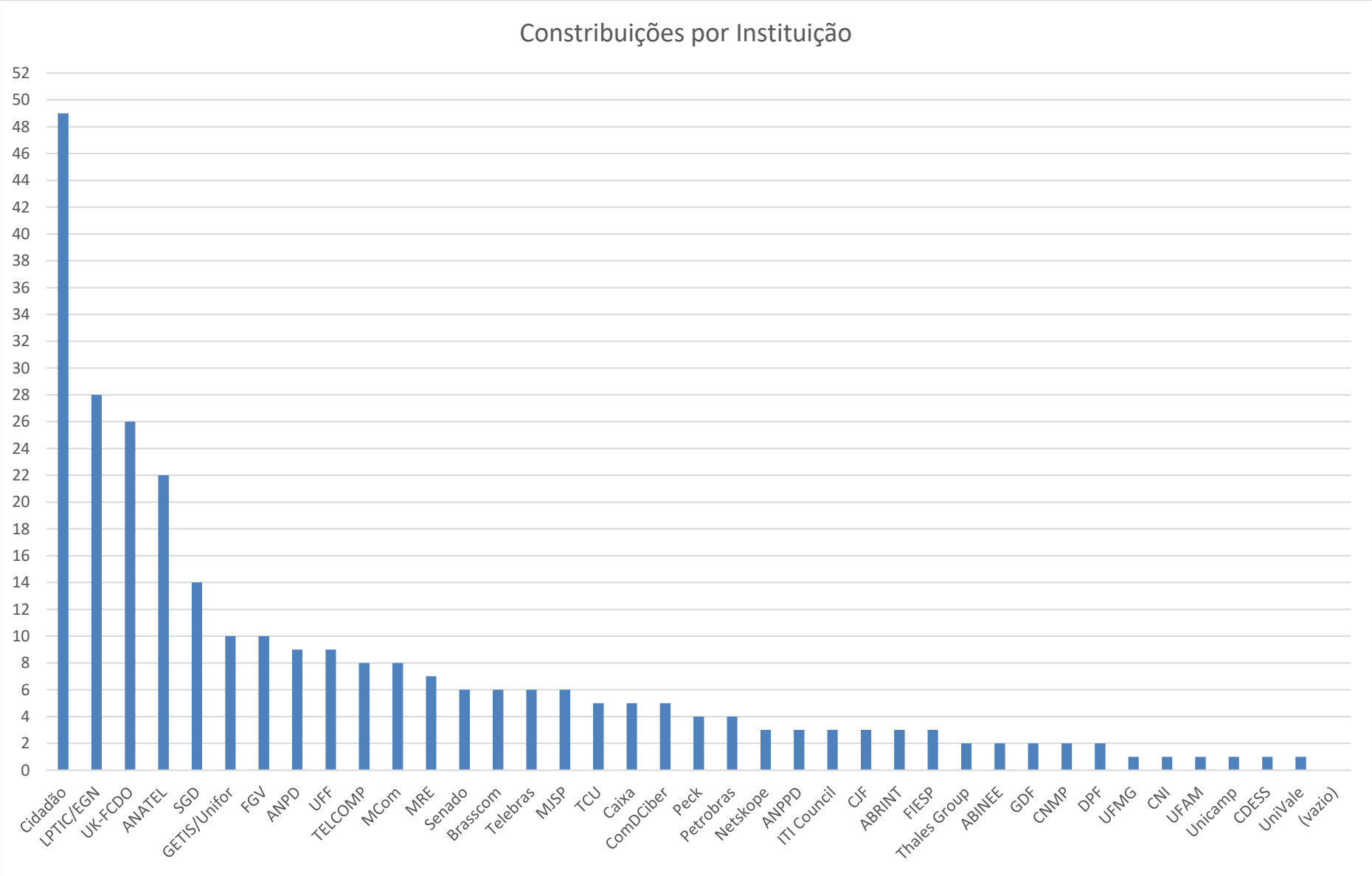
Parecer	Descrição
1-Adequada	A sugestão ou crítica apresentada foi considerada adequada, e incorporada ao texto
2-Parcialmente Adequada	A sugestão ou crítica apresentada foi considerada parcialmente adequada, implicando em uma alteração no texto diferente daquela proposta pelo autor
3-Inadequada	A sugestão ou crítica apresentada foi considerada inadequada, por ser de natureza infra legal, por contrariar uma premissa do projeto, ou o "espírito da lei" do projeto
4-Agradecimento	Parecer associado às manifestações de apoio explícitas ao projeto

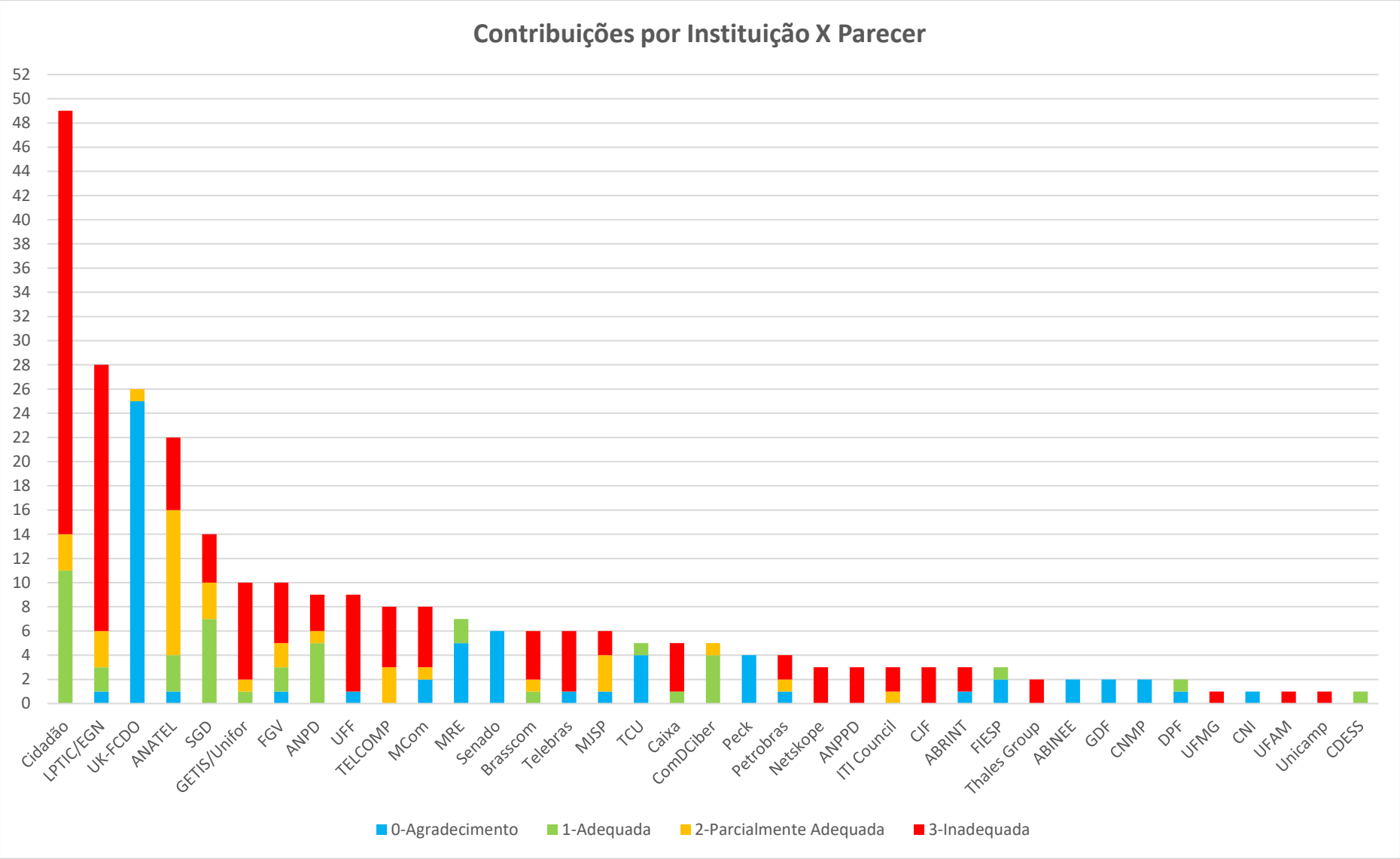
A distribuição das contribuições de acordo com essa categorização deu-se conforme ilustra o gráfico abaixo.



2.3.3 Da Categorização do "Instituição"

Estabeleceu-se uma "categoria de análise" para as instituições proponentes, que resultou no gráfico abaixo:


Constribuições por Instituição
52
50
48
46
44
42
40
38
36
34
32
30
28
26
24
22
20
18
16
14
12
10
8
6
4
2
0
Cidadão
LPTIC/EGN
UK-FCDO
ANATEL
SGD
GETIS/Unifor
FGV
ANPD
UFF
TELCOMP
MCom
MRE
Senado
Brasscom
Telebras
MJSP
TCU
Caixa
ComDCiber
Peck
Petrobras
Netskope
ANPPD
ITI Council
CJF
ABRINT
FIESP
Thales Group
ABINEE
GDF
CNMP
DPF
UFMG
CNI
UFAM
Unicamp
CDESS
UniVale
(vazio)

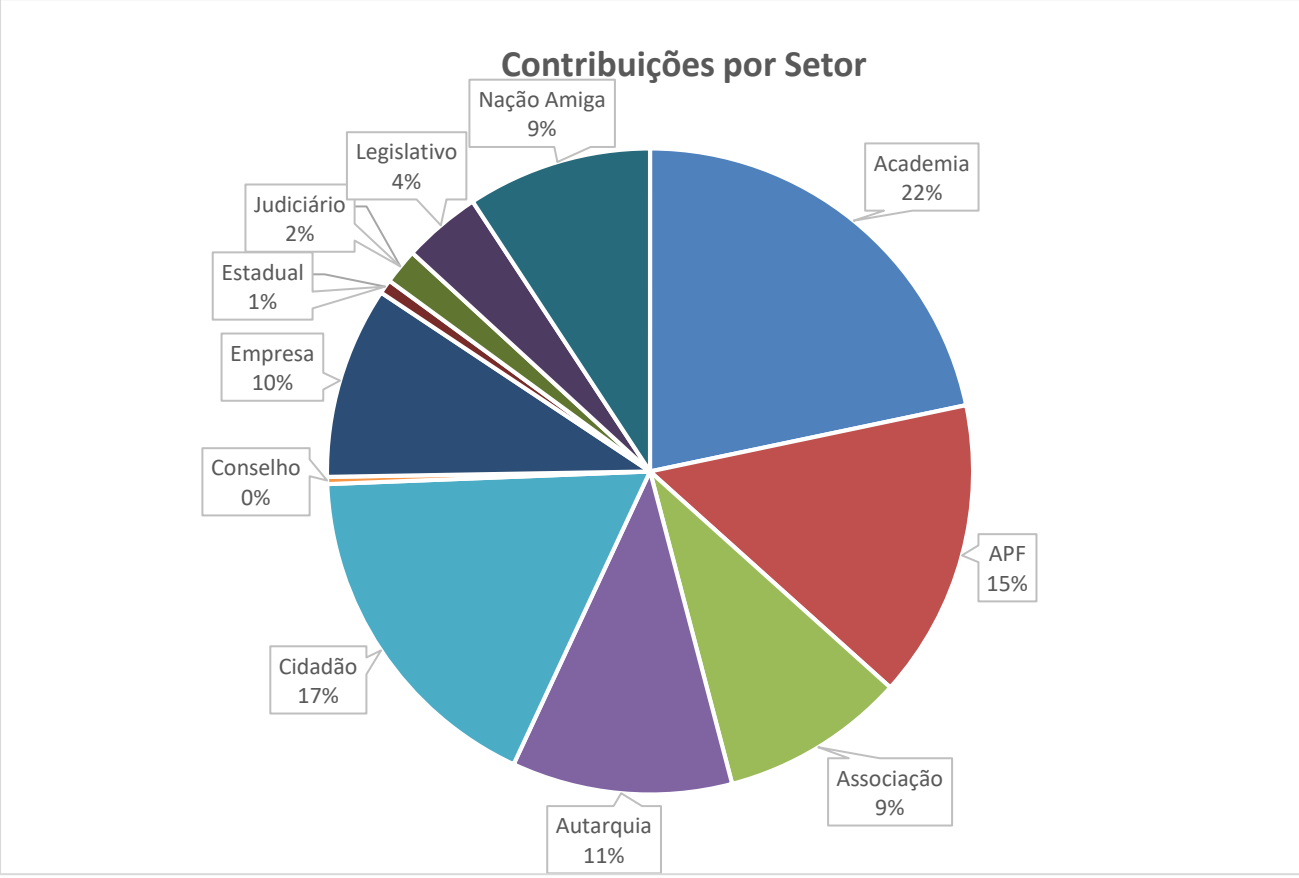

Contribuições por Instituição X Parecer
52
50
48
46
44
42
40
38
36
34
32
30
28
26
24
22
20
18
16
14
12
10
8
6
4
2
0
Cidadão
LPTIC/EGN
UK-FCDO
ANATEL
SGD
GETIS/Unifor
FGV
ANPD
UFF
TELCOMP
MCom
MRE
Senado
Brasscom
Telebras
MJSP
TCU
Caixa
ComDCiber
Peck
Petrobras
Netskope
ANPPD
ITI Council
CJF
ABRINT
FIESP
Thales Group
ABINEE
GDF
CNMP
DPF
UFMG
CNI
UFAM
Unicamp
CDESS
0-Agradecimento
1-Adequada
2-Parcialmente Adequada
3-Inadequada

2.3.4 Da Categorização do "Setor"

Optou-se por uma "categorização" das instituições por um dos "setores" conforme disposto na tabela abaixo:

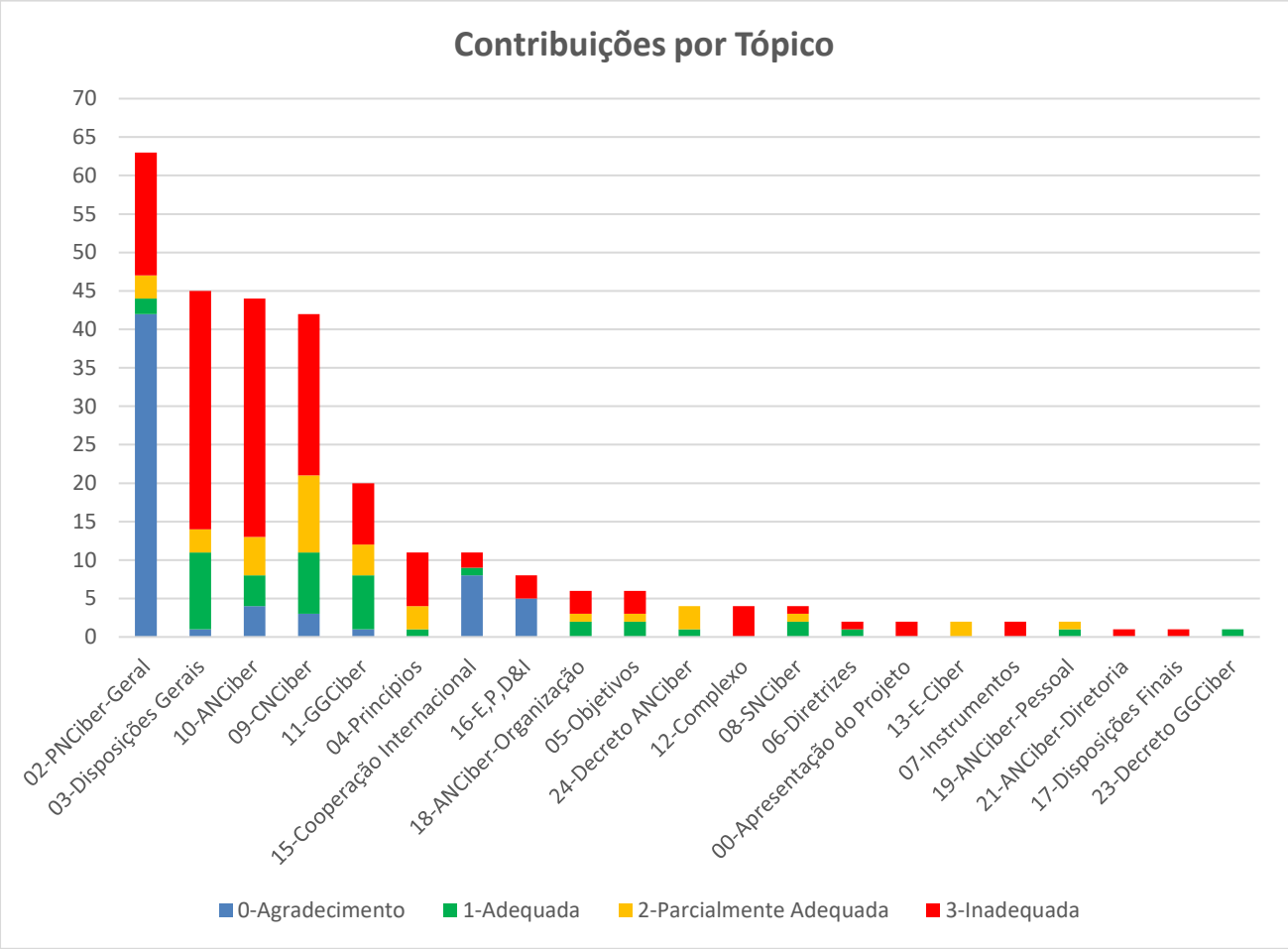
Setor	Descrição
Academia	Universidade ou Grupo de Pesquisa
APF	Administração Pública Federal direta
Associação	Associação de Empresas ou de Funcionários
Autarquia	Administração Pública Federal Indireta
Cidadão	Cidadão Individual
Conselho	Conselho Nacional de Desenvolvimento Econômico Social Sustentável
Empresa	Empresa Pública ou Privada
Estadual	Órgão Estadual
Judiciário	Órgão Relacionado ao Judiciário
Legislativo	Órgão Relacionado ao Legislativo

A distribuição das contribuições de acordo com essa categorização deu-se conforme ilustra o gráfico abaixo.



2.3.5 Da Categorização do "Tópico"

Optou-se por uma "categorização" dos tópicos (capítulos, seções e subseções) do anteprojeto, resultando na distribuição das contribuições conforme abaixo:



3 CONCLUSÕES

A Audiência Pública foi efetiva na obtenção de propostas que clarificaram ou aprimoraram diversos pontos do anteprojeto. Houve uma significativa participação de cidadãos interessados, da academia, do governo e de entidades representativas do empresariado nacional, além de nações amigas.

O grande quantitativo de manifestações expressas de apoio ao projeto, provenientes de todos os setores, somado às contribuições consideradas adequadas ou parcialmente adequadas superou o número de propostas consideradas inadequadas. Estas, por sua vez, em grande número, foram consideradas inadequadas por sugerirem detalhamentos pertinentes a documentos infra legais a serem implementados após a aprovação da PNCiber.

O significativo número de instituições sugeridas para integrarem o Comitê Nacional de Cibersegurança e o Gabinete de Gerenciamento de Cibercrises demonstrou também a elevada preocupação da sociedade com a temática, e seu interesse em contribuir para o aumento da cibersegurança e resiliência nacionais.

O Gabinete de Segurança Institucional da Presidência da República agradece a todos os que dedicaram seu tempo e intelecto em prol dessa urgente e relevante temática.

PNCiber – Relatório da Audiência Pública

ANEXO I

Audiência Pública da PNCiber – Contribuições

Responsável: Alexandro de Oliveira Paula			
Instituição: Telebras		**Título:** Servidor	
Tópico: 02-PNCiber-Geral	**Id#:** 7	**Parecer:** 0-Agradecimento	
Tipo de Contribuição: Apoio	**Artigo:**	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: De fato, uma Agência Reguladora para o assunto se faz necessário. Irá auxiliar na manutenção para controle mínimo de requisitos de segurança, tanto para o setor público quanto privado.			
Resposta: Agradecemos o apoio manifesto.			

Audiência Pública da PNCiber – Contribuições

Responsável: Breno de Castro Laranjo Vale			
Instituição: ABRINT		**Título:** Diretor de Projetos	
Tópico: 02-PNCiber-Geral	**Id#:** 24	**Parecer:** 0-Agradecimento	
Tipo de Contribuição: Apoio	**Artigo:**	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: A ABRINT apoia e reconhece a importância da Política Nacional de Cybersegurança e do Sistema Nacional de Cybersegurança. Do ponto de vista estrutural, a ABRINT concorda com a criação de uma agência reguladora na qualidade de entidade autárquica vinculada ao GSI, e recebe com satisfação seus padrões mínimos operacionais.			
Resposta: Agradecemos o apoio manifesto.			

Audiência Pública da PNCiber – Contribuições

Responsável: Carlos Renato Araújo Braga			
Instituição: TCU		**Título:** Diretor	
Tópico: 02-PNCiber-Geral	**Id#:** 39	**Parecer:** 0-Agradecimento	
Tipo de Contribuição: Apoio	**Artigo:**	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: Aproveitando a transmissão pela internet, esclarecer a sociedade brasileira a importância e o quanto esse tema afeta a todos e a cada um de nós, e oferecer um caminho que pode ajudar o governo a aperfeiçoar esse projeto de lei			
Resposta: Agradecemos o apoio manifesto.			

Audiência Pública da PNCiber – Contribuições

Responsável: Carlos Renato Araújo Braga			
Instituição: TCU		**Título:** Diretor	
Tópico: 02-PNCiber-Geral	**Id#:** 40	**Parecer:** 0-Agradecimento	
Tipo de Contribuição: Apoio	**Artigo:**	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: A lista de alto risco do TCU envolve temas ou problemas que abarcam o montante acima de 1 bilhão de reais. Somente um caso citado aqui pelo Doutor Marcelo [Malagutti] atingiu essa cifra ou afeta a vida de mais de um milhão de brasileiros. Como o Doutor Leonardo comentou, cerca de 150 milhões de brasileiros hoje já acessam serviços do Governo Federal, então com certeza esse é um problema que tem que estar na agenda do Estado Brasileiro.			
Resposta: Agradecemos o apoio manifesto.			

Audiência Pública da PNCiber – Contribuições

Responsável: Carlos Renato Araújo Braga			
Instituição: TCU		**Título:** Diretor	
Tópico: 02-PNCiber-Geral	**Id#:** 41	**Parecer:** 0-Agradecimento	
Tipo de Contribuição: Apoio	**Artigo:**	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: Nós vamos falar sobre o que? Sobre o fato de que proteção cibernética ocorre de maneira coletiva e não de maneira individual, e para isso nós temos que ter um articulador, e o articulador está sendo apresentado nesse projeto de lei que está em discussão hoje aqui.			
Resposta: Agradecemos o apoio manifesto.			

Audiência Pública da PNCiber – Contribuições

Responsável: Carlos Renato Araújo Braga			
Instituição: TCU		**Título:** Diretor	
Tópico: 02-PNCiber-Geral	**Id#:** 42	**Parecer:** 0-Agradecimento	
Tipo de Contribuição: Apoio	**Artigo:**	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: Algumas iniciativas do Poder Executivo Federal limitadas ao Poder Executivo Federal. Iniciativas do Poder Judiciário limitadas ao Poder Judiciário. Mas na fala anterior minha, eu disse que o problema é de todos nós. Nós temos que ter algo que pegue todos os setores, todos os órgãos públicos de todos os poderes, de todas as esferas, setor público, privado, pessoas jurídicas, e pessoas físicas. Então a gente precisa ter alguém para liderar esse processo no país inteiro, que, na proposta que está sendo colocada, seria aquele comitê e aquela agência, aquela autoridade que tá sendo proposta.			
Resposta: Agradecemos o apoio manifesto.			

Audiência Pública da PNCiber – Contribuições

Responsável: Esperidião Amin			
Instituição: Senado		**Título:** Senador	
Tópico: 02-PNCiber-Geral	**Id#:** 51	**Parecer:** 0-Agradecimento	
Tipo de Contribuição: Apoio	**Artigo:**	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: Quero dizer que fiz questão de aceder a esse convite e comparecer a esse ponto porque é muito oportuno e é importante que o governo tome a iniciativa de propor um projeto de lei sobre esta matéria. Por isso a minha presença significa pelo menos a certeza de que o parlamento brasileiro nos últimos anos tem despertado a sua atenção para o conjunto do assunto, do problema, do fator bem aportuguesado, cibersegurança.			
Resposta: Agradecemos o apoio manifesto.			

Audiência Pública da PNCiber – Contribuições

Responsável: Estela Aranha			
Instituição: MJSP		**Título:** Assessora	
Tópico: 02-PNCiber-Geral	**Id#:** 53	**Parecer:** 0-Agradecimento	
Tipo de Contribuição: Apoio	**Artigo:**	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: Obviamente não vou repetir aqui a relevância e a necessidade desse projeto. Isso é indiscutível. Isso, a necessidade de uma estratégia cybersegurança e a criação de órgãos e a criação do comitê, gerenciamento de crises, isso é indiscutível.			
Resposta: Agradecemos o apoio manifesto.			

Audiência Pública da PNCiber – Contribuições

Responsável: Franklin Silva Neto			
Instituição: MRE		**Título:** Conselheiro	
Tópico: 02-PNCiber-Geral	**Id#:** 59	**Parecer:** 0-Agradecimento	
Tipo de Contribuição: Apoio	**Artigo:**	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: Já foi mencionado aqui que o aumento da superfície de ataque a atividade maliciosas é em função da multiplicação dos dispositivos conectados, em função da necessidade cada vez maior de todos os aspectos da vida dependerem da internet, e isso também tem se traduzido, do ponto de vista da relação entre Estados, numa necessidade de trazer a questão da segurança cibernética para o centro das preocupações dos Estados.			
Resposta: Agradecemos o apoio manifesto.			

Audiência Pública da PNCiber – Contribuições

Responsável: Franklin Silva Neto			
Instituição: MRE		**Título:** Conselheiro	
Tópico: 02-PNCiber-Geral	**Id#:** 60	**Parecer:** 0-Agradecimento	
Tipo de Contribuição: Apoio	**Artigo:**	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: E eu pessoalmente fiquei muito feliz de ver que vai ter uma diretoria sendo criada na Agência, a Diretoria de Cibereducação. É, porque existe a percepção de que há um gap cada vez maior entre as atividades maliciosas e a capacidade de resposta, inclusive no nível cidadão.			
Resposta: Agradecemos o apoio manifesto.			

Audiência Pública da PNCiber – Contribuições

Responsável: Franklin Silva Neto			
Instituição: MRE		**Título:** Conselheiro	
Tópico: 02-PNCiber-Geral	**Id#:** 61	**Parecer:** 0-Agradecimento	
Tipo de Contribuição: Apoio	**Artigo:**	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: Nós no Ministério [das Relações Exteriores] também temos estados atentos e sempre ressaltamos a necessidade de cooperação internacional também no campo da educação cibernética, que nós vemos aí, que a criação da Agência poderá também estabelecer mecanismos de cooperação que permitam uma maior cibereducação no Brasil.			
Resposta: Agradecemos o apoio manifesto.			

Audiência Pública da PNCiber – Contribuições

Responsável: Giderclay Zebalos Bezerra			
Instituição: GDF		**Título:** Representante	
Tópico: 02-PNCiber-Geral	**Id#:** 67	**Parecer:** 0-Agradecimento	
Tipo de Contribuição: Apoio	**Artigo:**	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: Agradeço todo mundo que está aqui, fazendo essa união de esforços aí para uma coisa que a gente está bastante atrasado em relação ao mundo, e é uma ameaça real e constante aí.			
Resposta: Agradecemos o apoio manifesto.			

Audiência Pública da PNCiber – Contribuições

Responsável: Giderclay Zebalos Bezerra			
Instituição: GDF		**Título:** Representante	
Tópico: 02-PNCiber-Geral	**Id#:** 68	**Parecer:** 0-Agradecimento	
Tipo de Contribuição: Comentário	**Artigo:**	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: Precisamos aproveitar o potencial desses jovens que possuem expertise e visão única sobre o mundo virtual. A juventude pode trazer soluções inovadoras, identificar vulnerabilidades, e desenvolver medidas preventivas para proteger nossos sistemas e dados. Para isso, é fundamental criar oportunidades de aprendizado e colaboração, como feiras e hackatons, onde eles possam compartilhar conhecimentos e trabalhar em conjunto.			
Resposta: Certamente a ANCiber contará com a participação do GDF na discussão de suas resoluções sobre essa temática, seja por meio de convite à participação seja por interesse do GDF em participar das discussões públicas sobre o tema. Agradecemos o apoio manifesto.			

Audiência Pública da PNCiber – Contribuições

Responsável: Humberto Luiz Ribeiro			
Instituição: FIESP		**Título:** Professor	
Tópico: 02-PNCiber-Geral	**Id#:** 69	**Parecer:** 0-Agradecimento	
Tipo de Contribuição: Apoio	**Artigo:**	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: Aplaudimos, portanto, o propósito crítico e complexo, o propósito que vem em discussão.			
Resposta: Agradecemos o apoio manifesto.			

Audiência Pública da PNCiber – Contribuições

Responsável: Humberto Luiz Ribeiro			
Instituição: FIESP		**Título:** Professor	
Tópico: 02-PNCiber-Geral	**Id#:** 70	**Parecer:** 0-Agradecimento	
Tipo de Contribuição: Comentário	**Artigo:**	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: Nesse ponto, reforçar que, através, principalmente, do instrumento de inspeção que eu vi colocado na proposta, o tema prontidão começa a ser abordado pelo Governo Federal,			
Resposta: Agradecemos o apoio manifesto.			

Audiência Pública da PNCiber – Contribuições

Responsável: Jeferson Fued Nacif			
Instituição: MCom		**Título:** Servidor	
Tópico: 02-PNCiber-Geral	**Id#:** 100	**Parecer:** 0-Agradecimento	
Tipo de Contribuição: Apoio	**Artigo:**	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: Parabéns mais uma vez pela estrutura que foi desenhada para a política nacional, e pela ideia de construção da Agência Nacional de Segurança Cibernética, que também já era uma previsão que depois foi excluída da Estratégia de Segurança Cibernética.			
Resposta: Agradecemos o apoio manifesto.			

Audiência Pública da PNCiber – Contribuições

Responsável: Jefferson Gomes			
Instituição: CNI		**Título:** Professor	
Tópico: 02-PNCiber-Geral	**Id#:** 108	**Parecer:** 0-Agradecimento	
Tipo de Contribuição: Apoio	**Artigo:**	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: Eu gostaria de colocar na nossa proposição, fundamentalmente, a disponibilização do Sistema Indústria para quaisquer dos seus projetos, que sejam colocados para tentar avaliar todas as possibilidades de implementações que serão necessárias.			
Resposta: Agradecemos o apoio manifesto.			

Audiência Pública da PNCiber – Contribuições

Responsável: João Zanon			
Instituição: ANATEL		**Título:** Assessor	
Tópico: 02-PNCiber-Geral	**Id#:** 119	**Parecer:** 0-Agradecimento	
Tipo de Contribuição: Apoio	**Artigo:**	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: É importante o envolvimento de todos os entes de governo e uma coordenação de alto nível, com uma política de governo, um órgão dedicado para isso. Novamente, a gente parabeniza a iniciativa.			
Resposta: Agradecemos o apoio manifesto.			

Audiência Pública da PNCiber – Contribuições

Responsável: Kathryn Jones			
Instituição: UK-FCDO		**Título:** Chefe de Departamento	
Tópico: 02-PNCiber-Geral	**Id#:** 120	**Parecer:** 0-Agradecimento	
Tipo de Contribuição: Apoio	**Artigo:**	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: O Governo do Reino Unido congratula-se com a oportunidade de dar uma resposta à consulta do Brasil sobre a proposta de Política Nacional de Cibersegurança (PNCiber) e do Sistema Nacional de Segurança Cibernética (SNCiber). Em 2022, a Estratégia Nacional de Cibersegurança do Reino Unido (NCS do Reino Unido) reconheceu que os países que forem mais capazes de navegar pelas oportunidades e desafios da era digital serão mais seguros, mais resilientes e mais prósperos no futuro. Como parceiros, o Brasil e o Reino Unido podem navegar juntos por essas oportunidades e desafios para proteger e promover nossos interesses nacionais compartilhados e valores democráticos no e através do ciberespaço.			
Resposta: Nossa tradicional parceria com o Reino Unido, reforçada pelo Memorando de Entendimento firmado em 2022, estabelece uma sólida fundação para a fundamental troca de experiências nesse setor tão relevante. O GSI continuará a contar com o apoio do Governo de Sua Majestade, e se coloca ao dispor do mesmo para uma interação profícua para ambos os países.			

Audiência Pública da PNCiber – Contribuições

Responsável: Kathryn Jones			
Instituição: UK-FCDO		**Título:** Chefe de Departamento	
Tópico: 02-PNCiber-Geral	**Id#:** 121	**Parecer:** 0-Agradecimento	
Tipo de Contribuição: Apoio	**Artigo:**	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: Tivemos o prazer de constatar que o senhor considerou a Estratégia Nacional de Cibersegurança do Reino Unido como um modelo na "Exposição de Motivos" que precede o PNCiber. Também observamos suas reflexões sobre o Modelo de Maturidade Cibernética 2020 do Brasil, que foi implementado pela Universidade de Oxford e OEA com financiamento do Reino Unido. Estamos ansiosos para continuar a contribuir com a própria base de evidências do Brasil, apoiando a entrega de um Modelo de Maturidade Cibernética este ano, novamente implementado pelo Centro Global de Capacidade de Segurança Cibernética da Universidade de Oxford . Não tenho dúvidas de que trabalhar com a experiente equipe de Oxford à frente do PNCiber fornecerá insights adicionais em apoio às suas propostas.			
Resposta: A experiência acumulada pelo Reino Unido, bem como os ensinamentos colhidos na avaliação de maturidade foram de fundamental importância para a elaboração de nosso projeto, e ficamos muito gratos pelo apoio oferecido pelos senhores nessa nossa caminhada que agora se intensifica.			

Audiência Pública da PNCiber – Contribuições

Responsável: Kathryn Jones			
Instituição: UK-FCDO		**Título:** Chefe de Departamento	
Tópico: 02-PNCiber-Geral	**Id#:** 122	**Parecer:** 0-Agradecimento	
Tipo de Contribuição: Apoio	**Artigo:**	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: Considerando a PNCiber em sua totalidade, elogiamos o alto nível de ambição delineado em suas propostas. Com implementação e governança efetivas, essas reformas fornecerão uma base sólida para o Brasil aumentar sua capacidade de enfrentar os desafios de segurança cibernética. Algumas das semelhanças e diferenças entre as vossas propostas e a atual abordagem do Reino Unido são apresentadas em mais pormenor no anexo. As semelhanças incluem a criação de uma agência de segurança cibernética, a ênfase em mecanismos de governança inclusivos (reunindo setores público, privado e academia) e a garantia de que haja mecanismos para que os incidentes cibernéticos sejam considerados nos mais altos níveis de governo. Louvo também a ênfase nas cibercompetências e na educação – a lacuna de competências em cibersegurança é um desafio comum enfrentado por ambos os nossos países. Nos últimos dois anos, o Programa de Acesso Digital do Reino Unido tem apoiado as instituições de ensino do Brasil com ferramentas de formação de professores do ensino médio e desenvolvimento de um currículo de segurança online / segurança cibernética. Dada a proeminência da educação cibernética e tecnológica em suas propostas, gostaria de discutir os planos do Brasil no próximo Cyber & Digital Dialogue Brasil-Reino Unido, que esperamos que ocorra este ano.			
Resposta: Ficamos muito felizes em observar que o aprendizado de outras nações nos permitiu "atalhar" nosso caminho, aprendendo com os acertos e erros de outros, o que facilita nossa intenção de recuperar parte do atraso em que o Brasil se encontra nessa temática.			

Audiência Pública da PNCiber – Contribuições

Responsável: Kathryn Jones			
Instituição: UK-FCDO		**Título:** Chefe de Departamento	
Tópico: 02-PNCiber-Geral	**Id#:** 123	**Parecer:** 0-Agradecimento	
Tipo de Contribuição: Apoio	**Artigo:**	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: Reconhecemos e apoiamos o compromisso do PNCiber com estruturas de governança inclusivas que reúnam governo, setor privado, academia e órgãos reguladores.			
Resposta: Essa capacidade de coordenação nacional é o grande salto institucional que se busca com a PNCiber.			

Audiência Pública da PNCiber – Contribuições

Responsável: Kathryn Jones			
Instituição: UK-FCDO		**Título:** Chefe de Departamento	
Tópico: 02-PNCiber-Geral	**Id#:** 124	**Parecer:** 0-Agradecimento	
Tipo de Contribuição: Apoio	**Artigo:**	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: A proposta do Brasil também ressoa com a abordagem "Whole of Society" do Reino Unido para a cibernética. No âmbito da NCS do Reino Unido, os ministros são apoiados por grupos de governança de altos funcionários e por um National Cyber Advisory Board (NCAB), que é uma das formas de implementar uma abordagem de "toda a sociedade" através da governança da NCS.			
Resposta: Na PNCiber buscamos, de fato, explicitar esse modelo. No entanto, optamos por uma modelo mais abrangente, com um grande Comitê Nacional de Cibersegurança com a representação dos diversos setores da sociedade e uma maior abrangência de ministérios e outros setores envolvidos no Gabinete de Gestão de Cibercrises. Essa maior participação concede mais transparência e participação, ainda que possa trazer um custo na agilidade administrativa e deliberativa. Esse "trade off" deverá ser aprimorado com a experiência no funcionamento dessas instituições ao longo do tempo.			

Audiência Pública da PNCiber – Contribuições

Responsável: Kathryn Jones			
Instituição: UK-FCDO		**Título:** Chefe de Departamento	
Tópico: 02-PNCiber-Geral	**Id#:** 125	**Parecer:** 0-Agradecimento	
Tipo de Contribuição: Comentário	**Artigo:**	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: O Governo do Reino Unido incentiva as vítimas a reportarem incidentes de cibercrime através dos nossos mecanismos nacionais de comunicação de incidentes. No entanto, a comunicação não é atualmente obrigatória no Reino Unido. Atualmente, estimamos que apenas cerca de 2-10% dos crimes cibernéticos são relatados ao governo do Reino Unido, tornando-se um dos tipos de crime mais subnotificados no Reino Unido. Aumentar a denúncia de crimes cibernéticos é uma prioridade, pois nos permite construir uma melhor compreensão da ameaça e combatê-la de forma mais eficaz. Como resultado, o Reino Unido está atualmente planejando revisar seus requisitos de relatório de incidentes cibernéticos para os Regulamentos NIS 2018, de modo a exigir que os operadores informem sobre uma amplitude maior de incidentes, incluindo ransomware. Atualmente, o NIS do Reino Unido exige que as operadoras relatem incidentes que afetem a continuidade do serviço, e estamos avançando para requisitos de relatório que têm um impacto direto na segurança e resiliência dos operadores, e que afetam a continuidade do serviço ou têm o potencial de causar mais danos (como ataques de pré-posicionamento, espionagem, ransomware, etc.).			
Resposta: O incentivo à comunicação de ciberincidentes será uma tônica também da ANCiber. No entanto, alguns poderiam argumentar que o baixo percentual estimado de comunicação de cibercrimes no Reino Unido é um exemplo de que a abordagem estritamente de colaboração e construção de confiança não seja suficiente para elevar essa comunicação. Outrossim, uma abordagem que mescle a colaboração com o condão de impor sanções pode ser uma alternativa mais efetiva para a obtenção do resultado esperado.			

Audiência Pública da PNCiber – Contribuições

Responsável: Kathryn Jones			
Instituição: UK-FCDO		**Título:** Chefe de Departamento	
Tópico: 02-PNCiber-Geral	**Id#:** 126	**Parecer:** 0-Agradecimento	
Tipo de Contribuição: Comentário	**Artigo:**	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: Melhorar a resiliência da Infraestrutura Nacional Crítica do Reino Unido (CNI) é um compromisso fundamental da Estratégia Nacional de Cibersegurança do Reino Unido. O Governo tem 13 setores designados como críticos para o funcionamento diário do Reino Unido, e dentro destes sistemas específicos (incluindo ativos, redes, instalações e processos) são considerados CNI. Estes setores são: Química, Nuclear Civil, Comunicações (telecomunicações, radiodifusão, correios), Defesa, Serviços de Emergência (Polícia, Bombeiros e Salvamento, Ambulância, Guarda Costeira), Energia, Finanças, Alimentação, Governo, Saúde, Espaço, Transportes, Água. A definição oficial de CNI do governo do Reino Unido é: «Os elementos críticos das infraestruturas (a saber, ativos, instalações, sistemas, redes ou processos e os trabalhadores essenciais que os operam e facilitam), cuja perda ou comprometimento podem resultar em: Impacto prejudicial importante na disponibilidade, integridade ou prestação de serviços essenciais – incluindo os serviços cuja integridade, se comprometida, pode resultar em perdas significativas de vidas ou acidentes – tendo em conta impactos económicos ou sociais significativos; e/ou Impacto significativo na segurança nacional, na defesa nacional ou no funcionamento do Estado.» Não existe uma legislação única que cubra a ciberresiliência no Reino Unido. A maioria das CNI do Reino Unido é coberta por regulamentação baseada em setores individuais, com elementos de resiliência cibernética incluídos em requisitos de segurança mais amplos. A única exceção a isso são os regulamentos NIS. Os Regulamentos NIS entraram em vigor no Reino Unido em maio de 2018, como parte de um esforço a nível da UE para melhorar a resiliência cibernética dos serviços essenciais. Estabelecem requisitos legais para as organizações aumentarem o nível global de segurança (resiliência cibernética e física) das redes e dos sistemas de informação que são críticos para a prestação dos seus serviços. Abrangem organizações nos setores dos transportes, da energia, da água, da saúde, das infraestruturas digitais e dos serviços digitais (como a computação em nuvem). DSIT é o departamento do governo do Reino Unido responsável pelo NIS. O Governo do Reino Unido está atualmente a estudar formas de melhorar os regulamentos em matéria de SRI e realizamos uma consulta pública sobre este assunto no ano passado. O resultado desta consulta pode ser consultado aqui. Um elemento-chave destas propostas é a necessidade de incluir um novo subsetor na definição de serviços digitais - o dos "serviços geridos". Os serviços gerenciados, que o Reino Unido está definindo como a prestação de serviços de TI ou segurança em uma base on-line contínua, têm sido a fonte de uma série de ataques cibernéticos de alto perfil recentemente. É evidente que a sua utilização, ao mesmo tempo que traz muitos benefícios para as organizações, está também a criar novas ameaças e riscos. É intenção do Reino Unido melhorar a segurança global deste sector, integrando-os no âmbito destes regulamentos.			
Resposta: De forma similar, o Brasil historicamente trabalhou a cibersegurança com uma abordagem setorial, pautada no conceito d einfraestruturas críticas. No entanto, essa abordagem dá sinais de ter atingido seu limite de efetividade, sendo necessária uma visão mais integrada e coordenada nacionalmente. Similarmente ao que se observa no Reino Unido, inciamos a implementação de um modelo baseado em serviços essenciais como sugerido pelas normas NIS, modelo esse que sustenta a nossa			

abordagem do Complexo Nacional de Cibersegurança, o que nos permite ampliar a capacidade de atendimento de setores sem necessariamente incluí-los no contexto de infraestruturas críticas.

Audiência Pública da PNCiber – Contribuições

Responsável: Kathryn Jones			
Instituição: UK-FCDO		**Título:** Chefe de Departamento	
Tópico: 02-PNCiber-Geral	**Id#:** 127	**Parecer:** 0-Agradecimento	
Tipo de Contribuição: Comentário	**Artigo:**	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: Também vemos benefícios em uma estrutura baseada em resultados para avaliação de risco e gerenciamento de redes e sistemas de informação de entidades críticas que não depende de padrões fixos e inflexíveis, mudando assim o foco de "conformidade" para gerenciamento de risco "business as usual". O UK Cyber Assessment Framework provou ser eficaz nesse espaço e o Brasil pode querer considerar uma abordagem semelhante. Todas as organizações governamentais do Reino Unido adotaram o Cyber Assessment Framework como o principal padrão de segurança, que o governo do Reino Unido planeja garantir usando uma abordagem de garantia "GovAssure" uniforme e desenvolvida centralmente. Estamos trabalhando para entender novos riscos ou onde novas CNI estão surgindo como consequência da digitalização e das novas tecnologias, inclusive como parte de prioridades mais amplas, como a transição para o Net Zero.			
Resposta: A abordagem adotada na PNCiber, de um Complexo Nacional de Cibersegurança composto por ciberativos que dão sustentação a serviços essenciais, busca justamente atribuir fluidez e flexibiidade no tratamento da cibersegurança. De outra parte, o Tribunal de Contas da União tem uma proposta de arcabouços de conformidade para gerenciamento de ciber-riscos e de políticas públicas, e a Secretaria de Governo Digital tem outra. Assim, a ANCiber deverá optar por uma adaptação desses modelos.			

Audiência Pública da PNCiber – Contribuições

Responsável: Kathryn Jones			
Instituição: UK-FCDO		**Título:** Chefe de Departamento	
Tópico: 02-PNCiber-Geral	**Id#:** 128	**Parecer:** 0-Agradecimento	
Tipo de Contribuição: Comentário	**Artigo:**	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: Em janeiro de 2022, também publicamos a Estratégia de Segurança Cibernética do Governo, estabelecendo em detalhes pela primeira vez como construiremos um setor público resiliente à cibersegurança. O GCSS define como construiremos e manteremos nossas defesas cibernéticas; construindo maior resiliência cibernética em todas as organizações governamentais e trabalhando juntos para "defender como um só" - exercendo uma força defensiva maior do que a soma de nossas partes. Continuamos a fornecer uma ampla gama de suporte para aqueles que executam nossa CNI, incluindo aconselhamento e orientação técnica confiáveis, inteligência de ameaças atualizada e experiência líder mundial para resolver seus problemas de segurança cibernética mais difíceis. Além da consulta sobre os NEI, realizamos consultas públicas sobre novas políticas para promover a ciberresiliência, incluindo: acesso não autorizado a contas online e dados pessoais (Cyber Duty to Protect); resiliência e segurança de software; e melhor gerenciamento de riscos para nossa infraestrutura de armazenamento e processamento de dados essenciais.			
Resposta: A preocupação com a ciber-resiliência é um eixo central também da PNCiber, e nesse campo a troca de experiências entre o Brasil e o Reino Unido deve também ser uma prioridade nossa.			

Audiência Pública da PNCiber – Contribuições

Responsável: Luca Belli			
Instituição: FGV		**Título:** Professor	
Tópico: 02-PNCiber-Geral	**Id#:** 164	**Parecer:** 0-Agradecimento	
Tipo de Contribuição: Apoio	**Artigo:**	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: O Brasil conseguiu avançar enormemente nos últimos 3 anos por causa, justamente, da adoção de várias regulamentações setoriais. Eu acho que tá no 18º lugar no ranking das 20 economias, mas também, por coincidência, no ranking da UIT, do Cybersecurity Index da União Internacional de Comunicações. Ele subiu de 50 posições. Então, houve um avanço enorme nos últimos anos por causa dessa consciência da urgência. Porém, o que destacamos no nosso estudo é que essa abordagem é muito, muito setorial. Ou seja, regulamentação tomada pela ANATEL, pela ANAC, pela ANEEL. Essa é uma enorme vulnerabilidade do país, porque a cibersegurança não é enxergada como um conjunto sistêmico mas como setores. Para retomar aquela metáfora que foi utilizada antes, não adianta a sua casa ter portas de aço se as janelas estão abertas e ninguém sabe qual janela, qual porta tá aberta ou tá fechada, e ninguém sabe como coordenar. Essa é a função principal de uma agência. Eu parabenizo enormemente o GSI por essa proposta porque é essencial no país, e o país tem um atraso enorme. Não comparado simplesmente com a União Europeia. A ENISA na União Europeia foi criada em 2004, mas também com parceiros, por exemplo, de economias em desenvolvimento como a China. A CAC, a Cyberspace Administration of China, foi criada em 2014.			
Resposta: A coordenação das ações setoriais desenvolvidas no Brasil é um ponto fulcral do anteprojeto. Agradecemos o apoio manifesto.			

Audiência Pública da PNCiber – Contribuições

Responsável: Marcelo Câmara			
Instituição: MRE		**Título:** Diretor	
Tópico: 02-PNCiber-Geral	**Id#:** 178	**Parecer:** 0-Agradecimento	
Tipo de Contribuição: Apoio	**Artigo:**	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: Ganha urgência, portanto, a construção de uma governança interna de cibersegurança capaz de atender às diversas vertentes desse fenômeno, incluída a político-estratégica internacional, visando a assegurar um espaço cibernético aberto, seguro, estável, acessível e pacífico. Trata-se, a propósito, de tendência mundial, à qual convém ao Brasil estar atento.			
Resposta: Agradecemos o apoio manifesto.			

Audiência Pública da PNCiber – Contribuições

Responsável: Marcelo Câmara			
Instituição: MRE		**Título:** Diretor	
Tópico: 02-PNCiber-Geral	**Id#:** 179	**Parecer:** 0-Agradecimento	
Tipo de Contribuição: Apoio	**Artigo:**	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: Em vista do que precede, o MRE apoiará, no que couber, o projeto de Lei que cria a Política Nacional de Cibersegurança (PNCiber), no entendimento de que se trata de desenvolvimento necessário e urgente tanto no plano doméstico quanto no das Relações Exteriores.			
Resposta: Agradecemos o apoio manifesto.			

Audiência Pública da PNCiber – Contribuições

Responsável: Maxli Barroso Campos			
Instituição: LPTIC/EGN		**Título:** Pesquisador Líder	
Tópico: 02-PNCiber-Geral	**Id#:** 183	**Parecer:** 0-Agradecimento	
Tipo de Contribuição: Apoio	**Artigo:**	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: A LP TIC-Cibernética da Escola de Guerra Naval entende a necessidade da criação de um Sistema Nacional de Segurança Cibernética, tendo como Órgão Central - OC, o GSI. Entretanto, analisando a proposta de PNCiber em lide, concluímos que esta proposta está mais adequada, pois criando uma ANCiber subordinada ao GSI, o Sistema não perde sua importância e, ao mesmo tempo, desonera o GSI do trabalho de condução dessa tarefa. Em nosso ponto de vista toda a estrutura proposta é uma excelente ideia.			
Resposta: Agradecemos o apoio manifesto.			

Audiência Pública da PNCiber – Contribuições

Responsável: Neuri Luiz Mantovani			
Instituição: ABINEE		**Título:** Gerente	
Tópico: 02-PNCiber-Geral	**Id#:** 212	**Parecer:** 0-Agradecimento	
Tipo de Contribuição: Apoio	**Artigo:**	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: Gostaria de cumprimentar o GSI e a secretaria por essa importante iniciativa de criar, de estudar essa nova Política Nacional de Segurança Cibernética, que deverá ser então enviada para o Congresso Nacional.			
Resposta: Agradecemos o apoio manifesto.			

Audiência Pública da PNCiber – Contribuições

Responsável: Neuri Luiz Mantovani			
Instituição: ABINEE		**Título:** Gerente	
Tópico: 02-PNCiber-Geral	**Id#:** 213	**Parecer:** 0-Agradecimento	
Tipo de Contribuição: Apoio	**Artigo:**	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: A ABINEE e os seus associados têm uma larga experiência nos processos de averiguação, de conformidade, certificação de equipamentos, na aplicação de normas e padrões nacionais e internacionais, e referências de boas práticas do tema da segurança cibernética, onde certamente nós poderíamos contribuir de maneira relevante na discussão e decisão referente a essa Política Nacional de Segurança Cibernética.			
Resposta: Certamente a ANCiber contará com o apoio da ABINEE na definição de suas resoluções sobre essa temática, seja por meio de convite à participação seja por interesse da ABINEE em participar das discussões públicas sobre as AIRs. Agradecemos o apoio manifesto.			

Audiência Pública da PNCiber – Contribuições

Responsável: Patrícia Peck Pereira			
Instituição: Peck		**Título:** Advogada	
Tópico: 02-PNCiber-Geral	**Id#:** 235	**Parecer:** 0-Agradecimento	
Tipo de Contribuição: Apoio	**Artigo:**	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: Fico muito feliz de poder tratar dessa temática. É um tema extremamente importante, como foi dito. Estratégico, emergencial, e a gente está atrasado. O Brasil está muito atrasado com essa pauta. Eu acho que é importante dar o tom emergencial sobre isso.			
Resposta: Agradecemos o apoio manifesto.			

Audiência Pública da PNCiber – Contribuições

Responsável: Patrícia Peck Pereira			
Instituição: Peck		**Título:** Advogada	
Tópico: 02-PNCiber-Geral	**Id#:** 236	**Parecer:** 0-Agradecimento	
Tipo de Contribuição: Apoio	**Artigo:**	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: Realmente acredito que o melhor caminho é o que está sendo proposto pela política nacional, e é uma forma também de dar o indicativo não só para dentro do país mas para fora, dentro de um diálogo entre todos.			
Resposta: Agradecemos o apoio manifesto.			

Audiência Pública da PNCiber – Contribuições

Responsável: Patrícia Peck Pereira			
Instituição: Peck		**Título:** Advogada	
Tópico: 02-PNCiber-Geral	**Id#:** 237	**Parecer:** 0-Agradecimento	
Tipo de Contribuição: Apoio	**Artigo:**	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: Então, a gente tem que poder olhar todo esse plano maravilhoso que o Malagutti acabou de apresentar e dizer, vamos fazer acontecer? Por que tem a ANPD há 3 anos acontecendo, mas que não conseguiu cumprir tudo isso, então a gente não pode repetir a mesma coisa, e temos que fazer para todos. Então sim, é extremamente importante colaborar!			
Resposta: Agradecemos o apoio manifesto.			

Audiência Pública da PNCiber – Contribuições

Responsável: Paulo Barone			
Instituição: Senado		**Título:** Assessor	
Tópico: 02-PNCiber-Geral	**Id#:** 239	**Parecer:** 0-Agradecimento	
Tipo de Contribuição: Apoio	**Artigo:**	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: Para a questão Legislativa, é muito importante relacionar o aspecto que o Senador Izalci sempre menciona, que é: não basta discursar mas é preciso também acrescentar recursos a toda política pública. Não há estratégia que opere sem recursos alocados. Não adianta dialogar apenas. Todo mundo concorda.			
Resposta: Agradecemos o apoio manifesto.			

Audiência Pública da PNCiber – Contribuições

Responsável: Paulo Barone			
Instituição: Senado		**Título:** Assessor	
Tópico: 02-PNCiber-Geral	**Id#:** 240	**Parecer:** 0-Agradecimento	
Tipo de Contribuição: Apoio	**Artigo:**	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: Eu posso já me colocar à disposição para, a partir do momento em que essa proposta estiver tramitando no Congresso Nacional, a funcionar como interlocutor, como um polo de contato entre todos os cidadãos, todas as organizações da sociedade que têm interesse na questão, para aprimorar, para alongar a discussão, para ouvir outras posições, se for o caso, porque um dos mecanismos importantes no Congresso Nacional é a audiência pública. E também para fazer chegar aos interlocutores proponentes do Governo Federal aquelas sugestões que eventualmente requeiram maior negociação, porque eventualmente isso pode acontecer até no âmbito da criação de uma nova estrutura organizacional, como é o caso dessa agência reguladora.			
Resposta: Agradecemos o apoio manifesto.			

Audiência Pública da PNCiber – Contribuições

Responsável: Rogério Carvalho			
Instituição: Senado		**Título:** Senador	
Tópico: 02-PNCiber-Geral	**Id#:** 257	**Parecer:** 0-Agradecimento	
Tipo de Contribuição: Apoio	**Artigo:**	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: Eu não vou entrar no mérito do que a gente tem para fazer, mas o governo aponta a necessidade de conversar com a sociedade, abrir a importância deste tema numa audiência pública para dizer para todo mundo, nós todos, a sociedade inteira deve estar atenta à necessidade de termos uma regulamentação, e investimento, e acompanhar tudo que importa para nós.			
Resposta: Agradecemos o apoio manifesto.			

Audiência Pública da PNCiber – Contribuições

Responsável: Rogério Carvalho			
Instituição: Senado		**Título:** Senador	
Tópico: 02-PNCiber-Geral	**Id#:** 258	**Parecer:** 0-Agradecimento	
Tipo de Contribuição: Apoio	**Artigo:**	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: Eu quero dizer para vocês que o nosso mandato está à disposição, e acho que quanto mais discussões nós fizermos e quanto mais pessoas passarem a defender a necessidade dessa regulamentação geral, dessa lei, ou desse marco, ou desse, seja lá o nome que dê a essa formulação de um regramento, de uma agência, de uma estrutura para poder gerenciar. Quanto mais a gente envolver as pessoas nisso, mais preciso será e mais eficiente será; nós teremos, mais eficácia na intenção de nos protegermos e de proteger a sociedade. Então, muito obrigado. Parabéns pela iniciativa, e vamos trabalhar porque a gente já tá atrasado.			
Resposta: Agradecemos o apoio manifesto.			

Audiência Pública da PNCiber – Contribuições

Responsável: Valdemar Latance Neto			
Instituição: DPF		**Título:** Delegado	
Tópico: 02-PNCiber-Geral	**Id#:** 265	**Parecer:** 0-Agradecimento	
Tipo de Contribuição: Apoio	**Artigo:**	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: As finalidades principais do projeto são, resumidamente, unificar a colcha de retalhos regulatória do Brasil, diminuir o débito tecnológico nacional, e ampliar a participação brasileira na cooperação internacional sobre a temática. É impossível discordar dessas finalidades.			
Resposta: Agradecemos o apoio manifesto.			

Audiência Pública da PNCiber – Contribuições

Responsável: Vanessa Fusco			
Instituição: CNMP		**Título:** Promotora de Justiça	
Tópico: 02-PNCiber-Geral	**Id#:** 277	**Parecer:** 0-Agradecimento	
Tipo de Contribuição: Apoio	**Artigo:**	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: Como setor público e como órgão indispensável ao funcionamento da Justiça, que nós também possamos fazer a nossa parte, integremos esse sistema e essa luta, contra o cibercriminosos e para uma eficaz política de cibersegurança que tire o nosso Brasil na área da cibersegurança, desse atraso na estratégia. É, para os senhores terem uma ideia, se os senhores virem aí no Observatório da Cibersegurança das Américas, da OEA, Trinidad Tobago, desde 2013, tem uma estratégia de segurança, e nós só em 2020 que conseguimos construir a duras penas a nossa. E espero agora, não mais por decreto, mas sim por uma participação ampla que começa hoje, aqui nessa audiência pública.			
Resposta: Agradecemos o apoio manifesto.			

Audiência Pública da PNCiber – Contribuições

Responsável: Jeferson Fued Nacif			
Instituição: MCom		**Título:** Servidor	
Tópico: 03-Disposições Gerais	**Id#:** 101	**Parecer:** 0-Agradecimento	
Tipo de Contribuição: Apoio	**Artigo:**	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: Primeiro parabenizo pela iniciativa, Malagutti. É excelente podermos estar aqui discutindo abertamente esse tema tão importante, e por algumas inovações, inclusive esse glossário, que realmente vai trazer luz sobre assuntos e dúvidas que pairavam no tempo em que eu estava aqui [no GSI] em 2019.			
Resposta: Agradecemos o apoio manifesto.			

Audiência Pública da PNCiber – Contribuições

Responsável: Kathryn Jones			
Instituição: UK-FCDO		**Título:** Chefe de Departamento	
Tópico: 09-CNCiber	**Id#:** 129	**Parecer:** 0-Agradecimento	
Tipo de Contribuição: Comentário	**Artigo:**	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: O National Cyber Advisory Board (NCAB) está procurando desenvolver vínculos com contrapartes internacionais no devido tempo, incluindo compromissos conjuntos e compartilhamento de melhores práticas para a colaboração governo-indústria. Todos os ministros desempenham um papel na garantia de que o Reino Unido consolida a sua posição como uma ciberpotência responsável e democrática, capaz de proteger e promover os seus interesses no, e através do, ciberespaço. No entanto, existem certas responsabilidades atribuídas a determinados ministros e áreas do Governo do Reino Unido. Na prática, isto é gerido através da atribuição de «líderes de pilares» em todo o Governo, que asseguram a gestão de cada um dos cinco pilares delineados na Estratégia. Da mesma forma, embora o presidente seja claramente responsável por muitas das novas estruturas do PNCiber, o Brasil pode querer considerar como a responsabilidade política flui para o nível político em diferentes níveis.			
Resposta: No caso brasileiro, o Comitê Nacional de Cibersegurança (CNCiber) será o equivalente, guardadas as diferenças, ao NCAB britânico, com uma notável diferença no tocante ao número de ministérios e outras instituições representadas. Imagina-se que as "comissões" que podem ser criadas no CNCiber venham a ser utilizadas como grupos focais dos "pilares" temáticos da PNCiber.			

Audiência Pública da PNCiber – Contribuições

Responsável: Rodrigo Andrade Pereira Rosa			
Instituição: Petrobras		**Título:** Gerente	
Tópico: 09-CNCiber	**Id#:** 251	**Parecer:** 0-Agradecimento	
Tipo de Contribuição: Apoio	**Artigo:**	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: Venho colocar aqui a gente como, além de manifestar o interesse institucional da companhia, em participar inclusive aí numa das cadeiras como infraestrutura crítica.			
Resposta: A Petrobras certamente terá a oportunidade de participar do CNCiber na qualidade de entidade integrante do Compexo Nacional de Cibersegurança, cujo número de representantes previsto foi muito ampliado. Agradecemos o apoio manifesto.			

Audiência Pública da PNCiber – Contribuições

Responsável: Vanessa Fusco			
Instituição: CNMP		**Título:** Promotora de Justiça	
Tópico: 09-CNCiber	**Id#:** 278	**Parecer:** 0-Agradecimento	
Tipo de Contribuição: Apoio	**Artigo:**	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: O que eu gostaria de trazer como contribuição, primeiro é agradecer, por que nós fomos também contemplados em estar participando do comitê e também da Gestão de Cibercrises.			
Resposta: Agradecemos o apoio manifesto.			

Audiência Pública da PNCiber – Contribuições

Responsável: Patrícia Peck Pereira			
Instituição: Peck		**Título:** Advogada	
Tópico: 10-ANCiber	**Id#:** 238	**Parecer:** 0-Agradecimento	
Tipo de Contribuição: Apoio	**Artigo:** 18	**Inciso:** 0	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: É muito positivo ter um interlocutor único. É muito positivo em efeito internacional, tem um efeito de atrair mais investidores, um efeito de também subir no ranking da UIT.			
Resposta: Agradecemos o apoio manifesto.			

Audiência Pública da PNCiber – Contribuições

Responsável: Esperidião Amin			
Instituição: Senado		**Título:** Senador	
Tópico: 10-ANCiber	**Id#:** 52	**Parecer:** 0-Agradecimento	
Tipo de Contribuição: Apoio	**Artigo:**	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: Como se trata de um projeto que deve implicar na criação de uma agência própria, e eu pessoalmente concordo com isso, acho que é o nosso modelo, acho que é o mecanismo que o Brasil está utilizando para cuidar de políticas públicas realmente de Estado.			
Resposta: Agradecemos o apoio manifesto.			

Audiência Pública da PNCiber – Contribuições

Responsável: Kathryn Jones			
Instituição: UK-FCDO		**Título:** Chefe de Departamento	
Tópico: 10-ANCiber	**Id#:** 130	**Parecer:** 0-Agradecimento	
Tipo de Contribuição: Comentário	**Artigo:**	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: A criação do NCSC do Reino Unido em 2016 foi a conquista mais importante sob nossa Estratégia Nacional de Segurança Cibernética anterior 2016-2021. O Centro Nacional de Segurança Cibernética faz parte da GCHQ, a agência de inteligência de sinais do Reino Unido. O CEO da NCSC é um funcionário público de nível de Diretor Geral. O Ministro responsável pelo GCHQ e, portanto, pelo NCSC, é o Ministro dos Negócios Estrangeiros. Para o governo do Reino Unido, é importante que o NCSC seja a face pública autorizada da segurança cibernética, ao mesmo tempo em que tenha acesso à nossa inteligência mais sensível como um membro valioso da comunidade de inteligência. Alcançar esse equilíbrio com sucesso e criar a cultura e o equilíbrio de habilidades certos na organização é um dos maiores desafios. Para nós, é vital acertar esse equilíbrio.			
Resposta: A cultura institucional brasileira é muito distinta da britânica no tocante à inteligência, não sendo viável que uma agência como a ANCiber possa estar hierárquica e umbilicalmente ligada ao setor de inteligência de estado. Não obstante, espera-se que a ANCiber venha a integrar o Sistema Brasileiro de Inteligência, SISBIN, de forma a poder dispor da conhecimento de inteligência que a apoie em sua missão de melhorar a cibersegurança nacional.			

Audiência Pública da PNCiber – Contribuições

Responsável: Kathryn Jones			
Instituição: UK-FCDO		**Título:** Chefe de Departamento	
Tópico: 10-ANCiber	**Id#:** 131	**Parecer:** 0-Agradecimento	
Tipo de Contribuição: Apoio	**Artigo:**	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: O NCSC fornece a função técnica de gerenciamento de incidentes para incidentes cibernéticos nacionais graves, trabalhando em estreita colaboração com empresas de resposta a incidentes do setor (NCSC é o nosso CERT nacional). O NCSC tradicionalmente só gerencia incidentes cibernéticos de importância nacional, normalmente compreendendo cerca de 600-800 por ano (apenas uma pequena fração desses incidentes resulta em ativação do COBR).			
Resposta: O Brasil, historicamente, tem o CERT.Br como seu CERT nacional, e o CTIR Gov como um "CERT" para órgãos do governo federal. A PNCiber estabelece a criação de um outro "CERT" nacional, o CTIR.Br, que assumirá as funções de centralizador da REGIC, antes uma responsabilidade do CTIR Gov. Além dos órgãos governamentias, o novo CTIR.Br vai centralizar e coordenar as instituições que tenham seus ciberativos incluídos no Complexo Nacional de Cibersegurança. As entidades sem ativos no Complexo continuarão a poder trabalhar com tanto com seu tradicional parceiro, o CERT.Br, quanto com o CTIR.Br. Já o CTIR Gov passará a atuar como ETIR setorial da Presidência da República, subordinando-se ao CTIR.Br. Dessa forma, o Brasil manterá sua estrutura com dois CERT´s nacionais. O CTIR.Br, para os integrantes do Complexo e voluntários, sendo o CERT.Br outra opção, no espírito colaborativo proposto para a ANCiber.			

Audiência Pública da PNCiber – Contribuições

Responsável: Kathryn Jones			
Instituição: UK-FCDO		**Título:** Chefe de Departamento	
Tópico: 11-GGCiber	**Id#:** 132	**Parecer:** 0-Agradecimento	
Tipo de Contribuição: Apoio	**Artigo:**	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: Reconhecemos a importância de uma ampla coordenação e liderança política para os incidentes cibernéticos mais graves. Cabinet Office Briefing Room (COBR) é a abreviação do mecanismo através do qual a resposta do governo central do Reino Unido é ativada, monitorada e coordenada. O comparecimento ao COBR é determinado pela natureza da emergência, reunindo Ministros e Altos Funcionários de departamentos e agências relevantes. No sistema do Reino Unido, o COBR é ativado apenas para os incidentes cibernéticos mais graves e complexos que exigem uma resposta intergovernamental.			
Resposta: A PNCiber estabelece um "equivalente" ao COBR britânico, materializado por meio do Gabinete de Gerenciamento de Cibercrises (GGCiber). Ainda que no caso brasileiro o tamanho e a participação de diferentes segmentos do governo seja mais ampla, a finalidade e a mecânica de acionamento e escalada a instâncias mais elevadas do governo está presente nos dois modelos.			

Audiência Pública da PNCiber – Contribuições

Responsável: Kathryn Jones			
Instituição: UK-FCDO		**Título:** Chefe de Departamento	
Tópico: 15-Cooperação Internacional	**Id#:** 133	**Parecer:** 0-Agradecimento	
Tipo de Contribuição: Apoio	**Artigo:**	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: Na área da cooperação internacional, apoiamos a ênfase na cooperação em questões de segurança cibernética no PNCiber. Dada a liderança regional do Brasil na América Latina, apoiamos o Brasil a adotar uma postura mais proativa na capacitação internacional na região. Da mesma forma, esperamos que o Brasil continue a se envolver positivamente com a Counter Ransomware Initiative. O ransomware – e combater a ameaça do crime cibernético como um todo – continua sendo uma prioridade para o Reino Unido. Gostaríamos de dar mais ênfase ao combate ao crime cibernético nos planos do Brasil, dado o seu impacto.			
Resposta: Estaremos sempre dispostos e gratos por poder aprender mais com nações que, como o Reino Unido, têm a nos ensinar sobre cibersegurança, sempre respeitando as diferenças legais e culturais, e também a similaridade de valores e esperança num futuro mais pacífico, produtivo e cooperativo no ciberespaço.			

Audiência Pública da PNCiber – Contribuições

Responsável: Kathryn Jones			
Instituição: UK-FCDO		**Título:** Chefe de Departamento	
Tópico: 15-Cooperação Internacional	**Id#:** 134	**Parecer:** 0-Agradecimento	
Tipo de Contribuição: Apoio	**Artigo:**	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: Congratulamo-nos com a ênfase dada à cooperação internacional no PNCiber. A Estratégia Nacional de Cibersegurança do Reino Unido reconhece que a cooperação internacional é vital para alcançar todos os objetivos da estratégia cibernética do Reino Unido, além de ser fundamental para a segurança e prosperidade coletivas do sistema internacional. Embora a nível nacional o Reino Unido procure sempre alcançar uma vantagem estratégica, aumentaremos sempre as nossas hipóteses de sucesso, trabalhando em conjunto e garantindo que o ciberespaço continue a ser um lugar livre, aberto, pacífico e seguro para todos.			
Resposta: Esse é um ponto de concordância mútua histórica entre o Brasil e o Reino Unido.			

Audiência Pública da PNCiber – Contribuições

Responsável: Kathryn Jones			
Instituição: UK-FCDO		**Título:** Chefe de Departamento	
Tópico: 15-Cooperação Internacional	**Id#:** 135	**Parecer:** 0-Agradecimento	
Tipo de Contribuição: Comentário	**Artigo:**	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: O Reino Unido se esforça para mostrar liderança internacional, demonstrando e compartilhando o trabalho de política cibernética e digital com outros países e apoiando o desenvolvimento de capacidades por meio de instituições multilaterais importantes, como a Organização para a Cooperação e Desenvolvimento Econômico (OCDE) e a União Internacional de Telecomunicações (UIT). Estamos satisfeitos que a Anatel e a DSIT do Reino Unido tenham um diálogo regular sobre questões de segurança cibernética no contexto da UIT. Por meio do G20, estamos moldando um papel positivo para os membros do G20 em torno da segurança digital para desbloquear o crescimento e a inovação na economia.			
Resposta: O Brasil espera poder, em breve, ampliar sua liderança regional e global nessa área, e é motivo de orgulho o reconhecimento do excelente trabalho da ANATEL na UIT. Esperamos que o trabalho coordenado pela ANCiber possa refletir em um reconhecimento do potencial do Brasil também nos demais fóruns internacionais.			

Audiência Pública da PNCiber – Contribuições

Responsável: Kathryn Jones			
Instituição: UK-FCDO		**Título:** Chefe de Departamento	
Tópico: 15-Cooperação Internacional	**Id#:** 136	**Parecer:** 0-Agradecimento	
Tipo de Contribuição: Comentário	**Artigo:**	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: Definimos a prioridade da ação do Reino Unido para enfrentar a ameaça da ciberproliferação comercial, bem como planos iniciais para novas ações em que o Reino Unido possa desempenhar um papel de liderança. Também atualizamos e republicamos o Kit de Ferramentas de Dissuasão do Reino Unido, para definir nossa abordagem e servir como ferramenta nas discussões com parceiros internacionais. Como parte de um trabalho mais amplo para combater o crime cibernético, o Reino Unido, com Cingapura, está liderando o pilar político da Iniciativa Internacional de Combate ao Ransomware (CRI). Saudamos a participação do Brasil nessa iniciativa.			
Resposta: O Brasil, como mostrado na audiência pública e amplamente noticiado, é uma grande vítima global de ramsonware, e o país que mais paga resgates por esse tipo de crime no mundo. Outrossim, o GSI considera de extrema importância a participação do Brasil no CRI.			

Audiência Pública da PNCiber – Contribuições

Responsável: Kathryn Jones			
Instituição: UK-FCDO		**Título:** Chefe de Departamento	
Tópico: 15-Cooperação Internacional	**Id#:** 137	**Parecer:** 0-Agradecimento	
Tipo de Contribuição: Comentário	**Artigo:**	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: O diálogo internacional sobre as regras que regem o ciberespaço continua a evoluir e é uma prioridade para o Reino Unido. A Assembleia Geral da ONU de 2022 acolheu uma resolução que propõe um Programa de Ação Cibernético. O Reino Unido continua empenhado em manter a paz e a segurança internacionais através do desenvolvimento e implementação do Quadro das Nações Unidas para o comportamento responsável do Estado no ciberespaço.			
Resposta: O Brasil, em anos recentes, tem estado ativo nos fóruns globais de cibersegurança, e tem no Reino Unido um grande parceiro na busca pela paz e segurança internacionais, também na temática da cibersegurança.			

Audiência Pública da PNCiber – Contribuições

Responsável: Kathryn Jones			
Instituição: UK-FCDO		**Título:** Chefe de Departamento	
Tópico: 15-Cooperação Internacional	**Id#:** 138	**Parecer:** 0-Agradecimento	
Tipo de Contribuição: Comentário	**Artigo:**	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: A natureza internacional do cibercrime torna essencial a cooperação para combater as ameaças do ciberespaço. O Reino Unido observa que o Brasil ratificou a Convenção de Budapeste e, portanto, tem as infrações penais domésticas apropriadas, poderes de aplicação da lei e a capacidade de fornecer assistência de emergência e assistência jurídica mútua para ajudar nas investigações. Saudamos a adesão do Brasil e seu engajamento contínuo com os trabalhos da Convenção. O Reino Unido também observa que o Brasil é uma voz significativa nas discussões sobre o tratado da ONU sobre crimes cibernéticos e demonstrou apoio ao texto do projeto zero. Continuaremos a trabalhar em colaboração com o Brasil nesta área.			
Resposta: O Brasil agradece o apreço demonstrado pelo Reino Unido, o que nos anima a continuar em nosso esforço para colaborar internacionalmente pela paz e segurança internacionais no ciberespaço, e em particular no combate ao cibercrime transnacional.			

Audiência Pública da PNCiber – Contribuições

Responsável: Kathryn Jones			
Instituição: UK-FCDO		**Título:** Chefe de Departamento	
Tópico: 15-Cooperação Internacional	**Id#:** 139	**Parecer:** 0-Agradecimento	
Tipo de Contribuição: Apoio	**Artigo:**	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: O Reino Unido incentiva o Brasil a integrar sua abordagem ao crime cibernético tanto em sua estratégia cibernética nacional quanto em sua abordagem para o desenvolvimento de estratégias. A cibercriminalidade constitui uma parte substancial do Pilar 5 da Estratégia Nacional de Cibersegurança do Reino Unido sobre a luta contra as ameaças e, em particular, a exigência de uma resposta policial liderada por várias agências. O compartilhamento de informações sobre atividades criminosas, ameaças e vulnerabilidades entre agências é fundamental para enfrentar ameaças criminosas.			
Resposta: O combate ao cibercrime é um dos princípios fundamentais da PNCiber.			

Audiência Pública da PNCiber – Contribuições

Responsável: Kathryn Jones			
Instituição: UK-FCDO		**Título:** Chefe de Departamento	
Tópico: 15-Cooperação Internacional	**Id#:** 140	**Parecer:** 0-Agradecimento	
Tipo de Contribuição: Apoio	**Artigo:**	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: O Reino Unido também endossa a adesão do Brasil à Counter Ransomware Initiative. Este é um fórum internacional crescente para lidar com as principais questões de política de ransomware, compartilhar inteligência e projetar oportunidades de capacitação. Recomendamos que o Brasil capture isso em seus planos como um veículo para enfrentar essa ameaça de primeira linha.			
Resposta: Como já dissemos, o Brasil é uma grande vítima global de ransomware, e o GSI apoia firmemente a participação de nosso país na CRI.			

Audiência Pública da PNCiber – Contribuições

Responsável: Igor Monteiro Moraes			
Instituição: UFF		**Título:** Pesquisador	
Tópico: 16-E,P,D&I	**Id#:** 75	**Parecer:** 0-Agradecimento	
Tipo de Contribuição: Apoio	**Artigo:**	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: Primeiro eu queria parabenizar Marcelo [Malagutti] e ao GSI porque a gente ficou muito feliz de, ao ler o projeto, ter várias menções à academia, ao ensino, à pesquisa, e ao desenvolvimento, e por muitas vezes a gente é relegado, deixado de lado.			
Resposta: Agradecemos o apoio manifesto.			

Audiência Pública da PNCiber – Contribuições

Responsável: Kathryn Jones			
Instituição: UK-FCDO		**Título:** Chefe de Departamento	
Tópico: 16-E,P,D&I	**Id#:** 141	**Parecer:** 0-Agradecimento	
Tipo de Contribuição: Apoio	**Artigo:**	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: Apoiamos o foco do Brasil no desenvolvimento da cultura de segurança cibernética correta por meio de intervenções práticas. Por exemplo, descobrimos que o acesso a um ensino de alta qualidade - e materiais didáticos - é fundamental para a realização de intervenções em nível escolar. O Reino Unido oferece uma série de intervenções extracurriculares (o programa CyberFirst) em colaboração com mais de 200 empregadores da indústria, para inspirar mais jovens a selecionar Ciência da Computação como disciplina na escola (ciência da computação não é atualmente uma disciplina escolar obrigatória no Reino Unido). Esta atividade inclui cursos de verão fora do período letivo, competições nacionais e bolsas de graduação universitárias . O Reino Unido também oferece um programa ('CyberFirst: How to stay secure online') para jovens de 11 a 14 anos para aumentar sua conscientização sobre golpes e outras atividades maliciosas. Isso fica ao lado do currículo principal, mas não é obrigatório dentro dele. Outros programas que se relacionam com a estratégia do Brasil incluem o Cyber Explorers, que fornece materiais didáticos inovadores e envolventes para envolver os alunos na cibersegurança; e NCSC for Startups, que oferece financiamento e apoio ao empreendedorismo cibernético.			
Resposta: Temos a cibereducação como um dos pilares da cibersegurança, razão pela qual dedicamos boa parte de nossa proposta a essa temática, bem como à pesquisa, desenvolvimento e inovação, e certamente contaremos com a experiência e excelência do Reino Unido nessa temática para viabilizar o intercâmbio de estudantes, professores e pesquisadores entre nossos países, permitindo-nos a melhoria contínua dos processos e técnicas educacionais de ambos os países.			

Audiência Pública da PNCiber – Contribuições

Responsável: Kathryn Jones			
Instituição: UK-FCDO		**Título:** Chefe de Departamento	
Tópico: 16-E,P,D&I	**Id#:** 142	**Parecer:** 0-Agradecimento	
Tipo de Contribuição: Apoio	**Artigo:**	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: Também realizamos uma série de atividades para aumentar o número de profissionais que entram na força de trabalho cibernética (pós 18 bootcamps, como 'Upskill in Cyber'); assegurar a qualidade das ofertas de nível de graduação disponíveis em todo o Reino Unido e incentivar uma maior participação em estágios. Este último baseia-se na Taxa de Aprendizagem, que é um imposto pago pelos empregadores, que pode ser redistribuído pelas organizações que empregam aprendizes.			
Resposta: A melhoria da educação superior em cibersegurança, numa abordagem multisetorial, é uma das expectativas explicitadas na PNCiber, assim como a ampliação do ensino, da pesquisa e da qualificação profissional. As experiências do Reino Unido nessa seara serão de extrema valia para que o Brasil avance rápida e seguramente nessa linha.			

Audiência Pública da PNCiber – Contribuições

Responsável: Kathryn Jones			
Instituição: UK-FCDO		**Título:** Chefe de Departamento	
Tópico: 16-E,P,D&I	**Id#:** 143	**Parecer:** 0-Agradecimento	
Tipo de Contribuição: Apoio	**Artigo:**	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: Além de ter a legislação correta, o Reino Unido enfatiza a necessidade de treinamento para as agências de aplicação da lei, o judiciário e outros setores envolvidos no combate às ameaças cibernéticas para desenvolver capacidades multiagências.			
Resposta: Como bem observado pelo Governo de Sua Majestade, a cibereducação numa visão "whole of society" é uma das premissas da PNCiber. Essa visão enseja também a qualificação profissional em todas as esferas (Nacional, Estadual e Municipal) de governo e em todos os poderes (Executivo, Legislativo e Judiciário), bem como do cidadão comum. A capacidade de coordenação interagências e internacional também é assegurada ao Brasil pela proposta da PNCiber apresentada.			

Audiência Pública da PNCiber – Contribuições

Responsável: Kathryn Jones			
Instituição: UK-FCDO		**Título:** Chefe de Departamento	
Tópico: 16-E,P,D&I	**Id#:** 144	**Parecer:** 0-Agradecimento	
Tipo de Contribuição: Apoio	**Artigo:**	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: O Reino Unido está incentivando qualquer apoio à capacitação do Brasil, tanto nacional quanto internacionalmente. Em particular, o apoio do Brasil às iniciativas da ONU/Conselho da Europa para desenvolver capacidades regionais seria bem-vindo.			
Resposta: O Brasil vem buscando essa capacitação internacional e mecanismos de parceria e cooperação. Para exemplificar, muito recentemente foi realizado pelo GSI um treinamento do LAC4, destinado a profissionais de cibersegurança do governo, promovido com o apoio da União Europeia.			

Audiência Pública da PNCiber – Contribuições

Responsável: Carlos Renato Araújo Braga			
Instituição: TCU		**Título:** Diretor	
Tópico: 02-PNCiber-Geral	**Id#:** 43	**Parecer:** 1-Adequada	
Tipo de Contribuição: Comentário	**Artigo:**	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: Por fim, um alerta com respeito à possibilidade de ocorrer fragmentação, duplicidade, e sobreposição devido à multiplicidade de agentes reguladores. Fragmentação, duplicidade, e sobreposição são coisas que acontecem nas políticas públicas com relativa frequência, e isso não necessariamente é uma coisa ruim. Então, por vezes a gente tem coisas acontecendo, deixando espaços vazios. Hoje, por exemplo, nós temos isso. Aquelas políticas, elas não tratam de nada do setor privado, então, nitidamente, nós temos uma lacuna a ser preenchida, e há uma certa sobreposição também entre a política que trata de infraestrutura crítica e a atual política que trata de segurança da informação. Isso já foi, inclusive, mostrado ali pelo GSI na apresentação inicial. Então, isso é um alerta. Não quer dizer que isso seja necessariamente ruim, mas hoje nós temos agências que tangenciam o tema de segurança da informação e cibersegurança. A ANPD, a Anatel trata desse assunto, no que diz respeito à regulação do sistema de telecomunicações, outras agências reguladoras. Nós temos aí a proposta da criação de uma nova agência para cybersegurança. Existe no Congresso Nacional um projeto para regulamentação da IA, e lá também se prevê uma nova, a criação de uma nova agência. Então há que se ter um cuidado de ver como que essas agências vão trabalhar em coordenação, como foi falado antes, para que a gente não tenha regulações brigando entre si ou falta de regulação.			
Resposta: Entendemos que a existência da ANCiber possa, eventualmente, contribuir para evitar a proliferação de novas agências no sentido de regulação de novas tecnologias cibernéticas. Certamente, ao menos, no tocante ao impacto dessas tecnologias na cibersegurança, isso ocorrerá.			

Audiência Pública da PNCiber – Contribuições

Responsável: Humberto Luiz Ribeiro			
Instituição: FIESP		**Título:** Professor	
Tópico: 02-PNCiber-Geral	**Id#:** 71	**Parecer:** 1-Adequada	
Tipo de Contribuição: Comentário	**Artigo:**	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: Eventualmente, temos que discutir que nível de responsabilização temos que ter no arcabouço brasileiro para aqueles que foram negligentes de forma voluntária, proativamente negligentes, se é o caso.			
Resposta: Acreditamos que, na qualidade de agência reguladora da cibersegurança, a ANCiber terá condições de auxiliar nesse quesito. Não obstante, os instrumentos aplicáveis deverão ser regulados por meio de dispositivos infralegais, como no caso das resoluções exaradas pela ANCiber e aprovadas pelo CNCiber.			

Audiência Pública da PNCiber – Contribuições

Responsável: Sarah Melo Martins			
Instituição: Brasscom		**Título:** Representante	
Tópico: 03-Disposições Gerais	**Id#:** 259	**Parecer:** 1-Adequada	
Tipo de Contribuição: Preoc. ANPD	**Artigo:** 1	**Inciso:**	**Parágrafo:** 1
Texto Original: §1º Esta Lei aplica-se às pessoas físicas e jurídicas de direito público ou privado, sem prejuízo ao disposto na Lei nº 13.709, de 14 de agosto de 2018, no que diz respeito às ações de cibersegurança para proteção de dados pessoais.			
Crítica ou Sugestão: De acordo com o art. 46 da LGPD, a Autoridade Nacional de Proteção de Dados (ANPD) é o órgão responsável pela temática da segurança da informação envolvendo dados pessoais. Neste sentido, e para que se evite a edição de normativos conflitantes, a Brasscom sugere revisão da minuta de projeto de lei para evitar um possível conflito de competências entre esta e a futura ANCiber, por meio de ajuste do § 1º do Art. 1: "Art. 1 [...] § 1º Esta Lei aplica-se às pessoas físicas e jurídicas de direito público ou privado, sem prejuízo ao disposto na Lei nº 13.709, de 14 de agosto de 2018, no que diz respeito às ações de cibersegurança para proteção de dados pessoais e as competências atribuídas à Autoridade Nacional de Proteção de Dados (ANPD)." Alternativamente, deverá a lei deixar claro que as medidas de segurança afetas a proteção de dados pessoais deverão ser regulamentadas, exclusivamente, pela Autoridade Nacional de Proteção de Dados (ANPD).			
Resposta: A proposta foi considerada adequada e condizente com o "espírito" do anteprojeto de Lei, e foi incorporada ao texto.			

Audiência Pública da PNCiber – Contribuições

Responsável: Leonardo Rodrigo Ferreira			
Instituição: SGD		**Título:** Diretor	
Tópico: 03-Disposições Gerais	**Id#:** 150	**Parecer:** 1-Adequada	
Tipo de Contribuição: Alteração Legal	**Artigo:** 1	**Inciso:**	**Parágrafo:**
Texto Original: Art. 1 º. Esta Lei institui a Política Nacional de Cibersegurança, dispondo sobre seus princípios, objetivos, diretrizes e instrumentos, e cria o Sistema Nacional de Cibersegurança, que integra agentes públicos e privados da sociedade brasileira na proteção e na resiliência do ciberespaço de interesse nacional.			
Crítica ou Sugestão: O termo Política Nacional de Cibersegurança é citado diversas vezes pelo Projeto de Lei que dispõe sobre a referida Lei. Desse modo, indicamos definir a sigla PNCiber no art. 1º e utilizá-la das demais ocorrências que citam o termo "Política Nacional de Cibersegurança".			
Resposta: A proposta melhora a legibilidade do texto e foi incorporada.			

Audiência Pública da PNCiber – Contribuições

Responsável: Alan Denilson Lima Costa			
Instituição: ComDCiber		**Título:** Comandante	
Tópico: 03-Disposições Gerais	**Id#:** 1	**Parecer:** 1-Adequada	
Tipo de Contribuição: Preoc. DEFESA	**Artigo:** 3	**Inciso:**	**Parágrafo:**
Texto Original: As ações de ciberdefesa serão coordenadas pelo Ministério da Defesa por intermédio do Sistema Militar de Defesa Cibernética (SMDC).			
Crítica ou Sugestão: As ações de ciberdefesa serão coordenadas pelo Ministério da Defesa por intermédio do Comando de Defesa Cibernética, permanentemente ativado, com capacidade interagências e órgão central do Sistema Militar de Defesa Cibernética (SMDC). Justificativa: Citar o órgão responsável e não apenas o sistema (SMDC), qualificando-o corretamente, conforme seu emprego previsto.			
Resposta: A proposta melhora o texto, e foi incorporada.			

Audiência Pública da PNCiber – Contribuições

Responsável: Ivanildo de Oliveira da Silva			
Instituição: Cidadão		**Título:** Cidadão	
Tópico: 03-Disposições Gerais	**Id#:** 81	**Parecer:** 1-Adequada	
Tipo de Contribuição: Alteração Legal	**Artigo:** 4	**Inciso:** 0	**Parágrafo:**
Texto Original: IV - ciberefeito: dano, permanente ou temporário, indisponibilidade ou limitação da operação, total ou parcial, ou mudança de comportamento, de um ativo cibernético ou não, resultante de uma ciberofensa;			
Crítica ou Sugestão: A perda da confidencialidade e da integridade são também pilares da segurança, assim como a disponibilidade. Sugiro adaptar o inciso IV visando melhorar a redação para que seja mais explícito que a perda da integridade e confidencialidade seja um ciberefeito.			
Resposta: A proposta traz uma percepção distinta do "espírito" original do uso da palavra indisponibilidade, mas a sugestão é cabível e foi incorporada.			

Audiência Pública da PNCiber – Contribuições

Responsável: Arthur Pereira Sabbat			
Instituição: ANPD		**Título:** Diretor	
Tópico: 03-Disposições Gerais	**Id#:** 15	**Parecer:** 1-Adequada	
Tipo de Contribuição: Alteração Legal	**Artigo:** 4	**Inciso:** 0	**Parágrafo:**
Texto Original: XXI - serviços essenciais: serviços cujo mau funcionamento, uso indevido ou interrupção, mesmo que parcial, possa acarretar prejuízo à segurança nacional, e dos quais dependa o exercício de função essencial do Estado ou a prestação de serviço primordial à manutenção de atividades civis, sociais ou econômicas fundamentais aos interesses do Estado.			
Crítica ou Sugestão: No art. 4º, inciso XXI, sugere-se acrescentar o termo "...prejuízo à segurança nacional e à sociedade", uma vez que o conceito de segurança nacional está mais relacionado à soberania, à integridade territorial e à garantia aos cidadãos do exercício dos direitos e deveres constitucionais. Por isso, a sugestão é acrescentar o termo "sociedade".			
Resposta: A proposta melhora o texto, e foi incorporada.			

Audiência Pública da PNCiber – Contribuições

Responsável: Osmar Assis do Nascimento Filho			
Instituição: Cidadão		**Título:** Cidadão	
Tópico: 03-Disposições Gerais	**Id#:** 218	**Parecer:** 1-Adequada	
Tipo de Contribuição: Alteração Legal	**Artigo:** 4	**Inciso:** 0	**Parágrafo:**
Texto Original: XXI - serviços essenciais: serviços cujo mau funcionamento, uso indevido ou interrupção, mesmo que parcial, possa acarretar prejuízo à segurança nacional, e dos quais dependa o exercício de função essencial do Estado ou a prestação de serviço primordial à manutenção de atividades civis, sociais ou econômicas fundamentais aos interesses do Estado.			
Crítica ou Sugestão: Os serviços essenciais devem contemplar, simultaneamente, possibilidade de prejuízo à segurança nacional E funções essenciais do Estado? Não seria OU?			
Resposta: A proposta melhora o texto, e foi incorporada.			

Audiência Pública da PNCiber – Contribuições

Responsável: Arthur Pereira Sabbat			
Instituição: ANPD		**Título:** Diretor	
Tópico: 03-Disposições Gerais	**Id#:** 16	**Parecer:** 1-Adequada	
Tipo de Contribuição: Alteração Legal	**Artigo:** 4	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: Sugere-se, antes do art. 4º, a inserção de uma seção, que poderia ser a Seção I - Das Definições, uma vez que há outras seções intitulando temas dos artigos no Capítulo I.			
Resposta: A proposta melhora o texto, e foi incorporada.			

Audiência Pública da PNCiber – Contribuições

Responsável: Arthur Pereira Sabbat			
Instituição: ANPD		**Título:** Diretor	
Tópico: 03-Disposições Gerais	**Id#:** 17	**Parecer:** 1-Adequada	
Tipo de Contribuição: Alteração Legal	**Artigo:** 4	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: No art. 4º, sugere-se definir "cibercrise", uma vez que o termo no singular surge no inciso X do art. 14 e no inciso VI do art. 21.			
Resposta: A proposta melhora o texto, e foi incorporada.			

Audiência Pública da PNCiber – Contribuições

<table>
<tr><td colspan="4">Responsável: Leonardo Rodrigo Ferreira</td></tr>
<tr><td colspan="2">Instituição: SGD</td><td colspan="2">Título: Diretor</td></tr>
<tr><td>Tópico: 03-Disposições Gerais</td><td>Id#: 151</td><td colspan="2">Parecer: 1-Adequada</td></tr>
<tr><td>Tipo de Contribuição: Alteração Legal</td><td>Artigo: 5</td><td>Inciso: 0</td><td>Parágrafo:</td></tr>
<tr><td colspan="4">Texto Original:
Art. 5 º. A Política Nacional de Cibersegurança baseia-se nos seguintes princípios:
I - foco no cidadão, para fortalecer o elo mais fraco de qualquer instrumento de segurança;
(...)</td></tr>
<tr><td colspan="4">Crítica ou Sugestão:
Consideramos importante que o inciso I foque o cidadão como elo relevante do que como ponto frágil da segurança da informação, conforme sugestão a seguir:
Art. 5 º. A Política Nacional de Cibersegurança baseia-se nos seguintes princípios:
I - foco no cidadão, para fortalecer o elo fundamental para qualquer instrumento de segurança;
(...)</td></tr>
<tr><td colspan="4">Resposta:
A proposta melhora o texto, e foi incorporada.</td></tr>
</table>

Audiência Pública da PNCiber – Contribuições

Responsável: Arthur Pereira Sabbat			
Instituição: ANPD		**Título:** Diretor	
Tópico: 03-Disposições Gerais	**Id#:** 18	**Parecer:** 1-Adequada	
Tipo de Contribuição: Alteração Legal	**Artigo:**	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: O Capítulo I poderia ser "Disposições Gerais" aos moldes da Política Nacional de Barragens e da Política Nacional de Resíduos Sólidos, uma vez que o nome da Política já consta da ementa.			
Resposta: A proposta melhora o texto, e foi incorporada.			

Audiência Pública da PNCiber – Contribuições

Responsável: Vanessa Copeti Cravo			
Instituição: ANATEL		**Título:** GTCiber	
Tópico: 04-Princípios	**Id#:** 267	**Parecer:** 1-Adequada	
Tipo de Contribuição: Alteração Legal	**Artigo:** 5	**Inciso:**	**Parágrafo:**
Texto Original: Art. 5 º. A Política Nacional de Cibersegurança baseia-se nos seguintes princípios: ...			
Crítica ou Sugestão: Inclusão como princípio da PNCiber o respeito e a promoção dos direitos humanos e das garantias fundamentais;			
Resposta: A proposta melhora o texto, e foi incorporada.			

Audiência Pública da PNCiber – Contribuições

Responsável: Osmar Assis do Nascimento Filho			
Instituição: Cidadão		**Título:** Cidadão	
Tópico: 05-Objetivos	**Id#:** 219	**Parecer:** 1-Adequada	
Tipo de Contribuição: Alteração Legal	**Artigo:** 6	**Inciso:** 0	**Parágrafo:**
Texto Original: Art. 6 º. Visando proporcionar um ambiente digital que ofereça as melhores condições de segurança e estabilidade para o desenvolvimento nacional, a Política Nacional de Cibersegurança tem como objetivos: I - garantir a confidencialidade, a integridade, a autenticidade e a disponibilidade dos ciberativos de interesse da sociedade brasileira; ...			
Crítica ou Sugestão: Não está especificado o que seriam "ciberativos de interesse da sociedade". Recomenda-se complementar a ideia com a expressão "ciberativos de interesse nacional" ou ainda "ciberativos de interesse do Estado", para manter coerência com o especificado na Exposição de Motivos, assim como no art. 1º, caput, art. 4º, incisos IX e XXI e art. 5º, inciso IV.			
Resposta: A proposta melhora o texto, e foi incorporada.			

Audiência Pública da PNCiber – Contribuições

Responsável: Maxli Barroso Campos			
Instituição: LPTIC/EGN		**Título:** Pesquisador Líder	
Tópico: 05-Objetivos	**Id#:** 184	**Parecer:** 1-Adequada	
Tipo de Contribuição: Alteração Legal	**Artigo:** 6	**Inciso:** 0	**Parágrafo:**
Texto Original: IX - promover ações que contribuam para a segurança e para a estabilidade do ambiente digital global; e			
Crítica ou Sugestão: IX - promover ações que contribuam para a segurança e para a estabilidade do ciberespaço global; e			
Resposta: A proposta melhora o texto, e foi incorporada.			

Audiência Pública da PNCiber – Contribuições

Responsável: Osmar Assis do Nascimento Filho			
Instituição: Cidadão		**Título:** Cidadão	
Tópico: 06-Diretrizes	**Id#:** 220	**Parecer:** 1-Adequada	
Tipo de Contribuição: Alteração Legal	**Artigo:** 0	**Inciso:**	**Parágrafo:**
Texto Original: Art. 7 º. A Política Nacional de Cibersegurança como orientadora da formulação da Estratégia Nacional de Cibersegurança e de iniciativas correlatas. Art. 8 º. O aproveitamento da agilidade administrativa e da capacidade de pesquisa, desenvolvimento e inovação do setor privado como elemento indispensável para a consecução desta Política. Art. 9 º. A valorização da pesquisa científica da academia nacional, pública e privada, como elemento indispensável para a consecução desta Política.			
Crítica ou Sugestão: Os artigos 7º ao 9º estão elencados sem coesão. Ou se cria um único artigo indicando que as diretrizes serão elencadas nos incisos, ou alteram-se os textos dos artigos para viabilizar a leitura não topicalizada dos mesmos.			
Resposta: A proposta melhora o texto, e foi incorporada.			

Audiência Pública da PNCiber – Contribuições

Responsável: Maxli Barroso Campos			
Instituição: LPTIC/EGN		**Título:** Pesquisador Líder	
Tópico: 08-SNCiber	**Id#:** 185	**Parecer:** 1-Adequada	
Tipo de Contribuição: Alteração Legal	**Artigo:** 11	**Inciso:**	**Parágrafo:**
Texto Original: Art. 11 . Fica instituído o Sistema Nacional de Cibersegurança que agrega os Poderes da União, dos Estados, do Distrito Federal e dos Municípios, incluindo os Tribunais de Contas e os Ministérios Públicos, o setor privado, instituições de ensino e pesquisa, e demais agentes da sociedade, no que tange às ações de planejamento, execução e coordenação das atividades relacionadas à cibersegurança.			
Crítica ou Sugestão: Art. 11 . Fica instituído o Sistema Nacional de Cibersegurança que agrega os Poderes da União, dos Estados, do Distrito Federal e dos Municípios, incluindo os Tribunais de Contas e os Ministérios Públicos, o setor privado, instituições de ensino e pesquisa, e demais agentes da sociedade, no que tange às ações de planejamento, execução, integração e coordenação das atividades relacionadas à cibersegurança.			
Resposta: A proposta melhora o texto, e foi incorporada.			

Audiência Pública da PNCiber – Contribuições

Responsável: Leonardo Rodrigo Ferreira			
Instituição: SGD		**Título:** Diretor	
Tópico: 08-SNCiber	**Id#:** 152	**Parecer:** 1-Adequada	
Tipo de Contribuição: Alteração Legal	**Artigo:** 12	**Inciso:**	**Parágrafo:**
Texto Original: Art. 13 . Fica instituído o Comitê Nacional de Cibersegurança ("Comitê"), órgão de assessoramento ao Presidente da República na temática relacionada à cibersegurança, integrado por representantes da sociedade, do setor público, do setor privado e da academia.			
Crítica ou Sugestão: Apresentamos a sugestão de privilegiar o uso de siglas quando ocorrer a citação de termo já mencionado anteriormente pela minuta do texto proposto. Dessa forma, sugerimos o uso da sigla CNCiber para substituição das menções de Comitê Nacional de Cibersegurança. Indicamos observar essa oportunidade de melhoria para ocorrências análogas ao caso apresentado. Nesse cenário, apresentamos a seguinte sugestão: Art. 13 . Fica instituído o CNCiber, órgão de assessoramento ao Presidente da República na temática relacionada à cibersegurança, integrado por representantes da sociedade, do setor público, do setor privado e da academia.			
Resposta: A proposta melhora o texto, e foi incorporada.			

Audiência Pública da PNCiber – Contribuições

<table>
<tr><td colspan="4">Responsável: Rodrigo Azevedo Greco</td></tr>
<tr><td colspan="2">Instituição: Cidadão</td><td colspan="2">Título: Advogado</td></tr>
<tr><td>Tópico: 09-CNCiber</td><td>Id#: 252</td><td colspan="2">Parecer: 1-Adequada</td></tr>
<tr><td>Tipo de Contribuição: Alteração Legal</td><td>Artigo: 14</td><td>Inciso: 0</td><td>Parágrafo:</td></tr>
<tr><td colspan="4">Texto Original:</td></tr>
<tr><td colspan="4">Crítica ou Sugestão:
O primeiro é uma suposta competência normativa do comitê. O senhor falou que o comitê teria uma função de supervisão das atividades da agência, e, mas eu vi que aqui no artigo 14, inciso 2, ele tem uma competência para aprovar, por meio de resolução, atos normativos concernentes a cybersegurança. Eu fiquei na dúvida como essa competência normativa seria exercida pelo comitê, com a matéria, se não tem um conflito interagência, como separar essas competências normativas.</td></tr>
<tr><td colspan="4">Resposta:
Foi ajustada a redação das competências da ANCiber propor resoluções e do CNCiber aprovar tais resoluções, de forma a eliminar quaisquer possíveis dúvidas.</td></tr>
</table>

Audiência Pública da PNCiber – Contribuições

Responsável: Leonardo Rodrigo Ferreira			
Instituição: SGD		**Título:** Diretor	
Tópico: 09-CNCiber	**Id#:** 153	**Parecer:** 1-Adequada	
Tipo de Contribuição: Alteração Legal	**Artigo:** 14	**Inciso:** 0	**Parágrafo:**
Texto Original: Art. 14 . Compete ao Comitê: (...) X - determinar ao Diretor-Geral da ANCiber que notifique ao Ministro de Estado Chefe do Gabinete de Segurança Institucional, em caráter emergencial, a existência de uma cibercrise relevante para a segurança nacional, para que ele a informe ao Conselho Nacional de Defesa.			
Crítica ou Sugestão: O inciso X do art. 14 cita o termo cibercrise, todavia não identificamos proposta de definição do referido termo na minuta do Projeto de Lei. Assim, indicamos a necessidade de definir tal termo.			
Resposta: O termo cibercrise foi incluído no artigo 4.			

Audiência Pública da PNCiber – Contribuições

Responsável: Núcleo de Pesquisa em Concorrência, Política Pública, Inovação e Tecnologia (Comppit)			
Instituição: FGV		**Título:** Pesquisador	
Tópico: 09-CNCiber	**Id#:** 214	**Parecer:** 1-Adequada	
Tipo de Contribuição: Alteração Legal	**Artigo:** 14	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: Conforme o art. 14 do PL, o CNCiber é quem dispõe da competência de editar normas. A Agência, conforme o art. 18 do PL, não possui poder regulatório, mas um mandato essencialmente executivo ou, no máximo, propositivo. Considerando a composição plural e multissetorial do CNCiber (art. 15 do PL), convém se perguntar em que medida a criação da Agência protegeria a PNCiber de instabilidades e traria a autonomia que garante a prestação perene e consistente de políticas ao longo de diferentes governos. Isso, pois o órgão competente para elaborar as regras da PNCiber - peça central e determinante do Projeto - seria composto por uma série de representantes desprovidos de mandatos protegidos, indicados por uma variedade de fontes, tanto do governo quanto da sociedade civil.			
Resposta: A proposta melhora o texto, e foi incorporada.			

Audiência Pública da PNCiber – Contribuições

Responsável: Alan Denilson Lima Costa			
Instituição: ComDCiber		**Título:** Comandante	
Tópico: 09-CNCiber	**Id#:** 2	**Parecer:** 1-Adequada	
Tipo de Contribuição: Inclusão no CNCiber	**Artigo:** 15	**Inciso:** 0	**Parágrafo:**
Texto Original: O Comitê Nacional de Cibersegurança será composto por: (...) X - um representante da Comissão de Ciência, Tecnologia, Inovação, Comunicação e Informática do Senado Federal.			
Crítica ou Sugestão: X - o Comandante de Defesa Cibernética; Obs: não substitui o anterior, apenas ocupa esta posição como inciso, seguindo-se os demais componentes. Justificativa: Assim como a proposta da PF, durante a Aud Pub em 15 Jun 23, o CmtDCiber agregaria qualidade técnica ao comitê, pelo assessoramento direto e de alto nível pela autoridade proposta, além da incorporação das capacidades de interesse da Defesa Cibernética e da Segurança Nacional, como a busca de ameaças avançadas no ciberespaço.			
Resposta: A proposta melhora o texto, e foi incorporada.			

Audiência Pública da PNCiber – Contribuições

Responsável: Carlos Fonseca			
Instituição: CDESS		**Título:** Assessor	
Tópico: 09-CNCiber	**Id#:** 38	**Parecer:** 1-Adequada	
Tipo de Contribuição: Inclusão no CNCiber	**Artigo:** 15	**Inciso:**	**Parágrafo:**
Texto Original: Art. 15 . O Comitê Nacional de Cibersegurança será composto por:			
Crítica ou Sugestão: Confirmar o interesse do Conselho de Desenvolvimento Econômico Social Sustentável em ter assento no Comitê Nacional de Cibersegurança. Sugiro acrescentar numeral após o Art. 15 XIV com a seguinte redação: "um representante do Conselho de Desenvolvimento Econômico Social Sustentável".			
Resposta: A proposta foi incorporada ao texto.			

Audiência Pública da PNCiber – Contribuições

Responsável: Leonardo Rodrigo Ferreira			
Instituição: SGD		**Título:** Diretor	
Tópico: 09-CNCiber	**Id#:** 154	**Parecer:** 1-Adequada	
Tipo de Contribuição: Alteração Legal	**Artigo:** 15	**Inciso:**	**Parágrafo:**
Texto Original: Art. 15. O Comitê Nacional de Cibersegurança será composto por: (...) VII - um representante do Ministério da Gestão e da Inovação em Serviços Públicos; (...)			
Crítica ou Sugestão: Acerca do art. 15, sugere-se a inclusão de um representante da Secretaria de Governo Digital (SGD), como órgão central do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP). Embora a proposta já contemple um representante do Ministério da Gestão e da Inovação em Serviços Públicos (MGI), a atuação deste pode se referir às diversas temáticas tratadas no âmbito do órgão, como compras públicas, gestão de pessoas, patrimônio, entre outros. Por outro lado, a atuação da SGD se dará como representante de todos os órgãos pertencentes ao SISP. Nesse cenário, apresentamos a seguinte sugestão: Art. 15. O Comitê Nacional de Cibersegurança será composto por: (...) VII - um representante do Ministério da Gestão e da Inovação em Serviços Públicos; VIII - um representante do órgão central do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP) <ajuste da numeração dos incisos subsequentes>			
Resposta: A composição do CNCiber foi alterada, e a SGD foi incluída.			

Audiência Pública da PNCiber – Contribuições

Responsável: Valdemar Latance Neto			
Instituição: DPF		**Título:** Delegado	
Tópico: 09-CNCiber	**Id#:** 266	**Parecer:** 1-Adequada	
Tipo de Contribuição: Alteração Legal	**Artigo:** 15	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: Porque a PF não foi expressamente incluída no Sistema Nacional, especialmente no comitê e no Gabinete de Gerenciamento de Crises? Respeitosamente, não há razões constitucionais nem legais para essa exclusão. Além das razões constitucionais, razões práticas também apontam a pertinência da integração da instituição responsável pela apuração dos fatos criminosos no Sistema Nacional de Cybersegurança. Embora o PL tenha reservado uma vaga para o membro do Ministério da Justiça e da Segurança Pública, esse ponto, na nossa opinião, merece ser discutido, tendo em vista a existência de diversos órgãos dentro da estrutura do Ministério da Justiça. Concluindo, diante das circunstâncias nacionais no Sistema Nacional de Cybersegurança, a Polícia Federal deveria integrar o Comitê Nacional de Cybersegurança e o Gabinete de Gerenciamento de Cybercrimes sem prejuízo do outro indicado pelo Ministério da Justiça e da Segurança Pública responsável por outras áreas temáticas também relevantes na composição desses novos órgãos.			
Resposta: A PF não fora originalmente incluída nominalmente no CNCiber nem no GGCiber devido ao fato de que o MJSP, ao qual se subordina a PF, já estava presente em ambas as entidades. Ouvidos os argumentos da PF e de outros participantes da Audiência Pública, no entanto, entendeu-se apropriada a inclusão da PF tanto no CNCiber quanto no GGCiber (como ademais de algumas outras instituições), mesmo mantendo-se a representação de seus respectivos ministérios.			

Audiência Pública da PNCiber – Contribuições

Responsável: Vanessa Copeti Cravo			
Instituição: ANATEL		**Título:** GTCiber	
Tópico: 09-CNCiber	**Id#:** 268	**Parecer:** 1-Adequada	
Tipo de Contribuição: Inclusão no CNCiber	**Artigo:** 15	**Inciso:**	**Parágrafo:**
Texto Original: Art. 15 . O Comitê Nacional de Cibersegurança será composto por: ...			
Crítica ou Sugestão: Inclusão da Anatel como membro do Comitê Nacional de Cibersegurança (CNCiber): Anatel não regula qualquer infraestrutura. É um equívoco identificar o setor como apenas uma das IEC (e assim concorrer pela representação dessas infraestruturas). A Agência regula o setor que é responsável pela conectividade, que tem uma enorme superfície de ataque (redes); que é meio para a disseminação de ameaças; que todas as outras infraestruturas críticas (serviços essenciais, na terminologia da minuta) dependem; e cujas ações de promoção de cibersegurança tem um enorme impacto no ecossistema. Por fim, a Anatel também tem o mandato de representar o Brasil nos organismos internacionais de telecomunicações, em cujas agendas predominam os debates de cibersegurança. Assim, a inclusão de um assento para a Agência não seria apenas natural, mas necessário;			
Resposta: A proposta foi contemplada pela alteração da composição do CNCiber e do GGCiber, que incluiu as agências reguladoras de setores com infraestruturas críticas.			

Audiência Pública da PNCiber – Contribuições

Responsável: Osmar Assis do Nascimento Filho			
Instituição: Cidadão		**Título:** Cidadão	
Tópico: 10-ANCiber	**Id#:** 221	**Parecer:** 1-Adequada	
Tipo de Contribuição: Alteração Legal	**Artigo:** 18	**Inciso:** 0	**Parágrafo:**
Texto Original: VI - desenvolver capacidades nacionais de prevenção, monitoramento, detecção, análise e resposta, para detectar e gerenciar ciberincidentes;			
Crítica ou Sugestão: A autarquia deverá desenvolver capacidades nacionais ou promover o desenvolvimento? Sugere-se utilizar o termo "promover o desenvolvimento".			
Resposta: A proposta melhora o texto, e foi incorporada.			

Audiência Pública da PNCiber – Contribuições

Responsável: Vanessa Copeti Cravo			
Instituição: ANATEL		**Título:** GTCiber	
Tópico: 10-ANCiber	**Id#:** 269	**Parecer:** 1-Adequada	
Tipo de Contribuição: Alteração Legal	**Artigo:** 18	**Inciso:** 0	**Parágrafo:**
Texto Original: VII - promover a definição, a manutenção e a unidade do arcabouço jurídico nacional no campo da cibersegurança, por meio da emissão de pareceres não vinculativos sobre iniciativas legislativas ou regulatórias relativas à cibersegurança, levando em conta os desenvolvimentos internacionais;			
Crítica ou Sugestão: Competência para emissão de pareceres não vinculativos - a emissão desses pareceres viola a autonomia das ARs, que devem implementar as políticas públicas por meio de políticas regulatórias. Ademais, a existência de um parecer, ainda que não vinculativo de uma autoridade nacional, na prática vincularia os gestores das ARs ao seu resultado, sob pena de eventual responsabilização dos órgãos de controle ou poderia fomentar a judicialização das matérias por terceiros interessados, em caso de adoção de decisão contrária ao parecer. Sugestão, eliminar do texto a parte referente às iniciativas regulatórias: Art. 18, VII - promover a definição, a manutenção e a unidade do arcabouço jurídico nacional no campo da cibersegurança, por meio da emissão de pareceres não vinculativos sobre iniciativas legislativas, levando em conta os desenvolvimentos internacionais;			
Resposta: A proposta melhora o texto, e foi incorporada.			

Audiência Pública da PNCiber – Contribuições

Responsável: Osmar Assis do Nascimento Filho			
Instituição: Cidadão		**Título:** Cidadão	
Tópico: 10-ANCiber	**Id#:** 222	**Parecer:** 1-Adequada	
Tipo de Contribuição: Alteração Legal	**Artigo:** 18	**Inciso:** 0	**Parágrafo:**
Texto Original: XIV - avaliar e certificar produtos e serviços, no tocante à cibersegurança, diretamente ou por meio de parceiros credenciados pela ANCiber;			
Crítica ou Sugestão: Este inciso cria a necessidade de estabelecimento de competência específica para a ANCiber: a de estabelecer, por normativo próprio, os padrões e critérios para certificação de produtos e serviços e os padrões e critérios para credenciamento de parceiros. Tal competência não está explícita no texto legal.			
Resposta: A proposta melhora o texto, e foi incorporada.			

Audiência Pública da PNCiber – Contribuições

Responsável: Marcelo Câmara			
Instituição: MRE		**Título:** Diretor	
Tópico: 10-ANCiber	**Id#:** 180	**Parecer:** 1-Adequada	
Tipo de Contribuição: Alteração Legal	**Artigo:** 18	**Inciso:** 0	**Parágrafo:**

Texto Original:
XXII - estipular acordos bilaterais e multilaterais, com instituições, órgãos e agências de outros países para a participação do país em programas de cibersegurança, garantindo a necessária conexão com os demais órgãos da administração pública federal aos quais a lei atribui competências no campo da cibersegurança, em ações conjuntas, combinadas ou compartilhadas com o Ministério das Relações Exteriores;

Crítica ou Sugestão:
Com relação ao disposto no artigo 18, XXII, do PDL, observa-se que, segundo o disposto no artigo 7° da Convenção de Viena sobre o Direito dos Tratados - incorporada ao ordenamento jurídico brasileiro por meio do Decreto 7030/2019- , são considerados representantes do Estado para a adoção ou autenticação do texto de um tratado ou para expressar o consentimento do Estado em obrigar-se por um tratado, em virtude de suas funções e independentemente da apresentação de plenos poderes: a) os Chefes de Estado, os Chefes de Governo e os Ministros das Relações Exteriores, para a realização de todos os atos relativos à conclusão de um tratado; b) os Chefes de missão diplomática, para a adoção do texto de um tratado entre o Estado acreditante e o Estado junto ao qual estão acreditados; e c) os representantes acreditados pelos Estados perante uma conferência ou organização internacional ou um de seus órgãos, para a adoção do texto de um tratado em tal conferência, organização ou órgão.
Neste sentido, sugere-se que seja evidenciado não ter a Agência Nacional de Cibersegurança a competência para assumir compromissos internacionais em nome do Governo brasileiro, mas somente entendimentos de caráter interinstitucional e não vinculante. Nessa perspectiva, ao invés da expressão "estipular acordos bilaterais e multilaterais" seria mais indicada a redação "participar das negociações de acordos bilaterais e multilaterais".

Resposta:
A proposta melhora o texto, e foi incorporada.

Audiência Pública da PNCiber – Contribuições

Responsável: João Araújo Monteiro Neto			
Instituição: GETIS/Unifor		**Título:** Pesquisador	
Tópico: 11-GGCiber	**Id#:** 109	**Parecer:** 1-Adequada	
Tipo de Contribuição: Alteração Legal	**Artigo:** 20	**Inciso:**	**Parágrafo:**
Texto Original: Art. 20 . Institui-se o Gabinete de Gerenciamento de Cibercrises ("Gabinete") , órgão de assessoramento ao Presidente da República na gestão de cibercrises, integrado por representantes da sociedade, do setor público, do setor privado e da academia.			
Crítica ou Sugestão: Embora o art. 20 do Projeto e Lei preveja expressamente que o Gabinente de Gerenciamento de Cibercrises será integrado por "representantes da sociedade, do setor público, do setor privado e da academia", o art. 22 do PL, que disciplina a sua composição, não prevê representação para setores não governamentais.			
Resposta: O texto foi corrigido.			

Audiência Pública da PNCiber – Contribuições

Responsável: Leila Oliveira da Fonseca			
Instituição: Cidadão		**Título:** Pesquisadora	
Tópico: 11-GGCiber	**Id#:** 146	**Parecer:** 1-Adequada	
Tipo de Contribuição: Alteração Legal	**Artigo:** 20	**Inciso:**	**Parágrafo:**
Texto Original: Art. 20 . Institui-se o Gabinete de Gerenciamento de Cibercrises ("Gabinete") , órgão de assessoramento ao Presidente da República na gestão de cibercrises, integrado por representantes da sociedade, do setor público, do setor privado e da academia.			
Crítica ou Sugestão: Na composição de gerente de gerenciamento de crise Cibercrises, consta o setor privado e a academia, mas na descrição dos componentes (Art. 22) não aparecem representantes destes setores.			
Resposta: O texto foi corrigido.			

Audiência Pública da PNCiber – Contribuições

Responsável: Luca Belli			
Instituição: FGV		**Título:** Professor	
Tópico: 11-GGCiber	**Id#:** 165	**Parecer:** 1-Adequada	
Tipo de Contribuição: Alteração Legal	**Artigo:** 20	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: No artigo 20, eu me dei conta que ao falar do gabinete, a composição do gabinete é principalmente pública, de órgão público, que é bsolutamente coerente. Porém, logo no início no artigo 20, se reproduz a mesma formulação do artigo 14 falando que está aberto também à sociedade civil, empresas, e academia. Acho muito (Ininteligível) a essa formulação pode gerar um pouco de confusão.			
Resposta: O texto foi corrigido.			

Audiência Pública da PNCiber – Contribuições

Responsável: Arthur Pereira Sabbat			
Instituição: ANPD		**Título:** Diretor	
Tópico: 11-GGCiber	**Id#:** 19	**Parecer:** 1-Adequada	
Tipo de Contribuição: Alteração Legal	**Artigo:** 21	**Inciso:** 0	**Parágrafo:**
Texto Original: Art. 21 . Compete ao Gabinete: I - implementar medidas e ações voltadas à mitigação de consequências de ciberincidentes afetos ao Complexo Nacional de Cibersegurança; ...			
Crítica ou Sugestão: No art. 21, das competências do Gabinete de Gerenciamento de Cibercrises, no inciso I, consta "implementar medidas e ações voltadas à mitigação de consequências de ciberincidentes afetos ao Complexo Nacional de Cibersegurança;". Uma vez que a efetivação da implementação dessas medidas e ações caberá aos responsáveis pelos serviços essenciais, existe a possibilidade de que essa atribuição se torne difícil de exercer. Poderia ser, desse modo, "determinar a implementação", ou "orientar a implementação..."			
Resposta: A proposta melhora o texto, e foi incorporada.			

Audiência Pública da PNCiber – Contribuições

Responsável: Alan Denilson Lima Costa			
Instituição: ComDCiber		**Título:** Comandante	
Tópico: 11-GGCiber	**Id#:** 3	**Parecer:** 1-Adequada	
Tipo de Contribuição: Inclusão no GGCiber	**Artigo:** 22	**Inciso:** 0	**Parágrafo:**
Texto Original: O Gabinete de Gerenciamento de Cibercrises será composto por: (...) X - um representante da Comissão de Ciência, Tecnologia, Inovação, Comunicação e Informática do Senado Federal;			
Crítica ou Sugestão: X - o Comandante de Defesa Cibernética; Obs: não substitui o anterior, apenas ocupa esta posição como inciso, seguindo-se os demais componentes. Justificativa: As mesmas do Art. 15, somado ao fato de que, o Estado brasileiro já estaria enfrentando uma cibercrise e, assim, cresce de importância o assessoramento direto do Comandante de Defesa Cibernética ao Gabinete de Gerenciamento de Cibercrises.			
Resposta: A proposta melhora o texto, e foi incorporada.			

Audiência Pública da PNCiber – Contribuições

Responsável: Frederico Fernandes Neres			
Instituição: Caixa		**Título:** Gerente	
Tópico: 11-GGCiber	**Id#:** 62	**Parecer:** 1-Adequada	
Tipo de Contribuição: Inclusão no GGCiber	**Artigo:** 22	**Inciso:**	**Parágrafo:**
Texto Original: Art. 22 . O Gabinete de Gerenciamento de Cibercrises será composto por: ...			
Crítica ou Sugestão: Avaliar a participação de representantes da infraestrutura critica, tais como representante do setor financeiro, visando dar celeridade em possíveis respostas à crises, considerando a sensibilidade desse setor para a sociedade;			
Resposta: A proposta melhora o texto, e foi incorporada.			

Audiência Pública da PNCiber – Contribuições

Responsável: Leonardo Rodrigo Ferreira			
Instituição: SGD		**Título:** Diretor	
Tópico: 11-GGCiber	**Id#:** 155	**Parecer:** 1-Adequada	
Tipo de Contribuição: Alteração Legal	**Artigo:** 22	**Inciso:**	**Parágrafo:**
Texto Original: Art. 22. O Gabinete de Gerenciamento de Cibercrises será composto por: (...) VII - um representante do Ministério da Gestão e da Inovação em Serviços Públicos; (...)			
Crítica ou Sugestão: Sugere-se a inclusão de um representante do órgão central do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP) no Gabinete de Gerenciamento de Cibercrimes, pelos mesmos motivos expostos na sugestão da inclusão no Comitê Nacional de Cibersegurança. Nesse cenário, apresentamos a seguinte sugestão: Art. 22. O Gabinete de Gerenciamento de Cibercrises será composto por: (...) VII - um representante do Ministério da Gestão e da Inovação em Serviços Públicos; VIII - um representante do órgão central do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP) <ajuste da numeração dos incisos subsequentes>			
Resposta: A composição do GGCiber foi alterada, e a SGD foi contemplada.			

Audiência Pública da PNCiber – Contribuições

Responsável: Marcelo Câmara			
Instituição: MRE		**Título:** Diretor	
Tópico: 15-Cooperação Internacional	**Id#:** 181	**Parecer:** 1-Adequada	
Tipo de Contribuição: Alteração Legal	**Artigo:** 30	**Inciso:**	**Parágrafo:**
Texto Original: Art. 30 . As iniciativas de cooperação técnica internacional em cibersegurança, coerentes com a garantia da soberania e dos interesses nacionais, têm as seguintes finalidades:			
Crítica ou Sugestão: Com relação ao disposto no artigo 30, capítulo V, dentre outros, do PDL, sugere-se a utilização da expressão "cooperação internacional" em substituição a "cooperação técnica internacional" ao longo de todo o Projeto de Lei para a criação da Política Nacional de Cibersegurança (PNCiber). Assim seria afastada eventual associação às competências relativas à gestão da "cooperação técnica" da Agência Brasileira de Cooperação, previstas no Art. 16º do Decreto nº 11.357, de 1º de janeiro de 2023.			
Resposta: A proposta melhora o texto, e foi incorporada.			

Audiência Pública da PNCiber – Contribuições

<table>
<tr><td colspan="4">Responsável: Osmar Assis do Nascimento Filho</td></tr>
<tr><td colspan="2">Instituição: Cidadão</td><td colspan="2">Título: Cidadão</td></tr>
<tr><td>Tópico: 18-ANCiber-Organização</td><td>Id#: 223</td><td colspan="2">Parecer: 1-Adequada</td></tr>
<tr><td>Tipo de Contribuição: Alteração Legal</td><td>Artigo: 19</td><td>Inciso:</td><td>Parágrafo: 2</td></tr>
<tr><td colspan="4">Texto Original:
Art. 19 . A ANCiber submeterá anualmente ao Gabinete de Segurança Institucional da Presidência da República a sua proposta de orçamento, que será encaminhada ao Ministério do Planejamento e Orçamento para inclusão no projeto de lei orçamentária anual a que se refere o § 5º do art. 165 da Constituição Federal.</td></tr>
<tr><td colspan="4">Crítica ou Sugestão:
Está em conflito com o art. 20. Ou o encaminhamento será realizado diretamente pela ANCiber (texto do art. 20) ou pelo GSI (texto do art. 19).</td></tr>
<tr><td colspan="4">Resposta:
O Art. 19 foi excluído.</td></tr>
</table>

Audiência Pública da PNCiber – Contribuições

<table>
<tr><td colspan="4">Responsável: Rodrigo Azevedo Greco</td></tr>
<tr><td colspan="2">Instituição: Cidadão</td><td colspan="2">Título: Advogado</td></tr>
<tr><td>Tópico: 18-ANCiber-Organização</td><td>Id#: 253</td><td colspan="2">Parecer: 1-Adequada</td></tr>
<tr><td>Tipo de Contribuição: Alteração Legal</td><td>Artigo: 21</td><td>Inciso: 0</td><td>Parágrafo:</td></tr>
<tr><td colspan="4">Texto Original:</td></tr>
<tr><td colspan="4">Crítica ou Sugestão:
Terceiro ponto é, quando se fala de cobrança de taxas, fato gerador, contribuinte, valor, tem que estar previstos em lei. Eu não encontrei isso na, no projeto. Eu não sei se vai ser feito uma, num outro projeto de lei, prevendo e regulando a cobrança das, dessa taxa.</td></tr>
<tr><td colspan="4">Resposta:
O detalhamento das taxas e fatos geradores foi incluído no texto.</td></tr>
</table>

Audiência Pública da PNCiber – Contribuições

Responsável: Alan Denilson Lima Costa			
Instituição: ComDCiber		**Título:** Comandante	
Tópico: 19-ANCiber-Pessoal	**Id#:** 4	**Parecer:** 1-Adequada	
Tipo de Contribuição: Preoc. DEFESA	**Artigo:** 30	**Inciso:**	**Parágrafo:** 3
Texto Original: §3º As requisições aplicam-se aos servidores, aos militares e aos empregados.			
Crítica ou Sugestão: §3º As requisições aplicam-se aos servidores, aos empregados e aos militares, exceto aos que ocupem cargos no Sistema Militar de Defesa Cibernética (SMDC), por sua atuação em prol da Segurança Nacional. Justificativa: A atual provisão de cargos para o SMDC é insuficiente e, além disso, é agravada pela disputa com o setor privado de cibersegurança, o qual recruta muitos de seus integrantes no SMDC; a proposta não exclui a possibilidade da convocação, mas reduz o impacto sobre aqueles que já prestam seu serviço junto à Defesa Cibernética do País, em prol da Segurança Nacional.			
Resposta: A proposta melhora o texto, e foi incorporada.			

Audiência Pública da PNCiber – Contribuições

Responsável: Leonardo Rodrigo Ferreira			
Instituição: SGD		**Título:** Diretor	
Tópico: 23-Decreto GGCiber	**Id#:** 156	**Parecer:** 1-Adequada	
Tipo de Contribuição: Alteração Legal	**Artigo:** 4	**Inciso:**	**Parágrafo:**
Texto Original: Art. 4 º. O quórum de reunião do Gabinete de Gestão de Cibercrises será de dois terços dos membros e o quórum de aprovação será de maioria simples dos membros.			
Crítica ou Sugestão: O Gabinete de Gestão de Cibercrises desempenha papel de extrema relevância para o País, desse modo, é extremamente importante assegurar que sempre exista quórum mínimo para tratar as cibercrises. A redação atual não oferece alternativa de realização de reunião caso não exista presença de 2/3 dos membros, assim, se não existir a citada presença a reunião não ocorrerá. Nesse contexto, propomos que seja realizada reflexão sobre a necessidade de existir outra alternativa de quórum para caso de necessidade de 2ª chamada da reunião. Outro ponto importante é o quórum de aprovação que cita maioria simples dos membros. Indicamos para apreciação que, se aplicável, seja considerada a maioria dos membros presentes. Art. 4 º. O quórum de reunião do Gabinete de Gestão de Cibercrises será de dois terços dos membros e o quórum de aprovação será de maioria simples dos membros presentes.			
Resposta: A proposta melhora o texto, e foi incorporada.			

Audiência Pública da PNCiber – Contribuições

Responsável: Rodrigo Azevedo Greco			
Instituição: Cidadão		**Título:** Advogado	
Tópico: 24-Decreto ANCiber	**Id#:** 254	**Parecer:** 1-Adequada	
Tipo de Contribuição: Alteração Legal	**Artigo:** 17	**Inciso:** 0	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: Por fim, no anexo 3 do decreto que trata da estrutura da agência, é atribuído contato das competências do órgão de inteligência, uma delas é a subsidiar ou produzir conhecimento que subsidie o processo decisório da ANCiber, em especial aquele relacionado às análises de pedidos de autorizações, processos de revogação, e cancelamento de registros dos agentes regulados pela agência. Isso é algo que eu não encontrei no projeto de lei, e eu não entendi que registro é esse que os agentes regulares têm que fazer perante a agência. Isso tá só no decreto, não tá na lei.			
Resposta: A redação em tela buscava contemplar os sujeitos à regulação pela ANCiber, mas ficou carente de objetividade e clareza. A redação foi corrigida.			

Audiência Pública da PNCiber – Contribuições

Responsável: Estela Aranha			
Instituição: MJSP		**Título:** Assessora	
Tópico: 02-PNCiber-Geral	**Id#:** 54	**Parecer:** 2-Parcialmente Adequada	
Tipo de Contribuição: Comentário	**Artigo:**	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: Todos os países que você apresentou aqui, como os Estados Unidos, França, entre outros, eles todos têm uma política de estratégica cybersegurança, mas tem outras áreas de política cibernética que conversam, e muita institucionalidade. São várias instituições, e obviamente a política tem que ser coordenada, mas a execução dessa política, ela depende obviamente de muitos órgãos para poder se conseguir a execução delas. Então, e aí, trazer um pouco dessa discussão dessa interface, e é importante a gente pensar na interface desse sistema proposto com o que a gente já tem existente, inclusive por razões de competências, de atribuições legais ou constitucionais.			
Resposta: A intenção central é que a ANCiber seja a coordenadora das ações de cibersegurança dispersas nacionalmente, e que seja supervisionada pelo CNCiber, como dispõe o anteprojeto em debate. O CNCiber, de sua parte, foi bastante ampliado em decorrência das sugestões apresentadas na audiência pública.			

Audiência Pública da PNCiber – Contribuições

Responsável: Estela Aranha			
Instituição: MJSP		**Título:** Assessora	
Tópico: 02-PNCiber-Geral	**Id#:** 55	**Parecer:** 2-Parcialmente Adequada	
Tipo de Contribuição: Comentário	**Artigo:**	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: É importante a gente pensar na interface desse sistema proposto com o que a gente já tem existente, inclusive por razões de competências, de atribuições legais ou constitucionais. Tem a questão da defesa de cibernética, que, a defesa das infraestruturas críticas, que tem tanto o Ministério da Defesa quanto o (Ininteligível) que trabalha, e como é que a gente vai fazer isso. A diplomacia cibernética, o colega do Ministério das Relações Exteriores falou hoje, a questão de segurança cibernética ela é central na geopolítica, ela é central na discussão de guerra e paz. Não tem nada mais central que isso. Então, é uma matéria de defesa, é uma matéria de relações exteriores.			
Resposta: A interface existente no anteprojeto de lei em discussão se dá por meio do CNCiber, cuja participação foi bastante ampliada em decorrência das sugestões apresentadas na audiência pública.			

Audiência Pública da PNCiber – Contribuições

Responsável: Estela Aranha			
Instituição: MJSP		**Título:** Assessora	
Tópico: 02-PNCiber-Geral	**Id#:** 56	**Parecer:** 2-Parcialmente Adequada	
Tipo de Contribuição: Comentário	**Artigo:**	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: No projeto não diz exatamente quais são os serviços essenciais. Acho que seria interessante até estressar isso de alguma forma, na legislação, definir isso. A outra questão também que nos chamou atenção é a necessidade de ter estruturas flexíveis, uma vez que essas ameaças, elas não são estáticas, elas são imprevisíveis e cada dia mais novas.			
Resposta: Os serviços essenciais serão elencados no Complexo Nacional de Cibersegurança. O regramento para tal inclusão será proposto por meio de resolução proposta pela ANCiber e aprovada pelo CNCiber. Dessa forma, entende-se que exista transparência e flexibilidade, assim como agilidade, no trato do que possa ser essencial para a sociedade. O detalhamento do conceito, ou mesmo na abrangência dos serviços esenciais atuaria contra a proposta de flexibilidade defendida pela autora, o que não se pretende no projeto.			

Audiência Pública da PNCiber – Contribuições

Responsável: Maxli Barroso Campos			
Instituição: LPTIC/EGN		**Título:** Pesquisador Líder	
Tópico: 03-Disposições Gerais	**Id#:** 186	**Parecer:** 2-Parcialmente Adequada	
Tipo de Contribuição: Alteração Legal	**Artigo:** 4	**Inciso:** 0	**Parágrafo:**
Texto Original: XI - ciberinvestigação (ou investigação cibernética ou ciberforense): conjunto de medidas para análise de ciberincidentes voltado à identificação de técnicas, táticas, procedimentos e perpetradores, bem como das causas, extensão dos ciberefeitos, e modus operandi da ciberofensa ou de seu perpetrador.			
Crítica ou Sugestão: XI - ciberinvestigação (ou investigação cibernética ou Forense Computacional): conjunto de medidas para análise de ciberincidentes voltado à identificação de técnicas, táticas, procedimentos e perpetradores, bem como das causas, extensão dos ciberefeitos, e modus operandi da ciberofensa ou de seu perpetrador.			
Resposta: É plausível a inclusão do termo "forense computacional" à definição existente no anteprojeto de lei, mas como um termo adicional, sem a exclusão do termo "ciberforense".			

Audiência Pública da PNCiber – Contribuições

Responsável: Luiz Henrique Barbosa da Silva			
Instituição: TELCOMP		**Título:** Representante	
Tópico: 03-Disposições Gerais	**Id#:** 175	**Parecer:** 2-Parcialmente Adequada	
Tipo de Contribuição: Alteração Legal	**Artigo:** 0	**Inciso:**	**Parágrafo:**
Texto Original: Institui a Política Nacional de Cibersegurança e cria o Sistema Nacional de Cibersegurança			
Crítica ou Sugestão: INSTITUI A POLÍTICA NACIONAL DE CIBERSEGURANÇA (PNCIBER), O SISTEMA NACIONAL DE CIBERSEGURANÇA (SNCIBER) COM A CRIAÇÃO DA AGÊNCIA NACIONAL DE CIBERSEGURANÇA (ANCIBER)			
Resposta: Optou-se por um texto ligeiramente diverso daquele proposto, de forma a uma melhor adequação ao "espírito" da PNCiber.			

Audiência Pública da PNCiber – Contribuições

Responsável: Vanessa Copeti Cravo			
Instituição: ANATEL		**Título:** GTCiber	
Tópico: 03-Disposições Gerais	**Id#:** 270	**Parecer:** 2-Parcialmente Adequada	
Tipo de Contribuição: Alteração Legal	**Artigo:**	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: Necessidade de adequação do conceito de provedores essenciais: grande parte dos serviços regulados não são concessões e a terminologia "operador nacional" não está definida e não há certeza se abarcaria todos os serviços regulados pelas Agências Reguladoras e que correspondem à operação de infraestrutura crítica.			
Resposta: O conceito de operadores foi ajustado.			

Audiência Pública da PNCiber – Contribuições

Responsável: Luca Belli			
Instituição: FGV		**Título:** Professor	
Tópico: 04-Princípios	**Id#:** 166	**Parecer:** 2-Parcialmente Adequada	
Tipo de Contribuição: Alteração Legal	**Artigo:** 5	**Inciso:** 0	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: Um último ponto, eu acho que o Brasil tem realmente a possibilidade de se tornar um pioneiro na definição da cibersegurança. É realmente absurdo constatar, é, algo que é reiterado ao longo do nosso estudo, que o alvo, a principal preocupação da cibersegurança na enorme maioria das políticas, dos marcos legais nacionais são os ativos, não as pessoas. Os ativos são essenciais, mas a principal deveria ser o cidadão. Então não custa nada alterar a definição, colocando que a cibersegurança deveria ser o conjunto de ações voltado à garantir a proteção do cidadão e a confidencialidade, a integridade, e a autenticidade dos ativos. Então, esse é o ponto, que há uma falta enorme de todos os marcos regulatórios precedente. E aí, o Brasil tem a possibilidade de se tornar inovador nessa definição até a nível etimológico. Porquê? A proposta coloca muito bem como primeiro princípio o foco no cidadão, e logo depois destaca que o cidadão é o elo fraco da segurança, o que é verdade. A gente tem a possibilidade de reverter, a gente tem, não a possibilidade, a obrigação de reverter esta tendência, e aí no estudo colocamos justamente a conexão entre a cibersegurança e a soberania digital.			
Resposta: A importância do cidadão, como elemento focal da PNCiber, está expressa no primeiro princípio da política. De outra parte, considerar o cidadão como um "ciberativo", similarmente a hardware, software e dados, parece-nos inapropriado para a condição humana. Não obstante, foi reforçado o foco no cidadão por meio de uma alteração na redação do correspondente princípio da PNCiber.			

Audiência Pública da PNCiber – Contribuições

Responsável: Carlos Baigorri			
Instituição: ANATEL		**Título:** Presidente	
Tópico: 04-Princípios	**Id#:** 27	**Parecer:** 2-Parcialmente Adequada	
Tipo de Contribuição: Alteração Legal	**Artigo:** 5	**Inciso:**	**Parágrafo:**
Texto Original: Art. 5 º. A Política Nacional de Cibersegurança baseia-se nos seguintes princípios: ...			
Crítica ou Sugestão: Ainda com foco na abrangência do marco e dos seus objetivos, a promoção dos direitos humanos e garantias fundamentais deve ser expressamente incluída no rol de princípios.			
Resposta: A proposta melhora o texto, e foi incorporada.			

Audiência Pública da PNCiber – Contribuições

Responsável: Carlos Baigorri			
Instituição: ANATEL		**Título:** Presidente	
Tópico: 04-Princípios	**Id#:** 28	**Parecer:** 2-Parcialmente Adequada	
Tipo de Contribuição: Alteração Infralegal	**Artigo:** 5	**Inciso:**	**Parágrafo:**
Texto Original: Art. 5 º. A Política Nacional de Cibersegurança baseia-se nos seguintes princípios: ...			
Crítica ou Sugestão: Constata-se também a inexistência de qualquer menção à proteção de crianças e adolescentes no ciberespaço, um dos grandes desafios contemporâneos, inquestionavelmente exacerbados com a Pandemia do COVID-19. Nesse ponto, cabe lembrar compromissos brasileiros internacionais, visto que o Brasil aderiu em janeiro de 2022 à Recomendação da OCDE Children in the Digital Environment. Aproveita-se também a oportunidade para compartilhar que a Anatel mobilizou recursos de parceiros (Embaixada do Reino Unido no Brasil e Comitê Gestor da Internet no Brasil - CGI.br) para viabilizar a tradução e diagramação dos materiais da iniciativa da Child Online Protection da União Internacional de Telecomunicação - UIT, a qual conta com diretrizes específicas para elaboradores de políticas públicas. Os materiais estão disponíveis em: https://www.gov.br/anatel/pt-br/consumidor/destaques/publicacoes-orientam-pais-educadores-formuladores-de-politicas-e-industria-sobre-protecao-de-criancas-na-internet			
Resposta: A PNCiber é uma política nacional, e assim foca mais no "o que" do que no "como", até como forma de assegurar sua perenidade. Outrossim, não cabe esse tipo de detalhamento neste instrumento, mas sim em resoluções da Diretoria Colegiada da ANCiber a serem aprovadas pelo CNCiber oportunamente. De outra parte, os instrumentos serão os mesmos utilizados pelas demais agências reguladoras, conforme estipulado no marco regulatório vigente. Esses tópicos serão provavelmente regulados por normatização infralegal.			

Audiência Pública da PNCiber – Contribuições

Responsável: Maxli Barroso Campos			
Instituição: LPTIC/EGN		**Título:** Pesquisador Líder	
Tópico: 05-Objetivos	**Id#:** 187	**Parecer:** 2-Parcialmente Adequada	
Tipo de Contribuição: Alteração Legal	**Artigo:** 6	**Inciso:** 0	**Parágrafo:**
Texto Original: IV - fomentar a articulação do intercâmbio de informações de cibersegurança entre: a) as esferas do governo; b) o setor privado; e c) a sociedade em geral;			
Crítica ou Sugestão: IV - fomentar a articulação do intercâmbio de informações de cibersegurança e efetiva integração entre: a) União, Estados e Municípios; b) Poder Executivo, Legislativo e Judiciário; b) o setor privado; e c) a sociedade em geral; Obs: Destacar o impacto da Política na União, Estados e Municípios irá diminuir a percepção de que todas as ações da política ficarão limitadas apenas ao Governo Federal, tal como ocorre nos dias atuais. Importante destacar que promover a efetividade das ações em cibernética no Brasil irá demonstrar para o mundo que o espaço cibernético no Brasil estará preparado para receber os grandes players da indústria de tecnologia no mundo, sendo estratégico para as ações de Ciência, Tecnologia e Inovação. Por isso o alinhamento entre Cibernética e CT&I acabam convergindo.			
Resposta: O detalhamento das alíneas pode melhorar o texto. De outra parte, o detalhamento do "como" não é cabível numa política, que deve focar no "o que".			

Audiência Pública da PNCiber – Contribuições

Responsável: Osmar Assis do Nascimento Filho			
Instituição: Cidadão		**Título:** Cidadão	
Tópico: 08-SNCiber	**Id#:** 224	**Parecer:** 2-Parcialmente Adequada	
Tipo de Contribuição: Alteração Legal	**Artigo:** 11	**Inciso:**	**Parágrafo:**
Texto Original: Art. 11 . Fica instituído o Sistema Nacional de Cibersegurança que agrega os Poderes da União, dos Estados, do Distrito Federal e dos Municípios, incluindo os Tribunais de Contas e os Ministérios Públicos, o setor privado, instituições de ensino e pesquisa, e demais agentes da sociedade, no que tange às ações de planejamento, execução e coordenação das atividades relacionadas à cibersegurança.			
Crítica ou Sugestão: O que significa "agrega" no âmbito deste artigo? Seria o mesmo que a abrangência, já estabelecida no art. 1º e parágrafos? Recomenda-se a exclusão do artigo, caso se trate da abrangência.			
Resposta: O texto foi alterado para utilizar o termo " congrega".			

Audiência Pública da PNCiber – Contribuições

Responsável: Alan Denilson Lima Costa			
Instituição: ComDCiber		**Título:** Comandante	
Tópico: 09-CNCiber	**Id#:** 5	**Parecer:** 2-Parcialmente Adequada	
Tipo de Contribuição: Inclusão no CNCiber	**Artigo:** 15	**Inciso:** 0	**Parágrafo:**
Texto Original: (...) XVI - três representantes de entidades representativas das infraestruturas críticas;			
Crítica ou Sugestão: Aperfeiçoar o texto (representantes de entidades representativas...); seriam as atuais agências reguladoras, dos setores de infraestruturas críticas? Caso positivo, sugere-se incluir as agências reguladoras de todos os setores, não apenas 03. Justificativa: A presença das demais agências reguladoras (dos atuais 07 setores definidos pelo GSI/PR), daria melhor alinhamento contra as atuais ameaças e tem se mostrado produtivo e sinérgico, como na Cibersecurity & Infrastructure Security Agency (CISA), dos EUA e o Cyber and Infrastructure Security Center, da AUSTRÁLIA; no caso brasileiro, o GSI/PR proporciona um modelo, agora com a efetiva participação da cibernética, com o PL proposto.			
Resposta: Os reguladores de setores com infraestruturas críticas foram incorporados tanto ao CNCiber quanto ao GGCiber.			

Audiência Pública da PNCiber – Contribuições

Responsável: Carlos Baigorri			
Instituição: ANATEL		**Título:** Presidente	
Tópico: 09-CNCiber	**Id#:** 29	**Parecer:** 2-Parcialmente Adequada	
Tipo de Contribuição: Inclusão no CNCiber	**Artigo:** 15	**Inciso:** 0	**Parágrafo:**
Texto Original: (...) XVI - três representantes de entidades representativas das infraestruturas críticas;			
Crítica ou Sugestão: Embora reconheça a importância de todas as infraestruturas críticas e a sua interdependência, a Anatel defende a existência de um assento específico para a Agência no Comitê Nacional de Cibersegurança (CNCiber). A motivação está fundada no fato da Anatel não regular infraestrutura similar aos demais setores com infraestrutura crítica: a Anatel regula o setor que é responsável pela infraestrutura de toda a conectividade sob a qual é existente o ecossistema digital; que tem uma enorme superfície de ataque (redes); que é o principal meio para a disseminação de ameaças; de que todas as outras infraestruturas críticas (serviços essenciais, na terminologia da minuta) dependem; e cujas ações de promoção de cibersegurança tem um enorme impacto no ecossistema. Por fim, a Anatel também tem o mandato de representar o Brasil nos organismos internacionais de telecomunicações, em cujas agendas predominam os debates de cibersegurança. Dessa forma, é natural e necessário que a Agência seja integrantes permanente do CNCiber. Na mesma linha, defende também o seu assento no Gabinete de Gerenciamento de Cibercrises (GGCiber).			
Resposta: Os reguladores de setores com infraestruturas críticas foram incorporados tanto ao CNCiber quanto ao GGCiber.			

Audiência Pública da PNCiber – Contribuições

Responsável: Husani Durans de Jesus			
Instituição: ITI Council		**Título:** Presidente	
Tópico: 09-CNCiber	**Id#:** 72	**Parecer:** 2-Parcialmente Adequada	
Tipo de Contribuição: Inclusão no CNCiber	**Artigo:** 15	**Inciso:** 0	**Parágrafo:**

Texto Original:
(...)
XVI - três representantes de entidades representativas das infraestruturas críticas;

Crítica ou Sugestão:
O Brasil tem um cenário regulatório denso para segurança cibernética e o projeto de lei não menciona ou aborda adequadamente os papéis de várias partes interessadas importantes do governo. O ITI recomenda respeitosamente que o GSI revise o projeto de lei para garantir que as seguintes partes interessadas sejam incluídas no Comitê Nacional de Cibersegurança (CnCiber) e que seus regulamentos sejam consistentes entre si: Agência Nacional de Telecomunicações (ANATEL) A ANATEL é o órgão regulador do setor de telecomunicações, onde as questões de segurança cibernética são um tema inerente. Consequentemente, o ITI acredita que a ANATEL deve ser considerada uma parte interessada relevante e incluída no CnCiber. Adicionalmente, a ANATEL também deveria ter um papel mais dinâmico no diálogo com a ANCiber.
Autoridade Nacional de Proteção de Dados (ANPD) O artigo 46 da Lei Geral de Proteção de Dados (LGPD) estabelece que a ANPD é responsável pelas questões de segurança da informação relacionadas à proteção de dados pessoais. Diante disso, o ITI respeitosamente sugere que o GSI revise o projeto de lei para evitar um possível conflito de autoridades.
Banco Central do Brasil (BC) O BC é responsável por emitir regulamentos para instituições financeiras que operam no Brasil, que incluem a regulamentação de segurança cibernética. Por exemplo, na Resolução 4.893/2021, o BC determinou o conjunto mínimo de requisitos de cibersegurança para a contratação de serviços de nuvem e processamento de dados. Portanto, o ITI respeitosamente sugere que o GSI revise o projeto de lei para evitar um possível conflito de autoridades e inclua o BC na CnCiber.

Resposta:
Os reguladores de setores com infraestruturas críticas foram incorporados tanto ao CNCiber quanto ao GGCiber.

Audiência Pública da PNCiber – Contribuições

Responsável: Luiz Henrique Barbosa da Silva			
Instituição: TELCOMP		**Título:** Representante	
Tópico: 09-CNCiber	**Id#:** 170	**Parecer:** 2-Parcialmente Adequada	
Tipo de Contribuição: Inclusão no CNCiber	**Artigo:** 15	**Inciso:** 0	**Parágrafo:**
Texto Original: (...) XVI - três representantes de entidades representativas das infraestruturas críticas;			
Crítica ou Sugestão: Seria importante que todas as agências existentes integrassem o Conselho. O objetivo do mesmo é primordial no processo de assegurar a integração das ações. Nesse sentido, a proposta seria inserir um novo inciso para prever um representante de cada Agência Reguladora Federal e manter os 3 representantes de infraestruturas críticas mencionando entidades privadas. O que, então, daria ensejo à entidades da iniciativa privada terem representação além das próprias agências não concorrendo com elas no cargo. XVI - três representantes de entidades privadas representativas das infraestruturas críticas Novo inciso: XIX - um representante de cada Agência Federal.			
Resposta: Os reguladores de setores com infraestruturas críticas foram incorporados tanto ao CNCiber quanto ao GGCiber.			

Audiência Pública da PNCiber – Contribuições

Responsável: Maxli Barroso Campos			
Instituição: LPTIC/EGN		**Título:** Pesquisador Líder	
Tópico: 09-CNCiber	**Id#:** 188	**Parecer:** 2-Parcialmente Adequada	
Tipo de Contribuição: Inclusão no CNCiber	**Artigo:** 15	**Inciso:** 0	**Parágrafo:**
Texto Original: (...) XVI - três representantes de entidades representativas das infraestruturas críticas;			
Crítica ou Sugestão: XVI - três representantes de entidades representativas das infraestruturas críticas, sendo obrigatoriamente um representante o setor de telecomunicações (ANATEL?). Obs: Como basicamente o ciber espaço Brasileiro é criado pelos provedores de telecomunicação que integram os demais setores críticos, entendemos que a participação da ANATEL deva ser explicitada.			
Resposta: Os reguladores de setores com infraestruturas críticas foram incorporados tanto ao CNCiber quanto ao GGCiber.			

Audiência Pública da PNCiber – Contribuições

Responsável: João Araújo Monteiro Neto			
Instituição: GETIS/Unifor		**Título:** Pesquisador	
Tópico: 09-CNCiber	**Id#:** 110	**Parecer:** 2-Parcialmente Adequada	
Tipo de Contribuição: Alteração Infralegal	**Artigo:** 15	**Inciso:**	**Parágrafo:** 3
Texto Original: § 3º Os representantes de que tratam os incisos XIV a XVII, bem como seus suplentes, serão nomeados por ato do Presidente da República, permitida a delegação dessa nomeação ao Ministro de Estado Chefe do Gabinete de Segurança Institucional da Presidência da República.			
Crítica ou Sugestão: Deve-se repensar a forma de nomeação dos setores não governamentais. Em vista da preservação do multissetorialismo em sua substância, deve-se pensar em forma de participação dos setores representados na nomeação de seus representantes, para além da formalização da cadeira. Veja-se o exemplo do Comitê Gestor da Internet no Brasil - CGI.br, que tem descrito no seu marco normativo principal (Decreto nº 4.829/2003) a forma de constituição dos representantes dos setores não governamentais e as regras para sua eleição. Necessário, portanto, que a Lei que institui o Comitê Nacional de Cibersegurança apresente os critérios de representação dos setores não governamentais, sob risco de se colocar como um falso mutissetorialismo, sob gerência de um único ator, de caráter governamental.			
Resposta: Foi incluída uma exigência de experiência mínima para os integrantes do CNCiber.			

Audiência Pública da PNCiber – Contribuições

Responsável: Ivanildo de Oliveira da Silva			
Instituição: Cidadão		**Título:** Cidadão	
Tópico: 09-CNCiber	**Id#:** 82	**Parecer:** 2-Parcialmente Adequada	
Tipo de Contribuição: Alteração Legal	**Artigo:** 15	**Inciso:**	**Parágrafo:**
Texto Original: § 3º Os representantes de que tratam os incisos XIV a XVII, bem como seus suplentes, serão nomeados por ato do Presidente da República, permitida a delegação dessa nomeação ao Ministro de Estado Chefe do Gabinete de Segurança Institucional da Presidência da República.			
Crítica ou Sugestão: Sugiro por fim, a inclusão de um parágrafo que mencione os requerimentos mínimos dos integrantes que comporão o comitê, ou seja, não adianta de nada um colegiado composto por pessoas que não possuam conhecimento de segurança da informação. Assim, sugiro inserir conforme a seguir: § 8º Os integrantes indicados a compor o comitê definido no caput deste artigo deverão possuir comprovado conhecimento na área de segurança da informação por meio de cursos oficiais de instituições nacionais ou internacionais de segurança, certificações na área de segurança da informação, pós-graduação na área de segurança da informação ou, experiência em unidade de segurança da informação na área pública ou privada de pelo menos 2 anos.			
Resposta: Foi incluída uma exigência de experiência mínima para os integrantes do CNCiber.			

Audiência Pública da PNCiber – Contribuições

Responsável: Osmar Assis do Nascimento Filho			
Instituição: Cidadão		**Título:** Cidadão	
Tópico: 09-CNCiber	**Id#:** 225	**Parecer:** 2-Parcialmente Adequada	
Tipo de Contribuição: Inclusão no CNCiber	**Artigo:** 15	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: Por que não se incluiu um representante do GSI neste Comitê, se é o órgão supervisor da ANCiber? Por que não há representante fixo do Ministério da Educação no Comitê, uma vez que a atuação educacional é essencial para esta Política (vide competências da ANCiber no art. 18, incisos XXIII, XXV e XXVI) Sugestão: mais um representante da Defesa, totalizando 2, mais um representante do GSI e mais um representante do MDIC. Ou troca-se a adição de representante do MD por representante do MEC. Ainda como terceira via, viabilizar assento a um representante do CGI.br. Com isso, o Executivo supera as instituições científicas, somadas aos demais em pelo menos 1 voto.			
Resposta: A composição do CNCiber e do GGCiber foi alterada.			

Audiência Pública da PNCiber – Contribuições

Responsável: Sarah Melo Martins			
Instituição: Brasscom		**Título:** Representante	
Tópico: 09-CNCiber	**Id#:** 260	**Parecer:** 2-Parcialmente Adequada	
Tipo de Contribuição: Inclusão no CNCiber	**Artigo:** 15	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: As questões de cibersegurança sempre envolvem, em maior ou menor grau, as infraestruturas de telecomunicações. Considerando que a ANATEL é o órgão regulador do setor de telecomunicações, e já possui uma série de iniciativas em termos de certificação de equipamentos e regulamentação específica sobre requisitos de segurança cibernética aplicáveis a tais redes, a Brasscom respeitosamente sugere ao GSI que a Agência seja considerada como uma parte relevante nos processos de discussões sobre cibersegurança, inclusive com um papel mais ativo no diálogo com a Agência Nacional de Cibersegurança (ANCiber) e com participação também no Comitê Nacional de Cibersegurança que se pretende seja criado.			
Resposta: Os reguladores de setores com infraestruturas críticas foram incorporados tanto ao CNCiber quanto ao GGCiber.			

Audiência Pública da PNCiber – Contribuições

Responsável: Luca Belli			
Instituição: FGV		**Título:** Professor	
Tópico: 09-CNCiber	**Id#:** 167	**Parecer:** 2-Parcialmente Adequada	
Tipo de Contribuição: Alteração Legal	**Artigo:**	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: Um ponto essencial é facilitar a sinergia, a cooperação, e a articulação entre as várias agências. Porém, eu acho esse é uma deficiência da, do atual, da atual versão do texto porque se cria um gabinete e um comitê com participação governamental. Eu acho que se esquece de criar uma inclusão forte das agências reguladoras. Eu não concordo que seria demais trazer todas as agências reguladoras. Então, criar um conselho de coordenação, de interação e interagência não seria algo de radicalmente difícil. Isso aí é algo muito inovador. Isso aí é algo que poderia ter sido incluído no comitê mesmo.			
Resposta: As agências reguladoras responsáveis por setores conhecidos como infraestruturas críticas foram incluídas tanto no CNCiber quanto no GGCiber.			

Audiência Pública da PNCiber – Contribuições

Responsável: Carlos Baigorri			
Instituição: ANATEL		**Título:** Presidente	
Tópico: 10-ANCiber	**Id#:** 30	**Parecer:** 2-Parcialmente Adequada	
Tipo de Contribuição: Alteração Legal	**Artigo:** 18	**Inciso:** 0	**Parágrafo:**
Texto Original: VII - promover a definição, a manutenção e a unidade do arcabouço jurídico nacional no campo da cibersegurança, por meio da emissão de pareceres não vinculativos sobre iniciativas legislativas ou regulatórias relativas à cibersegurança, levando em conta os desenvolvimentos internacionais;			
Crítica ou Sugestão: VII - promover a definição, a manutenção e a unidade do arcabouço jurídico nacional no campo da cibersegurança, por meio da emissão de pareceres não vinculativos sobre iniciativas legislativas, levando em conta os desenvolvimentos internacionais; Justificativa: O texto destaca as competências de ações para a promoção de cibersegurança e ciber-resiliência, também mencionando a emissão de pareceres não vinculativos sobre iniciativas regulatórias, a fim de manter a unidade do arcabouço nacional. Embora salutar a interação entre coordenador nacional na matéria e reguladores setoriais, a emissão desses pareceres (sequer mencionando sobre eventual obrigatoriedade) viola a autonomia das Agências Reguladoras (ARs), que devem implementar as políticas públicas nas suas respectivas áreas de competência por meio de políticas regulatórias. Ademais, a existência de um parecer, ainda que não vinculativo de uma autoridade nacional, na prática atrelaria os gestores das Agências Reguladoras ao seu resultado, sob pena de eventual responsabilização dos órgãos de controle, ou mesmo poderia fomentar a judicialização das matérias por terceiros interessados, em caso de adoção de decisão contrária ao parecer.			
Resposta: A proposta melhora o texto e foi atendida. Ressalva-se que a temática da cibersegurança é competência principal da ANCiber, que atuará como coordenadora dessa temática inclusive com as demais agências reguladoras.			

Audiência Pública da PNCiber – Contribuições

Responsável: Carlos Baigorri			
Instituição: ANATEL		**Título:** Presidente	
Tópico: 10-ANCiber	**Id#:** 31	**Parecer:** 2-Parcialmente Adequada	
Tipo de Contribuição: Preoc. ANATEL	**Artigo:** 18	**Inciso:** 0	**Parágrafo:**
Texto Original: XIV - avaliar e certificar produtos e serviços, no tocante à cibersegurança, diretamente ou por meio de parceiros credenciados pela ANCiber;			
Crítica ou Sugestão: Art. 18, XIV - avaliar e certificar produtos e serviços, no tocante à cibersegurança, diretamente ou por meio de parceiros credenciados pela ANCiber, ressalvada a competência de certificação de produtos da Agência Nacional de Telecomunicações (Anatel); Justificativa: Embora certificação em segurança cibernética não se limite ao processo de conformidade de equipamentos de telecomunicações, envolvendo, por exemplo, certificação de produtos de segurança cibernética, cloud, criptografia, entre outros aspectos., a redação genérica do art. 18, XIV, do Anteprojeto da PNCiber causa incerteza quanto à preservação da competência da Agência. Ainda, não fica claro na proposta apresentada qual seria o foco da certificação (processos, software, infraestrutura, entre outros aspectos). A esse respeito, julga-se oportuno que seja dada uma clara sinalização ao mercado do que se pretende ser feito, identificando-se claramente as lacunas regulatórias que precisam ser endereçadas, sob o risco de onerar demasiadamente o setor produtivo, visto que a proposta prevê a arrecadação e aplicação de receitas da ANCiber, sem especificar sua origem.			
Resposta: A proposta melhora o texto e foi atendida, embora num escopo mais amplo de outras agências reguladoras que detenham a competência de certificação de produtos e serviços. Ressalva-se que a temática da cibersegurança é competência principal da ANCiber, que atuará como coordenadora dessa temática inclusive com as demais agências reguladoras.			

Audiência Pública da PNCiber – Contribuições

Responsável: Vanessa Copeti Cravo			
Instituição: ANATEL		**Título:** GTCiber	
Tópico: 10-ANCiber	**Id#:** 271	**Parecer:** 2-Parcialmente Adequada	
Tipo de Contribuição: Preoc. ANATEL	**Artigo:** 18	**Inciso:** 0	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: Deve ser preservada a competência de fiscalização das agências reguladoras, no seu setor, inclusive em matéria de cibersegurança, sob pena de violação das competências setoriais;			
Resposta: A proposta melhora o texto e foi atendida, embora num escopo mais amplo de outras agências reguladoras que detenham a competência de certificação de produtos e serviços. Ressalva-se que a temática da cibersegurança é competência principal da ANCiber, que atuará como coordenadora dessa temática inclusive com as demais agências reguladoras.			

Audiência Pública da PNCiber – Contribuições

Responsável: Carlos Baigorri			
Instituição: ANATEL		**Título:** Presidente	
Tópico: 10-ANCiber	**Id#:** 32	**Parecer:** 2-Parcialmente Adequada	
Tipo de Contribuição: Preoc. ANATEL	**Artigo:** 18	**Inciso:** 0	**Parágrafo:**
Texto Original: XVII - promover, apoiar e coordenar a realização de ciberinspeções regulares nos ciberativos integrantes do Complexo Nacional de Cibersegurança;			
Crítica ou Sugestão: XVII - promover, apoiar e coordenar a realização de ciberinspeções regulares nos ciberativos integrantes do Complexo Nacional de Cibersegurança, levando em conta as ações de fiscalização pertinentes realizadas pelas Agências Reguladoras. Justificativa: O texto traz disposições genéricas sobre a realização de ações para identificação de ciberameaças nos ciberativos do Complexo, que supostamente (relembre-se a complexidade e incerteza das definições trazidas que inovam o ordenamento jurídico) abrangeriam os ativos das prestadoras de serviços de telecomunicações, bem como de auditorias em processos de fiscalização para verificação de descumprimentos dos normativos da ANCiber. Novamente, precisa ser ressalvada a competência da Agência, que possui normativos próprios, os quais buscam implementar as políticas públicas estabelecidas; e que realiza ações de fiscalização e acompanhamento do setor nessa seara.			
Resposta: A proposta foi atendida por meio de uma nova redação do inciso XIV, que resguardou as competências de certificação eventualmente concedidas a outras agências reguladoras.			

Audiência Pública da PNCiber – Contribuições

Responsável: Kathryn Jones			
Instituição: UK-FCDO		**Título:** Chefe de Departamento	
Tópico: 10-ANCiber	**Id#:** 145	**Parecer:** 2-Parcialmente Adequada	
Tipo de Contribuição: Comentário	**Artigo:**	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: Contrastando com alguns outros países, o NCSC do Reino Unido não é um regulador. Isso significa que o NCSC do Reino Unido pode construir confiança com o setor privado de uma maneira que seria muito mais difícil se fosse um regulador. Isso significa que informações confidenciais referentes a incidentes cibernéticos podem ser compartilhadas com nosso NCSC sem que as organizações vítimas sintam que serão punidas. Mais informações sobre como o NCSC gerencia isso – e como ele funciona com os reguladores – podem ser encontradas no site do NCSC através do link abaixo. Observamos que a ANCiber pode ter poderes regulatórios, além de trabalhar em estreita colaboração com vítimas do setor privado de incidentes cibernéticos. Em algumas circunstâncias, isso pode funcionar como um desincentivo para as empresas cooperarem com a ANCiber, por isso recomendamos que isso seja cuidadosamente considerado.			
Resposta: Esse é um outro ponto em que a cultura institucional brasileira é distinta daquela britânica, sendo o modelo de agências reguladoras bastante bem assimilado pelo institucionalismo histórico brasileiro. A questão de um eventual desincentivo é tratada sob a ótica de que o condão regulador da ANCiber não deve ser usado como fonte primária de sua autoridade, que pretende-se seja mais pautada nos mecanismos de cooperação. Sob essa ótica, pretende-se que o primeiro mecanismo seja sempre o do Ajustamento de Conduta estabelecido em comum acordo entre a ANCiber e seus jurisdicionados, fiscalizado em seu cumprimento pela agência. Sanções administrativas e multas somente são esperadas em casos renitentes de descumprimento de normativos, ou em casos de omissão ou de negligência. Não obstante, a experiência brasileira recente mostra que a falta da capacidade de impor tais sanções, com o trabalho pautado estritamente na confiança e colaboração, não tem funcionado adequadamente, sendo necessário dispor de instrumentos que viabilizem "fazer valer" os normativos, nos caso extremos.			

Audiência Pública da PNCiber – Contribuições

Responsável: Arthur Pereira Sabbat			
Instituição: ANPD		**Título:** Diretor	
Tópico: 11-GGCiber	**Id#:** 20	**Parecer:** 2-Parcialmente Adequada	
Tipo de Contribuição: Alteração Legal	**Artigo:** 21	**Inciso:** 0	**Parágrafo:**
Texto Original: VI - determinar ao Diretor-Geral da ANCiber que notifique o Comitê Nacional de Cibersegurança, em caráter emergencial, a ocorrência de uma cibercrise considerada relevante.			
Crítica ou Sugestão: Ao final do rol de competências do Gabinete de Gerenciamento de Cibercrises, no art. 21, surge a expressão "cibercrise considerada relevante". A expressão "cibercrise relevante" também surge no inciso X do art. 14. Desse modo, com o fim de clarificar a expressão, e melhor ensejar sua aplicabilidade, sugere-se a inserção, ao final do art. 21, de um parágrafo único para explicar a abrangência da expressão em lide. Poderia ser algo como: "Parágrafo único. Considera-se cibercrise relevante aquela que..."			
Resposta: A proposta melhora o texto, e a definição de cibercrise foi incorporada no âmbito do Art. 4.			

Audiência Pública da PNCiber – Contribuições

Responsável: Luiz Henrique Barbosa da Silva			
Instituição: TELCOMP		**Título:** Representante	
Tópico: 11-GGCiber	**Id#:** 171	**Parecer:** 2-Parcialmente Adequada	
Tipo de Contribuição: Inclusão no GGCiber	**Artigo:** 22	**Inciso:**	**Parágrafo:** 4
Texto Original: § 4º O Gabinete reunir-se-á extraordinariamente, mediante convocação de seu presidente, para reuniões de caráter deliberativo em situações de crises originadas por ciberincidentes relevantes.			
Crítica ou Sugestão: incluir novo inciso para permitir a participação de representantes de Agências governamentais federais quando envolvidas na crise. Art. 22. O Gabinete de Gerenciamento de Cibercrises será composto por: Um representante de cada Agência Federal envolvida em determinado evento de crise §4º O Gabinete reunir-se-á extraordinariamente, mediante convocação de seu presidente, para reuniões de caráter deliberativo em situações de crises potenciais, iminentes ou originadas por ciberincidentes relevantes, quando será admitida a participação de um representante de Agências Federais envolvidas no evento da crise.			
Resposta: Os reguladores de setores com infraestruturas críticas foram incorporados tanto ao CNCiber quanto ao GGCiber. A despeito disso, está previsto o convite a outros participantes conforme a necessidade ou conveniência.			

Audiência Pública da PNCiber – Contribuições

Responsável: Carlos Baigorri			
Instituição: ANATEL		**Título:** Presidente	
Tópico: 11-GGCiber	**Id#:** 33	**Parecer:** 2-Parcialmente Adequada	
Tipo de Contribuição: Preoc. ANATEL	**Artigo:** 22	**Inciso:**	**Parágrafo:**
Texto Original: Art. 22 . O Gabinete de Gerenciamento de Cibercrises será composto por: ...			
Crítica ou Sugestão: Embora reconheça a importância de todas as infraestruturas críticas e a sua interdependência, a Anatel defende a existência de um assento específico para a Agência no Comitê Nacional de Cibersegurança (CNCiber). A motivação está fundada no fato da Anatel não regular infraestrutura similar aos demais setores com infraestrutura crítica: a Anatel regula o setor que é responsável pela infraestrutura de toda a conectividade sob a qual é existente o ecossistema digital; que tem uma enorme superfície de ataque (redes); que é o principal meio para a disseminação de ameaças; de que todas as outras infraestruturas críticas (serviços essenciais, na terminologia da minuta) dependem; e cujas ações de promoção de cibersegurança tem um enorme impacto no ecossistema. Por fim, a Anatel também tem o mandato de representar o Brasil nos organismos internacionais de telecomunicações, em cujas agendas predominam os debates de cibersegurança. Dessa forma, é natural e necessário que a Agência seja integrantes permanente do CNCiber. Na mesma linha, defende também o seu assento no Gabinete de Gerenciamento de Cibercrises (GGCiber).			
Resposta: Os reguladores de setores com infraestruturas críticas foram incorporados tanto ao CNCiber quanto ao GGCiber.			

Audiência Pública da PNCiber – Contribuições

Responsável: Vanusa Menditi Calegario			
Instituição: Petrobras		**Título:** Servidora	
Tópico: 11-GGCiber	**Id#:** 279	**Parecer:** 2-Parcialmente Adequada	
Tipo de Contribuição: Inclusão no GGCiber	**Artigo:** 22	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: Incluir na lista de composição do gabinete de gerenciamento de Cibercrises: representantes de entidades representativas das infraestruturas críticas.			
Resposta: A proposta foi contemplada pela inclusão no GGCiber das agências reguladoras de infraestruturas críticas.			

Audiência Pública da PNCiber – Contribuições

Responsável: Leonardo Rodrigo Ferreira			
Instituição: SGD		**Título:** Diretor	
Tópico: 13-E-Ciber	**Id#:** 157	**Parecer:** 2-Parcialmente Adequada	
Tipo de Contribuição: Alteração Legal	**Artigo:** 26	**Inciso:**	**Parágrafo:**
Texto Original: Art. 26 . A Estratégia Nacional de Cibersegurança ("Estratégia") objetiva criar as melhores condições para que o País possa se antecipar às ciberameaças e aproveitar as oportunidades presentes e futuras no setor cibernético.			
Crítica ou Sugestão: Sugerimos definir a sigla ENCiber para a Estratégia Nacional de Cibersegurança. Art. 26 . A Estratégia Nacional de Cibersegurança - ENCiber objetiva criar as melhores condições para que o País possa se antecipar às ciberameaças e aproveitar as oportunidades presentes e futuras no setor cibernético.			
Resposta: A sugestão de adoção de uma sigla para simplificar a legibilidade do texto foi acatada. No entanto, a opção foi pelo nome e-Ciber, já consolidado e de maior apelo popular.			

Audiência Pública da PNCiber – Contribuições

Responsável: Leonardo Rodrigo Ferreira			
Instituição: SGD		**Título:** Diretor	
Tópico: 13-E-Ciber	**Id#:** 158	**Parecer:** 2-Parcialmente Adequada	
Tipo de Contribuição: Alteração Legal	**Artigo:** 27	**Inciso:**	**Parágrafo:** 0
Texto Original: Art. 27 . A Estratégia deverá, no âmbito da cibersegurança: ... Parágrafo único. A Estratégia será atualizada quadrienalmente.			
Crítica ou Sugestão: Considerando o dinamismo das ameaças e vulnerabilidades no ambiente cibernético, ressaltamos a necessidade de a ENCiberser atualizada sempre que for necessário em decorrências de novas ciberameças e vulnerabilidades que afetem o ambiente cibernético. Art. 27 . A ENCiber deverá, no âmbito da cibersegurança: I - identificar os principais desafios; II - definir os eixos estruturantes; III - designar os objetivos estratégicos; e IV - estabelecer as ações estratégicas. Parágrafo único. A ENCiber será atualizada quadrienalmente ou sempre que existir qualquer tipo de mudança significativa no cenário de ciberameaças e de vulnerabilidades que possa afetar cibersegurança nacional.			
Resposta: Optou-se por um texto ligeiramente diverso daquele proposto, de forma a uma melhor adequação ao "espírito" da PNCiber.			

Audiência Pública da PNCiber – Contribuições

Responsável: Jeferson Fued Nacif			
Instituição: MCom		**Título:** Servidor	
Tópico: 18-ANCiber-Organização	**Id#:** 102	**Parecer:** 2-Parcialmente Adequada	
Tipo de Contribuição: Alteração Legal	**Artigo:**	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: Taxas de fiscalização devem ter previsão legal e instrumento específico determinando seus valores, como é o Fistel arrecadado pela Anatel.			
Resposta: O texto foi alterado para incorporar o detalhamento das taxas previstas.			

Audiência Pública da PNCiber – Contribuições

<table>
<tr><td colspan="4">Responsável: Carlos Baigorri</td></tr>
<tr><td colspan="2">Instituição: ANATEL</td><td colspan="2">Título: Presidente</td></tr>
<tr><td>Tópico: 19-ANCiber-Pessoal</td><td>Id#: 34</td><td colspan="2">Parecer: 2-Parcialmente Adequada</td></tr>
<tr><td>Tipo de Contribuição: Alteração Legal</td><td>Artigo: 30</td><td>Inciso:</td><td>Parágrafo:</td></tr>
<tr><td colspan="4">Texto Original:
Art. 30 . Fica a Agência Nacional de Cibersegurança autorizada a requisitar servidores de qualquer órgão ou entidade da Administração Pública Federal.
§1º O número máximo de servidores requisitados é limitado aos quantitativos anuais dispostos no ANEXO II.
§2º As requisições são irrecusáveis.
§3º As requisições aplicam-se aos servidores, aos militares e aos empregados.
§4º As requisições podem durar até 31 de dezembro de 2027 ou até o prazo de um ano a contar da posse dos primeiros aprovados em concurso público para o preenchimento do quadro de pessoal próprio da Agência Nacional de Cibersegurança, o que ocorrer primeiro.</td></tr>
<tr><td colspan="4">Crítica ou Sugestão:
Um ponto de preocupação para a Agência e seu quadro de servidores é a prerrogativa especial de requisição de servidores, concedendo à ANCiber uma prerrogativa de irrecusabilidade, que atualmente é limitada (por exemplo, concedida aos órgãos da Presidência da República). Essa prerrogativa pode impactar no quadro já defasado da Agência, impactando no cumprimento da missão institucional da Anatel, inclusive nas atividades relacionadas à segurança cibernética. Nessa esteira, sugere-se a harmonização com as regras já existentes referentes à cessão de servidores no âmbito da Administração Pública Federal.
Ressalta-se que tal preocupação reside no fato de que a Autoridade Nacional de Proteção de Dados, por exemplo, acaba por requerer diversos servidores da Anatel, até de forma natural, em razão da especialização dos servidores com os temas do ambiente digital, mas também com regulação, análise de impacto regulatório, agenda regulatória, acompanhamento, fiscalização e controle de obrigações, dentre outros.</td></tr>
<tr><td colspan="4">Resposta:
Observamos que o Artigo 30, do Anexo I do anteprojeto, ao tempo em que faculta a possibilidade da ANCiber requisitar pessoal da administração pública federal (APF), impõe limites quantitativos e temporais restritos para tal. Isso reflete uma materialização do reconhecimento de que há uma severa carência de pessoal de cibersegurança no Brasil, e em particular na APF. Como deixa claro o §4º, tão logo ocorra o preenchimento do quadro de pessoal próprio da ANCiber as requisitados retornarão a seus órgãos de origem.
Igualmente relevante é a existência do Art. 31, que permite à ANCiber contratar profissionais temporários para o preenchimento de seu quadro, de forma a reduzir a necessidade de requisição de profissionais.
Outrossim, fica clara a intenção de se produzir o menor impacto possível na APF.
Entretanto, não seria uma atitude responsável excluir a possibilidade de requisição de pessoal, sob risco de inviabilização da ANCiber.
De toda sorte, revisamos o texto do anteprojeto de forma a colocar limitações ainda mais severas às requisições, no melhor espírito de cooperação e compreensão das dificuldades apontadas pela Anatel e pelo ComDCiber.</td></tr>
</table>

Audiência Pública da PNCiber – Contribuições

Responsável: Leonardo Rodrigo Ferreira			
Instituição: SGD		**Título:** Diretor	
Tópico: 24-Decreto ANCiber	**Id#:** 159	**Parecer:** 2-Parcialmente Adequada	
Tipo de Contribuição: Alteração Legal	**Artigo:** 3	**Inciso:**	**Parágrafo:**
Texto Original: Art. 3 º. A ANCiber tem a seguinte estrutura organizacional: I - Diretoria Colegiada; II - Secretaria-Geral; III - Procuradoria Federal Especializada; IV - Ouvidoria; V - Auditoria Interna; VI - Corregedoria; VII - Inteligência; VIII - Superintendências; e IX - Gerências.			
Crítica ou Sugestão: Ao analisarmos as competências das unidades citadas pelo art. 3º, não localizamos unidade com competência específica de execução de fiscalização. Dessa forma, é fundamental esse destaque nas competências destacadas pelo documento ou, no que couber, definir unidade específica na estrutura organização para operacionalização das fiscalizações.			
Resposta: Os anteprojetos de estruturas regimentais serão adaptados para refletirem as alterações propostas na Audiência Pública, posto que essas afetaram a estrutura da PNCiber.			

Audiência Pública da PNCiber – Contribuições

Responsável: Carlos Baigorri			
Instituição: ANATEL		**Título:** Presidente	
Tópico: 24-Decreto ANCiber	**Id#:** 35	**Parecer:** 2-Parcialmente Adequada	
Tipo de Contribuição: Alteração Legal	**Artigo:**	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: Embora a minuta da PNCiber e anexos não abordem o detalhamento da estrutura regimental da ANCiber, cabe apontar que a minuta do Anexo I do Anteprojeto de Decreto que instala o Comitê Nacional de Cibersegurança, o Gabinete de Gestão de Cibercrises, a Agência Nacional de Cibersegurança, e aprova suas Estruturas Regimentais, prevê Superintendências. Por outro lado, a apresentação do GSI na Audiência Pública assinalou a estrutura da ANCiber composta de Diretorias. Ademais, nas cinco diretorias apresentadas nota-se a inexistência de estrutura específica de acompanhamento e controle de obrigações. Na experiência da Anatel, a existência de estrutura específica justifica-se pela relevância, complexidade e necessidade de acompanhamento junto a todos setores e atores. Ainda, é importante refletir se tal estrutura precisa estar prevista no Decreto ou se pode ficar a cargo da definição pela própria Agência, em seu Regimento Interno. Cita-se como exemplo o caso da Anatel, cujo Regulamento, aprovado pelo Decreto nº 2.338, de 7 de outubro de 1997, trouxe inicialmente um rol mínimo de Superintendências a constarem em sua estrutura (art. 61). Com a evolução e o tempo, percebeu-se que, dada a dinâmica envolvida, tal estrutura deveria ser aprovada e atualizada pela própria Agência, em seu Regimento Interno. Neste sentido, em 2001, por meio do Decreto nº 3.873, tal artigo 61 foi ajustado na linha de permitir essa maior dinamicidade.			
Resposta: A estrutura da ANCiber, tal qual pensada no GSI durante a elaboração do anteprojeto, prevê 5 diretorias, cada uma com 2 a 4 superintendências, as quais encerram gerências. A apresentação da minuta do decreto demonstra a intenção do GSI de dar mais transparência ao processo. Mas, como bem observa a ANATEL, não contempla o detalhamento da estrutura organizacional da ANCiber, o qual aliás, pretende-se que seja detalhado por meio de uma Resolução da primeira Diretoria da ANCiber. Isso posto, informamos que a intenção corrente é a de o orgão de acompanhamento de obrigações a que se refere a ANATEL seja parte da Diretoria de Regulação da ANCiber, a qual disporia de uma Superintendência de Regulação (onde haverá uma Gerência de Coordenação Interagências, tema de outra preocupação demonstrada pela Anatel) e uma Superintendência de Fiscalização, que encerra uma Gerência de Ajustamento, responsável pelo acompanhamento e controle de obrigações. Não obstante, pretende-se uma revisão da minuta do decreto apresentada à luz das alterações decorrentes das sugestões apresentadas na Audiência Pública.			

Audiência Pública da PNCiber – Contribuições

Responsável: Carlos Baigorri			
Instituição: ANATEL		**Título:** Presidente	
Tópico: 24-Decreto ANCiber	**Id#:** 36	**Parecer:** 2-Parcialmente Adequada	
Tipo de Contribuição: Alteração Legal	**Artigo:**	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: VIII - Ciberativos, Serviços Essenciais e Infraestrutura Crítica Por fim, a Agência também considera louvável a tentativa de afastamento do desafiador conceito de infraestrutura crítica, com a utilização do conceito de "ciberativo" e "serviços essenciais". No entanto, considerando a tradição já existente nos normativos (PNSIC, ENSIC e PLANSIC) e instituições brasileiras, sugere-se o retorno à utilização do conceito de infraestrutura crítica. Justamente pelo abandono do conceito de infraestrutura crítica, a minuta traz a ideia dos serviços essenciais e provedores de serviços essenciais. Essa última terminologia traz dúvidas sobre a abrangência, visto que muito serviços essenciais (por exemplo, serviços de telecomunicações) não são objeto de concessão. Ademais, também não está definido o que seria um operador nacional. Assim, não há clareza sobre o escopo e se todas as infraestruturas críticas detidas e operadas pelo setor privado estariam abarcadas na PNCiber.			
Resposta: A explicação da motivação para a adoção de serviços essenciais em oposição a infraestruturas críticas encontra-se no documento Apresentação do Projeto, seção 3.3. Ademais, essa lógica se coaduna com a evolução observada na Europa (NIS2) e em Israel, grandes centros de cibersegurança mundiais. No tocantre aos "operadores", o art. 4 foi ajustado.			

Audiência Pública da PNCiber – Contribuições

Responsável: Maxli Barroso Campos			
Instituição: LPTIC/EGN		**Título:** Pesquisador Líder	
Tópico: 00-Apresentação do Projeto	**Id#:** 189	**Parecer:** 3-Inadequada	
Tipo de Contribuição: Alteração Legal	**Artigo:**	**Inciso:**	**Parágrafo:** 0

Texto Original:
Estabelecimento de um modelo centralizado de governança no âmbito nacional, por meio da criação de um Sistema Nacional de Cibersegurança. Essa ação reflete uma das recomendações do Senado, de 2014.

Crítica ou Sugestão:
Em relação à "governança no âmbito nacional" do setor cibernético, entende-se que seria necessário mencionar como seria o papel dos seguintes atores:
- CGI.br - Comitê Gestor da Internet no Brasil; - CTIR.Gov - Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo (a presente exposição de motivos de política menciona o CTIR.Br);
- Rede Federal de Gestão de Incidentes Cibernéticos (Decreto n. 10.748, de 16 de julho de 2021);
- Conselho Nacional de Proteção de Dados, organismo consultivo vinculado à Autoridade Nacional de Proteção de Dados (ANPD) (interação com a LGPD);
- ITI - Instituto de Tecnologia da Informação, responsável pelo ICP Brasil: Infraestrutura de Chaves públicas brasileira;
- Agência Nacional de Telecomunicações (Anatel) Obs.: Conforme mencionado no site da ANATEL (disponível em: https://www.gov.br/anatel/pt-br/assuntos/seguranca-cibernetica), "A segurança cibernética é agenda prioritária da Agência Nacional de Telecomunicações (Anatel) e motivou a edição do Regulamento de Segurança Cibernética aplicada ao Setor de Telecomunicações e do Ato de Requisitos de Segurança Cibernética para Equipamentos para Telecomunicações.".

Resposta:
A relação com o CGI já se encontra definida no Art. 1 º, § 2º do anteprojeto.
A relação com o CTIR Gov já se encontra definida no Art. 41, § 2º.
A relação com a Rede Federal de Gestão de Incidentes Cibernéticos (REGIC) já se encontra definida no mesmo Art. 41, que explicita os impactos do Projeto de Lei no tocante ao Decreto 10.748.
A relação com a LGPD, e assim com a ANPD e o Conselho Nacional de Proteção de Dados, foi estabelecida já no Art. 1 º, § 1º, no Art. 15, inciso XIV, no Art. 22, inciso XIV e no Art. 16.
Não há necessidade de estabelecimento de mencionar o papel do ITI uma vez que o mesmo não é afetado pelo anteprojeto, permanecendo inalterado.
No tocante às agências reguladoras, o entendimento expresso no anteprojeto é o de que haverá uma coordenação, pela ANCiber, das atividades de regulação da Cibersegurança com as atividades específicas dos reguladores setoriais das diversas áreas dos diversos poderes. A visão da Anatel da cibersegurança como "agenda prioritária" é muito bem recebida pelo GSI, assim como a priorização da cibersegurança por qualquer outro agente regulador setorial. A proposta do PNCiber é de que a ANCiber coordene as ações de todos esses agentes setoriais, como explicitado no anteprojeto. Isso está explicitado no Art. 18, inciso XXXVI, que estabelece que é competência da ANCiber "articular-se com as autoridades reguladoras públicas para exercer suas competências em setores específicos de atividades econômicas e governamentais sujeitas à regulação".
Sem prejuízo disso, o texto foi alterado para contemplar a partcipação das agências reguladoras ligadas a infraestruturas críticas no CNCiber e no GGCiber.

Audiência Pública da PNCiber – Contribuições

Responsável: Núcleo de Pesquisa em Concorrência, Política Pública, Inovação e Tecnologia (Comppit)			
Instituição: FGV		**Título:** Pesquisador	
Tópico: 00-Apresentação do Projeto	**Id#:** 215	**Parecer:** 3-Inadequada	
Tipo de Contribuição: Comentário	**Artigo:**	**Inciso:**	**Parágrafo:** 0

Texto Original:

Crítica ou Sugestão:

A apresentação do anteprojeto (item 3.2) explica que o projeto foca em serviços essenciais, transversais a diferentes setores, em detrimento da noção de Infraestruturas Críticas (IC). Nos termos do art. 4º, inc. XXI, a noção de serviço essencial abarca todos os serviços que atendem ambas as seguintes condições: (i) seu mau funcionamento deve ser prejudicial à segurança nacional e (ii) deste serviço deve depender função essencial do Estado ou prestação de serviço imprescindível para manter atividades "fundamentais aos interesses do Estado". O anteprojeto carece de critérios objetivos mais rígidos para determinar essencialidade de serviço, ao que a noção de IC pode contribuir. Identificar setores críticos como eixos estruturantes não significa considerar setores inteiros como IC: na realidade, seria apenas a primeira etapa de uma definição de IC. Conforme metodologia apontada pela Agência da União Europeia de Cibersegurança (ENISA), a definição de IC ocorre em três estágios, em linhas gerais: (i) a identificação de setores críticos, para então (ii) reconhecer em cada um deles serviços críticos, nos quais (iii) se identificam ativos e serviços-base críticos. A proteção legal da IC deve se ocupar dessa terceira categoria. Exemplo desse modelo é a Lei espanhola nº 8/2011, de proteção de infraestrutura crítica. Nela, entende-se que identificar IC deve partir da definição de setores estratégicos, que consistem em áreas garantidoras do exercício da autoridade do Estado e da segurança nacional. Anexos, a lei elenca como setores estratégicos a administração pública, o espaço, as indústrias nuclear e química, as instalações de investigação, água, energia, saúde, tecnologias de informação e comunicação, transporte, alimentação e os sistemas financeiro e tributário.

Conforme a metodologia legal espanhola, diante dos setores estratégicos, a identificação deve se tornar mais específica, reconhecendo em cada setor serviços essenciais, isto é, aqueles necessários à manutenção de funções sociais básicas ou do funcionamento de instituições públicas. Elencados os serviços essenciais, a preocupação deve se focar então na infraestrutura estratégica - o aparato tanto físico quanto tecnológico de que dependem os serviços em questão. Finalmente, a IC é entendida como a parcela da infraestrutura estratégica cujo bom funcionamento é crucial aos serviços essenciais, sendo necessariamente insubstituível. Fica claro, portanto, que a adoção do paradigma de IC tem a capacidade de trazer especificidade - e não mais vagueza - à proteção de serviços essenciais.

Mais do que isso, incluir IC como parte central do modelo promoveria harmonização em relação recente Plano Nacional de Segurança de Infraestruturas Críticas (decreto nº 11.200/2022), que remonta à Estratégia Nacional de Segurança prevista no Decreto nº 10.222/2020. O Plano Nacional, em seu ponto 4, determina a elaboração de planos setoriais voltados à segurança de IC, em se tratando de atividades consideradas críticas (águas, energia, transporte, comunicações, finanças, biossegurança e bioproteção, e defesa). O decreto atribui a ministérios específicos a função de elaboração de tais planos. Caso houvesse no anteprojeto de lei orientações quanto à IC, isso seria relevante também a fim de informar e possivelmente parametrizar a atividade de cada ministério.

Resposta:

A PNCiber é uma política nacional, e assim foca mais no "o que" do que no "como", até como forma de assegurar sua perenidade. Outrossim, não cabe esse tipo de detalhamento neste instrumento, mas

sim em resoluções da Diretoria Colegiada da ANCiber a serem aprovadas pelo CNCiber oportunamente.
De outra parte, os instrumentos serão os mesmos utilizados pelas demais agências reguladoras, conforme estipulado no marco regulatório vigente.

Audiência Pública da PNCiber – Contribuições

Responsável: Alexandro de Oliveira Paula			
Instituição: Telebras		**Título:** Servidor	
Tópico: 02-PNCiber-Geral	**Id#:** 8	**Parecer:** 3-Inadequada	
Tipo de Contribuição: Alteração Infralegal	**Artigo:**	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: Que seja proposta uma política incisiva e rígida, dentro do referido Plano, sobre avaliação de ataques que envolvam Engenharia Social. Como é de conhecimento do GSI e demais profissionais em Segurança Cibernética, muitas das brechas inerentes à ataques são oriundas de falha humana. Ataques de Phishing, Pharming, Spoofing, entre outros, dependem de Engenharia Social. Uma abordagem com sistemas de processos (ex.: uso de PDCA e SWOT, de forma obrigatória) contra Engenharia Social, possivelmente mitigaria muitos ataques de baixa e média complexidades;			
Resposta: A sugestão foi anotada para implementação oportuna, por meio dos instrumentos infra legais aplicáveis.			

Audiência Pública da PNCiber – Contribuições

Responsável: Alexandro de Oliveira Paula			
Instituição: Telebras		**Título:** Servidor	
Tópico: 02-PNCiber-Geral	**Id#:** 9	**Parecer:** 3-Inadequada	
Tipo de Contribuição: Alteração Infralegal	**Artigo:**	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: Sugiro que seja dada atenção, no referido Plano, à ações contra ataques DDoS. Como sabem, este ataque é o principal no que concerne à queda de sistemas, principalmente para serviços públicos.			
Resposta: A sugestão foi anotada para implementação oportuna, por meio dos instrumentos infra legais aplicáveis.			

Audiência Pública da PNCiber – Contribuições

Responsável: Alexandro de Oliveira Paula			
Instituição: Telebras		**Título:** Servidor	
Tópico: 02-PNCiber-Geral	**Id#:** 10	**Parecer:** 3-Inadequada	
Tipo de Contribuição: Alteração Infralegal	**Artigo:**	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: Independente dos modelos europeus (UIT, NIS2, ...), sugiro que o plano abarque outras formas, mais específicas, de análise de ambiente. Sugiro que seja inserida cláusulas de análise de risco personalizada, para cada ambiente;			
Resposta: A sugestão foi anotada para implementação oportuna, por meio dos instrumentos infra legais aplicáveis.			

Audiência Pública da PNCiber – Contribuições

Responsável: Alexandro de Oliveira Paula			
Instituição: Telebras		**Título:** Servidor	
Tópico: 02-PNCiber-Geral	**Id#:** 11	**Parecer:** 3-Inadequada	
Tipo de Contribuição: Alteração Infralegal	**Artigo:**	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: Concordo com os dados referentes ao Ramsonware. Autores recentes sugerem que seja dada atenção ao Backup Incremental no referido Plano. Fazer com que os participantes do sistema do plano atualizem seus backups pode ser uma premissa para proteção contra ataques de Ramsonware. A TELEBRAS, por exemplo, possui uma estrutura de backup de missão crítica em seu data center, de TIER IV.			
Resposta: A sugestão foi anotada para implementação oportuna, por meio dos instrumentos infra legais aplicáveis.			

Audiência Pública da PNCiber – Contribuições

Responsável: Alexandro de Oliveira Paula			
Instituição: Telebras		**Título:** Servidor	
Tópico: 02-PNCiber-Geral	**Id#:** 12	**Parecer:** 3-Inadequada	
Tipo de Contribuição: Alteração Infralegal	**Artigo:**	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: Quanto à segurança cibernética em sistema elétricos, concordo com a ponderação da criticidade de segurança para sistemas eletromecânicos. Porém, lembro que os parques de Smart Grids têm crescido no Brasil. Fui profissional de automação em Subestações elétricas digitais. Seria interessante ler alguns artigos de minha autoria sobre segurança em Smart Grids. Seguem os links: "Uma arquitetura de automação adaptada para Smart Grids contra ataques cibernéticos" - https://repositorio.unb.br/handle/10482/44132 "STRAYER: a Smart Grid adapted automation Architecture against cyberattacks" - https://www.sciencedirect.com/user/error/ATP-2?pii=S221421262200076X			
Resposta: A sugestão foi anotada para implementação oportuna, por meio dos instrumentos infra legais aplicáveis.			

Audiência Pública da PNCiber – Contribuições

Responsável: Arthur Pereira Sabbat			
Instituição: ANPD		**Título:** Diretor	
Tópico: 02-PNCiber-Geral	**Id#:** 21	**Parecer:** 3-Inadequada	
Tipo de Contribuição: Preoc. ANPD	**Artigo:**	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: Em abstrato, a ANPD ressalta a importância de que, em todas as discussões que envolvam o PL em si, e, de modo específico, as competências da ANCiber, tenha-se em mente a constante preocupação em não haver justaposição de atribuições com a Autoridade Nacional de Proteção de Dados (ANPD), e de disposições do PL com a LGPD. Para tanto, em nome de maior contribuição, destaca-se a relevância de que haja participação da Autoridade por ocasião das mencionadas discussões, tanto no âmbito do Executivo, quanto no âmbito do Legislativo.			
Resposta: A sugestão foi anotada para implementação oportuna, por meio dos instrumentos infra legais aplicáveis.			

Audiência Pública da PNCiber – Contribuições

Responsável: Estela Aranha			
Instituição: MJSP		**Título:** Assessora	
Tópico: 02-PNCiber-Geral	**Id#:** 57	**Parecer:** 3-Inadequada	
Tipo de Contribuição: Comentário	**Artigo:**	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: A questão do Comitê de Crise é uma questão importante, mas ele tem alguns requisitos que seria interessante ter essa abertura para essa imprevisibilidade dessas novas ameaças.			
Resposta: O GGCiber ("Comitê de Crise") prevê a possibilidade de convite a não-membros conforme o interesse e a necessidade no tocante à crise em andamento, o que confere flexibilidade ao ente diante da imprevisibilidade das novas ameaças.			

Audiência Pública da PNCiber – Contribuições

Responsável: Estela Aranha			
Instituição: MJSP		**Título:** Assessora	
Tópico: 02-PNCiber-Geral	**Id#:** 58	**Parecer:** 3-Inadequada	
Tipo de Contribuição: Comentário	**Artigo:**	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: Outro ponto super importante que a gente ressalta, que seria o papel central desse novo órgão ou dessa nova instituição é a questão da autonomia. A Autonomia Nacional em relação a cybersegurança, liderar o desenvolvimento tecnológico nesta área e de toda a cadeia de suprimentos digitais.			
Resposta: A escolha do modelo de Autarquia Especial e agência reguladora para a ANCiber teve como principal fator justamente a autonomia. De outra parte, a PNCiber prevê diversos instrumentos de fomento voltados à inserção do País na cadeia global de valor de cibersegurança, por meio de estímulos à pesquisa, desenvolvimento e inovação nacionais sem, no entanto, criar barreiras protecionistas que possam dificultar o acesso ao estado da arte da tecnologia disponível no mercado mundial de produtos e serviços de cibersegurança.			

Audiência Pública da PNCiber – Contribuições

Responsável: Husani Durans de Jesus			
Instituição: ITI Council		**Título:** Presidente	
Tópico: 02-PNCiber-Geral	**Id#:** 73	**Parecer:** 3-Inadequada	
Tipo de Contribuição: Alteração Legal	**Artigo:**	**Inciso:**	**Parágrafo:**
Texto Original:			

Crítica ou Sugestão:

O ITI gostaria de recomendar enfaticamente que o GSI deixe claro que nenhuma das disposições do projeto de lei deve ser interpretada como um mandato para usar tecnologia nacional ou armazenamento local de dados, pois isso entraria em conflito inadvertidamente com os objetivos do projeto de lei de garantir a confidencialidade, integridade, autenticidade e disponibilidade de ciberativos de interesse da sociedade brasileira.

Manter e aumentar a capacidade de desenvolver tecnologias-chave e garantir sua disponibilidade no futuro é uma preocupação legítima e um objetivo inquestionável de qualquer governo. A indústria de tecnologia reconhece os sinceros objetivos de interesse público e deseja ser um parceiro ativo e construtivo do Brasil na consecução desses objetivos. No entanto, essa abordagem pode levar erroneamente a uma falsa premissa de que equipamentos e tecnologias nacionais devem ser priorizados em relação aos estrangeiros, o que poderia aumentar o custo e atrasar a disponibilidade destes últimos. Vale ressaltar que o ecossistema da Internet é uma infraestrutura interconectada digital e global, onde riscos e ameaças estão em constante evolução. Isso significa que as soluções e os esforços de segurança cibernética devem ser igualmente dinâmicos, altamente interoperáveis e adaptáveis, buscando enfrentar as ameaças em constante mudança enfrentadas por essas novas tecnologias. Portanto, as soluções de segurança cibernética não devem ser priorizadas simplesmente porque são produzidas localmente, mas porque são mais efetivas e estão alinhadas com as melhores práticas e padrões internacionais, independentemente de onde foram desenvolvidas ou fabricadas.

Embora reconheçamos que o projeto de lei proposto não obriga o uso de produtos, serviços ou infraestrutura locais, gostaríamos de destacar a preocupação decorrente de uma abordagem de política industrial, que é o conceito de soberania tecnológica. Muitas vezes ouvimos a suposição errônea de que soluções e tecnologias nacionais, bem como a localização forçada de dados, são fatores importantes para a segurança cibernética. No entanto, conforme explicado no relatório do ITIF intitulado "The False Promise of Data Nationalism"2, a metodologia tecnológica e procedimental para armazenamento e transferência de dados, bem como o tipo de tecnologia empregada, experiência do usuário, conhecimento dos envolvidos e boas relações institucionais as práticas determinarão o grau de segurança das informações, não o local da instalação onde os dados são armazenados. De fato, exigir a localização dos dados como base para sua segurança acarretaria uma falsa sensação de segurança, já que sua localização não tem impacto positivo na segurança. Pelo contrário, uma percepção de maior segurança, apesar de empregar tecnologias menos avançadas, seria extremamente perigosa para os objetivos de segurança nacional, especialmente porque os criminosos cibernéticos têm melhor conhecimento de onde os dados estão localizados. Para dar um exemplo de como políticas baseadas em "soberania" podem impactar negativamente a segurança de um país - em 2015, a Ucrânia aprovou uma lei exigindo que todas as empresas armazenem e tratem dados pessoais em servidores localizados no país. Essa lei criou um ponto de falha, tornando mais fácil para outros países espionar a Ucrânia e interromper sua rede implantando malware e outros ataques a empresas locais. Uma semana antes da invasão russa, o parlamento da Ucrânia aprovou uma legislação que permite que os dados sejam transferidos para fora do país usando tecnologia de nuvem estrangeira. Essa ação frustrou os ataques russos às redes de computadores da Ucrânia durante a invasão. Esse exemplo mostra que o Brasil deve considerar

todos os possíveis desdobramentos ao tomar decisões sobre a contratação de serviços ou investimentos em tecnologias desenvolvidas nacionalmente.
Resposta: Não são encontradas no texto do anteprojeto proposto quaisquer disposições que possam ensejar percepções no sentido de se pretender um "mandato de nacionalização de produtos ou serviços".

Audiência Pública da PNCiber – Contribuições

Responsável: Maxli Barroso Campos			
Instituição: LPTIC/EGN		**Título:** Pesquisador Líder	
Tópico: 02-PNCiber-Geral	**Id#:** 190	**Parecer:** 3-Inadequada	
Tipo de Contribuição: Dúvida	**Artigo:**	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: Como se pretende tratar os Software e Hardware utilizados no monitoramento de segurança e das telecomunicações, como os switch de rede, hub, etc, de origem estrangeira, tendo em vista a existência dos conhecidos backdoor?			
Resposta: A PNCiber é uma política nacional, e assim foca mais no "o que" do que no "como", até como forma de assegurar sua perenidade. Outrossim, não cabe esse tipo de detalhamento neste instrumento, mas sim em resoluções da Diretoria Colegiada da ANCiber a serem aprovadas pelo CNCiber oportunamente. De outra parte, os instrumentos serão os mesmos utilizados pelas demais agências reguladoras, conforme estipulado no marco regulatório vigente. Esses tópicos serão provavelmente regulados por normatização infralegal.			

Audiência Pública da PNCiber – Contribuições

Responsável: Maxli Barroso Campos			
Instituição: LPTIC/EGN		**Título:** Pesquisador Líder	
Tópico: 02-PNCiber-Geral	**Id#:** 191	**Parecer:** 3-Inadequada	
Tipo de Contribuição: Dúvida	**Artigo:**	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: Há intensão de se adotar um Modelo de Maturidade em Segurança Cibernética, com estabelecimento de metas para se alcançar essas maturidades progressivamente, em especial pelas Infraestruturas Críticas Nacionais, a exemplo do IGovTI, implantado pelo TCU na administração Pública Federal?			
Resposta: A PNCiber é uma política nacional, e assim foca mais no "o que" do que no "como", até como forma de assegurar sua perenidade. Outrossim, não cabe esse tipo de detalhamento neste instrumento, mas sim em resoluções da Diretoria Colegiada da ANCiber a serem aprovadas pelo CNCiber oportunamente. De outra parte, os instrumentos serão os mesmos utilizados pelas demais agências reguladoras, conforme estipulado no marco regulatório vigente. Esses tópicos serão provavelmente regulados por normatização infralegal.			

Audiência Pública da PNCiber – Contribuições

Responsável: Paulo Emerson de Oliveira Pereira			
Instituição: Cidadão		**Título:** Cidadão	
Tópico: 02-PNCiber-Geral	**Id#:** 241	**Parecer:** 3-Inadequada	
Tipo de Contribuição: Alteração Legal	**Artigo:**	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: Incluir o cidadão / povo como coresposáveis na proteção e combate aos crimes cibernéticos, colocando o Brasil e legislação brasileira em nível de destaque e inovação mundial;			
Resposta: Por definição, o cidadão é corresponsável pela segurança.			

Audiência Pública da PNCiber – Contribuições

Responsável: Paulo Emerson de Oliveira Pereira			
Instituição: Cidadão		**Título:** Cidadão	
Tópico: 02-PNCiber-Geral	**Id#:** 242	**Parecer:** 3-Inadequada	
Tipo de Contribuição: Alteração Infralegal	**Artigo:**	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: Seguir as boas práticas preconizadas na ISO38500, ISO31000, ISO27014, NIST, CSIRT e outras normas relacionadas ao Plano de Continuidade de Negócios, Gestão de Continuidade de Negócios e Sistema de Gestão de Continuidade de Negócios;			
Resposta: A sugestão foi anotada para implementação oportuna, por meio dos instrumentos infra legais aplicáveis.			

Audiência Pública da PNCiber – Contribuições

Responsável: Paulo Emerson de Oliveira Pereira			
Instituição: Cidadão		**Título:** Cidadão	
Tópico: 02-PNCiber-Geral	**Id#:** 243	**Parecer:** 3-Inadequada	
Tipo de Contribuição: Comentário	**Artigo:**	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: Em decorrência da possibilidade do PL perder a referência no trâmite do legislativo, a GSI e SGD devem publicar um Decreto ou Normativo para o amadurecimento das boas práticas e constuição operacional dos procedimentos para o tratamento de incidentes e desastres. A lei pode demorar a ficar aprovada e disonível, e temos urgência em melhor proteger o País, a Soberania, a Liberdade, a Nação e o povo brasileiro. A operação e os procedimentos de contigência funcionam independente das decisões de sala de crise, pois temos que ter a cadeia de custódia, e evidências e procedimentos para a gestão de crises, e que funcionam de maneira imparcial; Precisamos ter a condição de congelar o crime cibernético para que seja tratado adequadamente, interropendo os ataques e danos; Devemos deixar claro que dados da soberania e independência nacional só fiquem hospedados em data centers e clouding nacionais, em território brasileiro, principalmente os dados estratégicos, sensíveis, econômicos e financeiros; Dados públicos, LAI, da transparência não podem ser utilizados para tratamento de dados sem os respectivos convênios e termos de responsabilidade e finalidaade. Todos os órgãos são obrigados a cooperar com o programa de tranasparência do governo feno federal, incluindo todos os poderes sem excessões; Todos os órgãos minimamente tem de possuir backups e restores testados. Em todos sistemas, serviços devem-se aplicar as técnicas de desenvolvimento seguro, pilha OWASP, e as técnicas de minimização, anonimização, criptografia, e segmentação dos dados, conforme a função, cargo e nível de acesso. Deve-se definir a tabela de temporalidade, classificação do nível de acesso à informação e bloqueio dos robôs de captura para mineração de dados.			
Resposta: Já existem normativos para essa temática exarados pelo GSI, e aplicáveis no âmbito da Administração Pública Federal.			

Audiência Pública da PNCiber – Contribuições

Responsável: Sarah Melo Martins			
Instituição: Brasscom		**Título:** Representante	
Tópico: 02-PNCiber-Geral	**Id#:** 261	**Parecer:** 3-Inadequada	
Tipo de Contribuição: Alteração Legal	**Artigo:**	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: O ecossistema da Internet se refere a uma infraestrutura interconectada digital e global, onde riscos e ameaças estão em constante evolução. Isso significa que as soluções e os esforços de cibersegurança devem ser igualmente dinâmicos, altamente interoperáveis e adaptáveis, buscando enfrentar as ameaças em constante mudança que apresentam riscos a essas novas tecnologias. Portanto, soluções de cibersegurança não devem ser priorizadas por serem produzidas localmente, mas sim quando demonstrarem estar alinhadas com as melhores práticas e padrões internacionais, independentemente de onde foram fabricadas. Neste mesmo sentido, importante endereçar a equivocada suposição de que o local de armazenamento dos dados seja um fator relevante para a cibersegurança. Conforme explicado no relatório do ITIF intitulado "The False Promise of Data Nationalism"1, a metodologia tecnológica e procedimental de armazenamento e transferência de dados, bem como o tipo de tecnologia empregada, experiência do usuário, conhecimento dos envolvidos e boas práticas institucionais irão determinar o quão segura é a informação, e não a localização da instalação onde os dados são armazenados. De fato, exigir a localização dos dados como base para sua segurança acarretaria uma falsa sensação de segurança, já que sua localização não tem impacto positivo em termos de cibersegurança. Pelo contrário, uma falsa percepção de que as informações estão melhor protegidas por estarem armazenadas localmente, apesar de empregar tecnologias menos avançadas, seria extremamente perigosa para os objetivos de segurança nacional, especialmente porque os criminosos cibernéticos têm melhor conhecimento de onde os dados estão localizados, facilitando assim os ataques e o comprometimento de informações relevantes. Embora reconheçamos que esta não é uma proposta direta no texto existente, a Brasscom gostaria de compartilhar com o GSI o entendimento de que a ideia de fortalecer a indústria nacional em cibersegurança, embora seja legítima, poderá equivocadamente estabelecer a premissa de que se deve priorizar equipamentos e tecnologias nacionais em detrimento das estrangeiras. Em última instância, poderá também trazer uma eventual interpretação de obrigatoriedade do uso de tecnologia nacional ou armazenamento local de dados. Entendemos que essas premissas contrariam os objetivos listados no próprio PL de Ciber, especialmente o que se refere à garantia da confidencialidade, integridade, autenticidade e disponibilidade dos ativos cibernéticos de interesse para sociedade brasileira. Por tal razão, reforçamos a preocupação de que o texto de anteprojeto a ser enviado ao Congresso Nacional incorpore esta premissa de maneira clara, garantindo assim o livre fluxo transfronteiriço de dados, honrando inclusive compromissos constantes de acordos internacionais firmados pelo Brasil.			
Resposta: Não são encontradas no texto do anteprojeto proposto quaisquer disposições que possam ensejar percepções de "priorização de equipamentos e tecnologias nacionais em detrimento das estrangeiras".			

Audiência Pública da PNCiber – Contribuições

Responsável: Vanusa Menditi Calegario			
Instituição: Petrobras		**Título:** Servidora	
Tópico: 02-PNCiber-Geral	**Id#:** 280	**Parecer:** 3-Inadequada	
Tipo de Contribuição: Alteração Infralegal	**Artigo:**	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: Avaliar se seria pertinente incluir alguma orientação em termos de IA.			
Resposta: A inteligência artificial é uma tecnologia específica. A PNCiber não se propõe a tratar de uma tecnologia específica, mas sim da temática de cibersegurança.			

Audiência Pública da PNCiber – Contribuições

Responsável: Luiz Henrique Barbosa da Silva			
Instituição: TELCOMP		**Título:** Representante	
Tópico: 03-Disposições Gerais	**Id#:** 172	**Parecer:** 3-Inadequada	
Tipo de Contribuição: Alteração Legal	**Artigo:** 1	**Inciso:**	**Parágrafo:** 1
Texto Original: §1º Esta Lei aplica-se às pessoas físicas e jurídicas de direito público ou privado, sem prejuízo ao disposto na Lei nº 13.709, de 14 de agosto de 2018, no que diz respeito às ações de cibersegurança para proteção de dados pessoais.			
Crítica ou Sugestão: §1º Esta Lei aplica-se às pessoas físicas e jurídicas de direito público ou privado. §2º Sem prejuízo ao disposto na Lei nº 13.709, de 14 de agosto de 2018, esta lei inclui ações de cibersegurança para proteção de dados pessoais.			
Resposta: A proposta inplicaria numa alteração inadequada do sentido do texto original. Não estão previstas no anteprojeto da PNCiber ações de cibersegurança para proteção de dados pessoais.			

Audiência Pública da PNCiber – Contribuições

Responsável: Maxli Barroso Campos			
Instituição: LPTIC/EGN		**Título:** Pesquisador Líder	
Tópico: 03-Disposições Gerais	**Id#:** 192	**Parecer:** 3-Inadequada	
Tipo de Contribuição: Dúvida	**Artigo:** 2	**Inciso:**	**Parágrafo:**
Texto Original: Art. 2 º. A Política Nacional de Cibersegurança é o documento de mais alto nível que orienta a atividade de cibersegurança no País.			
Crítica ou Sugestão: Uma das premissas das recentes Políticas Nacionais nesta área prevê o correto alinhamento do emprego da cibersegurança e sua contribuição com o desenvolvimento e inovação da indústria 4.0. A visão e alinhamento da cibersegurança juntamente as ações do MCTIC são fundamentais e essenciais para o emprego das novas tecnologias com impacto em todos os ministérios, para o mercado e para o Estado. Outro aspecto importante diz respeito ao emprego da Política no desenvolvimento da indústria e diminuição na dependência tecnológica? Como documento de mais alto nível, como a Política irá trabalhar para melhor integração do Governo Federal com todos os outros entes da Federação? Sendo uma prefeitura o elo mais fraco do ente federativo, como as ações da Política irá refletir em todos os rinções deste país de grande dimensão? Compreendemos que a Política deveria deixar mais claro como esta lacuna será resolvida, na medida que o GSI hoje não alcança os Estados e muitos menos as prefeituras.			
Resposta: O alcance nacional será dado pela PNCiber, que estabelece a ANCiber como agência regulatória para a cibersegurança. Observa-se que tal alcance não é extensível ao GSI, sendo específico da ANCiber, e exclusivamente para a temática da Cibersegurança. Outrossim, quaisquer novas tecnologias com impacto em cibersegurança estarão no escopo da PNCiber e de seu órgão executivo, a ANCiber.			

Audiência Pública da PNCiber – Contribuições

Responsável: Arthur Pereira Sabbat			
Instituição: ANPD		**Título:** Diretor	
Tópico: 03-Disposições Gerais	**Id#:** 22	**Parecer:** 3-Inadequada	
Tipo de Contribuição: Preoc. DEFESA	**Artigo:** 3	**Inciso:**	**Parágrafo:** 0
Texto Original:			
Crítica ou Sugestão: No art 3º, parágrafo único, consta que as ações de cibersegurança e de ciberdefesa deverão, sempre que possível, ser planejadas e executadas de forma coordenada pelas instituições competentes. Sugere-se substituir "sempre que possível" por "sempre que necessário", uma vez que as áreas de cibersegurança e de ciberdefesa são bastante distintas entre si, em sua natureza e em seus objetivos.			
Resposta: Conceitualmente, a defesa é um subconjunto da segurança, com características específicas. Outrossim, a ciberdefesa é um subconjunto da cibersegurança. A PNCiber trata do superconjunto, a cibersegurança, e por essa razão aborda a necessária inclusão e delimitação da ciberdefesa, objeto do Ministério da Defesa (MD). De outra parte, a ANCiber é proposta como a grande coordenadora das ações de cibersegurança. Considerando-se essas duas premissas é que o texto proposto foi "sempre que possível". Faculta-se ao MD o entendimento de eventual impossibilidade, por exemplo por questões de sigilo. A substituição de "possível" por "necessário" tornaria mais difícil a pretendida coordenação de ações pela ANCiber. Por conseguinte, entende-se não adequada a substituição.			

Audiência Pública da PNCiber – Contribuições

Responsável: Maxli Barroso Campos			
Instituição: LPTIC/EGN		**Título:** Pesquisador Líder	
Tópico: 03-Disposições Gerais	**Id#:** 193	**Parecer:** 3-Inadequada	
Tipo de Contribuição: Alteração Legal	**Artigo:** 3	**Inciso:**	**Parágrafo:** 0
Texto Original: Parágrafo único. As ações de cibersegurança e de ciberdefesa deverão, sempre que possível, ser planejadas e executadas de forma coordenada pelas instituições competentes.			
Crítica ou Sugestão: Remover o Parágrafo Único. Acreditamos que em algum dos artigos se deva trabalhar o tema cibergovernança, com a correta integração de todos os entes do Estado Brasileiro, do alinhamento das ações de cibersegurança e ciberdefesa, buscando maior integração, troca de conhecimento e experiência, assim como formação dual de profissionais. A integração e colaboração em ciber é essencial para se alcançar o sucesso em qualquer estratégia na área.			
Resposta: Esse parágrafo confere à ANCiber sua mais importante característica: a coordenação das ações isoladas em cibersegurança, a unificação da "colcha de retalhos" que caracteriza a cibersegurança nacional. Não se vislumbra de que forma a permanência desse texto possa implicar em uma menor integração, troca de conhecimento e experiência ou formação "dual" (cujo sentido não ficou claro) de profissionais, ou dificulte a integração e colaboração. Dessa forma, o texto será mantido.			

Audiência Pública da PNCiber – Contribuições

Responsável: Ivanildo de Oliveira da Silva			
Instituição: Cidadão		**Título:** Cidadão	
Tópico: 03-Disposições Gerais	**Id#:** 83	**Parecer:** 3-Inadequada	
Tipo de Contribuição: Comentário	**Artigo:** 4	**Inciso:** 0	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: Quando se trata de cibersegurança os recursos humanos (pessoas) também são considerados ativos quem precisam de atenção e são foco de ataques como os de engenharia social, visando comprometer a infraestrutura física, lógica ou dados. Além disso, instalações físicas também podem ser considerados ativos. Sugiro alterar o inciso visando ajustar a definição de ciberativo incluindo essa realidade.			
Resposta: Não é adequado considerar um cidadão como um ciberativo, nem pela perspectiva humana, nem pela perspectiva técnica.			

Audiência Pública da PNCiber – Contribuições

Responsável: Luiz Henrique Barbosa da Silva			
Instituição: TELCOMP		**Título:** Representante	
Tópico: 03-Disposições Gerais	**Id#:** 173	**Parecer:** 3-Inadequada	
Tipo de Contribuição: Alteração Legal	**Artigo:** 4	**Inciso:** 0	**Parágrafo:**
Texto Original: ciberativo (ou ativo cibernético): hardware, software ou dados utilizados para o processamento e transmissão eletrônicos de informações;			
Crítica ou Sugestão: A definição de ciberativo deve ser mais completa para permitir, também, a interpretação da integração dos elementos e não só a visão individualizada dos mesmos, o que se consegue com o termo sistemas e, ainda, prever a infraestrutura essencial sobre o qual está trafegando ou se refere um ataque, o qual acaba por se inserir em ativo cibernético, a exemplo de antes de telecomunicações ou cabos de fibra ótica, ou postes, dutos ou condutos que os suportam. Redação proposta: ciberativo (ou ativo cibernético): infraestrutura, sistemas, hardware, software ou dados utilizados para dar suporte ou realizar o processamento e transmissão eletrônicos de informações;			
Resposta: Se a referência a "sistemas" pretende abarcar "sistemas digitais", como os exemplos aduzem, isso seria hardware. Se estiver se referindo a "sistemas de informação", isso é software (e até dados). Antenas de telecomunicações, cabos de fibra ótica, postes, dutos ou condutos são, em essência, equipamentos. Portanto, são hardware.			

Audiência Pública da PNCiber – Contribuições

Responsável: Rafael Gomes da Silva			
Instituição: Netskope		**Título:** Representante	
Tópico: 03-Disposições Gerais	**Id#:** 245	**Parecer:** 3-Inadequada	
Tipo de Contribuição: Alteração Legal	**Artigo:** 4	**Inciso:** 0	**Parágrafo:**

Texto Original:
ciberativo (ou ativo cibernético): hardware, software ou dados utilizados para o processamento e transmissão eletrônicos de informações;

Crítica ou Sugestão:
Neste parágrafo não se leva em consideração recursos em nuvem, sendo no momento atual, plataforma amplamente utilizada pelos organismos governamentais e empresas de cunho privado. Entendemos que o uso de determinadas plataformas deveriam ser enquadradas como ciberativo.
Outro ponto é a questão do usuário, haja visto que com a adoção da modalidade de trabalho remoto ou até mesmo o híbrido, o usuário manipula dados a partir de qualquer local, bastando ter um acesso a um computador habilitado a acessar o ambiente interno quanto o ambiente me nuvem.
Portanto, entendemos que o usuário categorizado como colaborador, pode ser um agente categorizado como ciberativo capaz de manipulação de dados.
Dados, neste contexto poderia ser especificado também como informação, pois o vazamento de de informações é um dos grandes pilares dos ataques sofridos. Portando, entendemos que a informação também fazer parte do contexto classificado como ciberativo, uma vez que na denominação do cibercrime temos "crime praticado contra, ou por meio de, ciberativos" a informação entra como um dos vetores que possam ser alvos.

Resposta:
Os recursos em nuvem também são hardware, software ou dados. De fato, como o próprio autor indica, dados podem ser informações. E dados estão incluídos na definição de ciberativos apresentada no anteprojeto. Indo ainda mais distante na linha de argumentação do autor, a hierarquia DIKW (dado, informação, conhecimento e sabedoria) implicaria em, se considerarmos informação adicionalmente a dados, sermos levados a considerar também conhecimento e sabedoria como ciberativos. Mas isso é desnecessário, posto que os 3 subsequentes derivam do primeiro, e assim, ao incluirmos dados, inclui-se os demais.

Audiência Pública da PNCiber – Contribuições

Responsável: Ivanildo de Oliveira da Silva			
Instituição: Cidadão		**Título:** Cidadão	
Tópico: 03-Disposições Gerais	**Id#:** 84	**Parecer:** 3-Inadequada	
Tipo de Contribuição: Comentário	**Artigo:** 4	**Inciso:** 0	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: Considerando que pessoas e instalações físicas não foram consideradas no inciso I, sugiro adaptar o inciso II visando considerar não somente ações tomadas no ciberespaço. Afinal, engenharia social não acontece somente no ciberespaço.			
Resposta: A delimitação do escopo do projeto de lei deve ser específica. A engenharia social não ocorre, de fato, somente no ciberespaço. Mas somente se ela se refletir em ações no ciberespaço elas serão objeto desta lei. Se o uso da engenharia social for outro, ele pode (e deve) estar contemplado em outro marco legal.			

Audiência Pública da PNCiber – Contribuições

Responsável: Luiz Henrique Barbosa da Silva			
Instituição: TELCOMP		**Título:** Representante	
Tópico: 03-Disposições Gerais	**Id#:** 174	**Parecer:** 3-Inadequada	
Tipo de Contribuição: Alteração Legal	**Artigo:** 4	**Inciso:** 0	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: O termo ciberofensa deveria envolver de forma ampla o cidadão e não só ao espaço cibernético e seus ativos materiais. Texto proposto: ciberofensa (ou ofensa cibernética): conjunto de ações tomadas no ciberespaço contra um ciberativo ou pessoa física ou jurídica ou titular de direitos;			
Resposta: Primeiro cumpre observar que a definição não contempla apenas ativos materiais, como infere o autor, posto que dados e software são inerentemente imateriais. Segundo, ações tomadas contra pessoas são objeto de leis específicas, fora do contexto da presente proposta. Incluí-las neste projeto poderia levar a uma sobreposição de marcos regulatórios, que poderia ensejar insegurança jurídica. Outrossim, considerando-se o escopo da presente lei, entende-se que o texto deva ser mantido como proposto.			

Audiência Pública da PNCiber – Contribuições

Responsável: Osmar Assis do Nascimento Filho			
Instituição: Cidadão		**Título:** Cidadão	
Tópico: 03-Disposições Gerais	**Id#:** 226	**Parecer:** 3-Inadequada	
Tipo de Contribuição: Alteração Legal	**Artigo:** 4	**Inciso:** 0	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: O ciberefeito sob o âmbito da mudança de comportamento também tem que considerar mudanças de comportamento de pessoas físicas ou jurídicas afetadas pela ciberofensa, sob o risco de se desconsiderar, conceitualmente, para efeitos jurídicos, as previsões estabelecidas na Lei nº 12.737, de 30 de novembro de 2012, na Lei nº 13.185, de 4 de novembro de 2015 e na Lei nº 14.155, de 27 de maio de 2021.			
Resposta: Não se desconsidera tais efeitos. No entanto, como bem explicitado pelo autor, eles estão contemplados em legislação específica. Por conseguinte, fora do contexto da PNCiber.			

Audiência Pública da PNCiber – Contribuições

Responsável: Ivanildo de Oliveira da Silva			
Instituição: Cidadão		**Título:** Cidadão	
Tópico: 03-Disposições Gerais	**Id#:** 85	**Parecer:** 3-Inadequada	
Tipo de Contribuição: Comentário	**Artigo:** 4	**Inciso:** 0	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: Sugiro não limitar a definição de ciberameaça, removendo a parte final do texto: "por meio de ciberofensa".			
Resposta: A delimitação é necessária para a menutenção da integridade do escopo da PNCiber. Um ataque físico de vandalismo, por exemplo, a um ciberativo, não está no escopo da PNCiber, mas sim de um outro marco regulatório.			

Audiência Pública da PNCiber – Contribuições

Responsável: Ivanildo de Oliveira da Silva			
Instituição: Cidadão		**Título:** Cidadão	
Tópico: 03-Disposições Gerais	**Id#:** 86	**Parecer:** 3-Inadequada	
Tipo de Contribuição: Comentário	**Artigo:** 4	**Inciso:** 0	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: A menos que se adapte as definições, sugiro reescrever esse inciso visando melhora a definição de incidente cibernético.			
Resposta: Não ficou clara a melhoria pretendida.			

Audiência Pública da PNCiber – Contribuições

Responsável: Osmar Assis do Nascimento Filho			
Instituição: Cidadão		**Título:** Cidadão	
Tópico: 03-Disposições Gerais	**Id#:** 227	**Parecer:** 3-Inadequada	
Tipo de Contribuição: Alteração Legal	**Artigo:** 4	**Inciso:** 0	**Parágrafo:**

Texto Original:
ciberexploração (ou exploração cibernética): conjunto de atividades voltadas ao robustecimento da consciência situacional, à produção de conhecimento de inteligência de fonte cibernética e ao levantamento de vulnerabilidades, que utiliza técnicas, táticas e procedimentos semelhantes àqueles empregados nos ciberataques, diferindo deles principalmente por não buscar a produção de ciberefeitos;

Crítica ou Sugestão:
Considera-se importante explicitar até que ponto a ciberexploração ou exploração cibernética é considerada violação do art. 154-A do Código Penal? "Art. 154-A. Invadir dispositivo informático de uso alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita: Pena - reclusão, de 1 (um) a 4 (quatro) anos, e multa." Com relação às competências estabelecidas para o CISC Gov.br, estabelecido pela Portaria SGD/MGI nº 852, de 28 de março de 2023, no art. 16, incisos V e VIII, questiona-se se seriam enquadrados como ciberexploração de acordo com a conceituação estabelecida neste projeto de lei. "Art. 16. São serviços que compõem o CISC Gov.br: [...] V - análise não-invasiva e contínua de vulnerabilidades em ativos de informação; [...] VII - atividades de inteligência de ameaças cibernéticas;"

Resposta:
A ciberexploração praticada sem autorização legal seria enquadrável nas disposições legais indicadas. Observa-se, no entanto, que tal atividade fica restrita ao âmbito da ciberdefesa, e assim submetida a regulamentação específica.

Audiência Pública da PNCiber – Contribuições

Responsável: Andréia Vatinet			
Instituição: Thales Group		**Título:** Representante	
Tópico: 03-Disposições Gerais	**Id#:** 13	**Parecer:** 3-Inadequada	
Tipo de Contribuição: Alteração Legal	**Artigo:** 4	**Inciso:** 0	**Parágrafo:** 0
Texto Original:			
Crítica ou Sugestão: Nossa sugestão seria adicionar a alínea C como parte das finalidades da Ciberdefesa (C) Identificar e Governar; Proteger; Detectar e responder e Treinar.			
Resposta: A alteração não é aplicável.			

Audiência Pública da PNCiber – Contribuições

Responsável: Ivanildo de Oliveira da Silva			
Instituição: Cidadão		**Título:** Cidadão	
Tópico: 03-Disposições Gerais	**Id#:** 87	**Parecer:** 3-Inadequada	
Tipo de Contribuição: Comentário	**Artigo:** 4	**Inciso:** 0	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: A ciberdefesa e a ciberguerra são definições distintas. O sentido que o inciso XV está inserindo associa a ciberdefesa somente a defesa de guerra cibernética. Dessa forma sugiro inserir definições com a devida segmentação como: - ciberguerra: nesta estariam inseridas as atribuições afetas ao Ministério da Defesa. - ciberdefesa: nesta estariam inseridas as atribuições dos órgãos da Administração Pública. Ambas, ciberdefesa e ciberguerra podem se fazer valer da cibersegurança.			
Resposta: O autor não parece referir-se à terminologia proposta do anteprojeto, mas sim a um conceito pessoal ou de terceiros sobre a temática. A terminologia usada no anteprojeto especifica claramente o que se pretende.			

Audiência Pública da PNCiber – Contribuições

Responsável: Breno de Castro Laranjo Vale			
Instituição: ABRINT		**Título:** Diretor de Projetos	
Tópico: 03-Disposições Gerais	**Id#:** 25	**Parecer:** 3-Inadequada	
Tipo de Contribuição: Alteração Legal	**Artigo:** 4	**Inciso:** 0	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: A ABRINT discorda do endereçamento dado a busca de transversalidade da cybersegurança, seja em razão da ausência ainda de definições claras sobre defesa e segurança, seja em função do aparente afastamento das infraestruturas críticas do universo cyber.			
Resposta: As definições de (ciber)defesa e (ciber)segurança foram detalhadas no Art. 4. O suposto "afastamento" do conceito de infraestruturas críticas não ocorre. Infraestruturas críticas continuarão sendo tratadas como tal em outras esferas da segurança, que não aquelas da cibersegurança, pelos motivos exaustivamente expressos na apresentação do projeto, seção 3.3.			

Audiência Pública da PNCiber – Contribuições

Responsável: Igor Monteiro Moraes			
Instituição: UFF		**Título:** Pesquisador	
Tópico: 03-Disposições Gerais	**Id#:** 76	**Parecer:** 3-Inadequada	
Tipo de Contribuição: Alteração Legal	**Artigo:** 4	**Inciso:** 0	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: Quem define o que são serviços essencias? A ANCiber? Esclarecer esse ponto no texto.			
Resposta: O conceito de serviços essenciais é estabelecido no Art. 4, inciso XXI. Conforme estipulado no Art. 25, ciberativos que dão sustentação a "serviços essenciais" integrarão o Complexo Nacional de Cibersegurança. De outra parte. O Art. 18, inciso X, indica que a ANCiber propõe ao CNCiber os integrantes do Complexo, enquanto o Art. 14, inciso V dispõe que o CNCiber aprova o Complexo. Por conseguinte, os componentes dos Serviços Essenciais são propostos pela ANCiber, e aprovados pelo CNCiber.			

Audiência Pública da PNCiber – Contribuições

Responsável: Maxli Barroso Campos			
Instituição: LPTIC/EGN		**Título:** Pesquisador Líder	
Tópico: 03-Disposições Gerais	**Id#:** 194	**Parecer:** 3-Inadequada	
Tipo de Contribuição: Alteração Infralegal	**Artigo:** 4	**Inciso:** 0	**Parágrafo:**
Texto Original: XXI - serviços essenciais: serviços cujo mau funcionamento, uso indevido ou interrupção, mesmo que parcial, possa acarretar prejuízo à segurança nacional, e dos quais dependa o exercício de função essencial do Estado ou a prestação de serviço primordial à manutenção de atividades civis, sociais ou econômicas fundamentais aos interesses do Estado.			
Crítica ou Sugestão: XXI - Serviços essenciais cujo mau funcionamento ... Paragrafo único: para os fins dessa Politica são considerados serviços essenciais os definidos na lei XXXXX (ou listar os serviços essenciais aqui)			
Resposta: Não é plausível estipular em lei um rol taxativo dos serviços essenciais, quanto mais num processo de digitalização continuada pelo qual passa a sociedade brasileira. Essa delimitação na PNCiber faria com que sua atualização se tornasse demasiado complexa. Por tal razão o Complexo Nacional de Cibersegurança, que considera os serviços essenciais, é aprovado por meio de Resolução da Anciber aprovada pelo Comitê Nacional de Cibersegurança, sujeita a AIR, o que confere simultaneamente agilidade e transparência ao processo.			

Audiência Pública da PNCiber – Contribuições

Responsável: Osmar Assis do Nascimento Filho			
Instituição: Cidadão		**Título:** Cidadão	
Tópico: 03-Disposições Gerais	**Id#:** 228	**Parecer:** 3-Inadequada	
Tipo de Contribuição: Alteração Legal	**Artigo:** 4	**Inciso:** 0	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: Os serviços essenciais estarão tanto sob a ótica do GSI quanto do MD? Poderão estar sob atuação de cibersegurança e ciberdefesa simultaneamente? Em assim sendo, o MD terá que sujeitar suas ações de ciberdefesa à ANCiber?			
Resposta: Conceitualmente, a defesa é um subconjunto da segurança, com características específicas. Outrossim, a ciberdefesa é um subconjunto da cibersegurança. A PNCiber trata do superconjunto, a cibersegurança, e por essa razão aborda a necessária inclusão e delimitação da ciberdefesa, objeto do Ministério da Defesa (MD). De outra parte, a ANCiber é proposta como a grande coordenadora das ações de cibersegurança. Considerando-se essas duas premissas é que o Art. 3, Parágrafo Único, propõe que "sempre que possível" as ações do MD e da ANCiber devem ser coordenadas. Faculta-se ao MD o entendimento de eventual impossibilidade, por exemplo por questões de sigilo.			

Audiência Pública da PNCiber – Contribuições

Responsável: Maxli Barroso Campos			
Instituição: LPTIC/EGN		**Título:** Pesquisador Líder	
Tópico: 03-Disposições Gerais	**Id#:** 195	**Parecer:** 3-Inadequada	
Tipo de Contribuição: Alteração Legal	**Artigo:** 4	**Inciso:** 0	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: XXIII - Ciberespaço: ambiente virtual formado pelos ciberativos conectados em rede, onde informações digitais são armazenadas, transmitidas e acessadas. É um espaço virtual onde ocorrem interações, trocas de informações e atividades por meio desses dispositivos eletrônicos digitais.			
Resposta: O anteprojeto utiliza por 7 vezes o termo ciberespaço sem especificá-lo, por entender que o termo já é de domínio público e uma definição específica no anteprojeto de lei seria desnecessária e talvez até contraproducente.			

Audiência Pública da PNCiber – Contribuições

Responsável: Leonardo Rodrigo Ferreira			
Instituição: SGD		**Título:** Diretor	
Tópico: 03-Disposições Gerais	**Id#:** 160	**Parecer:** 3-Inadequada	
Tipo de Contribuição: Alteração Legal	**Artigo:** 4	**Inciso:**	**Parágrafo:**
Texto Original: Art. 4 º. Para os fins desta Lei, considera-se: (...)			
Crítica ou Sugestão: Indica-se que os termos e definições adotados para a Política em questão estejam constantes do Glossário de Segurança da Informação (Portaria GSI/PR 93 de 2019) e que tal Decreto seja referenciado pelo art. 4º da seguinte forma: Art. 4º. Os temos e definições adotados pela PNCiber constam do Glossário de Segurança da Informação, conforme a Portaria Nº 93 GSI/PR, de 18 de outubro de2021, e suas alterações. A adoção do referido Glossário possibilita a centralização e padronização de todos os termos e definições relevantes para a Segurança da Informação.			
Resposta: Não é plausível uma lei federal subordinar-se a uma portaria, que é ministerial. No caso em tela, o princípio aplicável é o lex superior derogat inferioris (lei superior derroga a inferior). Quando aprovada a Lei, o glossário será necessariamente atualizado, pois uma portaria não pode contrariar uma lei.			

Audiência Pública da PNCiber – Contribuições

Responsável: Maxli Barroso Campos			
Instituição: LPTIC/EGN		**Título:** Pesquisador Líder	
Tópico: 03-Disposições Gerais	**Id#:** 196	**Parecer:** 3-Inadequada	
Tipo de Contribuição: Comentário	**Artigo:** 4	**Inciso:**	**Parágrafo:**

Texto Original:

Art. 4 º. Para os fins desta Lei, considera-se:

I - ciberativo (ou ativo cibernético): hardware, software ou dados utilizados para o processamento e transmissão eletrônicos de informações;

II - ciberofensa (ou ofensa cibernética): conjunto de ações tomadas no ciberespaço contra um ciberativo;

III - cibercrime (ou crime cibernético): crime praticado contra, ou por meio de, ciberativos;

IV - ciberefeito: dano, permanente ou temporário, indisponibilidade ou limitação da operação, total ou parcial, ou mudança de comportamento, de um ativo cibernético ou não, resultante de uma ciberofensa;

V - cibercapacidade (ou capacidade cibernética): conjunto de habilidades e competências cibernéticas que se reforçam mutuamente implementadas por meios técnicos, físicos e processuais visando atingir um objetivo comum;

VI - ciberameaça (ou ameaça cibernética): circunstância ou evento com potencial para impactar adversamente indivíduos ou organizações (incluindo ativos, operações, funções, imagem ou reputação) por meio de ciberofensas;

Crítica ou Sugestão:

Estas novas antologias não estão alinhadas com o atual Glossário de Segurança da Informação do GSI. Importante realizar este correto alinhamento e levar em consideração em um estudo de viabilidade que será necessário se revisar todas as políticas e normas já criadas anteriormente. Não seria mais prudente se manter o que já temos como cultura na área durante anos, seja em segurança cibernética, seja na defesa cibernética.

Fica como sugestão o desenvolvimento de uma proposta de Taxionomia em Cibernética (um trabalho de GT para padronizar as ontologias em diferentes categorias como criptografia, serviços de segurança, segurança de rede, segurança em hardware, dentre outros. Assim os profissionais da área no Brasil, independente do setor de atuação sempre terão o mesmo entendimento, facilitando a troca de experiência e colaboração, ampliando a sinergia.

Resposta:

Entendemos que o termo "antologias" deva, na verdade, ser "ontologias". Sendo assim, a explicação da motivação para o uso terminologia escolhida foi pormenorizada na Apresentação do Projeto, seção 4, inclusive no tocante aos glossários do GSI e do MD, conforme subseção 4.5

Audiência Pública da PNCiber – Contribuições

Responsável: Osmar Assis do Nascimento Filho			
Instituição: Cidadão		**Título:** Cidadão	
Tópico: 03-Disposições Gerais	**Id#:** 229	**Parecer:** 3-Inadequada	
Tipo de Contribuição: Alteração Legal	**Artigo:** 4	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: Faltou a definição de "ciberinspeções", utilizada no art. 18, inciso XVII.			
Resposta: A definição de ciberinspeção encontra-se no Art. 4º, inciso XVIII			

Audiência Pública da PNCiber – Contribuições

Responsável: Sarah Melo Martins			
Instituição: Brasscom		**Título:** Representante	
Tópico: 03-Disposições Gerais	**Id#:** 262	**Parecer:** 3-Inadequada	
Tipo de Contribuição: Alteração Legal	**Artigo:** 4	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: Com o objetivo de definir fatos e atos ocorridos no espaço cibernético, a lei estabelece diversas definições que parecem-nos muito amplas e inespecíficas. Considerando que essas definições são cruciais para definir os princípios, objetivos e diretrizes da Política Nacional de Cibersegurança e delinear as competências das entidades do Sistema Nacional de Cibersegurança, entendemos que estes conceitos devem ser objeto de maior precisão, principalmente para fins de segurança jurídica. Como exemplo, citamos a definição de "cibercrime", "ciberincidente", "ciber ameaça", entre outros, que poderiam ser amadurecidos durante o debate a fim de serem melhor conceituados.			
Resposta: A conceituação pretendida foi explicitada na proposta da terminologia adotada, não havendo dúvida sobre o conteúdo pretendido. Ademais, é sabido que há décadas se debate sobre a terminlogia de cibersegurança, sem que exista uma convergência sobre esta temática, mas sim um conjunto de diferentes glossários utilizados com maior ou menor frequência. Outrossim, não é plausível adiar o andamento do projeto à espera de uma terminologia "melhor conceituada".			

Audiência Pública da PNCiber – Contribuições

Responsável: Vanessa Copeti Cravo			
Instituição: ANATEL		**Título:** GTCiber	
Tópico: 03-Disposições Gerais	**Id#:** 272	**Parecer:** 3-Inadequada	
Tipo de Contribuição: Preoc. DEFESA	**Artigo:** 4	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: Exclusão do tema de defesa da PNCiber deixando tão somente os temas da construção de capacidades civis (crimes cibernéticos; medidas técnicas; organizacionais; construção de capacidades - conscientização, capacitação e P&D&I; e cooperação), com a consequente exclusão de todas definições afetas ao tema de defesa. A união dos temas traz grande complexidade ao projeto que precisa nacionalmente promover a articulação de todos poderes, entes da federação, atores e setores. Embora meritório o esforço, traz uma complexidade muito grande e desnecessária ao projeto, cuja maior missão é o estabelecimento da instituição nacional de cibersegurança;			
Resposta: A PNCiber é uma política nacional voltada à cibersegurança. Conceitualmente, a defesa é um subconjunto da segurança. Por conseguinte, a PNCiber deve, NECESSARIAMENTE, abordar a questão da ciberdefesa.			

Audiência Pública da PNCiber – Contribuições

Responsável: Vanessa Copeti Cravo			
Instituição: ANATEL		**Título:** GTCiber	
Tópico: 03-Disposições Gerais	**Id#:** 273	**Parecer:** 3-Inadequada	
Tipo de Contribuição: Alteração Legal	**Artigo:** 4	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: Abandono do conceito de ciberativo e Complexo de Ciberativos e retorno aos conceito de infraestrutura crítica que já está enraizado no ordenamento e nas políticas públicas. A criação desse novo conceito adiciona complexidade ao anteprojeto e inova o ordenamento, trazendo muitas incertezas, enquanto que o conceito de infraestrutura já está amadurecido nos normativos e nas instituições brasileiras;			
Resposta: A explicação da motivação para a adoção de serviços essenciais em oposição a infraestruturas críticas encontra-se no documento Apresentação do Projeto, seção 3.3. Ademais, essa lógica se coaduna com a evolução observada na Europa (NIS2) e em Israel, grandes centros de cibersegurança mundiais.			

Audiência Pública da PNCiber – Contribuições

Responsável: Vanusa Menditi Calegario			
Instituição: Petrobras		**Título:** Servidora	
Tópico: 03-Disposições Gerais	**Id#:** 281	**Parecer:** 3-Inadequada	
Tipo de Contribuição: Alteração Legal	**Artigo:** 4	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: Avaliar a inclusão de algo em termos de "ciberconscientização", talvez como item f): XIV - cibersegurança (ou segurança cibernética): conjunto de ações voltadas à confidencialidade, integridade, autencidade e disponibilidade de ciberativos, por meio da: a) ciberdissuasão; b) ciberproteção; c) ciber-resiliência; d) ciberinvestigação; e) ciberexploração.			
Resposta: A chamada ciberconscientização está incluída no contexto da criação de uma cultura nacional de cibersegurança, prevista no anteprojeto de lei.			

Audiência Pública da PNCiber – Contribuições

Responsável: Jeferson Fued Nacif			
Instituição: MCom		**Título:** Servidor	
Tópico: 03-Disposições Gerais	**Id#:** 103	**Parecer:** 3-Inadequada	
Tipo de Contribuição: Alteração Infralegal	**Artigo:** 5	**Inciso:** 0	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: A PNCiber fala da importância da cooperação internacional mas tal importância precisa estar impressa na estrutura da ANCiber com uma Diretoria Internacional.			
Resposta: A estrutura regimental da ANCiber somente será definida por meio de uma resolução publicada após a nomeação da primeira diretoria. Para se chegar a este ponto, é necessária a apresentação do projeto de lei ao Congresso, sua aprovação, a edição de um decreto instalando as instituições criadas (CNCiber, ANCiber e GGCiber) a nomeação de seus integrantes pelas diferentes instituições, a sabatina de alguns deles pelo Senado Federal, a posse da primeira diretoria, a apresentação do projeto de resolução ao CNCiber e sua aprovação. Por conseguinte, é inadequada a previsão de uma diretoria específica no anteprojeto de lei.			

Audiência Pública da PNCiber – Contribuições

Responsável: Leonardo Rodrigo Ferreira			
Instituição: SGD		**Título:** Diretor	
Tópico: 03-Disposições Gerais	**Id#:** 161	**Parecer:** 3-Inadequada	
Tipo de Contribuição: Alteração Legal	**Artigo:** 5	**Inciso:** 0	**Parágrafo:**
Texto Original: Art. 5 º. A Política Nacional de Cibersegurança baseia-se nos seguintes princípios: X - transparência, para assegurar a cibersegurança como indutora do sigilo das informações imprescindíveis à segurança da sociedade e do Estado, à inviolabilidade da intimidade da vida privada, da honra e da imagem das pessoas;			
Crítica ou Sugestão: Art. 5 º. A Política Nacional de Cibersegurança baseia-se nos seguintes princípios: X - proteção da informação, para assegurar a cibersegurança como indutora do sigilo das informações imprescindíveis à segurança da sociedade e do Estado, à inviolabilidade da intimidade da vida privada, da honra e da imagem das pessoas;			
Resposta: O princípio maior á o da transparência, e não o da proteção da informação.			

Audiência Pública da PNCiber – Contribuições

Responsável: Vanessa Copeti Cravo			
Instituição: ANATEL		**Título:** GTCiber	
Tópico: 03-Disposições Gerais	**Id#:** 274	**Parecer:** 3-Inadequada	
Tipo de Contribuição: Alteração Legal	**Artigo:** 17	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: Avaliação da vinculação direta à Presidência da República pela importância e transversalidade do tema, que envolve todos os Ministérios. Ademais, o GSI tem um quadro de servidores com predominância dos quadros militares. A vinculação à Presidência reforçaria o caráter civil que o tema precisa endereçar;			
Resposta: A definição do GSI como ministério para vinculação da ANCiber foi feita em estrita concordância com as disposições legais, conforme esclarecido na "Apresentação do Projeto", seção 3.4.			

Audiência Pública da PNCiber – Contribuições

Responsável: Carlos Baigorri			
Instituição: ANATEL		**Título:** Presidente	
Tópico: 03-Disposições Gerais	**Id#:** 37	**Parecer:** 3-Inadequada	
Tipo de Contribuição: Preoc. DEFESA	**Artigo:**	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: Não obstante a Anatel vislumbre mérito na congregação dos temas de defesa e capacidade civil em segurança cibernética, não é possível afastar o grau de complexidade que trouxe ao Anteprojeto (vide rol de terminologias), especialmente considerando que é um marco nacional e que não dialoga tão somente com o setor público. Ao contrário. Nesse sentido, sugere-se a reavaliação para focar tão somente na construção das capacidades civis necessárias para o enfretamento dos desafios (crimes cibernéticos; capacidades técnicas; medidas organizacionais; cooperação; e sensibilização, conscientização e capacitação).			
Resposta: A PNCiber é uma política nacional voltada à cibersegurança. Conceitualmente, a defesa é um subconjunto da segurança. Por conseguinte, a PNCiber deve, NECESSARIAMENTE, abordar a questão da ciberdefesa.			

Audiência Pública da PNCiber – Contribuições

Responsável: Frederico Fernandes Neres			
Instituição: Caixa		**Título:** Gerente	
Tópico: 04-Princípios	**Id#:** 63	**Parecer:** 3-Inadequada	
Tipo de Contribuição: Alteração Infralegal	**Artigo:** 5	**Inciso:** 0	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: Sugerimos ajustar o Art. 5 º, inciso I para: "foco no cidadão, capacitando-o a se tornar o elo mais forte da segurança;"			
Resposta: A proposta tornaria o texto utópico, desconexo da realidade.			

Audiência Pública da PNCiber – Contribuições

Responsável: Maxli Barroso Campos			
Instituição: LPTIC/EGN		**Título:** Pesquisador Líder	
Tópico: 04-Princípios	**Id#:** 197	**Parecer:** 3-Inadequada	
Tipo de Contribuição: Alteração Infralegal	**Artigo:** 5	**Inciso:** 0	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: Do nosso ponto de vista ter como foco o cidadão foi uma excelente abordagem. Mas não ficou claro como a Política irá privilegiar ações amplas de conscientização de segurança cibernética com capilaridade para todo o território nacional de forma inclusiva e irrestrita. Em se pensando nas novas gerações seria importante deixar registrado a mudança de cultura a partir das primeiras idades com realização de desenvolvimento de talentos na área, assim como fazem Israel, Espanha, EUA e outros países.			
Resposta: Uma Política deve ser um documento focado em "o que", e não em "como". Para este último, espera-se que o detalhamento se dê na Estratégia quadrienal e nos Planos anuais.			

Audiência Pública da PNCiber – Contribuições

Responsável: Rafael Gomes da Silva			
Instituição: Netskope		**Título:** Representante	
Tópico: 04-Princípios	**Id#:** 246	**Parecer:** 3-Inadequada	
Tipo de Contribuição: Alteração Legal	**Artigo:** 5	**Inciso:** 0	**Parágrafo:**
Texto Original: foco no cidadão, para fortalecer o elo mais fraco de qualquer instrumento de segurança;			
Crítica ou Sugestão: Ao considerar sistemas computacionais como infra-estruturas críticas o mais importante relacionado a eles faz menção as informações hospedadas e manipuladas pelos cidadãos/usuários. Um evento de cibercrime tenta indisponibilizar sistemas e também comprometer sigilos, expor informações, dentre outras ocorrências. Portanto o vazamento de dados deve ser reavaliado para que seja revisto como um dos focos durante o evento de cibercrime.			
Resposta: O vazamento de dados é objeto da LGPD, e não do presente anteprojeto de Lei.			

Audiência Pública da PNCiber – Contribuições

Responsável: Núcleo de Pesquisa em Concorrência, Política Pública, Inovação e Tecnologia (Comppit)			
Instituição: FGV		**Título:** Pesquisador	
Tópico: 04-Princípios	**Id#:** 216	**Parecer:** 3-Inadequada	
Tipo de Contribuição: Comentário	**Artigo:** 5	**Inciso:** 0	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: No tema da coordenação federativa, apontado como um dos princípios da PNCiber, além de um de seus objetivos (art. 6, inc. IV), consideramos ser proveitoso ao anteprojeto um tratamento mais assertivo sobre a questão, delimitando o que caberia aos Estados e Municípios. Assim, a União poderia, por exemplo, estabelecer diretamente os mecanismos e instrumentos mais vinculantes, no sentido de que Estados e Municípios, no que for definido como serviço essencial/infraestrutura crítica pela União, devam celebrar convênios. Ou, ainda que não se entenda por uma competência privativa da União a partir do texto constitucional (art. 22, IV), há a possibilidade de criação de uma disposição mais explícita e detalhada não somente de que as agências podem estabelecer convênios, mas os termos de tais acordos, com um conteúdo mínimo capaz de atender o objetivo da Lei para uma efetiva Política Nacional de Cibersegurança.			
Resposta: Uma Política deve ser um documento focado em "o que", e não em "como". Para este último, espera-se que o detalhamento se dê na Estratégia quadrienal e nos Planos anuais. Ademais, há uma PEC, citada na Exposição de Motivos, em tramitação no Senado Federal, que estipula as competências dos entes federados sobre a cibersegurança e a ciberdefesa.			

Audiência Pública da PNCiber – Contribuições

Responsável: Jeferson Fued Nacif			
Instituição: MCom		**Título:** Servidor	
Tópico: 04-Princípios	**Id#:** 104	**Parecer:** 3-Inadequada	
Tipo de Contribuição: Alteração Legal	**Artigo:** 5	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: Incluir conceitos relacionados à proteção dos direitos humanos fundamentais entre os princípios.			
Resposta: Os direitos humanos fundamentais são estipulados na Constituição Federal, sendo desnecessário inserí-los como princípios de uma lei ordinária.			

Audiência Pública da PNCiber – Contribuições

Responsável: Maxli Barroso Campos			
Instituição: LPTIC/EGN		**Título:** Pesquisador Líder	
Tópico: 04-Princípios	**Id#:** 198	**Parecer:** 3-Inadequada	
Tipo de Contribuição: Alteração Infralegal	**Artigo:** 5	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: Entende-se que seria necessário mencionar neste item como seria a interação com a Política Nacional de Segurança da Informação e seus documentos derivados; em princípio, estes normativos necessitam de ser reescritos.			
Resposta: Não é necessário descrever a interação com a PNSI. Nos casos em que os documentos dela derivados conflitem com os dispositivos da PNCiber eles serão gradualmente alterados. Esse é o processo legislativo usual. A nova legislação se sobrepõe àquela existente, e eventuais conflitos são pacificados pelo judiciário ou pela redação de novos dispositivos, posteriormente.			

Audiência Pública da PNCiber – Contribuições

Responsável: Vanessa Copeti Cravo			
Instituição: ANATEL		**Título:** GTCiber	
Tópico: 04-Princípios	**Id#:** 275	**Parecer:** 3-Inadequada	
Tipo de Contribuição: Alteração Infralegal	**Artigo:**	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: Inclusão do tema de proteção das crianças e adolescentes no ciberespaço, em aderência às recomendações da OCDE e as diretrizes da União Internacional de Telecomunicações no tema. Destaca-se que o Brasil aderiu à Recomendação da OCDE em 26/01/2022. Referências: https://www.itu-cop-guidelines.com/_files/ugd/24bbaa_b5fec426d50d4a21b721489099b5781f.pdf https://www.gov.br/anatel/pt-br/consumidor/destaques/publicacoes-orientam-pais-educadores-formuladoresde- politicas-e-industria-sobre-protecao-de-criancas-na-internet https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0389			
Resposta: A PNCiber é uma política nacional, e assim foca mais no "o que" do que no "como", até como forma de assegurar sua perenidade. Outrossim, não cabe esse tipo de detalhamento neste instrumento, mas sim em resoluções da Diretoria Colegiada da ANCiber a serem aprovadas pelo CNCiber oportunamente. De outra parte, os instrumentos serão os mesmos utilizados pelas demais agências reguladoras, conforme estipulado no marco regulatório vigente. Esses tópicos serão provavelmente regulados por normatização infralegal.			

Audiência Pública da PNCiber – Contribuições

Responsável: Rafael Gomes da Silva			
Instituição: Netskope		**Título:** Representante	
Tópico: 05-Objetivos	**Id#:** 247	**Parecer:** 3-Inadequada	
Tipo de Contribuição: Alteração Infralegal	**Artigo:** 6	**Inciso:** 0	**Parágrafo:**
Texto Original: garantir a confidencialidade, a integridade, a autenticidade e a disponibilidade dos ciberativos de interesse da sociedade brasileira;			
Crítica ou Sugestão: Reforçamos a necessidade de rever o termo ciberativo e incluir sistemas em nuvem, bem como a informação manipulada.			
Resposta: Os recursos em nuvem também são hardware, software ou dados. E dados estão incluídos na definição de ciberativos apresentada no anteprojeto. Conforme a hierarquia DIKW (dado, informação, conhecimento e sabedoria) sabedoria advém de conhecimento, o qual advém de informação, que advém de dados. Por conseguinte, "informação manipulada" está contemplada na definição apresentada no anteprojeto de Lei.			

Audiência Pública da PNCiber – Contribuições

Responsável: Andréia Vatinet			
Instituição: Thales Group		**Título:** Representante	
Tópico: 05-Objetivos	**Id#:** 14	**Parecer:** 3-Inadequada	
Tipo de Contribuição: Alteração Legal	**Artigo:** 6	**Inciso:** 0	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: Nossa sugestão seria complementar a frase "fomentar a participação do Brasil na cadeia produtiva global de produtos e serviços voltados à cibersegurança ". A frase completa ficaria da seguinte forma: VI - Fomentar a participação do Brasil na cadeia produtiva global de produtos e serviços voltados à cibersegurança e soluções de proteção de dados (gestão de chaves de acesso, criptografia, tokenização , dentre outras). A gestão das chaves de criptografia devem ser feitas localmente não podendo ser realizada em provedores de serviços estrangeiros para garantir a soberania dos dados.			
Resposta: A proposta cria um detalhamento desnecessário e potencialmente restritivo ao texto.			

Audiência Pública da PNCiber – Contribuições

Responsável: Diego Marcos Moreira			
Instituição: ANPPD		**Título:** Representante	
Tópico: 05-Objetivos	**Id#:** 46	**Parecer:** 3-Inadequada	
Tipo de Contribuição: Alteração Legal	**Artigo:** 6	**Inciso:** 0	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: Onde se diz "fomentar o combate ao cibercrime" acrescentar "e ciberameaças".			
Resposta: A ênfase é no combate ao crime. Ameaças não são combatidas, mas mitigadas.			

Audiência Pública da PNCiber – Contribuições

Responsável: Maxli Barroso Campos			
Instituição: LPTIC/EGN		**Título:** Pesquisador Líder	
Tópico: 06-Diretrizes	**Id#:** 199	**Parecer:** 3-Inadequada	
Tipo de Contribuição: Alteração Legal	**Artigo:** 7	**Inciso:**	**Parágrafo:**
Texto Original: Art. 7 º. A Política Nacional de Cibersegurança como orientadora da formulação da Estratégia Nacional de Cibersegurança e de iniciativas correlatas.			
Crítica ou Sugestão: Art. 7 º. A Política Nacional de Cibersegurança como orientadora da formulação da Estratégia Nacional de Cibersegurança e da Estratégia da Ciência, Tecnologia e Inovação Obs: Fica o ponto de vista que a falta de alinhamento com o MCTIC irá repercutir em implantação e projetos na área de tecnologia que irão no médio e longo prazo impactar diretamente a eficácia das estratégicas de cibersegurança.			
Resposta: A proposta limitaria o alcance da PNCiber a esses dois marcos. O texto original, de outra parte, confere amplitude à PNCiber.			

Audiência Pública da PNCiber – Contribuições

Responsável: Leila Oliveira da Fonseca			
Instituição: Cidadão		**Título:** Pesquisadora	
Tópico: 07-Instrumentos	**Id#:** 147	**Parecer:** 3-Inadequada	
Tipo de Contribuição: Alteração Legal	**Artigo:** 10	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: Os instrumentos da PNCiber poderiam ser apenas o Sistema Nacional de Cibersegurança, a Estratégia Nacional e o Plano Nacional. A cooperação internacional juntamente com o ensino, pesquisa, desenvolvimento e a inovação (capítulos V, VI) respectivamente integram o ecossistema da Cibersegurança, assim como a governança cibernética, cultura de Cibersegurança, parcerias nacionais, capacitação técnica, devendo portanto constar nos objetivos da Política e serem mais detalhados na Estratégia, no Plano, nos eixos estruturantes iniciativas e ações. Assim a PNCiber ficaria mais enxuta, sucinta e objetiva, viabilizando a sua praticidade.			
Resposta: No âmbito da cibersegurança entende-se a cooperação, internacional ou nacional, como instrumento essencial, da mesma forma que a pesquisa e a capacitação. Outrossim, a alteração proposta alteraria o "espírito da lei".			

Audiência Pública da PNCiber – Contribuições

Responsável: Maxli Barroso Campos			
Instituição: LPTIC/EGN		**Título:** Pesquisador Líder	
Tópico: 07-Instrumentos	**Id#:** 200	**Parecer:** 3-Inadequada	
Tipo de Contribuição: Alteração Legal	**Artigo:** 10	**Inciso:**	**Parágrafo:**
Texto Original: Art. 10 . São instrumentos da Política Nacional de Cibersegurança: I - o Sistema Nacional de Cibersegurança; II - a Estratégia Nacional de Cibersegurança; III - o Plano Nacional de Cibersegurança; IV - a cooperação internacional; V - o ensino, a pesquisa, o desenvolvimento e a inovação tecnológica em cibersegurança.			
Crítica ou Sugestão: Obs: Fica o ponto de vista que a falta de alinhamento com o MCTIC irá repercutir em implantação e projetos na área de tecnologia que irão no médio e longo prazo impactar diretamente a eficácia das estratégicas de cibersegurança.			
Resposta: O texto não enseja "falta de alinhamento com o MCTIC". Pelo contrário, o MCTIC é membro permanente do CNCiber. Ademais, a PNCiber presume que a ANCiber estará atenta ao impacto de novas tecnologias na cibersegurança, e apresentando resoluções no sentido de sanar ou mitigar tais impactos.			

Audiência Pública da PNCiber – Contribuições

Responsável: Leonardo Rodrigo Ferreira			
Instituição: SGD		**Título:** Diretor	
Tópico: 08-SNCiber	**Id#:** 162	**Parecer:** 3-Inadequada	
Tipo de Contribuição: Alteração Legal	**Artigo:** 12	**Inciso:** 0	**Parágrafo:**
Texto Original: Art. 12 . O Sistema Nacional de Cibersegurança constitui-se de: I - o Comitê Nacional de Cibersegurança (CNCiber); II - a Agência Nacional de Cibersegurança (ANCiber); III - o Gabinete de Gerenciamento de Cibercrises; e IV - o Complexo Nacional de Cibersegurança.			
Crítica ou Sugestão: Recomenda-se a inclusão da Secretaria de Governo Digital (SGD) na constituição do Sistema Nacional de Cibersegurança, considerando a atuação como órgão central do SISP e a responsabilidade pela elaboração da Estratégia Nacional de Governo Digital (ENGD) - inciso III e XVIII do Art. 22.do Decreto nº 11.437 de 17 de março de 2023. Nesse cenário, apresentamos a seguinte sugestão: Art. 12. O Sistema Nacional de Cibersegurança constitui-se de: I - o Comitê Nacional de Cibersegurança (CNCiber); II - a Agência Nacional de Cibersegurança (ANCiber); III - o Gabinete de Gerenciamento de Cibercrises; IV - o Complexo Nacional de Cibersegurança; e V - a Secretaria de Governo Digital (SGD)			
Resposta: A SGD já está contemplada com a participação no CNCiber e no GGCiber, na qualidade de infraestrutura crítica. Ademais, ciberativos relativos à SGD devem necessariamente integrar o Complexo Nacional de Cibersegurança. Outrossim, a SGD já está incluída no sistema por outros meios.			

Audiência Pública da PNCiber – Contribuições

Responsável: Jeferson Fued Nacif			
Instituição: MCom		**Título:** Servidor	
Tópico: 09-CNCiber	**Id#:** 105	**Parecer:** 3-Inadequada	
Tipo de Contribuição: Alteração Legal	**Artigo:** 14	**Inciso:** 0	**Parágrafo:**
Texto Original: Art. 14 . Compete ao Comitê: ... II - aprovar, por meio de resolução, os atos normativos concernentes à cibersegurança nacional; ...			
Crítica ou Sugestão: Comitê deve ter papel opinativo, consultivo, e não o normativo, que caberá à ANCiber, a fim de evitar sobreposição de atribuições.			
Resposta: O objetivo desse papel normativo é conceder transparência e abrangência aos atos normativos exarados pela ANCiber, em consonância com a cultura institucional das agências reguladoras no Brasil.			

Audiência Pública da PNCiber – Contribuições

Responsável: Ivanildo de Oliveira da Silva			
Instituição: Cidadão		**Título:** Cidadão	
Tópico: 09-CNCiber	**Id#:** 88	**Parecer:** 3-Inadequada	
Tipo de Contribuição: Comentário	**Artigo:** 14	**Inciso:** 0	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: O inciso X do artigo 14 considera que a ANCiber ficará vinculada ao Gabinete de Segurança Institucional. Porém, apesar do relevante trabalho do GSI, sugiro que o debate acerca de a qual Ministério deveria estar vinculado a ANCiber seja retomado, visando o consenso acerca dessa temática. Além disso, deve-se diferenciar os incidentes que são relevantes em termos de segurança nacional, daqueles que não envolvem Guerra Cibernética.			
Resposta: Não existe inciso X nem no Art. 14 da PNCiber, nem no Anexo I, que estabelece a ANCiber. Não obstante, o texto "Apresentação do Projeto", seção 3.4 explica claramente o motivo da vinculação da ANCiber ao GSI.			

Audiência Pública da PNCiber – Contribuições

Responsável: Diego Marcos Moreira			
Instituição: ANPPD		**Título:** Representante	
Tópico: 09-CNCiber	**Id#:** 47	**Parecer:** 3-Inadequada	
Tipo de Contribuição: Alteração Legal	**Artigo:** 14	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: Acrescentar "contribuir com a ANCiber com propostas de estratégias pcom recomendações à Autarquia ANPD na fiscalização do cumprimento da LGPD".			
Resposta: A fiscalização do cumprimento da LGPD não deve ser atividade da ANCiber. Não obstante, o Art. 18, inciso XXXIV estipula que a ANCiber deve "comunicar às autoridades competentes as infrações penais das quais tiver conhecimento;".			

Audiência Pública da PNCiber – Contribuições

Responsável: Maxli Barroso Campos			
Instituição: LPTIC/EGN		**Título:** Pesquisador Líder	
Tópico: 09-CNCiber	**Id#:** 201	**Parecer:** 3-Inadequada	
Tipo de Contribuição: Inclusão no CNCiber	**Artigo:** 14	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: Art. 14. O Comitê Nacional de Cibersegurança será composto por: [...] Entende-se que seria necessário mencionar como seria a inclusão dos atores acima mencionados no âmbito desse Comitê. A composição do CNCiber foi alterada. Neste item, está prevista a participação de um representante do Ministério de Relações Exteriores. Não seria oportuno mencionar que esse representante deveria ser, obrigatoriamente, um profissional com a formação de um ciberdiplomata"? Assim, não seria conveniente criar um cargo, no âmbito do Ministério de Relações Exteriores, chamado "Ciberdiplomata", o qual seria então esse representante no Comitê da Agência a ser criada? Observações a respeito da "Ciberdiplomacia": - esse tema foi tratado pelo Presidente da Microsoft, Brad Smith, em um evento, dedicado à cibersegurança, (conforme: https://news.microsoft.com/pt-pt/2018/11/05/ciberdiplomacia-como-arma-para-salvar-o-mundo-e-o-tema-que-traz-brad-smith-a-portugal/) em que Brad Smith defendeu a diplomacia como solução para manter a paz mundial e a coordenação de esforços para fazer face às inúmeras ameaças virtuais que surgem diariamente. O evento ocorreu em Portugal em 2018. - No mesmo viés, a União Europeia atua em "AUMENTO DA CIBERDIPLOMACIA", como é possível observar na página do Conselho Europeu: "A União Europeia e os seus Estados-Membros promovem resolutamente um ciberespaço aberto, livre, estável e seguro, no qual os direitos humanos, as liberdades fundamentais e o Estado de direito sejam plenamente respeitados no interesse da estabilidade social, do crescimento económico, da prosperidade e da integridade da vida livre e sociedades democráticas. - A União está envidando grandes esforços para se proteger contra as ciberameaças de países terceiros, nomeadamente através de uma resposta diplomática conjunta denominada "conjunto de ferramentas para a ciberdiplomacia". Essa resposta inclui cooperação e diálogo diplomático, medidas preventivas contra ataques cibernéticos e sanções. A Estratégia de Cibersegurança da UE, adotada em dezembro de 2020 pela Comissão Europeia e o Serviço Europeu para a Ação Externa - SEAE, (serviço diplomático da EU), fortalece a resposta diplomática da UE aos ciberataques." Disponível em: https://www.consilium.europa.eu/es/policies/cybersecurity			
Resposta: Não cabe à PNCiber, mas sim ao MRE, determinar ou não a criação do cargo ou título de "ciberdiplomata".			

Audiência Pública da PNCiber – Contribuições

Responsável: Maxli Barroso Campos			
Instituição: LPTIC/EGN		**Título:** Pesquisador Líder	
Tópico: 09-CNCiber	**Id#:** 202	**Parecer:** 3-Inadequada	
Tipo de Contribuição: Alteração Legal	**Artigo:** 14	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: O "Comitê" está estabelecido em caráter deliberativo, ou seja, possui poder de regulamentação por meio de resoluções, conforme art. 14, inciso II, art. 15, § 4º. Dessa forma, é estranha às suas competências de assessoramento a determinação estabelecida no inciso X, uma vez que se reveste de caráter emergencial, devendo prescindir da necessidade de atuação colegiada, além do fato de o paciente da determinação ser exatamente o Diretor-Geral da ANCiber, que preside o Comitê. esta competência deve ser estabelecida diretamente à ANCiber, ainda que diretamente como competência de seu Diretor-Geral.			
Resposta: A proposta			

Audiência Pública da PNCiber – Contribuições

Responsável: Osmar Assis do Nascimento Filho			
Instituição: Cidadão		**Título:** Cidadão	
Tópico: 09-CNCiber	**Id#:** 230	**Parecer:** 3-Inadequada	
Tipo de Contribuição: Alteração Legal	**Artigo:** 14	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: Quanto a composição, apesar de constar o Ministério da Justiça e Segurança Pública, não consta explicitamente a Policial Federal, órgão no qual há peritos que são muitas vezes chamados em incidentes de segurança da informação. Assim como, não constam a PRF e a ABIN. Considerando o modal rodoviário nacional como o principal para escoamento da produção, é salutar que a PRF seja inserida. Quanto a ABIN, considerando que há uma unidade de inteligência na futura estrutura da ANCiber, é salutar que a ABIN possua cadeira no comitê. Dessa forma, sugiro alterar o inciso II da seguinte forma: - três representantes do Ministério da Justiça e Segurança Pública (1 do MJSP, 1 do quadro de peritos de informática da PF e 1 da Coordenação de Segurança da PRF). Sugiro incluir um representante da Agência Brasileira de Inteligência.			
Resposta: A composição do CNCiber foi alterada de forma a considerar a Polícia Federal, adicionalmente ao MJSP, por sua competência legal na apuração de cibercrimes federais. No tocante à ABIN, considerando-se que a ANCiber deverá integrar o SISBIN, não é necessário incluir a ABIN no CNCiber.			

Audiência Pública da PNCiber – Contribuições

Responsável: Ivanildo de Oliveira da Silva			
Instituição: Cidadão		**Título:** Cidadão	
Tópico: 09-CNCiber	**Id#:** 89	**Parecer:** 3-Inadequada	
Tipo de Contribuição: Inclusão no CNCiber	**Artigo:** 15	**Inciso:** 0	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: Minha sugestão é que a Sociedada Brasileira de Computação (SBC) tenha um representante no Comitê Nacional de Cibersegurança -- seja um dos três representantes de entidades da sociedade com atuação relacionada à cibersegurança, seja um dos três representantes de instituições científicas, tecnológicas e de inovação. A SBC representa a comunidade científica de computação com mais de 20 mil associados e tem histórico de participação em comitês e conselhos da mesma natureza que o CNCiber. É também parceira em ações conjuntas do TSE para testes das urnas eletrônicas há anos. O perfil dos indicados pela SBC será de especialistas técnicos nos aspectos computacionais da cibersegurança. A SBC também tem forte atuação na educação e está trabalhando na definição de um currículo referencial para cursos de bacharelado de cibersegurança. O objetivo é que ele seja uma DCN do Ministério da Educação. Esse referencial pode servir como base para ações da diretoria de cibereducação da ANCiber. A SBC tem como finalidades principais: o Incentivar atividades de ensino, pesquisa e desenvolvimento em computação e informática no Brasil; o Zelar pela preservação e aprimoramento do espírito crítico, responsabilidade profissional e personalidade nacional da comunidade técnico-científica que atua no setor de computação no país; o Manter-se permanentemente atenta à política governamental que afeta as atividades de computação no Brasil, no sentido de assegurar a emancipação tecnológica do país; o Promover a disseminação do conhecimento científico, através de reuniões, congressos, conferências e publicações; o Contribuir para o desenvolvimento científico e tecnológico do país.			
Resposta: A composição do CNCiber, no tocante aos membros permanentes, pressupõe apenas entidades de Estado. De outra parte, os representantes da sociedade se colocam como membros não-permanentes, onde se encontram grupos destinados a permitir a representação de entidades as mais diversas. A SBC, enquanto entidade focada em pesquisa, pode se fazer representar conforme o Art. 15, inciso XVII. Sem prejuízo do disposto no mesmo Art. 15, § 4º, que dispõe que "o Comitê poderá convidar especialistas ou representantes de instituições relevantes para participarem de suas reuniões, mas esses convidados não terão direito a voto nas deliberações."			

Audiência Pública da PNCiber – Contribuições

Responsável: Igor Monteiro Moraes			
Instituição: UFF		**Título:** Pesquisador	
Tópico: 09-CNCiber	**Id#:** 77	**Parecer:** 3-Inadequada	
Tipo de Contribuição: Inclusão no CNCiber	**Artigo:** 15	**Inciso:** 0	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: Considerando a relevância da Sociedade Brasileira de Computação (SBC) no cenário nacional de cibersegurança, por meio de sua Comissão Especial em Segurança da Informação e de Sistemas Computacionais (CESeg), propõe-se uma alteração no inciso XVII do artigo 15 do presente projeto de lei que institui a Política Nacional de Cibersegurança (PNCiber) e o Sistema Nacional de Cibersegurança (SNCiber). Embora a SBC já esteja enquadrada nesse inciso como uma instituição científica, tecnológica e de inovação, é de suma importância a inclusão de uma cadeira específica para a SBC/CESeg no Comitê Nacional de Cibersegurança, além das três cadeiras já descritas. A CESeg tem desempenhado um papel fundamental na área de segurança da informação e sistemas computacionais, organizando a 23 anos o Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais (SBSeg). Esse evento científico, realizado anualmente pela SBC sob a responsabilidade da CESeg, representa o principal fórum do país para a divulgação de resultados de pesquisas, debates, intercâmbio de ideias e atividades relevantes nesse campo. A participação da SBC/CESeg no Comitê Nacional de Cibersegurança fortalecerá ainda mais a representatividade e o conhecimento técnicocientífico necessário para promover a segurança cibernética de forma eficaz e abrangente. Dessa forma, sugere-se que o inciso XVII seja alterado ou que seja inserido um novo inciso para incluir explicitamente a reserva de cadeiras para a SBC/CESeg. Essa medida contribuirá para a integração da comunidade brasileira de pesquisadores e profissionais atuantes na área de segurança da informação e sistemas computacionais, ampliando a participação das i instituições de reconhecido destaque e expertise no setor			
Resposta: A composição do CNCiber, no tocante aos membros permanentes, pressupõe apenas entidades de Estado. De outra parte, os representantes da sociedade se colocam como membros não-permanentes, onde se encontram grupos destinados a permitir a representação de entidades as mais diversas. A SBC, enquanto entidade focada em pesquisa, pode se fazer representar conforme o Art. 15, inciso XVII. Sem prejuízo do disposto no mesmo Art. 15, § 4º, que dispõe que "o Comitê poderá convidar especialistas ou representantes de instituições relevantes para participarem de suas reuniões, mas esses convidados não terão direito a voto nas deliberações."			

Audiência Pública da PNCiber – Contribuições

Responsável: Eduardo James Pereira Souto			
Instituição: UFAM		**Título:** Pesquisador	
Tópico: 09-CNCiber	**Id#:** 50	**Parecer:** 3-Inadequada	
Tipo de Contribuição: Inclusão no CNCiber	**Artigo:** 15	**Inciso:** 0	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: sugiro remover a menção ao GSI até que se defina a qual ministério ficará vinculado a ANCiber, após amplo debate.			
Resposta: A definição do GSI como ministério para vinculação da ANCiber foi feita em estrita concordância com as disposições legais, conforme esclarecido na "Apresentação do Projeto", seção 3.4.			

Audiência Pública da PNCiber – Contribuições

Responsável: Ivanildo de Oliveira da Silva			
Instituição: Cidadão		**Título:** Cidadão	
Tópico: 09-CNCiber	**Id#:** 90	**Parecer:** 3-Inadequada	
Tipo de Contribuição: Comentário	**Artigo:** 15	**Inciso:**	**Parágrafo:** 3
Texto Original: § 5º O Comitê reunir-se-á ordinariamente, em periodicidade bimestral, mediante convocação de seu presidente			
Crítica ou Sugestão: § 5º O Comitê reunir-se-á ordinariamente, em periodicidade semestral, mediante convocação de seu presidente Obs: Consideramos ser mais realista fazer reuniões ordinárias semestrais, devido ao grande numero de participantes do comitê.			
Resposta: A proposta tornaria muito demorada aprovação de Resoluções da ANCiber, e assim engessaria o processo de regulação de uma área por natureza dinâmica.			

Audiência Pública da PNCiber – Contribuições

Responsável: Maxli Barroso Campos			
Instituição: LPTIC/EGN		**Título:** Pesquisador Líder	
Tópico: 09-CNCiber	**Id#:** 203	**Parecer:** 3-Inadequada	
Tipo de Contribuição: Alteração Legal	**Artigo:** 15	**Inciso:**	**Parágrafo:** 5
Texto Original:			
Crítica ou Sugestão: Onde se diz "A partir de 1º de janeiro de 2014" alterar para data válida.			
Resposta: A data está correta, como se encontra na referida lei.			

Audiência Pública da PNCiber – Contribuições

Responsável: Diego Marcos Moreira			
Instituição: ANPPD		**Título:** Representante	
Tópico: 09-CNCiber	**Id#:** 48	**Parecer:** 3-Inadequada	
Tipo de Contribuição: Alteração Legal	**Artigo:** 15	**Inciso:**	**Parágrafo:** 0
Texto Original:			
Crítica ou Sugestão: É importante que haja representatividade da sociedade que representa a área da computação em suas pesquisas, porque sem a representação de quem de fato está na ponta do processo e na formação científica dos profissionais da área nenhum sistema estará bem representado. Minha sugestão é que a Sociedade Brasileira de Computação (SBC) através da sua Comissão Especial da Segurança da Informação e dos Sistemas Computacionais (CESeg) tenha uma das cadeiras no Comitê Nacional de Cibersegurança (CNCiber), e seja representada. Além do mais, a SBC através da CESeg e da sua comissão de Educação vem trabalhando a alguns anos da construção do referencial de formação para a proposição dos Cursos de Bacharelado em CiberSegurança. Em resumo, sem pessoas formadas na prática e escassez de mão de obra é muito difícil a sustentação de qualquer programa ou comitê, e portanto essa representatividade é fundamental.			
Resposta: A composição do CNCiber, no tocante aos membros permanentes, pressupõe apenas entidades de Estado. De outra parte, os representantes da sociedade se colocam como membros não-permanentes, onde se encontram grupos destinados a permitir a representação de entidades as mais diversas. A SBC, enquanto entidade focada em pesquisa, pode se fazer representar conforme o Art. 15, inciso XVII. Sem prejuízo do disposto no mesmo Art. 15, § 4º, que dispõe que "o Comitê poderá convidar especialistas ou representantes de instituições relevantes para participarem de suas reuniões, mas esses convidados não terão direito a voto nas deliberações."			

Audiência Pública da PNCiber – Contribuições

Responsável: Aldri Luiz dos Santos			
Instituição: UFMG		**Título:** Pesquisador	
Tópico: 09-CNCiber	**Id#:** 6	**Parecer:** 3-Inadequada	
Tipo de Contribuição: Inclusão no CNCiber	**Artigo:** 15	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: Incluir explicitamente na composição do Comitê Nacional de Cibersegurança (CNCiber): - um representante da Comissão Especial em Segurança da Informação e de Sistemas Computacionais da Sociedade Brasileira de Computação (CESeg/SBC).			
Resposta: A composição do CNCiber, no tocante aos membros permanentes, pressupõe apenas entidades de Estado. De outra parte, os representantes da sociedade se colocam como membros não-permanentes, onde se encontram grupos destinados a permitir a representação de entidades as mais diversas. A SBC, enquanto entidade focada em pesquisa, pode se fazer representar conforme o Art. 15, inciso XVII. Sem prejuízo do disposto no mesmo Art. 15, § 4º, que dispõe que "o Comitê poderá convidar especialistas ou representantes de instituições relevantes para participarem de suas reuniões, mas esses convidados não terão direito a voto nas deliberações."			

Audiência Pública da PNCiber – Contribuições

Responsável: Célio Vinícius Neves de Albuquerque			
Instituição: UFF		**Título:** Pesquisador	
Tópico: 09-CNCiber	**Id#:** 44	**Parecer:** 3-Inadequada	
Tipo de Contribuição: Inclusão no CNCiber	**Artigo:** 15	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: Incluir explicitamente na composição do Comitê Nacional de Cibersegurança (CNCiber): - um representante da Comissão Especial em Segurança da Informação e de Sistemas Computacionais da Sociedade Brasileira de Computação (CESeg/SBC).			
Resposta: A composição do CNCiber, no tocante aos membros permanentes, pressupõe apenas entidades de Estado. De outra parte, os representantes da sociedade se colocam como membros não-permanentes, onde se encontram grupos destinados a permitir a representação de entidades as mais diversas. A SBC, enquanto entidade focada em pesquisa, pode se fazer representar conforme o Art. 15, inciso XVII. Sem prejuízo do disposto no mesmo Art. 15, § 4º, que dispõe que "o Comitê poderá convidar especialistas ou representantes de instituições relevantes para participarem de suas reuniões, mas esses convidados não terão direito a voto nas deliberações."			

Audiência Pública da PNCiber – Contribuições

Responsável: Débora Christina Muchaluat Saade			
Instituição: UFF		**Título:** Pesquisador	
Tópico: 09-CNCiber	**Id#:** 45	**Parecer:** 3-Inadequada	
Tipo de Contribuição: Inclusão no CNCiber	**Artigo:** 15	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: Incluir explicitamente na composição do Comitê Nacional de Cibersegurança (CNCiber): - um representante da Comissão Especial em Segurança da Informação e de Sistemas Computacionais da Sociedade Brasileira de Computação (CESeg/SBC).			
Resposta: A composição do CNCiber, no tocante aos membros permanentes, pressupõe apenas entidades de Estado. De outra parte, os representantes da sociedade se colocam como membros não-permanentes, onde se encontram grupos destinados a permitir a representação de entidades as mais diversas. A SBC, enquanto entidade focada em pesquisa, pode se fazer representar conforme o Art. 15, inciso XVII. Sem prejuízo do disposto no mesmo Art. 15, § 4º, que dispõe que "o Comitê poderá convidar especialistas ou representantes de instituições relevantes para participarem de suas reuniões, mas esses convidados não terão direito a voto nas deliberações."			

Audiência Pública da PNCiber – Contribuições

Responsável: Diogo Menezes Ferrazani Mattos			
Instituição: UFF		**Título:** Pesquisador	
Tópico: 09-CNCiber	**Id#:** 49	**Parecer:** 3-Inadequada	
Tipo de Contribuição: Inclusão no CNCiber	**Artigo:** 15	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: A composição proposta para o CNCiber é muito rica e diversificada. É de se imaginar que todas as entidades elencadas tenham um grande interesse no tema e desejem fazer parte das importantes discussões e decisões que certamente surgirão. Entretanto, nota-se que a maior parte de tais entidades tem um grande, legítimo e importante interesse em comum na segurança e proteção cibernéticas que é mais do ponto de vista de usuários dos sistemas e potenciais vítimas de algum ciberataque. Na composição do CNCiber falta um peso maior de verdadeiros especialistas no assunto central do comitê, que comungam do interesse comum pela segurança cibernética, mas que, além disso, têm experiência, competência e conhecimentos técnicos profundos exatamente nos temas de interesse do Comitê. Conforme foi apontado durante a audiência pública pelo Prof. Igor Monteiro Moraes da Universidade Federal Fluminense (instante 3:26:26 da gravação), o Brasil tem o privilégio de contar com um grande e consolidado grupo de especialistas altamente qualificados em segurança cibernética, os quais estão reunidos em torno da Comissão Especial de Segurança da Informação e de Sistemas Computacionais (CE-Seg) da Sociedade Brasileira de Computação (SBC). Tais especialistas, majoritariamente docentes e pesquisadores da área acadêmica, têm tido destacada atuação em vários episódios importantes na vida nacional tais como, por exemplo, avaliação da segurança de sistemas eletrônicos de votação (sejam do TSE, do Senado ou da Câmara). Muitos deles têm também destaque internacional em trabalhos de pesquisa, desenvolvimento e aplicação de técnicas de segurança em diversos cenários que serão certamente do interesse do CNCiber. Cabe destacar ainda que tais especialistas têm uma grande interação entre si e organizam, há mais de 20 anos consecutivos, o maior evento acadêmico nacional voltado exclusivamente para segurança cibernética: o SBSeg - Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais. Por estas e várias outras razões, é imperioso que seja alocada uma posição exclusiva e permanente no CNCiber para um representante da Comissão Especial em Segurança da Informação (CS-Seg) da SBC. O meio acadêmico tem por vocação (e dever de ofício) contribuir, ensinar, treinar e esclarecer a sociedade. Não é diferente com os membros da CE-Seg da SBC, o quais estão ávidos por poder finalmente ajudar de forma mais organizada e perene a melhorar as condições de segurança cibernética no país, com propostas, ideias e estratégias aprendidas em anos e anos de estudos e pesquisas, tanto no Brasil como no exterior. O CNCiber não pode abrir mão de contar com tal nível de contribuição de forma permanente em seus quadros. Seria um grande desperdício não ter um canal direto e permanente com todo o setor acadêmico brasileiro especializado em pesquisa, desenvolvimentos e formação de mão-de-obra qualificada na área de segurança da informação e proteção de dados. Pelo exposto, solicito que o CNCiber atribua uma cadeira exclusiva e permanente para um representante da Comissão de Segurança da Sociedade Brasileira de Computação.			
Resposta: A composição do CNCiber, no tocante aos membros permanentes, pressupõe apenas entidades de Estado. De outra parte, os representantes da sociedade se colocam como membros não-permanentes, onde se encontram grupos destinados a permitir a representação de entidades as mais diversas. A SBC, enquanto entidade focada em pesquisa, pode se fazer representar conforme o Art. 15, inciso XVII. Sem prejuízo do disposto no mesmo Art. 15, § 4º, que dispõe que "o Comitê poderá convidar			

especialistas ou representantes de instituições relevantes para participarem de suas reuniões, mas esses convidados não terão direito a voto nas deliberações."

Audiência Pública da PNCiber – Contribuições

Responsável: Marco A. Amaral Henriques			
Instituição: Unicamp		**Título:** Pesquisador	
Tópico: 09-CNCiber	**Id#:** 182	**Parecer:** 3-Inadequada	
Tipo de Contribuição: Inclusão no CNCiber	**Artigo:** 15	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: Dada a especial relevância da Sociedade Brasileira de Computação no cenário nacional de cibersegurança, por meio de sua comissão especial de segurança (CE-SEG), sugiro que uma das vagas no Comitê Nacional de Cibersegurança descritas no inciso XVII seja para reservada para a SBC- CE-Seg.			
Resposta: A composição do CNCiber, no tocante aos membros permanentes, pressupõe apenas entidades de Estado. De outra parte, os representantes da sociedade se colocam como membros não-permanentes, onde se encontram grupos destinados a permitir a representação de entidades as mais diversas. A SBC, enquanto entidade focada em pesquisa, pode se fazer representar conforme o Art. 15, inciso XVII. Sem prejuízo do disposto no mesmo Art. 15, § 4º, que dispõe que "o Comitê poderá convidar especialistas ou representantes de instituições relevantes para participarem de suas reuniões, mas esses convidados não terão direito a voto nas deliberações."			

Audiência Pública da PNCiber – Contribuições

Responsável: Michelle Silva Wangham			
Instituição: UniVale		**Título:** Pesquisador	
Tópico: 09-CNCiber	**Id#:** 211	**Parecer:** 3-Inadequada	
Tipo de Contribuição: Inclusão no CNCiber	**Artigo:** 15	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: Entende-se que o Poder Judiciário está sub-representado na composição do Comitê Nacional de Cibersegurança frente à quantidade de órgãos do Poder Executivo. Um único assento, na representação do CNJ, se mostra incapaz de representar as todas as especificidades dos diversos ramos do Poder Judiciário. Solicita-se que o Conselho da Justiça Federal possua assento no Comitê, representando a Justiça Federal, e recomenda-se que sejam incluídos um representante da Justiça Eleitoral, um representante da Justiça do Trabalho, um representante da Justiça Militar e um representante da Justiça Estadual.			
Resposta: O Conselho Nacional de Justiça (CNJ) é uma instituição pública que visa a aperfeiçoar o trabalho do Judiciário brasileiro, principalmente no que diz respeito ao controle e à transparência administrativa e processual. Sua missão é promover o desenvolvimento do Poder Judiciário em benefício da sociedade, por meio de políticas judiciárias e do controle da atuação administrativa e financeira. Outrossim, é o órgão adequado para representar o judiciário junto ao CNCiber e ao GGCiber.			

Audiência Pública da PNCiber – Contribuições

Responsável: Renato Solimar Alves			
Instituição: CJF		**Título:** Servidor	
Tópico: 09-CNCiber	**Id#:** 248	**Parecer:** 3-Inadequada	
Tipo de Contribuição: Inclusão no CNCiber	**Artigo:** 15	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: Uma vez que o Comitê Nacional de Cibersegurança tem atuação deliberativa e de aprovação (de "Estratégia Nacional de Cibersegurança, Plano Nacional de Cibersegurança, Complexo Nacional de Cibersegurança"), deve-se pensar numa estrutura deliberativa, seja por voto qualificado, seja por consenso. Não se pode deixar a cargo de Decreto disciplinar a forma de deliberação para aprovação desses instrumentos, ante o risco de insegurança que decorre. Necessário, portanto, que a Lei que disciplina o Comitê Nacional de Cibersegurança apresente os critérios de suas deliberações para atendimento da segurança jurídica esperada deste órgão.			
Resposta: A PNCiber é uma política nacional, e assim foca mais no "o que" do que no "como", até como forma de assegurar sua perenidade. Outrossim, não cabe esse detalhamento da operacionalização das instituições neste instrumento, mas sim em ato do executivo, como descrito no anteprojeto.			

Audiência Pública da PNCiber – Contribuições

Responsável: João Araújo Monteiro Neto			
Instituição: GETIS/Unifor		**Título:** Pesquisador	
Tópico: 09-CNCiber	**Id#:** 111	**Parecer:** 3-Inadequada	
Tipo de Contribuição: Alteração Legal	**Artigo:** 16	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: Outro ponto que eu achei, talvez, precisarei de um pouco mais, de um pouco mais de detalhes, é, qual seria a, o papel do Comitê Gestorial de Segurança da Informação, que ainda existem no GSI, mas esse ponto não é esclarecido muito bem na proposta. Então, poderia até uma superposição de dois órgãos basicamente iguais, então eu sugiro também talvez detalhar como essa sucessão poderia acontecer.			
Resposta: Não se pretende interferir no funcionamento do CGSI. O que se pretende é que as funções relativas à cibersegurança sejam assumidas pela PNCiber e seus intrumentos. O que resguarda a Segurança da Informação que não seja afeto à cibersegurança continuará sob a égide da PNSI e do CGSI. Ressalta-se que a PNSI foi instituída por meio de decreto presidencial, e assim tem seu escopo limitado à APF.			

Audiência Pública da PNCiber – Contribuições

Responsável: Luca Belli			
Instituição: FGV		**Título:** Professor	
Tópico: 09-CNCiber	**Id#:** 168	**Parecer:** 3-Inadequada	
Tipo de Contribuição: Alteração Legal	**Artigo:**	**Inciso:**	**Parágrafo:**
Texto Original: XIV - avaliar e certificar produtos e serviços, no tocante à cibersegurança, diretamente ou por meio de parceiros credenciados pela ANCiber;			
Crítica ou Sugestão: Não ficou claro no texto que tipo de modelo de maturidade iremos empregar para certificação? Já temos iniciativas no Brasil nesta área, lideradas pela ANATEL, INMETRO, ITI - Existe uma corrente internacional que se torna impossível garantir a certificação de produtos e serviços, na medida em que é impossível se garantir a cadeia de fornecimento. Fica como sugestão a proposição de realizar acompanhamentos de aquisições complexas e estratégicas para o país. De qualquer forma, esta iniciativa acaba se chocando com as ações na área de CT&I.			
Resposta: A PNCiber é uma política nacional, e assim foca mais no "o que" do que no "como", até como forma de assegurar sua perenidade. Outrossim, não cabe esse tipo de detalhamento neste instrumento, mas sim em resoluções da Diretoria Colegiada da ANCiber a serem aprovadas pelo CNCiber oportunamente.			

Audiência Pública da PNCiber – Contribuições

Responsável: Maxli Barroso Campos			
Instituição: LPTIC/EGN		**Título:** Pesquisador Líder	
Tópico: 10-ANCiber	**Id#:** 204	**Parecer:** 3-Inadequada	
Tipo de Contribuição: Alteração Infralegal	**Artigo:** 17	**Inciso:** 0	**Parágrafo:**
Texto Original: XV - fiscalizar e aplicar sanções em caso de descumprimento dos normativos estipulados pela ANCiber, mediante processo administrativo que assegure o contraditório, a ampla defesa e o direito de recurso;			
Crítica ou Sugestão: . A ANCiber será um órgão auditor? A missão da ANCiber é ser um órgão regulador, operativo ou auditor? . Também não ficou claro se estes normativos serão adotados de padrões consolidados internacionalmente ou serão desenvolvidos em território nacional, usando as excelentes qualificações de nossos profissionais, com envolvimento de toda a sociedade.			
Resposta: A ANCiber será uma agência reguladora, que como suas congêneres tem atribuições reguladoras, operativas e de fiscalização. No tocante aos padrões a serem adotados, a PNCiber é uma política nacional, e assim foca mais no "o que" do que no "como", até como forma de assegurar sua perenidade. Outrossim, não cabe esse tipo de detalhamento neste instrumento, mas sim em resoluções da Diretoria Colegiada da ANCiber a serem aprovadas pelo CNCiber oportunamente.			

Audiência Pública da PNCiber – Contribuições

Responsável: Maxli Barroso Campos			
Instituição: LPTIC/EGN		**Título:** Pesquisador Líder	
Tópico: 10-ANCiber	**Id#:** 205	**Parecer:** 3-Inadequada	
Tipo de Contribuição: Dúvida	**Artigo:** 17	**Inciso:** 0	**Parágrafo:**
Texto Original: XXIV - realizar atividades de comunicação e de promoção da conscientização em matéria de cibersegurança, a fim de contribuir para o desenvolvimento de uma cultura nacional sobre o tema;			
Crítica ou Sugestão: Obs: - Sendo um documento de Estado e estando a missão de educação com o Ministério da Educação, estas ações deveriam ser feitas por meio de colaboração e integração com aquele Ministério. Fica a recomendação de sempre que possível indicar o ente federativo que é responsável por diferentes atividades descritas nesta política. - Uma ação simples, inclusive, seria a inclusão nos curriculos básicos matérias relacionadas com a cibernética, dentro de uma Estratégia de Estado, com a participação de todos os Ministérios e o entendimento do problema e impactos de uma incidente cibernético.			
Resposta: A sugestão foi anotada para implementação oportuna, por meio dos instrumentos infra legais aplicáveis.			

Audiência Pública da PNCiber – Contribuições

Responsável: Maxli Barroso Campos			
Instituição: LPTIC/EGN		**Título:** Pesquisador Líder	
Tópico: 10-ANCiber	**Id#:** 206	**Parecer:** 3-Inadequada	
Tipo de Contribuição: Alteração Infralegal	**Artigo:** 17	**Inciso:** 0	**Parágrafo:**
Texto Original: XXVI - promover a formação, o crescimento técnico e profissional e a qualificação de recursos humanos na área de cibersegurança..			
Crítica ou Sugestão: Obs: A falta de líderes (decisores) nas diferentes esferas do poder com o conhecimento e entendimento do problema precisa ser resolvida, começando com um amplo trabalho de conscientização dos nossos políticas, que serão responsáveis por garantir recursos financeiros para esta iniciativa. Seria oportuno não apenas privilegiar o conhecimento técnico, mas principalmente o de gestão e com visão estratégica. São duas abordagens extremamente diferentes. O técnico por mais que ele seja preparado, ele depende de ordem e indicação da necessidade de se implementar ou melhor determinado requisito de segurança. Inclusive a formação destes líderes poder começar com todos os integrantes do Gabinete de Gerenciamento de Cibercrises ("Gabinete")			
Resposta: A sugestão foi anotada para implementação oportuna, por meio dos instrumentos infra legais aplicáveis.			

Audiência Pública da PNCiber – Contribuições

Responsável: Maxli Barroso Campos			
Instituição: LPTIC/EGN		**Título:** Pesquisador Líder	
Tópico: 10-ANCiber	**Id#:** 207	**Parecer:** 3-Inadequada	
Tipo de Contribuição: Comentário	**Artigo:** 17	**Inciso:** 0	**Parágrafo:**
Texto Original: Art. 17 . Fica criada a Agência Nacional de Cibersegurança (ANCiber), autarquia sob regime especial, com autonomia administrativa e financeira e patrimônio próprio, vinculada ao Gabinete de Segurança Institucional da Presidência da República, com foro e sede no Distrito Federal.			
Crítica ou Sugestão: O artigo 17 considera que a ANCiber ficará vinculada ao Gabinete de Segurança Institucional. Porém, apesar do relevante trabalho do GSI, sugiro que o debate acerca de a qual Ministério deveria estar vinculado a ANCiber seja retomado, visando o consenso acerca dessa temática			
Resposta: A definição do GSI como ministério para vinculação da ANCiber foi feita em estrita concordância com as disposições legais, conforme esclarecido na "Apresentação do Projeto", seção 3.4.			

Audiência Pública da PNCiber – Contribuições

Responsável: Ivanildo de Oliveira da Silva			
Instituição: Cidadão		**Título:** Cidadão	
Tópico: 10-ANCiber	**Id#:** 91	**Parecer:** 3-Inadequada	
Tipo de Contribuição: Alteração Legal	**Artigo:** 17	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: A ANCIber poderia reunir todas as condições para se tornar em um grande Centro de Cibernética no Brasil, com capacidade de atuar em ambiente interagências, assim como ocorre em Bon na Alemanha. Referência: https://www.defesanet.com.br/cyberwar/noticia/1500/alemanha-inaugura-centro-de-defesa-cibernetica-em-bonn/ O texto não deixa claro que a ANCiber será um órgão apenas regulador ou operativo, com a missão também de atuar em ambiente interagências em tempo real, realizando a integração com todos os stakeholders e com condições de realizar ações de mitigação de ataques cibernéticos.			
Resposta: A ANCiber será uma agência reguladora, que como suas congêneres tem atribuições reguladoras, operativas e de fiscalização. A atribuição de coordenação dos envolvidos encontra-se prevista no Art. 18, inciso XXXVI.			

Audiência Pública da PNCiber – Contribuições

Responsável: João Araújo Monteiro Neto			
Instituição: GETIS/Unifor		**Título:** Pesquisador	
Tópico: 10-ANCiber	**Id#:** 112	**Parecer:** 3-Inadequada	
Tipo de Contribuição: Dúvida	**Artigo:** 17	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: A competência elencada no inciso VI, do art. 18 ("desenvolver capacidades nacionais de prevenção, monitoramento, detecção, análise e resposta, para detectar e gerenciar ciberincidentes") defere amplos poderes à Anciber, inclusive no âmbito preventivo. É necessário olhar com parcimônia o deferimento de poderes amplos de prevenção a ciberincidentes ao Estado, posto que é necessária a preservação e avanço dos direitos digitais, especialmente de privacidade. Dessa forma, é necessária a insituição de medida de contraprestação à amplitude de poderes deferidos à Anciber através da formulação de mecanismos de supervisão e escrutínio público de sua atuação. De forma semelhante, é necessário que a Anciber promova a garantia da criptografia em seus diversos contextos, devendo o texto do PL prever expressamente tal previsão. A criptografia na camada de transporte (no protocolo HTTP, TLS ou SSL) e nas comunicações (end-to-end) se mostra reconhecidamente como meio de promoção de direitos fudamentais em âmbito digital. A criptografia representa especial meio de promoção da cibersegurança, devendo-se ter em mente que a inclusão de backdoors ou outros mecanismos que venham a desconstituir a criptografia end-to-ende nfraquece essa tecnologia para todos os usuários da rede, trazendo abalos para a estabilidade da internet. Nesse sentido, a Comissão Global pela Estabilidade do Ciberespaço reconhece os mecanismos criptográficos como parte do Núcleo da Internet, consentâneo aos elementos críticos da infraestrutura da Internet, estatuindo uma norma de não prejuízo por agentes estatais e não estatais em vista à ciberestabilidade.			
Resposta: As capacidades de monitoramento estipuladas no referido artigo são limitadas à finalidade de detecção e gerenciamento de ciberincidentes. Nesse contexto, diferentemente do que alegam os autores, não se confere "amplos poderes" à ANCiber. Adicionalmente, todas as ações da ANCiber devem ser aprovadas pelo CNCiber, do qual participam o CNJ, o CNMP, e a ANPD, órgãos responsáveis pela manutenção dos direitos individuais, inclusive aqueles digitais. Ademais, o regramento de direitos digitais, que antecede a PNCiber, não é alterado em nenhum ponto pelo presente anteprojeto. Dessa forma, permanecem todas as proteções ao cidadão asseguradas pelo arcabouço legal pátrio. Ao contrário do que depreende o autor, pretende-se que a ANCiber seja um importante instrumento para ampliar a proteção ao cidadão, como refletido no Art. 5, inciso I. Por fim, não há nenhuma referência a potenciais ações contra a criptografia na camada de transporte no anteprojeto em análise.			

Audiência Pública da PNCiber – Contribuições

Responsável: Rodrigo Azevedo Greco			
Instituição: Cidadão		**Título:** Advogado	
Tópico: 10-ANCiber	**Id#:** 255	**Parecer:** 3-Inadequada	
Tipo de Contribuição: Alteração Legal	**Artigo:** 18	**Inciso:** 0	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: Ainda no tema de certificação de produtos, a Anatel, hoje, ela já certifica equipamentos de telecomunicações, inclusive levando em consideração aspectos relacionados a cybersegurança. A dúvida que fica é se a ANCiber estaria propondo requisitos novos que deveriam ser levados em consideração pela Anatel no processo de certificação que ela conduz, ou se os produtos estariam sujeitos a uma dupla certificação pela Anatel e pela, e pela ANCiber.			
Resposta: Na ausência de uma agência nacional específica para regular as atividades de cibersegurança no País, agências setoriais como ANATEL, BACEN, ANEEL e diversas outras assumiram, setorialmente, essa lacuna. O que se pretende é que a ANCiber se coordene com as demais agências para que a certificação, inclusive no âmbito da cibersegurança. seja a mais transparente possível, evitando-se a duplicidade de esforços sempre que possível.			

Audiência Pública da PNCiber – Contribuições

Responsável: Rodrigo Azevedo Greco			
Instituição: Cidadão		**Título:** Advogado	
Tópico: 10-ANCiber	**Id#:** 256	**Parecer:** 3-Inadequada	
Tipo de Contribuição: Alteração Legal	**Artigo:** 18	**Inciso:** 0	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: Do ponto de vista comportamental, a preocupação da ABRINT se estende além do diálogo institucional e alcança o respeito às competências das outras agências reguladoras. Compartilhar iniciativas é relevante e necessário, mas não se pode deixar de lado as competências setoriais.			
Resposta: As competências originárias de todas as agências reguladoras estão inteiramente preservadas. De outra parte, a cibersegurança não é competência originária de nenhuma delas, e a ausência de uma coordenação nacional sobre o tema é um dos elos que enfraquece a cibersegurança nacional. e que, como reconhece a própria ANATEL, carece de uma centralização. Não obstante, as agências reguladoras de setores considerados infraestruturas críticas foram incluídas no CNCiber de forma a ampliar a possibilidade de diálogo e coordenação intersetorial da ANCiber.			

Audiência Pública da PNCiber – Contribuições

Responsável: João Araújo Monteiro Neto			
Instituição: GETIS/Unifor		**Título:** Pesquisador	
Tópico: 10-ANCiber	**Id#:** 113	**Parecer:** 3-Inadequada	
Tipo de Contribuição: Comentário	**Artigo:** 18	**Inciso:** 0	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: Sugere-se retirar o termo "não vinculativos" por total desnecessidade no contexto, uma vez que foge ao teor desta lei qualquer ingerência sobre as competências jurídicas pré-estabelecidas no ordenamento.			
Resposta: A alteração não é aplicável.			

Audiência Pública da PNCiber – Contribuições

Responsável: Osmar Assis do Nascimento Filho			
Instituição: Cidadão		**Título:** Cidadão	
Tópico: 10-ANCiber	**Id#:** 231	**Parecer:** 3-Inadequada	
Tipo de Contribuição: Alteração Legal	**Artigo:** 18	**Inciso:** 0	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: Sobre o CTIR.br, comentar se haverá integração com outros centros de resposta a incidentes, como os mantidos pelo CERT.br e pela RNP.			
Resposta: Conforme previsto no Art. 41, o CTIR.Br operará como centralizador da REGIC, nos moldes do disposto no Decreto 10.748. Outrossim, sua relação com as demais entidades já se encontra determinada.			

Audiência Pública da PNCiber – Contribuições

Responsável: Igor Monteiro Moraes			
Instituição: UFF		**Título:** Pesquisador	
Tópico: 10-ANCiber	**Id#:** 78	**Parecer:** 3-Inadequada	
Tipo de Contribuição: Alteração Legal	**Artigo:** 18	**Inciso:** 0	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: Um ponto que eu queria destacar é a criação do CTIR.Br, que também acho um ponto extremamente positivo, ter um centro de reação aos incidentes cibernéticos, porém não é destacado como se articularia com o CTIR Gov, que já existe, e também com os outros dois sítio nacionais, que são o CERT.Br e o CAIS da RNP. Eu lembro que esse ponto, aliás, essa confusão que existe no Brasil, que é o único país que tem vários sítios nacionais, foi destacado numa reunião do grupo de segurança da informação, das TIC do BRICS, que foi (Ininteligível) aqui em Brasília. Eu fui convidado pelo Jefferson (Ininteligível), é, há cinco anos. Eu lembro que os parceiros do BRICS destacaram a dificuldade de se coordenar por causa dessa existência de 3 sítios nacionais múltiplos. Aí, uma solução para resolver, e até criar uma coordenação na agência, isso aí é a criação de uma rede nacional de cibersegurança, que destacavam o nosso estudo, no modelo do European Cybersecurity Competence Centre and Network, que foi criado somente o ano passado e que cria, basicamente, uma rede de centros de pesquisa, é, centros acadêmicos, e centros de resposta-ataque para coordenar essa resposta e também para compartilhar boas práticas.			
Resposta: O CTIR.Br assumirá a função de centralizador da Rede Nacional de ETIRs setoriais, hoje chamada Rede Federal de Gestão e Tratamento de Incidentes Cibernéticos (REGIC). Será também o centralizador dos incidentes dos integrantes do Complexo Nacional de Cibersegurança. E assumirá ainda a função de CTIR nacional no tocante à representação do país no exterior, observando-se que a ANCiber pode delegar essa responsabilidade a outros interessados sob sua coordenação. O CTIR Gov, conforme dispõe o Art. 41, § 2º, deixará de ser o centralizador da REGIC e passará a atuar como ETIR setorial dos órgãos da Presidência da República, ligando-se ao CTIR.Br. O CERT.Br e o CAIS da RNP continuarão tendo suas atribuições usuais, podendo, eventualmente, integrarem-se ao CTIR.Br.			

Audiência Pública da PNCiber – Contribuições

Responsável: Luca Belli			
Instituição: FGV		**Título:** Professor	
Tópico: 10-ANCiber	**Id#:** 169	**Parecer:** 3-Inadequada	
Tipo de Contribuição: Alteração Legal	**Artigo:** 18	**Inciso:** 0	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: XIV: "avaliar e certificar produtos e serviços, no tocante à cibersegurança, diretamente ou por meio de parceiros credenciados pela ANCiber;", como será feita essa certificação dos produtos e serviços, bem como avaliar se há sombreamento quanto à homologação de produtos realizada pela ANATEL;			
Resposta: A PNCiber é uma política nacional, e assim foca mais no "o que" do que no "como", até como forma de assegurar sua perenidade. Outrossim, não cabe esse tipo de detalhamento neste instrumento, mas sim em resoluções da Diretoria Colegiada da ANCiber a serem aprovadas pelo CNCiber oportunamente. Não se percebe a possibilidade de "sombreamento" com a ANATEL (e nem com outras agências reguladoras), pois que a ANCiber será a responsável pelo tocante à cibersegurança, e coordenará com as demais agências reguladoras a certificação de produtos e serviços no tocante a essa temática.			

Audiência Pública da PNCiber – Contribuições

Responsável: Frederico Fernandes Neres			
Instituição: Caixa		**Título:** Gerente	
Tópico: 10-ANCiber	**Id#:** 64	**Parecer:** 3-Inadequada	
Tipo de Contribuição: Preoc. ANATEL	**Artigo:** 18	**Inciso:** 0	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: Além das questões relativas propriamente à estrutura institucional desenhada para a PNCiber, o Projeto também apresenta características que geram incerteza quanto à forma de sua inserção no ordenamento jurídico existente. A PNCiber não surge de um vácuo regulatório, mas deve ser compatibilizada com regras existentes, inclusive explicitando quando deverá se sobrepor em eventual situação de conflito. Por exemplo, vale citar a competência da ANCiber de avaliar e certificar produtos e serviços, no tocante à cibersegurança (art. 18, XIV), que gera possível sobreposição com as atividades da Anatel e do INMETRO.			
Resposta: Não se percebe a possibilidade de "sobreposição" com as atividades da ANATEL (e nem com outras agências reguladoras) ou o INMETRO, posto que a ANCiber será a responsável nacional pelos padrões de certificação no tocante à cibersegurança, e coordenará com as demais agências reguladoras e cewrtificadoras a certificação de produtos e serviços no tocante a essa temática.			

Audiência Pública da PNCiber – Contribuições

Responsável: Núcleo de Pesquisa em Concorrência, Política Pública, Inovação e Tecnologia (Comppit)			
Instituição: FGV		**Título:** Pesquisador	
Tópico: 10-ANCiber	**Id#:** 217	**Parecer:** 3-Inadequada	
Tipo de Contribuição: Comentário	**Artigo:** 18	**Inciso:** 0	**Parágrafo:**

Texto Original:

Crítica ou Sugestão:

A Anatel tem avançado com algumas iniciativas relacionadas à certificação em cibersegurança. No início de 2021, a Anatel publicou o Ato nº 77/20214, que estabelece requisitos de segurança cibernética para equipamentos de telecomunicações. Em março deste ano, publicou o Ato nº 2436/20235, que aprova os requisitos mínimos mandatórios de segurança cibernética para avaliação da conformidade de equipamentos CPE (Customer Premises Equipment).

Nesse sentido, preocupa-nos a intenção do GSI de criar um novo esquema de certificação, sob responsabilidade da futura Agência Nacional de Cibersegurança, que seria complementar e independente ao da ANATEL.

A criação de um novo e amplo arcabouço de certificação traria custos ainda maiores aos fabricantes de equipamentos de TIC, além de atrasar a disponibilização de novas tecnologias no mercado brasileiro, devido ao caráter burocrático e complexo inerente a processos de certificação. Em última análise, tornaria o acesso a novas soluções de cibersegurança mais difícil e caro, indo contra o objetivo perseguido pelo próprio PL de Ciber.

De qualquer forma, a Brasscom gostaria de reforçar o seu posicionamento geral de que não recomenda entidades ou terceiros autorizados por entidades a certificar serviços, pois já existem acreditações reconhecidas globalmente, tais como ISO 27701, CSA STAR, SOC, dentre outras.

Por exemplo, a verificação de segurança dos centros de dados e serviços do provedor de serviços de nuvem (CSP) é realizada por auditores terceirizados independentes para garantir que o CSP implementou as medidas de segurança apropriadas, e de acordo com os padrões internacionais, para obter as certificações de segurança relevantes. Os CSPs receberam os credenciamentos e certificações mais influentes e reconhecidos internacionalmente em segurança de sistemas e informações, incluindo controles de segurança física em data centers e controles específicos para provedores de serviços em nuvem, como a certificação ISO 27017, que é o código de melhores práticas publicado pela International Organization for Standardization ("ISO"). Em outras palavras, ao invés de criar esquemas nacionais próprios de certificações, o Brasil deveria avançar para implementar estruturas que reconheçam selos e certificados internacionais, garantindo-se assim a inserção do país nas cadeias globais de valor, promovendo as melhores práticas internacionais e evitando obstáculos à adoção, no país, de tecnologia de ponta das mais modernas.

Resposta:

A PNCiber visa coordenar as ações de cibersegurança atualmente tomadas em âmbito setorial, como aquelas citadas, que foram adotadas pela ANATEL (e por outras agências reguladoras setoriais) justamente pela falta de um ente responsável nacionalmente pela temática. O processo de certificação em cibersegurança já é adotado em diversos países por agências congêneres à ANCiber. Outrossim, a preocupação foi anotada e será levada em consideração quando da definição dos critários e do processo de certificação em cibersegurança a ser promovido pela ANCiber.

Audiência Pública da PNCiber – Contribuições

Responsável: Sarah Melo Martins			
Instituição: Brasscom		**Título:** Representante	
Tópico: 10-ANCiber	**Id#:** 263	**Parecer:** 3-Inadequada	
Tipo de Contribuição: Preoc. ANATEL	**Artigo:** 18	**Inciso:** 0	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: Várias competências colidem diretamente com competências setoriais das Agências Reguladoras (ARs) que precisam ser mantidas. Sugere-se a alteração do texto, por exemplo no tema da certificação, para ressalvar as competências da Anatel. Sugestão: Art. 18, XIV - avaliar e certificar produtos e serviços, no tocante à cibersegurança, diretamente ou por meio de parceiros credenciados pela ANCiber, ressalvada a competência de certificação de produtos da Agência Nacional de Telecomunicações (Anatel);			
Resposta: A ANATEL avançou na certificação em cibersegurança setorial na ausência de um órgão específico para o tema (assim como a ANEEL e o BACEN). Com a entrada em operação da ANCiber, que tem a responsabilidade de coordenação nacional na temática, haverá a necessidade de articulação desta com suas congêneres para que, no tocante à cibersegurança, os critérios de certificação sejam estabelecidos pela ANCiber. Isso é o que está disposto no anteprojeto de lei.			

Audiência Pública da PNCiber – Contribuições

Responsável: Vanessa Copeti Cravo			
Instituição: ANATEL		**Título:** GTCiber	
Tópico: 10-ANCiber	**Id#:** 276	**Parecer:** 3-Inadequada	
Tipo de Contribuição: Preoc. ANATEL	**Artigo:** 18	**Inciso:** 0	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: A certificação de produtos pode conflitar com as atribuições da Anatel como órgão certificador de produtos de telecomunicações.			
Resposta: Não se observa a perspectiva de conflito com as atribuições da Anatel, em particular no tocante ao tema da certificação. A ANATEL avançou certificações em cibersegurança na ausência de um órgão específico para o tema (assim como a ANEEL e o BACEN). Com a entrada em operação da ANCiber, com essa responsabilidade específica, haverá a necessidade de articulação desta com suas congêneres para que, no tocante à cibersegurança, os critérios de certificação sejam estabelecidos pela ANCiber.			

Audiência Pública da PNCiber – Contribuições

Responsável: Jeferson Fued Nacif			
Instituição: MCom		**Título:** Servidor	
Tópico: 10-ANCiber	**Id#:** 106	**Parecer:** 3-Inadequada	
Tipo de Contribuição: Preoc. ANATEL	**Artigo:** 18	**Inciso:** 0	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: XV: Importante deixar clara a forma de fiscalização que será realizada, possivelmente dando clareza no uso de critérios claros de avaliação das instituições (com possível uso de frameworks de mercado);			
Resposta: A PNCiber é uma política nacional, e assim foca mais no "o que" do que no "como", até como forma de assegurar sua perenidade. Outrossim, não cabe esse tipo de detalhamento neste instrumento, mas sim em resoluções da Diretoria Colegiada da ANCiber a serem aprovadas pelo CNCiber oportunamente.			

Audiência Pública da PNCiber – Contribuições

Responsável: Frederico Fernandes Neres			
Instituição: Caixa		**Título:** Gerente	
Tópico: 10-ANCiber	**Id#:** 65	**Parecer:** 3-Inadequada	
Tipo de Contribuição: Alteração Infralegal	**Artigo:** 18	**Inciso:** 0	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: XXIX: Esclarecer como a sociedade será ouvida, dando clareza quanto aos dispositivos que serão utilizados para contato pela e com a sociedade.			
Resposta: A PNCiber é uma política nacional, e assim foca mais no "o que" do que no "como", até como forma de assegurar sua perenidade. Outrossim, não cabe esse tipo de detalhamento neste instrumento, mas sim em resoluções da Diretoria Colegiada da ANCiber a serem aprovadas pelo CNCiber oportunamente.			

Audiência Pública da PNCiber – Contribuições

Responsável: Frederico Fernandes Neres			
Instituição: Caixa		**Título:** Gerente	
Tópico: 10-ANCiber	**Id#:** 66	**Parecer:** 3-Inadequada	
Tipo de Contribuição: Alteração Infralegal	**Artigo:** 18	**Inciso:** 0	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: A competência elencada no inciso XXIX, do art. 18 ("ouvir a sociedade em matérias de interesse relevante e prestar contas sobre suas atividades e planejamento") não deve ser mera retórica, mas devem ser instituídos parâmetros mínimos para transparência e prestação de contas das ações da Anciber. De forma semelhante, a oitiva da sociedade em matérias de interesse relevante deve ter parâmetros mínimos fixados em Lei, delimitando critérios de eleição das "matérias de interesse relevante", e mecanismos dessa oitiva. É necessário, portanto, que se insira no texto normativo os mecanismos de participação popular, dentre os quais as audiências públicas, tomada de subsídios, consultas a especiais, dando ênfase à participação popular. De forma semelhante, é necessária a definição de parâmetros mínimos para a prestação de contas da Anciber à sociedade, instrumentalizando mecanismos como a Avaliação de Impacto Regulatório, ex ante, e a Avaliação de Resultado Regulatório, ex post, além de portais de publicização de suas atividades e formalização de sua agenda regulatória. A prestação de contas à sociedade deve ser enxergada para além do caráter passivo de demonstração de resultados, mas deve poder ser viável ao escrutínio público, através de um fórum público de tomada e julgamento. Para que o fórum público de prestação de conta possa existir, é necessária a existência concomitante de três requisitos [1]: é necessário que a agência seja obrigada a informar ao fórum sobre sua conduta; deve haver possibilidade de o fórum questionar a adequação da informação ou legitimidade da conduta; e o fórum deve poder julgar sua conduta, resultando em consequências para a agência. [1] BOVENS, Mark. Analysing and Assessing Accountability: A Conceptual Framework. In: European Law Journal, Vol. 13, No. 4, July 2007, p. 447-468.			
Resposta: A PNCiber é uma política nacional, e assim foca mais no "o que" do que no "como", até como forma de assegurar sua perenidade. Outrossim, não cabe esse tipo de detalhamento neste instrumento, mas sim em resoluções da Diretoria Colegiada da ANCiber a serem aprovadas pelo CNCiber oportunamente. De outra parte, os instrumentos serão os mesmos utilizados pelas demais agências reguladoras, conforme estipulado no marco regulatório vigente.			

Audiência Pública da PNCiber – Contribuições

Responsável: João Araújo Monteiro Neto			
Instituição: GETIS/Unifor		**Título:** Pesquisador	
Tópico: 10-ANCiber	**Id#:** 114	**Parecer:** 3-Inadequada	
Tipo de Contribuição: Alteração Infralegal	**Artigo:** 18	**Inciso:** 0	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: Apesar da competência do Ministério da Educação e do Ministério da Ciência e Tecnologia, a forma como estão definidas suas participações nos incisos XXV e XXVI, comprometem a autonomia administrativa e de regulação da ANCiber. Assim, sugiro trocar a expressão "em Coordenação" que consta ao final de ambos os incisos para "com o apoio".			
Resposta: Não se entende haver "comprometimento da autonomia" da ANCiber nos temas expostos. A coordenação é uma necessidade, quando mais de um órgão está envolvido em uma atividade cooperativa.			

Audiência Pública da PNCiber – Contribuições

Responsável: Ivanildo de Oliveira da Silva			
Instituição: Cidadão		**Título:** Cidadão	
Tópico: 10-ANCiber	**Id#:** 92	**Parecer:** 3-Inadequada	
Tipo de Contribuição: Alteração Legal	**Artigo:** 18	**Inciso:** 0	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: é preciso que haja previsão de como se darão as receitas e formas de arrecadação para sustento da ANCiber. Nesse sentido o comentário é para que haja a inserção de previsão, específica sobre os mecanismos de financiamento da ANCiber que não poderá onerar setores de infraestruturas críticas. XXX - arrecadar e aplicar suas receitas;			
Resposta: As receitas da ANCiber estã detalhadas no ANEXO I, Art. 21.			

Audiência Pública da PNCiber – Contribuições

Responsável: Luiz Henrique Barbosa da Silva			
Instituição: TELCOMP		**Título:** Representante	
Tópico: 10-ANCiber	**Id#:** 176	**Parecer:** 3-Inadequada	
Tipo de Contribuição: Alteração Legal	**Artigo:** 18	**Inciso:** 0	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: Sugere-se que a deliberação sobre suas competências esteja fora da própria ANCiber, restando a possibilidade de esta atribuição pertencer ao "Comitê", evitando assim o esgotamento de discussão sobre sua competência dentro de sua própria estrutura. LEMBRANDO QUE ESTE INCISO RETIRA DO PRÓPRIO GSI A CAPACIDADE DE ATUAÇÃO DE SUPERVISÃO SOBRE A INTERPRETAÇÃO DESTA LEI QUANDO NA ESFERA ADMINISTRATIVA, POR FORÇA DE ESTABELECIMENTO DA PRÓPRIA LEI.			
Resposta: O texto segue o padrão estipulado para as demais agências reguladoras no arcabouço institucional pátrio.			

Audiência Pública da PNCiber – Contribuições

Responsável: Osmar Assis do Nascimento Filho			
Instituição: Cidadão		**Título:** Cidadão	
Tópico: 10-ANCiber	**Id#:** 232	**Parecer:** 3-Inadequada	
Tipo de Contribuição: Alteração Legal	**Artigo:** 18	**Inciso:** 0	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: No art. 18, sobre as competências da ANCiber, sugere-se que as competências referentes aos incisos XXXII e XXXIII sejam atribuídas ao Comitê Nacional de Cibersegurança, uma vez que há previsão, no art. 14, sobre as competências do referido Comitê, no inciso I - propor políticas, diretrizes, estratégias e normas relacionadas à cibersegurança nacional; e no inciso II - aprovar, por meio de resolução, os atos normativos concernentes à cibersegurança nacional. Desse modo, se manteria o alinhamento de atribuições.			
Resposta: À ANCiber cabe propor resoluções. Ao CNCiber compete propor políticas e aprovar as resoluções da ANCiber. Por conseguinte, não há conflito.			

Audiência Pública da PNCiber – Contribuições

Responsável: Arthur Pereira Sabbat			
Instituição: ANPD		**Título:** Diretor	
Tópico: 10-ANCiber	**Id#:** 23	**Parecer:** 3-Inadequada	
Tipo de Contribuição: Alteração Legal	**Artigo:** 18	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: O Artigo 18 da proposta de projeto de lei em questão estabelece o escopo de atuação da Agência Nacional de Cibersegurança (ANCiber), incluindo a responsabilidade por certificação de produtos e serviços. Entendemos que a certificação de segurança cibernética é uma ferramenta que é recorrentemente implementada para abordar questões de cibersegurança em algumas jurisdições, como na União Europeia, Estados Unidos, China, Singapura e Austrália. O ITI acompanhou de perto essas discussões1 e reconhece e respeita que os governos têm o direito de preparar, aplicar e manter regulamentos para certificação. Caso o Brasil, porventura, decida buscar esquemas de certificação, recomendamos enfaticamente que os formuladores de políticas públicas utilizem padrões internacionais de cibersegurança baseados em consenso como referência. No entanto, o ITI gostaria de ressaltar que a avaliação de certificação apenas analisa as informações de segurança em um momento específico no tempo. Embora certificações possam ser úteis em determinados casos, elas não são apropriadas para todos os produtos, serviços ou casos, e abordam apenas um aspecto pontual da segurança cibernética. Além disso, gostaríamos de ressaltar que a criação de uma ampla estrutura de certificação de produtos e serviços de TI não é aconselhável, pois os esquemas de certificação devem ser baseados em risco e ter um escopo claramente definido. Não existe um esquema de certificação de produto e serviço de tamanho único, "one-size-fits-all", que possa ser aplicado a uma vasta gama de tecnologias de tecnologia da informação e comunicação (TIC). Ademais, a certificação pode ser onerosa para fornecedores, levando a "trade-offs" indesejáveis, como impactar negativamente a inovação, limitar o poder de escolha do consumidor e atrasar a disponibilidade de novas tecnologias no mercado brasileiro. Por último, tornaria o acesso a novas soluções de cibersegurança mais caras e de difícil acesso, indo contra o objetivo do projeto de lei em questão. Além disso, a Agência Nacional de Telecomunicações (Anatel) já possui um esquema de certificação de segurança cibernética para equipamentos de telecomunicações e o estabelecimento de um esquema secundário pode levar a sistemas conflitantes e burocráticos.			
Resposta: A contribuição foi registrada e será considerada oportunamente, quando do estabelecimento dos normativos aplicáveis.			

Audiência Pública da PNCiber – Contribuições

Responsável: Husani Durans de Jesus			
Instituição: ITI Council		**Título:** Presidente	
Tópico: 10-ANCiber	**Id#:** 74	**Parecer:** 3-Inadequada	
Tipo de Contribuição: Alteração Infralegal	**Artigo:** 18	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: As competências da Anciber (Agência Nacional de Cibersegurança) devem ser pensadas com a potencial convergência com as funções da ANPD (Autoridade Nacional de Proteção de Dados). A título de exemplo, a Lei 13.709/2018 ("Lei Geral de Proteção de Dados Pessoais") atribui à ANPD a competência para "I - zelar pela proteção dos dados pessoais, nos termos da legislação"(conf. Art. 55-J, inciso I), o que inclui a adoção de medidas de segurança técnicas e administrativa (art. 46, caput). De forma mais clara, o § 1º da Lei 13.709/2018 estatui a competência da ANPD em dispor sobre padrões técnicos mínimos para a segurança e sigilo dos dados. Tais competências podem conflitar diretamente com diversas atribuição da Anciber no escopo da redução de riscos à cibersegurança. Há a necessidade de pensar em quais casos as competências da ANPD prevalecerão, e em quais terá prevalência a Anciber, descrevendo expressa e objetivamente no texto do Projeto de Lei. De forma semelhante, deve-se ter em mente a necessidade de compatibilização das atribuições da Anciber com o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br), mantido pelo Núcleo de Informação e Coordenação do ponto Br (NIC.br), que tem como missão institucional aumentar os níveis de segurança e de capacidade de tratamento de incidentes das redes conectadas à Internet no Brasil, tendo atuação direta no escopo da cibersegurança. Portanto, há a necessidade de compatibilização das atribuições da Anciber com o CERT.Br, inclusive aquelas pedagógicas e de gestão de cibercrise.			
Resposta: O trabalho da ANCiber e da ANPD será coordenado, cabendo à primeira a regulação da cibersegurança e à segunda aquela da proteção de dados pessoais. Ademais, a ANPD participa do CNCiber, que supervisiona o funcionamento da ANCiber. No tocantre ao CERT.Br, o funcionamento do mesmo já ocorre em paralelo com o do CTIR Gov, sem que sejam observados conflitos.			

Audiência Pública da PNCiber – Contribuições

Responsável: João Araújo Monteiro Neto			
Instituição: GETIS/Unifor		**Título:** Pesquisador	
Tópico: 10-ANCiber	**Id#:** 115	**Parecer:** 3-Inadequada	
Tipo de Contribuição: Alteração Legal	**Artigo:** 18	**Inciso:**	**Parágrafo:**
Texto Original: XIV - avaliar e certificar produtos e serviços, no tocante à cibersegurança, diretamente ou por meio de parceiros credenciados pela ANCiber;			
Crítica ou Sugestão: É de extrema relevância que no caso de sistemas específicos e já em funcionamento como o caso de telecomunicações, sejam mantidas as competências plenas, visto que há todo um expertise com requisitos para a funcionalidade plena de toda a rede de telecomunicações e que não pode ser ignorado. Ademais as agências estão abrangidas pela política e eventuais instrumentos normativos da ANCiber quanto à cibersegurança, sem que isso impacte outros elementos relevantes na certificação. Talvez o caminho seja que a ANCiber não realize certificação mas estabeleça os requisitos, condições e normativas especícidas sem prejuízo de outras normas estabelecidas no âmbito técnico, inclusive INMETRO e ABNT. É preciso definir a priori o que seria o escopo da certificação caso se pretenda manter essa competência, definindo-se minimante quais elementos eatriam abrangidos por esta certificação. Não obstante, visando resguardar o conhecimento específico e técnico das agências por hora sugeriremos a inclusão de exceção conforme abaixo. XIV - avaliar e certificar produtos e serviços, no tocante à cibersegurança, diretamente ou por meio de parceiros credenciados pela ANCiber, exceto quando lei especial prever a competência de outras entidades públicas para a certificação de serviços ou produtos;			
Resposta: A ANATEL avançou na certificação em cibersegurança setorial na ausência de um órgão específico para o tema (assim como a ANEEL e o BACEN). Com a entrada em operação da ANCiber, que tem a responsabilidade de coordenação nacional na temática, haverá a necessidade de articulação desta com suas congêneres para que, no tocante à cibersegurança, os critérios de certificação sejam estabelecidos pela ANCiber. Isso é o que está disposto no anteprojeto de lei.			

Audiência Pública da PNCiber – Contribuições

Responsável: Luiz Henrique Barbosa da Silva			
Instituição: TELCOMP		**Título:** Representante	
Tópico: 10-ANCiber	**Id#:** 177	**Parecer:** 3-Inadequada	
Tipo de Contribuição: Preoc. ANATEL	**Artigo:** 18	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: Recomenda-se a inclusão da competência para fiscalizar, avaliar ou auditar as estruturas infraestrutura crítica, tais como: geração e fornecimento de energia elétrica, fornecimento de água e de telecomunicações.			
Resposta: A proposta foge ao escopo da cibersegurança, objeto do anteprojeto de lei.			

Audiência Pública da PNCiber – Contribuições

Responsável: Renato Solimar Alves			
Instituição: CJF		**Título:** Servidor	
Tópico: 10-ANCiber	**Id#:** 249	**Parecer:** 3-Inadequada	
Tipo de Contribuição: Alteração Legal	**Artigo:** 18	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: sugiro aguardar a definição de a qual Ministério ficará vinculado a ANCiber antes de atribuí-la ao GSI, conforme explicado em sugestões acima.			
Resposta: A definição do GSI como ministério para vinculação da ANCiber foi feita em estrita concordância com as disposições legais, conforme esclarecido na "Apresentação do Projeto", seção 3.4.			

Audiência Pública da PNCiber – Contribuições

Responsável: Ivanildo de Oliveira da Silva			
Instituição: Cidadão		**Título:** Cidadão	
Tópico: 10-ANCiber	**Id#:** 93	**Parecer:** 3-Inadequada	
Tipo de Contribuição: Alteração Legal	**Artigo:** 19	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: Sobre processos de homologação de software seguro, há inciativias nesse sentido dentro do INMETRO.			
Resposta: A partir da criação da ANCiber caberá a esta coordenar as ações nesse sentido.			

Audiência Pública da PNCiber – Contribuições

Responsável: Breno de Castro Laranjo Vale			
Instituição: ABRINT		**Título:** Diretor de Projetos	
Tópico: 10-ANCiber	**Id#:** 26	**Parecer:** 3-Inadequada	
Tipo de Contribuição: Alteração Legal	**Artigo:**	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: Do ponto de vista comportamental, a preocupação da ABRINT se estende além do diálogo institucional e alcança o respeito às competências das outras agências reguladoras. Compartilhar iniciativas é relevante e necessário, mas não se pode deixar de lado as competências setoriais.			
Resposta: As competências originárias de todas as agências reguladoras estão inteiramente preservadas. De outra parte, a cibersegurança não é competência originária de nenhuma delas, e a ausência de uma coordenação nacional sobre o tema é um dos elos que enfraquece a cibersegurança nacional. e que, como reconhece a própria ANATEL, carece de uma centralização. Não obstante, as agências reguladoras de setores considerados infraestruturas críticas foram incluídas no CNCiber de forma a ampliar a possibilidade de diálogo e coordenação intersetorial da ANCiber.			

Audiência Pública da PNCiber – Contribuições

Responsável: Igor Monteiro Moraes			
Instituição: UFF		**Título:** Pesquisador	
Tópico: 10-ANCiber	**Id#:** 79	**Parecer:** 3-Inadequada	
Tipo de Contribuição: Alteração Legal	**Artigo:**	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: Esta competência poderia ser migrada diretamente para o Diretor-Geral da ANCiber, uma vez que preside o "Gabinete", além de que evitaria a necessidade de deliberação colegiada para determinação de cunho emergencial.			
Resposta: Não se trata de iniciativa do Diretor-Geral, mas sim do GGCiber.			

Audiência Pública da PNCiber – Contribuições

Responsável: Osmar Assis do Nascimento Filho			
Instituição: Cidadão		**Título:** Cidadão	
Tópico: 11-GGCiber	**Id#:** 233	**Parecer:** 3-Inadequada	
Tipo de Contribuição: Alteração Legal	**Artigo:** 21	**Inciso:** 0	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: É necessário um olhar atento às competências do Gabinente de Gerenciamento de Cibercrises, tendo em vista o cuidado para não converter suas funções institucionais em pavimento para a concretização de medidas antidemocráticas e ilegítimas. De forma semelhante à análise das competências da Anciber, deve haver uma forma de supervisão ou escrutínio público das ações do Gabinente de Gerenciamento de Cibercrises, como contrapeso à amplitude de suas prerrogativas. É possível sugerir como forma de contrapeso, a inclusão do Ministério dos Direitos Humanos, tendo em vista a preservação da legitimidade do gerenciamento de crise ante o risco de excessos estatais e conversão do Gabinete em pavimento para um tecnoautoritarismo.			
Resposta: As competências do GGCiber são essencialmente de curto prazo e relacionadas a uma crise em andamento. Quaisquer eventuais desvios serão passíveis de responsabilização posterior. Ademais, estão presentes no GGCiber o CNJ e o CNMP, que deverão alertar o GGCiber no caso de alguma atitude que avance sobre os direitos individuais.			

Audiência Pública da PNCiber – Contribuições

Responsável: João Araújo Monteiro Neto			
Instituição: GETIS/Unifor		**Título:** Pesquisador	
Tópico: 11-GGCiber	**Id#:** 116	**Parecer:** 3-Inadequada	
Tipo de Contribuição: Alteração Legal	**Artigo:** 21	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: Corrigir de XIII para XIV.			
Resposta: Houve perda de objeto na proposição devido à alteração da composição do GGCiber.			

Audiência Pública da PNCiber – Contribuições

Responsável: Osmar Assis do Nascimento Filho			
Instituição: Cidadão		**Título:** Cidadão	
Tópico: 11-GGCiber	**Id#:** 234	**Parecer:** 3-Inadequada	
Tipo de Contribuição: Alteração Legal	**Artigo:** 22	**Inciso:**	**Parágrafo:** 2
Texto Original: § 3º O Gabinete reunir-se-á ordinariamente, em periodicidade bimestral, para reuniões de caráter informativo e consultivo.			
Crítica ou Sugestão: § 3º O Gabinete reunir-se-á ordinariamente, em periodicidade semestral, para reuniões de caráter informativo e consultivo Obs: Consideramos ser mais realista fazer reuniões ordinárias semestrais, devido ao grande numero de participantes do gabinete			
Resposta: É importante que os membros do GGCiber estejam familiarizados entre si e com a dinâmica deliberativa do Gabinete, de sorte que quando necessário o gerenciamento de uma crise não se perca tempo por falta dessa familiaridade ou de maturidade processual.			

Audiência Pública da PNCiber – Contribuições

Responsável: Maxli Barroso Campos			
Instituição: LPTIC/EGN		**Título:** Pesquisador Líder	
Tópico: 11-GGCiber	**Id#:** 208	**Parecer:** 3-Inadequada	
Tipo de Contribuição: Alteração Legal	**Artigo:** 22	**Inciso:**	**Parágrafo:** 3
Texto Original:			
Crítica ou Sugestão: Quanto a composição, apesar de constar o Ministério da Justiça e Segurança Pública, não consta explicitamente a Policial Federal, órgão no qual há peritos que são muitas vezes chamados em incidentes de segurança da informação. Assim como, não constam a PRF e a ABIN. Considerando o modal rodoviário nacional como o principal para escoamento da produção, é salutar que a PRF seja inserida. Quanto a ABIN, considerando que há uma unidade de inteligência na futura estrutura da ANCiber, é salutar que a ABIN possua cadeira no Gabinete de Gerenciamento de Cibercrises. Dessa forma, sugiro alterar o inciso II da seguinte forma: - três representantes do Ministério da Justiça e Segurança Pública (1 do MJSP, 1 do quadro de peritos de informática da PF e 1 da Coordenação de Segurança da PRF). Sugiro incluir um representante da Agência Brasileira de Inteligência. Sugiro por fim, a inclusão de um parágrafo que mencione os requerimentos mínimos dos integrantes que comporão o Gabinete, ou seja, não adianta de nada um colegiado composto por pessoas que não possuam conhecimento de segurança da informação. Assim, sugiro inserir conforme a seguir: § 7º Os integrantes indicados a compor o Gabinete de Gerenciamento de Cibercrises definido no caput deste artigo deverão possuir comprovado conhecimento na área de segurança da informação por meio de cursos oficiais de instituições nacionais ou internacionais de segurança, certificações na área de segurança da informação, pós-graduação na área de segurança da informação ou, experiência em unidade de segurança da informação na área pública ou privada de pelo menos 2 anos.			
Resposta: A composição do GGCiber foi alterada, de forma a contemplar mais participantes. A despeito disso, está previsto o convite a outros participantes conforme a necessidade ou conveniência.			

Audiência Pública da PNCiber – Contribuições

Responsável: Ivanildo de Oliveira da Silva			
Instituição: Cidadão		**Título:** Cidadão	
Tópico: 11-GGCiber	**Id#:** 94	**Parecer:** 3-Inadequada	
Tipo de Contribuição: Inclusão no GGCiber	**Artigo:** 22	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: Embora a gestão de cibercrises seja uma atribuição relacionada à segurança nacional, é necessário que o Gabinete preveja a representação de setores não governamentais como forma de supervisão das ações estatais e garantia da legitimidade de suas medidas.			
Resposta: O Art. 22, § 5º, preve a participação de convidados especialistas ou representantes de instituições relevantes para participarem de suas reuniões. Ademais, estão presentes no GGCiber o CNJ e o CNMP, que deverão alertar o GGCiber no caso de alguma atitude que avance sobre os direitos individuais ou desconfigure a legitimidade de suas medidas.			

Audiência Pública da PNCiber – Contribuições

Responsável: João Araújo Monteiro Neto			
Instituição: GETIS/Unifor		**Título:** Pesquisador	
Tópico: 11-GGCiber	**Id#:** 117	**Parecer:** 3-Inadequada	
Tipo de Contribuição: Inclusão no GGCiber	**Artigo:** 22	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: Obs: A proposta do Gabinete de Gerenciamento de cibercrises é essencial. Somente não foi identificado a realização de exercícios de simulação, seja para construção dos normativos, seja para mobilizar os gestores sobre a necessidade de se executar os planos. De nada adianta um plano bem elaborado se o teste e avaliação de sua efetividade não é feito? Os exercícios podem ser feito via table-top ou até mesmo uma simulação real. Esta necessidade, inclusive, pode estar linkada com o item XIX - promover, apoiar e participar de exercícios nacionais e internacionais relativos à simulação de eventos e ciberincidentes de natureza cíclica, a fim de aumentar a ciber-resiliência do país;			
Resposta: A PNCiber é uma política nacional, e assim foca mais no "o que" do que no "como", até como forma de assegurar sua perenidade. Outrossim, não cabe esse tipo de detalhamento neste instrumento, mas sim em resoluções da Diretoria Colegiada da ANCiber a serem aprovadas pelo CNCiber oportunamente. De outra parte, os instrumentos serão os mesmos utilizados pelas demais agências reguladoras, conforme estipulado no marco regulatório vigente.			

Audiência Pública da PNCiber – Contribuições

<table>
<tr><td colspan="4">Responsável: Maxli Barroso Campos</td></tr>
<tr><td colspan="2">Instituição: LPTIC/EGN</td><td colspan="2">Título: Pesquisador Líder</td></tr>
<tr><td>Tópico: 11-GGCiber</td><td>Id#: 209</td><td colspan="2">Parecer: 3-Inadequada</td></tr>
<tr><td>Tipo de Contribuição: Alteração Infralegal</td><td>Artigo: 22</td><td>Inciso:</td><td>Parágrafo:</td></tr>
<tr><td colspan="4">Texto Original:</td></tr>
<tr><td colspan="4">Crítica ou Sugestão:
Entende-se que o Poder Judiciário está sub-representado na composição do Comitê Nacional de Cibersegurança frente à quantidade de órgãos do Poder Executivo. Um único assento, na representação do CNJ, se mostra incapaz de representar as todas as especificidades dos diversos ramos do Poder Judiciário. Solicita-se que o Conselho da Justiça Federal possua assento no Comitê, representando a Justiça Federal, e recomenda-se que sejam incluídos um representante da Justiça Eleitoral, um representante da Justiça do Trabalho, um representante da Justiça Militar e um representante da Justiça Estadual.</td></tr>
<tr><td colspan="4">Resposta:
O Conselho Nacional de Justiça (CNJ) é uma instituição pública que visa a aperfeiçoar o trabalho do Judiciário brasileiro, principalmente no que diz respeito ao controle e à transparência administrativa e processual. Sua missão é promover o desenvolvimento do Poder Judiciário em benefício da sociedade, por meio de políticas judiciárias e do controle da atuação administrativa e financeira.
Outrossim, é o órgão adequado para representar o judiciário junto ao CNCiber e ao GGCiber.</td></tr>
</table>

Audiência Pública da PNCiber – Contribuições

Responsável: Renato Solimar Alves			
Instituição: CJF		**Título:** Servidor	
Tópico: 11-GGCiber	**Id#:** 250	**Parecer:** 3-Inadequada	
Tipo de Contribuição: Inclusão no GGCiber	**Artigo:** 22	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: Na definição do complexo Nacional de Cibersegurança, em alinhamento a terminologia, mais utilizada e difundido, nacional e internacionalmente, poderia usar o termo "infraestruturas críticas em vez de serviços essenciais. no art. 4º, inciso XXI, alteraria para infraestrutura crítica, explicando que se trata dos serviços essenciais, mantendo a definição destes.			
Resposta: A explicação da motivação para a adoção de serviços essenciais em oposição a infraestruturas críticas encontra-se no documento Apresentação do Projeto, seção 3.3.			

Audiência Pública da PNCiber – Contribuições

Responsável: Leila Oliveira da Fonseca			
Instituição: Cidadão		**Título:** Pesquisadora	
Tópico: 12-Complexo	**Id#:** 148	**Parecer:** 3-Inadequada	
Tipo de Contribuição: Alteração Legal	**Artigo:** 24	**Inciso:**	**Parágrafo:**

Texto Original:

Art. 24. Institui-se o Complexo Nacional de Cibersegurança ("Complexo"), composto pelo conjunto de ciberativos que dão sustentação a serviços essenciais.

§ 1º O Complexo será materializado na forma de documento homônimo; § 2º O Complexo será atualizado anualmente, ou quando o Comitê Nacional de Cibersegurança entender necessário.

Crítica ou Sugestão:

Considerando a exposição de motivos, o qual argumenta pela criação do Complexo Nacional de Cibersegurança em função dos serviços essenciais, recomenda-se a não criação do referido Complexo.

Como é de conhecimento do GSI, foi instituído, por meio da Resolução CREDEN/GSI-PR nº 23, de 16 de dezembro de 2022, o Grupo Técnico de Segurança de Infraestruturas Críticas (GT-SIC) do Governo Digital, composto por todos as diretorias da SGde outros órgãos e entidades relacionadas. A instituição de tal Grupo Técnico foi embasada em decisão da Câmara de Relações Exteriores e Defesa Nacional do Conselho de Governo (CREDEN), que passou a considerar a temática Governo Digital como uma área prioritária composta por infraestruturas críticas, para fins de segurança nacional. Assim, por exemplo, a conta gov.br, pela qual o cidadão tem acesso, a partir de login único, a serviços digitais oferecidos pelo governo federal, é uma das infraestruturas críticas do Governo Digital. E como tal, precisa ser protegida, bem como ter sua reputação preservada diante da sociedade brasileira.

No âmbito do GT-SIC do Governo Digital, está em andamento a criação de uma metodologia para identificação e priorização de infraestruturas críticas do Governo Digital. Com o uso dela, todos os sistemas informacionais do Poder Executivo Federal serão inventariados e passarão por uma análise de segurança para que sejam identificados aqueles sistemas (e suas dependências) que devem ser considerados como infraestruturas críticas, e para obtenção de uma lista menor e priorizada das principais infraestruturas críticas que precisarão de maior atenção.

Embora o GSI tenha exposto sobre uma possível diferença entre infraestruturas críticas e serviços essenciais ao se referir sobre sistemas informacionais, o entendimento desta Secretaria de Governo Digital é de que todo sistema informacional deve ser considerado como essencial para a transformação digital de uma política pública, ou no mínimo parte da cadeia de suprimentos de um serviço público digital ou necessário para alguma operação administrativa, que não deixa de ser essencial para o adequado funcionamento das políticas públicas.

Um exemplo claro disso é o Sistema Eletrônico de Informações (SEI), que é um sistema de tramitação processual utilizado em diversos órgãos de todos os poderes e esferas. Tal sistema não tem o cidadão como seu usuário final, mas sua eventual indisponibilidade pode impactar seriamente em diversas outras operações do órgão, tendo como consequência indireta impactos sobre os direitos dos cidadãos. Assim, na lógica do GSI, se o SEI é considerado um serviço essencial, e a maioria dos órgãos usam o SEI, todos esses órgãos deverão compor o Complexo proposto? Não parece adequado para a afirmação de que "onde tudo é prioritário, nada é prioridade".

Assim, diante do entendimento da SGD, e das atividades executadas no âmbito do Grupo Técnico de Segurança de Infraestruturas Críticas (GT-SIC) do Governo Digital, recomenda-se a não criação do Complexo Nacional de Cibersegurança. Ao invés disso, sugere-se manter a atuação do Ministério da Gestão e da Inovação em Serviços Públicos, órgão responsável pela área prioritária do Governo Digital, para as atividades propostas pelo Complexo. Além disso, recomenda-se expandir a

identificação de infraestruturas críticas e abrangência do futuro Plano Setorial de Infraestruturas Críticas do Governo Digital para os poderes judiciário e legislativo, e para as esferas estadual e municipal a partir de 2025. Tal recomendação está alinhada com a atuação da Secretaria de Governo Digital no âmbito da Estratégia Nacional de Governo Digital.
Resposta: A explicação da motivação para a adoção de serviços essenciais em oposição a infraestruturas críticas encontra-se no documento Apresentação do Projeto, seção 3.3.

Audiência Pública da PNCiber – Contribuições

Responsável: Leonardo Rodrigo Ferreira			
Instituição: SGD		**Título:** Diretor	
Tópico: 12-Complexo	**Id#:** 163	**Parecer:** 3-Inadequada	
Tipo de Contribuição: Alteração Legal	**Artigo:** 24	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: Para fins de harmonização do arcabouço nacional, a Brasscom entende que a Política Nacional de Segurança de Infraestrutura Crítica deveria ser utilizada como referência para identificação dos setores envolvidos no Complexo Nacional de Cibersegurança (Art. 24). Mais especificamente, recomenda-se a supressão do termo "serviços essenciais", e a incorporação de definição de "Infraestrutura Crítica" - conforme previsto na mencionada Política. Muito embora entendamos a preocupação apresentada pelo GSI quando da exposição sobre o texto proposto, preocupa a amplitude do conceito de serviços essenciais atualmente constante da proposta, o que poderá gerar insegurança jurídica relevante quando da implementação de eventual regulamentação. Ademais, para fins de segurança jurídica e maior clareza do normativo, a Brasscom sugere o estabelecimento adicional de uma lista exaustiva identificando especificamente os setores abarcados nesta definição.			
Resposta: A explicação da motivação para a adoção de serviços essenciais em oposição a infraestruturas críticas encontra-se no documento Apresentação do Projeto, seção 3.3.			

Audiência Pública da PNCiber – Contribuições

Responsável: Sarah Melo Martins			
Instituição: Brasscom		**Título:** Representante	
Tópico: 12-Complexo	**Id#:** 264	**Parecer:** 3-Inadequada	
Tipo de Contribuição: Alteração Legal	**Artigo:** 24	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: O estabelecimento de um Complexo Nacional de Cibersegurança que congrega todos os ciberativos que dão suporte a serviços essenciais deve ser visto com cautela. O estabelecimento de diretrizes de cunho obrigatório para prestadores de serviço essenciais com ciberativos no Complexo pode gerar uma convergência com outros entes normatizadores e fiscalizadores setoriais, como a ANATEL, ANPD e outros. Veja-se a definição de Serviço Essencial (art. 4º, inciso XXI, do PL): "serviços cujo mau funcionamento, uso indevido ou interrupção, mesmo que parcial, possa acarretar prejuízo à segurança nacional, e dos quais dependa o exercício de função essencial do Estado ou a prestação de serviço primordial à manutenção de atividades civis, sociais ou econômicas fundamentais aos interesses do Estado". A amplitude de tal conceito leva à insegurança jurídica como cerne do Complexo Nacional de Cibersegurança. É necessário, portanto, que se definam os setores que compõe o rol de serviços essenciais, como o faz a Diretiva (UE) 2022/555 no panorama da Comunidade Europeia. A formulação de um conjunto de ciberativos, com especial normatização, gera uma convergência direta com as competências normatizadoras e fiscalizadoras da ANATEL, posto que, para fins do Projeto de Lei, tem-se como ciberativo "hardware, software ou dados utilizados para o processamento e transmissão eletrônicos de informações" (conforme art. 4º inciso I, do PL), que pode conflitar com a infraestrutura de telecomunicação, suporte para o desenvolvimento da internet. Veja-se, nesse sentido, a Lei 9.472 de 1997 que atribui à Internet o caráter de Serviço de Valor Adicionado que utiliza como suporte a infraestrutura das telecomunicações: "Art. 61. Serviço de valor adicionado é a atividade que acrescenta, a um serviço de telecomunicações que lhe dá suporte e com o qual não se confunde, novas utilidades relacionadas ao acesso, armazenamento, apresentação, movimentação ou recuperação de informações." Por conseguinte, é necessário que haja a delimitação de competências para a normativação do Complexo, tendo em vista que o potencial conflito regulatório com entidades como a ANATEL, repercutindo em possíveis desdobramentos da regulação da internet, objeto de debate legislativo contemporâneo.			
Resposta: A explicação da motivação para a adoção de serviços essenciais em oposição a infraestruturas críticas encontra-se no documento Apresentação do Projeto, seção 3.3. De outra parte, A ANATEL avançou na certificação em cibersegurança setorial na ausência de um órgão específico para o tema (assim como a ANEEL e o BACEN). Com a entrada em operação da ANCiber, que tem a responsabilidade de coordenação nacional na temática, haverá a necessidade de articulação desta com suas congêneres para que, no tocante à cibersegurança, os critérios de certificação sejam estabelecidos pela ANCiber. Isso é o que está disposto no anteprojeto de lei.			

Audiência Pública da PNCiber – Contribuições

Responsável: João Araújo Monteiro Neto			
Instituição: GETIS/Unifor		**Título:** Pesquisador	
Tópico: 12-Complexo	**Id#:** 118	**Parecer:** 3-Inadequada	
Tipo de Contribuição: Alteração Legal	**Artigo:** 25	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: Sugiro remover a limitação temporal das requisições deixando a cargo do Diretor a gestão do pessoal.			
Resposta: São vários os objetivos dessa limitação temporal. Primeiro, o de se evitar um permanente risco de desmonte de equipes preparadas por outras instituições. Segundo, o de assegurar a composição de uma equipe permanente da própria ANCiber. Terceiro, o de garantir a estabilidade operacional da ANCiber, sem o risco de "retorno" do pessoal requisitado para os órgãos de origem.			

Audiência Pública da PNCiber – Contribuições

<table>
<tr><td colspan="4">Responsável: Ivanildo de Oliveira da Silva</td></tr>
<tr><td colspan="2">Instituição: Cidadão</td><td colspan="2">Título: Cidadão</td></tr>
<tr><td>Tópico: 15-Cooperação Internacional</td><td>Id#: 95</td><td colspan="2">Parecer: 3-Inadequada</td></tr>
<tr><td>Tipo de Contribuição: Alteração Legal</td><td>Artigo: 30</td><td>Inciso:</td><td>Parágrafo:</td></tr>
<tr><td colspan="4">Texto Original:</td></tr>
<tr><td colspan="4">Crítica ou Sugestão:
Quanto a cooperação internacional poderia dar mais ênfase ao intercâmbio, compartilhamento de informações conhecimentos, capacitação que, consequentemente, irão possibilitar a projeção internacional e a colaboração por uma ordem internacional mais segura, próspera e aberta.</td></tr>
<tr><td colspan="4">Resposta:
A PNCiber é uma política nacional, e assim foca mais no "o que" do que no "como", até como forma de assegurar sua perenidade. Outrossim, não cabe esse tipo de detalhamento neste instrumento, mas sim em resoluções da Diretoria Colegiada da ANCiber a serem aprovadas pelo CNCiber oportunamente.
De outra parte, os instrumentos serão os mesmos utilizados pelas demais agências reguladoras, conforme estipulado no marco regulatório vigente.</td></tr>
</table>

Audiência Pública da PNCiber – Contribuições

<table>
<tr><td colspan="4">Responsável: Leila Oliveira da Fonseca</td></tr>
<tr><td colspan="2">Instituição: Cidadão</td><td colspan="2">Título: Pesquisadora</td></tr>
<tr><td>Tópico: 15-Cooperação Internacional</td><td>Id#: 149</td><td colspan="2">Parecer: 3-Inadequada</td></tr>
<tr><td>Tipo de Contribuição: Alteração Infralegal</td><td>Artigo: 30</td><td>Inciso:</td><td>Parágrafo:</td></tr>
<tr><td colspan="4">Texto Original:</td></tr>
<tr><td colspan="4">Crítica ou Sugestão:
Apesar de nobre a proposta de inclusão desde o ensino fundamental de temas relacionados a segurança da informação, isso não resolve o problema atual que é a capacitação de corpo técnico com conhecimento em segurança da informação, resposta incidentes, gerenciamento de vulnerabilidades, entre diversas outras cadeiras da temática. Assim, sugiro a adaptação integral do capítulo visando não apenas ter a norma programática para as futuras gerações, mas também o fomento da capacitação de servidores públicos em cursos oficiais de segurança da informação, com a imposição às administrações dos órgãos a reserva de orçamento tanto para área de segurança, quanto específico para educação cibernética.
Sugiro o debate com especialistas nas áreas de segurança e que foram capacitados em cursos oficiais de instituições nacionais e internacionais, acerca de quais são os cursos ou capacitações mais efetivas para a melhoria da segurança cibernética nacional.
Por fim, sugiro que seja inserido no futuro capítulo que a infraestrutura de especialistas de segurança dos órgãos da administração pública, assim como do Exército por meio da infraestrutura de capacitação de Guerra Cibernética e Eletrônica, a capacitação contínua de servidores membros da Administração Pública em número mínimo de 10 servidores por ano. Uma lista de cadastramento e ordem da capacitação deverá ser mantida pela ANCiber visando moralizar a participação. Os servidores capacitados deverão estar lotados nas unidades responsáveis pela segurança da informação dos órgãos da administração pública. Deverá ser realizado, por fim, repasse financeiro ao órgão que realizar a capacitação, visando não comprometer suas rotinas orçamentárias internas.</td></tr>
<tr><td colspan="4">Resposta:
A PNCiber é uma política nacional, e assim foca mais no "o que" do que no "como", até como forma de assegurar sua perenidade. Outrossim, não cabe esse tipo de detalhamento neste instrumento, mas sim em resoluções da Diretoria Colegiada da ANCiber a serem aprovadas pelo CNCiber oportunamente.
De outra parte, os instrumentos serão os mesmos utilizados pelas demais agências reguladoras, conforme estipulado no marco regulatório vigente.</td></tr>
</table>

Audiência Pública da PNCiber – Contribuições

Responsável: Ivanildo de Oliveira da Silva			
Instituição: Cidadão		**Título:** Cidadão	
Tópico: 16-E,P,D&I	**Id#:** 96	**Parecer:** 3-Inadequada	
Tipo de Contribuição: Alteração Infralegal	**Artigo:**	**Inciso:**	**Parágrafo:** 0
Texto Original:			
Crítica ou Sugestão: Sobre o incentivo a ações de pesquisa e desenvolvimento, uma sugestão é adotar um programa como o programa de P&D da ANEEL. https://www.gov.br/aneel/pt-br/assuntos/pesquisa-e-desenvolvimento/programa-de-pesquisa-e-desenvolvimento-tecnologico			
Resposta: A sugestão foi anotada para implementação oportuna, por meio dos instrumentos infra legais aplicáveis.			

Audiência Pública da PNCiber – Contribuições

Responsável: Igor Monteiro Moraes			
Instituição: UFF		**Título:** Pesquisador	
Tópico: 16-E,P,D&I	**Id#:** 80	**Parecer:** 3-Inadequada	
Tipo de Contribuição: Alteração Infralegal	**Artigo:**	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: Incluir políticas públicas de educação desde o maternal;			
Resposta: A sugestão foi anotada para implementação oportuna, por meio dos instrumentos infra legais aplicáveis.			

Audiência Pública da PNCiber – Contribuições

Responsável: Paulo Emerson de Oliveira Pereira			
Instituição: Cidadão		**Título:** Cidadão	
Tópico: 16-E,P,D&I	**Id#:** 244	**Parecer:** 3-Inadequada	
Tipo de Contribuição: Alteração Infralegal	**Artigo:**	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: Sugere-se a inclusão do seguinte profissional: "Advogado Especializado em Direito Digital e Crimes Cibernéticos", cargo de nível superior, com atribuições voltadas para os procedimentos de compliance, de acordo com a necessidade e nível de adequação às normas legais. Realiza auditorias especializadas para identificar riscos de segurança da informação, proteção de dados, propriedade intelectual e riscos regulatórios. É capaz de elaborar políticas internas de segurança da informação, elaborar regulação interna para tratamento de dados pessoais, em conformidade com a LGPde demais legislações do arcabouço regulatório brasileiro da área; planos de recuperação de dados, planos de incidentes de segurança da informação e demais políticas afetas à área de segurança da informação e crimes cibernéticos.			
Resposta: O arcabouço legal e institucional brasileiro prevê que os serviços jurídicos das agências reguladoras sejam providos por Procuradores Federais.			

Audiência Pública da PNCiber – Contribuições

Responsável: Maxli Barroso Campos			
Instituição: LPTIC/EGN		**Título:** Pesquisador Líder	
Tópico: 17-Disposições Finais	**Id#:** 210	**Parecer:** 3-Inadequada	
Tipo de Contribuição: Alteração Legal	**Artigo:** 43	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: sugiro inserir após o termo "no setor regulado pela ANCiber" a expressão "em âmbito privado"			
Resposta: O dispositivo legal segue o padrão adotado para as demais agências reguladoras nacionais. A alteração criaria uma distorição em relação à cultura institucional brasileira para agências reguladoras.			

Audiência Pública da PNCiber – Contribuições

<table>
<tr><td colspan="4">Responsável: Ivanildo de Oliveira da Silva</td></tr>
<tr><td colspan="2">Instituição: Cidadão</td><td colspan="2">Título: Cidadão</td></tr>
<tr><td>Tópico: 18-ANCiber-Organização</td><td>Id#: 97</td><td colspan="2">Parecer: 3-Inadequada</td></tr>
<tr><td>Tipo de Contribuição: Alteração Legal</td><td>Artigo: 3</td><td>Inciso:</td><td>Parágrafo:</td></tr>
<tr><td colspan="4">Texto Original:
Art. 4 º. É vedada a indicação para a Diretoria Colegiada: ...</td></tr>
<tr><td colspan="4">Crítica ou Sugestão:
Sugiro inserir um inciso conforme a seguir: VI - de membro que não possua comprovado conhecimento na área de segurança da informação por meio de cursos oficiais de instituições nacionais ou internacionais de segurança, certificações na área de segurança da informação, pós-graduação na área de segurança da informação ou, experiência em unidade de segurança da informação na área pública ou privada de pelo menos 2 anos.</td></tr>
<tr><td colspan="4">Resposta:
Os requisitos para cargos de diretoria de agências reguladoras já estão descritos na Lei 9.986 de 18 de julho de 2000, em seu art. 5º, e são mais restritivos que os sugeridos pelo autor.</td></tr>
</table>

Audiência Pública da PNCiber – Contribuições

<table>
<tr><td colspan="4">Responsável: Ivanildo de Oliveira da Silva</td></tr>
<tr><td colspan="2">Instituição: Cidadão</td><td colspan="2">Título: Cidadão</td></tr>
<tr><td>Tópico: 18-ANCiber-Organização</td><td>Id#: 98</td><td colspan="2">Parecer: 3-Inadequada</td></tr>
<tr><td>Tipo de Contribuição: Alteração Legal</td><td>Artigo: 4</td><td>Inciso:</td><td>Parágrafo:</td></tr>
<tr><td colspan="4">Texto Original:
Art. 11 . A edição e a alteração de atos normativos de interesse geral dos agentes econômicos será, nos termos do regulamento, precedida da realização de Análise de Impacto Regulatório (AIR), que conterá informações e dados sobre os possíveis efeitos do ato normativo.</td></tr>
<tr><td colspan="4">Crítica ou Sugestão:
Menciona-se AIR, importante trazer também o conceito de ARR - Avaliação de Resultado Regulatório conforme Decreto 10.411.</td></tr>
<tr><td colspan="4">Resposta:
O anteprojeto reflete as disposições legais correntemente vigentes no arcabouço legal das agências reguladoras nacionais. Os decretos aplicáveis serão contemplados no marco infralegal a ser adotado posteriormente à entrada da PNCiber em vigor.</td></tr>
</table>

Audiência Pública da PNCiber – Contribuições

<table>
<tr><td colspan="4">Responsável: Jeferson Fued Nacif</td></tr>
<tr><td colspan="2">Instituição: MCom</td><td colspan="2">Título: Servidor</td></tr>
<tr><td>Tópico: 18-ANCiber-Organização</td><td>Id#: 107</td><td colspan="2">Parecer: 3-Inadequada</td></tr>
<tr><td>Tipo de Contribuição: Alteração Legal</td><td>Artigo: 11</td><td>Inciso:</td><td>Parágrafo:</td></tr>
<tr><td colspan="4">Texto Original:
Art. 33 . Na composição da primeira Diretoria da Agência Nacional de Cibersegurança, visando implementar a transição para o sistema de mandatos não coincidentes, o Diretor-Geral e demais Diretores serão nomeados pelo Presidente da República, observados os seguintes prazos de mandato:
...</td></tr>
<tr><td colspan="4">Crítica ou Sugestão:
Sugiro inserir um parágrafo conforme a seguir: § 3 Os integrantes indicados a compor deverão possuir comprovado conhecimento na área de segurança da informação por meio de cursos oficiais de instituições nacionais ou internacionais de segurança, certificações na área de segurança da informação, pós-graduação na área de segurança da informação ou, experiência em unidade de segurança da informação na área pública ou privada de pelo menos 2 anos.</td></tr>
<tr><td colspan="4">Resposta:
Os requisitos para cargos de diretoria de agências reguladoras já estão descritos na Lei 9.986 de 18 de julho de 2000, em seu art. 5º, e são mais restritivos que os sugeridos pelo autor.</td></tr>
</table>

Audiência Pública da PNCiber – Contribuições

Responsável: Ivanildo de Oliveira da Silva			
Instituição: Cidadão		**Título:** Cidadão	
Tópico: 21-ANCiber-Diretoria	**Id#:** 99	**Parecer:** 3-Inadequada	
Tipo de Contribuição: Alteração Legal	**Artigo:** 33	**Inciso:**	**Parágrafo:**
Texto Original:			
Crítica ou Sugestão: Segundo ponto diz respeito ao escopo dos produtos e serviços que estariam sendo avaliados pela agência. No Artigo 18, inciso 14, quando trata da competência da agência, diz que compete a agência avaliar produtos e serviços, vírgula, no tocante a cybersegurança. Mas o anexo 1, artigo 21, inciso 8º, quando trata das receitas da agência, lista dentre elas as taxas de certificação de produtos e serviços de cybersegurança. Ao meu ver são conceitos distintos.			
Resposta: É competência da ANCiber: definir padrões de certificação e avaliação; definir padrões de acreditação de avaliadores e certificadores; avaliar e certificar produtos e serviços de cibersegurança, inclusive por meio de acreditados. E, para tal, pode cobrar as taxas dispostas no anteprojeto.			

PNCiber – Relatório da Audiência Pública

ANEXO II

Audiência pública sobre a criação da Política Nacional de Cibersegurança

Brasília/DF.
19 de Junho de 2023

SR. MARCELO MALAGUTTI, MESTRE DE CERIMÔNIA - Os congresso, e comecei a partir dos cidadãos a desembolsarem um valor mais significativo para colocar mais gente à disposição de fazer esse trabalho. E outra questão importante que pesou muito para nós é a questão da capacidade atual do Brasil de coordenar suas ações. Então não adianta fazer um projeto tão ambicioso quanto é, por exemplo, a equivalente à agência francesa que tem 3.600 funcionários, porque não seria possível implementar isso no Brasil nesse momento. Como a maioria já deve ter percebido, o projeto prevê uma implantação gradual ao longo de 5 anos, e essa intenção é exatamente da gente conseguir desenvolver maturidade, desenvolver expertise, processos, protocolos, procedimentos, para que a gente possa então, num futuro próximo, daqui a 5 anos talvez, dar passos maiores. Mas por hora, então, a nossa preocupação é tornar esse projeto factível, viável, realizável, sem envolver tudo aquilo que a gente consideraria ideal para o desenvolvimento do projeto. Bom. As críticas e sugestões aqui apresentadas, elas serão todas registradas e, como eu dizia, no prazo máximo de 30 dias, nós vamos publicar no nosso site aqui do GSI a nossa, o nosso relatório final, considerando, se possível, todas as sugestões e críticas apresentadas. É um trabalho hercúleo porque antes da audiência de hoje nós já recebemos, de vários ministérios, quase uma centena de sugestões de alterações. Graças a Deus, a maioria delas é pontual, palavras específicas, uma frase ou outra. Ninguém apresentou nenhuma proposta que mexa na estrutura do projeto, o que mostra uma boa resiliência do projeto, uma vez que essas propostas não estão fazendo alterações substanciais, e mostra também uma percepção da urgência, da relevância desse processo. Que fazer uma ampla discussão novamente de todo o processo, porque é assim não assado, levaria uma, à um tempo maior de maturação, um tempo que, no nosso entendimento, eu labuto na área há mais de 30 anos, é um tempo que nós não temos. Se nós formos discutir mais 5 anos, nós estaremos 5 anos mais atrasados do que os 15 que nós já estamos em relação à outros países da mesma estatura geopolítica do Brasil mundialmente, que já implementaram as suas agências, já desenvolveram suas maturidades. Eu queria observar que esse modelo de audiência pública que nós estamos adotando aqui, ele é um modelo de captação de sugestões. Não é um debate. Nós não vamos então fazer aqui uma discussão das ideias apresentadas, nós vamos coletar todas as ideias. Favoráveis, contrárias, não interessa. Nós vamos anotar todas elas. A gravação vai ser disponibilizada depois para alguém que queira conferir, mas nós vamos fazer uma transcrição da gravação e pegar cada uma das sugestões para fazer as nossas ponderações sobre elas. Então, eu sou sobrenome italiano. A gente tipicamente é conhecido por ser sangue-quente, mas vocês podem falar à

vontade, criticar a vontade, que eu prometo que nós não vamos debater, nós não vamos responder. Nós simplesmente vamos tomar nota de tudo com a intenção de fazer uma análise fria, calma, ponderada, e considerar isso tudo para frente. Então eu vou repetir, não haverá debate. Nessa linha, pede-se que aqueles que forem fazer as suas manifestações o façam sem referência, sejam positivas ou negativas, às referências dos colegas que tenham falado antes. Então, se um colega veio e falou o oposto do que eu penso, eu digo, eu acho que o melhor é fazer A, mesmo que alguém tenha dito que o melhor é fazer B. Não vou fazer referência ao que o outro disse antes, eu não concordo com o colega que disse. Vamos evitar esse tipo de coisa exatamente para manter o fluxo funcionando bem, podermos ouvir mais gente, mais ideias, mais sugestões, e mais críticas. Cada uma das, das manifestações vai ser ouvida com respeito, serenidade, e urbanidade. Estamos aqui num ambiente colaborativo, a cibersegurança exige colaboração, e essa é a nossa intenção aqui. Então, igualmente, nós esperamos que as pessoas que façam as apresentações o façam considerando essa serenidade e essa urbanidade, lembrando que é um trabalho muito intenso de muita gente envolvida. E por fim, nós lembramos que o objeto dessa audiência pública é aquele anteprojeto que foi apresentado. Nenhuma outra consideração sobre nenhum outro tema diverso daquele será registrada ou tolerada aqui. Então, não se espera a discussão de perspectivas ou percepções políticas mas sim uma discussão da temática que foi colocada, que é um projeto de lei de uma política nacional de cibersegurança complexa, ampla, de um peso significativo para os cofres públicos. Muita gente questionou, puxa, mas 600 milhões de reais é muito dinheiro? Como será demonstrado aqui, é muito pouco, considerado o custo de não fazê-la, então nós temos que pensar nesses aspectos todos e considerar isso tudo na hora de fazermos as apresentações e as ponderações. Vou repetir para ficar bem claro para todo mundo que, presente ou remoto, que aqueles que desejarem enviar suas considerações por e-mail poderão fazê-lo até às 23:59. O fato de não estarem aqui presentes não inviabiliza a participação popular. Como eu disse, a nossa intenção é coletar o maior número possível de sugestões e críticas. Então, aquelas pessoas que estiverem nos assistindo online ou que venham assistir depois o vídeo, que vai ficar disponível na internet, e queiram fazer suas contribuições poderão fazê-lo até às 23:59 de hoje. Por que isso? Porque hoje é o dia da audiência pública. Às 00 horas e 1 minuto de amanhã nós já estaremos elaborando o relatório com as considerações de hoje, então nós não pretendemos ficar coletando mais sugestões posterior, porque senão o trabalho não acaba nunca. E como nós temos um prazo legal de 30 dias a partir do minuto de amanhã, nós já estaremos trabalhando, já estaremos contando esses 30 dias. Isso tudo posto, eu peço desculpas a vocês por qualquer inconveniente que possa ter

acontecido ou vir a acontecer no dia de hoje, e assumo aqui a nossa imaturidade, digamos, para tocar um projeto desse tipo. A nossa inexperiência, talvez, mais do que imaturidade, a nossa inexperiência para tocar um projeto desse tipo. Mas esperamos que os senhores e senhoras nos apoiem, nos entendam, e nos perdoem por qualquer incômodo, qualquer coisa que venha atrapalhá-los ou incomodá-los. Agora passamos a aguardar aqui a chegada das autoridades. Já estamos aqui com diversos dos nossos palestrantes convidados presentes aqui no prédio. Alguns deles, por questões de voo ou de outros compromissos, nos pediram para fazer uma mudança na agenda divulgada ontem, então nós vamos ter a abertura feita pelo nosso Ministro e logo em seguida o Senador Esperidião Amin, uma pessoa muito atuante na causa da cibersegurança e da ciberdefesa há muitos anos. Ele nos pediu para fazer a primeira, a primeira palestra porque ele tem que ir para uma CPMI que está em andamento no Senado, então ele vai ter que se deslocar para lá. Então ele vai ser o nosso primeiro palestrante, e em seguida a gente vai tentar, na medida do possível, respeitar aquela agenda prevista e seguir em frente. Cada um dos palestrantes do primeiro grupo de convidados vai ter até 10 minutos e aí, bom, todos vão entender que alguém pode passar 12 minutos, alguém pode falar 6 minutos, mas a ideia de até 12 minutos, até, não, até 10 minutos. E depois, passadas as duas autoridades previstas, nós abriremos a palavra para todos os presentes, aqueles que queiram se manifestar, que poderão falar por até 3 minutos cada um, expondo suas ideias, suas propostas, suas críticas, e sugestões. É um modelo previsto, e se tudo correr bem, se as coisas funcionarem dentro desse cronograma que nós previmos, por volta do 12:30, 12:40 nós devemos conseguir encerrar a nossa audiência de hoje. Caso não seja possível, caso todos queiram falar, todos queiram apresentar ideias e sugestões, para mim não tem problema. Nós podemos aqui até às 18 horas. Depois das 18 horas nós temos que fechar o auditório. Mas, é, por mim nós ficamos aqui, discutimos tudo porque é a nossa intenção, coletar o máximo possível de críticas e sugestões de todos aqueles que queiram contribuir. Então, ficamos aqui agora aguardando a chegada das autoridades, e nós temos uma equipe identificada aí, preto com um cracházinho branco pendurado. É, fiz em caso de necessidade de alguma coisa, de algum material, de algum, de algum formulário. Nós temos inclusive o formulário aqui de críticas e sugestões, onde identificado o artigo, inciso, a linha, é possível fazer as sugestões e submeter aqui pessoalmente. Entregando para o nosso pessoal, a gente coloca no rol das considerações a serem tratadas. Adentro o auditório aqui, os nossos convidados, as autoridades.

Sem mais delongas, convido o Ministro Amaro à fazer a abertura oficial do nosso evento, e novamente agradecemos a presença de todos.

SR. MINISTRO MARCOS ANTONIO AMARO - Senhoras e senhores, muito bom dia. Eu quero inicialmente agradecer aqui a presença que muito nos honra do Senador Esperidião Amin, na pessoa de quem eu agradeço aqui a presença de todos, né? A proposta da política nacional de cibersegurança, ou de cybersegurança como alguns preferem, elaborada pelo GSI, objeto desta audiência pública, visa atender a um conjunto de necessidades identificadas por diferentes instituições e especialistas desde ao menos o ano de 2014, de forma melhorar a governança acional sobre essa temática, adequando o que há de mais moderno no mundo ao arcabouço e a cultura institucional do nosso país. Tal política da maior urgência e relevância, posto que conforme evidenciado em audiência pública do Senado em 19 de maio de 2023, o número de ciberincidentes envolvendo o Brasil é desproporcionalmente elevado em relação à sua população e a sua economia. Neste contexto, a intenção fulcral da política é abarcar o conjunto da sociedade brasileira, coordenando a atuação nacional matemática. A proposta ora sobre escrutínio público apresenta princípios objetivos e diretrizes que a fundamentam. A partir desse conjunto de pressupostos estabelecem-se os instrumentos destinados à materializar a política. Um instrumento central é a criação do Sistema Nacional de Cibersegurança, da qual constam o Comitê Nacional de Cibersegurança, composto por representantes do Governo, da sociedade, da academia, e do setor privado, cuja finalidade é supervisionar e orientar as atividades da Agência Nacional de Cibersegurança, uma agência regulatória que observa transversalidade da cibernética e que materializará as ações como braço executivo da política. O gabinete de gerenciamento de cibercrises, a ser composto por representantes dos diferentes órgãos do Governo e responsável por atuar quando da ocorrência de cibercrises, e o Complexo Nacional de Cibersegurança, um inventário de ciberativos, hardware, software, e dados, que sustentem sistemas essenciais à sociedade brasileira a serem jurisdicionados pela política nacional de cibersegurança. Além do Sistema Nacional de Cibersegurança, os instrumentos incluem ainda a Estratégia Nacional de Ciberegurança agora orientada pela política, o Plano Nacional de Cibersegurança destinada a desdobrar a estratégia em ações anuais, a Cooperação Internacional, e o ensino, pesquisa, desenvolvimento, e inovação em cibersegurança. Nós do GSI entendemos que esse escrutínio público proverá subsídios importantes para a melhoria de nossa proposta, facilitando sua futura tramitação junto ao Congresso Nacional. Por isso agradecemos imensamente o interesse e a presença física ou virtual de todos os que se dedicaram e que dedicam o seu precioso tempo para participar desta audiência pública. Muito obrigado. Declaro abertos os trabalhos desta audiência pública e convido o Senador Esperidião Amin fazer uso da palavra.

SR. SENADOR ESPERIDIÃO AMIN - Muito bom dia a todos.

NÃO IDENTIFICADO - Bom dia.

SR. SENADOR ESPERIDIÃO AMIN - Quero dizer que fiz questão de aceder a esse convite e comparecer a esse ponto porque é muito oportuno e é importante que o governo tome a iniciativa de propor um projeto de lei sobre esta matéria. Por isso a minha presença significa pelo menos a certeza de que o parlamento brasileiro nos últimos anos tem despertado a sua atenção para o conjunto do assunto, do problema, do fator bem aportuguesado, cibersegurança. Durante um bom tempo nós brasileiros achamos que isso não era para nós, e esses dados sobre a desproporcionalidade dos ataques que têm sido pespegados contra o nosso interesse nacional, isso é apenas a ponta do iceberg da nossa real responsabilidade. Por isto estou aqui acompanhado do consultor do Senado Tarcísio, que é ligado à Comissão de Relações Exteriores da Defesa Nacional, de um assessor do Senado, do chefe de gabinete Eduardo Siqueira, que tem dedicado seu tempo a este assunto especialmente a partir de 2019, como eu posso pedir que ateste o (Ininteligível) que tem de alguma forma acompanhado este assunto. Efetivamente em 2019, o seio da Comissão de Relações Exteriores de Defesa Nacional, por uma coincidência motivados por um homônimo, o General Amin, que não é meu parente e que era na época o chefe da Defesa Cibernética do Exército, nós começamos a dedicar ao tema uma atenção especial na Comissão de Relações Exteriores de Defesa Nacional com foco em três pontos. Primeiro, não se dá importância a um assunto sem cuidar da parte orçamentária financeira dele. Vira romance, e as primeiras providências modestas foram tomadas a partir de então. Segundo, a criação de uma subcomissão que seria permanente, e que foi, teve o seu funcionamento obstaculizado pela pandemia e agora foi novamente proposta na primeira reunião da Comissão de Relações Exteriores de Defesa Nacional e foi aprovada, ficando com boa parte das suas atribuições cometidas ao Senador Astronauta Marcos Pontes e outra parte sob minha responsabilidade. E finalmente, também, o marco legal. Nós chegamos a estudar isso, a própria minuta da justificativa que nos foi entregue, ao mencionar que o Senado fez movimentos nesse sentido atesta o fato de não ter justificado completamente fora. Mas como se trata de um projeto que deve implicar na criação de uma agência própria, e eu pessoalmente concordo com isso, acho que é o nosso modelo, acho que é o mecanismo que o Brasil está utilizando para cuidar de políticas públicas realmente de Estado. Esse modelo que é europeu mas foi consagrado no Brasil, eu acho que deve ser utilizado. Fiz questão de vir aqui para dizer, concordo com todas as observações feitas pelo Ministro, não posso dizer eu mesmo sobre o conteúdo porque nós vamos aguardar naturalmente a proposição. Mas quero dizer, farei tudo o que estiver ao meu alcance para que

esse projeto seja iluminado pela consciência mais viva do Congresso Nacional, porque, repetindo o que eu disse no início, é oportuno e importante. Vamos continuar acompanhando a audiência da nossa Casa, até porque temos (Ininteligível) sessão da Comissão de Relações Exteriores de Defesa Nacional hoje também. Então eu me despeço fisicamente, mas estaremos atentos, e repito, apoiando essa iniciativa, esta audiência especificamente que é o cumprimento democrático mais legítimo para a geração de uma proposta de lei que visa tratar de um assunto de Estado, do nosso Estado do Brasil. Obrigado.

SR. MARCELO MALAGUTTI, MESTRE DE CERIMÔNIA - Dando seguimento à nossa agência, à nossa agenda. Perdão. Tá tão impregnado o assunto aqui que (Ininteligível) trocando as palavras. À nossa agenda, então prevê agora uma breve explanação por um pequeno incidente sofrido no, pelo nosso secretário hoje. Ele não vai estar presente. Vocês vão ter que me aturar aí nos próximos 20 minutos fazendo uma breve explicação do que está por detrás dessa, dessa proposta. A política, ela se baseia num contexto que é conhecido muito proximamente por muitos de vocês, que é um, de um incremento muito significativo, não apenas do número de incidentes, mas da complexidade dos incidentes que atingem o país. E uma das questões essenciais, um dos incidentes mais famosos, foi exatamente esse do STJ, que é muito relevante para quem labuta na área de direito internacional e particularmente de relações internacionais no sentido de que desde pelo menos 1926 entende-se que a capacidade de aplicar a justiça numa porção do território é o que define soberania. E a partir do momento que um incidente cibernético priva o país da capacidade de aplicar a lei no seu território, há um ataque direto à soberania do país. Não interessa se o ataque foi promovido por alguém de fora ou se foi promovido por alguém de dentro. A soberania do país está ameaçada nesse contexto. Então nós temos, além desse incidente, nós temos alguns outros que afetam, por exemplo, o nosso direito enquanto cidadãos de fazer compra. É muito interessante que as pessoas falam, ah, prejudicou a Renner. Sim, mas prejudicou também mais de 2 milhões de pessoas que deixaram de fazer compra no site da Renner naquele, naquele momento. Ou nós temos o caso do ConecteSUS que privou várias pessoas do direito de ir e vir. Para poder entrar e sair do país precisava ter lá o cartão de vacinação, e as pessoas não conseguiam emitir seu cartão de vacinação porque o sistema estava indisponível por causa de um incidente cibernético. Nós temos ainda outro, outra rede grande de lojas de varejo, mas também em particular chama atenção o caso do CNPEM aí, em que o nosso maior acelerador de, de partículas, um instrumento de pesquisa do mais elevado custo e relevância para o país, ficou indisponível por causa de um incidente cibernético. Nós temos o ataque à justiça estadual, e aqui aparece a do DF que é mais próxima

do nosso dia a dia, mas atingiu Rio Grande do Sul, atingiu São Paulo, atingiu Sergipe, então nós tivemos já diversos, diversos incidentes. E nós temos também um caso muito emblemático. Eu pediria a todos que memorizassem esse número, 1 bilhão, ele vai voltar um pouco a frente aí. Mas um único incidente cibernético de pequena duração ocorrido em fins de 2022 provocou um prejuízo de 1 bilhão contabilizável, palpável, palatável ali nos cofres do INSS. E nós temos o mais novo fenômeno mundial que é o do ransomware, e o Brasil vive uma triste realidade. Ele é o segundo país mais atacado por ransomware e é o país que mais paga ransomware no mundo. Como nós não estamos preparados para nos defender, somos atacados, e aí a solução tem sido pagar, o que realimenta o ciclo vicioso dos criminosos. Eles, se paga, se rende, então eles vão fazer mais. Isso posto, nós tenhamos a consideração que o nosso Ministro e o Senador mencionaram à pouco, posições incompatíveis do Brasil com relação à realidade de incidências mundiais. Nós temos a sexta maior população do mundo, a oitava maior economia em termos de poder de compra comparado, não em termos absolutos mas poder de compra comparado, nós temos a segunda maior superfície de ataque, o maior, o segundo maior governo digital do mundo, perdemos apenas para Coreia do Sul, e nós temos o segundo maior número de ciberataques, se não do mundo, pelo menos das Américas. Esse número é questionado, depende do Instituto de Pesquisa, mas é um número muito significativo. E, no entanto, nós ocupamos a décima oitava posição no índice internacional de, de cibersegurança. Um país que tem uma superfície de ataque, um nível de oferta significativo como o nosso de serviços e que tem uma cultura de cibersegurança tão, é, baixo, tão ínfimo, pode ser claramente um save haven, né? Um paraíso para, para aqueles que pretendem cometer cibercrimes. Bom. A nossa proposta, ela tem como modelo um conjunto de ideias que nasceram na Europa. Por que nós escolhemos esses países? Porque são aqueles que institucionalmente, culturalmente são mais próximos, no arco dos países mais desenvolvidos, são aqueles mais próximos do nosso, da nossa cultura, do nosso modelo institucional. Mas nós, além de usarmos o modelo NIS2, que é recente, é de dezembro do ano passado, adotado pela União Europeia, nós também nos preocupamos com o modelo da UIT, né, a União Internacional de Telecomunicações, que é um órgão da ONU, e nos preocupamos com o modelo de Oxford da, de maturidade de Oxford, que foi o modelo utilizado para avaliação das capacidades brasileiras adotado pela OEA, Organização dos Estados Americanos há alguns anos para avaliar a América Latina como um todo. O formato é de um Sistema Nacional, o nosso Ministro mencionou isso há pouco, que prevê 3 instituições, 3 órgãos com diferentes funções. Um deles, um comitê supervisor que avalia e sugere medidas a serem adotadas pela agência, a centralizadora que é o órgão executivo, e um gabinete de crise,

porque partirmos do princípio que por melhor que venha à ser a nossa segurança, por melhor que venha à ser a nossa cultura de proteção, incidentes ocorrerão, crises aparecerão, e nós vamos ter que resolvê-las e atuar sobre elas. Nessa lógica tá prevista a existência de um gabinete de crise, que pode inclusive escalar a situação para o Conselho Nacional de Defesa e acionar o Presidente da República no caso de um incidente de graves proporções. Isso tudo já faz parte do nosso projeto. Bom. A meta é dotar o Brasil de um arcabouço compatível internacionalmente, nossos colegas do Ministério das Relações Exteriores aqui vão fazer comentários a respeito. Nós temos agora alguns acordos internacionais aos quais nós aderimos, e nós temos obrigações a cumprir com relação a esses acordos, então nós temos que estar preparados para poder atuar adequadamente nesse contexto. E, o interesse antigo do Brasil é de ter a condição de ser o fazedor de normas e não apenas um tomador de normas. Nós queremos poder participar dos fóruns internacionais, dos debates internacionais, mas para isso nós precisamos ter maturidade, nós precisamos ter uma estrutura compatível. Então, esses aí são os pontos essenciais. Os nossos eixos estruturantes são 3. Muita gente se preocupa quando a gente fala na existência de uma agência porque, ah, mais uma agência reguladora, mais um instrumento de cobrança. Bom. A proposta, ela começa na cooperação. Já mencionei há pouco, cooperação é um elemento essencial para a cibersegurança. Nenhum país se defende sozinho, nós precisamos cooperar internacionalmente. Nenhuma instituição, internamente, se defende sozinha. Nós precisamos ter a cooperação de diversas entidades. No entanto, apenas a cooperação não resolve. Nós precisamos de regulação. Nós temos aí, o colega do TCU deve comentar, eles criticam, tem um relatório emitido em, publicado em julho do ano passado, em que eles apontam a falta de coordenação entre as diferentes instâncias dos órgãos governamentais. Nós temos iniciativas da Justiça, nós temos iniciativas no Legislativo, nós temos iniciativa no Executivo. Mas essas iniciativas, elas não são coordenadas, elas não são sincronizadas, porque apenas a cooperação, como eu dizia, não é suficiente para garantir isso. Então, um dos outros objetivos, o nosso segundo grupo de objetivos, é exatamente de ter um órgão capaz de fazer uma regulação, uma regulação que possa passar pelo escrutínio dos diversos órgãos da sociedade, diversas (Ininteligível) da sociedade, daí a existência do comitê. Então a agência não pretende ser apenas um cuspidor de regras, mas sim um órgão que vai ter uma supervisão, um debate, para avaliar se aquelas regras podem ou não ser implementadas e como podem ou não ser implementadas. E por fim, nós temos a necessidade de controle. O controle parte do princípio de que a regulação por si só não funciona. Nós tentamos convencer as pessoas, nós tentamos convencer as instituições. Nós temos regras, mas muitas vezes as regras não são cumpridas na cultura brasileira, e uma das preocupações

nossas na adaptação dos modelos estrangeiros do Brasil é entender a cultura, fazer uma adequação para a cultura brasileira. E nós temos aqui no Brasil um fenômeno da lei que pega e a lei que não pega, é parte da nossa realidade, então nós precisamos ter um mecanismo de controle que assegure que aquela lei que se pretende implementar seja de fato cumprida, seja de fato seguida. A estrutura toda do documento prevê que nós vamos fazer normas, essas normas supervisionadas por um comitê amplo, e uma vez que definiu-se uma norma de determinado nível de segurança para um determinado tipo de serviço essencial, busca-se um termo de cooperação, um termo de ajustamento de conduta, o famoso TAC. Então nós vamos buscar e estabelecer um planejamento, um determinado órgão jurisdicionado para dizer, eu preciso de dois anos para fazer uma implementação. Então nós vamos estabelecer um termo de ajustamento de conduta, vamos acompanhar esse processo, e a partir do momento que se perceba algum desvio entra a questão do controle para se fazer cumprir aquilo que foi acordado. Então, ao contrário de que algumas pessoas perceberam, a intenção não é simplesmente colocar regra para começar a cobrar, é se colocar uma regra que busca elevar o nível de segurança e que se planeje, de forma cooperativa, a adequação daquela instituição àquela regra. E a partir daí, se houver, vou usar uma expressão popular, corpo mole daquela, daquele órgão, entrar com os instrumentos de cobrança e de controle para fazer, fazer valer o que foi acordado. Bom. Isso posto, nós temos aí algumas características relevantes para demonstrar a urgência e relevância do tema. Já em abril de 2014, na esteira do Caso Snowden, uma CPI do Senado, a CPI da Espionagem Eletrônica, disse que era necessário a existência, a criação, o debate de uma agência no âmbito do Poder Executivo Federal para poder regular a cibersegurança do país. Depois, houve uma certa confusão sociopolítica e econômica no Brasil nesse período de 2014 para cá, e em 2020 foi publicada a nossa E-Ciber, e a E-Ciber, ela, a nossa estratégia nacional de cibersegurança, ela tinha alguns defeitos. Ela foi uma iniciativa para tentar recolocar o tema na pauta, o tema da cibersegurança na pauta, mas ela tinha alguns defeitos. Ela foi implementada por decreto, e portanto ela só tinha alcance no Poder Executivo Federal, e ela não tinha o suporte de uma política. Nasceu uma estratégia sem o suporte de uma política, portanto ela se torna um tanto quanto inócua. Em julho de 2022, eu mencionei um relatório do TCU que não sugere explicitamente uma agência, mas sugere, demanda a criação de uma estrutura, de um órgão capaz de centralizar, o que tem ampla autoridade, capaz de centralizar as ações de segurança da informação e segurança cibernética. A União Europeia lançou a diretriz NIS2, que apertou a margem de interpretação em relação à NIS1 lá de 2016 com a intenção de tornar mais difícil para os estados membros da União Europeia fazerem corpo mole com relação à segurança de um, de um desses

estados. Então, o caso emblemático era o caso que reportavam que os italianos e os espanhóis não estavam fazendo as coisas com o mesmo grau de seriedade dos franceses e dos britânicos, então era necessário apertar um pouco mais a regra para que a insegurança de um não comprometesse a segurança da coletividade. Então, seguindo mais ou menos essa linha, a gente percebeu a existência da, de uma situação similar aqui no Brasil. No relatório da transição de governo no fim de dezembro foi, a palavra cibernético aparece uma única vez, mas aparece nessa frase, que o Brasil enfrenta riscos de segurança cibernética e de apagões na agenda de governo digital. Então o novo governo percebeu, na análise que fazia do governo, que a gente estava um pouco descoordenado no sentido da segurança cibernética nacional ou da cibersegurança, como eu prefiro chamar. Já no primeiro dia do novo governo foi criada então uma, o gérmen, né, uma semente de uma nova estrutura em que o nosso antigo Departamento de Segurança da Informação foi transformado na Secretaria de Segurança da Informação e Cibernética. Foi uma transformação de nome, uma transformação de caráter político para elevar o status da instituição. O governo não tinha como, por decreto, ampliar a estrutura do antigo departamento com a criação da secretaria, mas ele deu um status maior para representar a importância da temática. Nomearam então um assessor especial, esse que vos fala. Eu sou o único dos assessores do Ministro que tem uma função única. Eu brinco que eu sou homem do samba de uma nota só. Eu só trabalho com a política nacional de cibersegurança 100% do meu tempo. Os outros assessores assessoram o Ministro em diversos assuntos diferentes. Eu tenho uma única função estabelecida, que é tentar melhorar a proposta, tentar fazer essa política avançar o mais rapidamente possível. Novamente, um exemplo do reforço que se pretende dar, da importância que se denota com relação a esse assunto. E, nós já iniciarmos, no planejamento do PPA desse ano, a separação da temática de segurança da informação daquela, da cibersegurança de forma a, naquele momento em que a discussão da agência, da política, do comitê, do gabinete de gestão de cibercrises entrar no Congresso, a gente já tem os instrumentos orçamentários previstos. A gente brinca que estamos criando a conta no banco. A gente não bota dinheiro, mas a gente tava criando a conta. Na hora que alguém assinar o cheque, a gente já pode colocar dentro do, do plano plurianual. Então, nesse contexto, vamos acelerar aqui um pouco. Nós temos ainda, é, o Fórum Econômico Mundial, o Fórum Econômico Mundial que aponta que a tecnologia vai desequilibrar ainda mais a relação entre os países. Então as desigualdades vão se acentuar, as pessoas que têm condições de utilizar tecnologias, as pessoas e os países, vão se beneficiar disso, mas os países que não estiverem adequadamente preparados vão aumentar o gap tecnológico deles entre os países, com os países avançados. Depois nós temos um relatório muito

interessante, e um dos autores, o autor-chefe dele tá aqui presente para falar sobre ele, em que um grupo de acadêmicos da FGV Direito fez uma pesquisa ampla e escreveu literalmente que, em 2023, a falta de uma Agência Nacional de Cibersegurança. Quase tivemos que fazer aqui o inquérito administrativo porque todo mundo sempre chamou no governo de Segurança Cibernética, e nós tínhamos adotado 20 dias antes no nome Cibersegurança como o novo modelo, e de repente saiu o relatório deles com esse nome. Vamos verificar de onde foi o vazamento de informação. É, mas que não seria aceitável o Brasil nesse momento não ter essa, essa agência. Então, nós queremos agora ouvir a opinião dele, depois de ter vido o relatório para detalhar um pouco mais a discussão. E por fim, nós temos alguns formadores de opinião, a FIESP também aqui representado, a CNI também aqui representada, o Senado Federal, o TCU, todos aqui presentes. Infelizmente, o pessoal da Associação Brasileira de Estudos de Defesa não pode vir, mas a FGV também tá aqui representando o meio acadêmico. Como eu dizia na abertura, nós temos praticamente 100 órgãos representados aqui, inscritos para essa audiência, no universo de mais de 160 pessoas inscritas, então, assim, é um tema que chamou a atenção, que movimentou grande parte da sociedade, são órgãos muito representativos como vemos aí. Nós temos uma, uma discussão interessante que foi uma mudança de abordagem dentro do GSI com relação ao que nós estamos fazendo na política. A nossa lógica de serviços essenciais é diferente da lógica de infraestruturas críticas que o, que o GSI trabalhava até recentemente, trabalha ainda, mas ela não é antagônica. O que acontece é que os serviços essenciais, eles abarcam um conjunto de áreas, mas não abarcam outras áreas. Então, dentro do serviço essencial, essencial, nós ainda temos, perdão. Dentro de uma infraestrutura crítica nós ainda temos ativos que são cibernéticos e não-cibernéticos. Para exemplificar, algo como 97% das barragens brasileiras são como aquelas de Mariana, Brumadinho, que deixam tão triste lembrança na, na sociedade brasileira, que eram basicamente montes de terra que represavam um grande volume de água. Não tem nenhum equipamento eletromecânico ou cibernético associado à ele que possa representar um risco. Por conseguinte, enquanto infraestrutura crítica, ela é relevante, ela tem que ser monitorada, ela tem que ser cuidada, ela tem que ser observada. Mas, do ponto de vista cibernético, a gente não têm absolutamente nenhuma capacidade de fazer nada com relação a ela. Logo a segurança cibernética desses órgãos, dessas instalações é pouco relevante do ponto de vista nacional. Entendido aí a diferença entre uma coisa e outra? É importante para o país cuidar delas, mas não do ponto de vista cibernético. De outra parte, nós temos os casos reportados na, nas notícias de jornal que eu apresentei no começo, em que a justiça foi fortemente afetada por incidentes cibernéticos, têm sido fortemente afetada por icidentes cibernéticos, mas não é

considerado infraestrutura crítica. Claro, poderiam alguns sugerir, então vamos colocar a justiça como uma infraestrutura crítica. Por que não? Bom. Na saúde, o ConecteSUS, o vazamento, o ransomware no Laboratório Fleury por duas vezes e mais outros tantos exemplos seriam similares, então vamos incluir a saúde como outra infraestrutura crítica. E aí vamos incluir um incidente envolvendo o Inep e o Enem, e então vamos incluir a educação como infraestrutura crítica, e por conseguinte vamos incluir a sociedade brasileira inteira como infraestrutura crítica porque em diferentes pontos, em diferentes momentos, algum deles vai ser atacado e vai gerar um impacto da sociedade. Bom. Eu mencionei há pouco que nós temos ativos cibernéticos ou não, mas se nós pensarmos sobre a ótica da transversalidade, também mencionada pelo Ministro, nós temos aí alguns ativos específicos nessas infraestruturas críticas ou não-críticas que nos interessam do ponto de vista da cibersegurança, da elevação da cibersegurança nacional. E essa visão de pegar aquilo que é importante, relevante, ou essencial, o nome que adotamos, foi a opção que nós adotamos na concepção, na elaboração da proposta que hoje está em discussão aqui. Espero ter conseguido deixar claro para vocês a visão. Então, basicamente, vamos lá. Qual é a diferença? Nós tínhamos as verticais de, de serviços, nós temos por exemplo telecomunicações, nós temos por exemplo energia elétrica, e a maioria delas, combustíveis, a maioria delas têm agências reguladoras como segmento econômico, como um setor econômico. A nossa proposta é uma agência reguladora transversal que vai cuidar de elementos específicos que afetam infraestruturas críticas ou não-críticas, mas tentando dar uma coordenação para elevar a segurança cibernética de todas elas. Essa é a mudança de chave essencial na nossa proposta de uma agência reguladora que não é numa vertical. Bom. Isso posto, temos aqui o nosso comitê, um comitê que apresenta uma representatividade muito, muito interessante na nossa ótica porque temos alguns órgãos do Executivo específicos ali, alguns Ministérios, nós temos alguns órgãos que são de governo mas não são do Executivo, como por exemplo a nossa querida Autoridade Nacional de Proteção de Dados, mas nós temos também o Conselho Nacional do Ministério Público, Conselho Nacional de Justiça. Não vou citar todos os nomes. E nós temos naquele grupo laranja lá 3 representantes de 4 grupos, totalizando 12, que são grupos distintos relacionados à nossa área. Alguns nos perguntam, por que a Anatel, por exemplo, não faz parte do comitê como membro nato. Bom. A gente poderia pensar nesse hipótese. Praticamente tudo da cibernética trafega pela, pela Anatel, então vamos colocar a Anatel ali. Só que se a gente olhar o mundo afora, o que é que acontece? Os americanos não se preocupam tanto com as telecomunicações quanto se preocupam com o grid de energia elétrica, então a ANEEL poderia dizer, por que eu não estou no comitê? E assim, novamente, nós poderíamos, por indução, levar a um comitê que teria 251

membros. Logo a lógica que nós adotamos foi, teremos 3 representantes de infraestruturas críticas que a cada 2 anos poderão ser trocados, intercambiados, e é uma decisão que cabe a eles se candidatarem e ao Presidente da República nomeá-los ou não. Então se tornam, digamos, um embate político, que aquele com o melhor argumento ou melhor capacidade de lobby, ou seja, qual for o argumento utilizado, vai ser capaz de, de conseguir participar ou não. Nenhum, nenhuma infraestrutura crítica como membro nato, mas todas elas com capacidade de participação. E igualmente nós teremos, por exemplo, instituições de pesquisa e tecnologia, basicamente universidades e centros de pesquisa, mas nós teremos também empresas. As empresas que trabalham com cibersegurança poderão ter seus 3 representantes nomeados ali. E por fim, elementos que atuam no campo da cibersegurança mas que não necessariamente são governo nem pesquisa, vou dar exemplo simples aqui, o Comitê Gestor da Internet, o CertBR, que podem estar no quarto grupo como membros, participando num determinado momento. Qual é a lógica? A lógica é oxigenar a discussão, é ter mais membros, mais participantes, e permitir então um debate mais amplo, sem necessariamente ser um debate legislativo. A estrutura de agência regulatória no Brasil permite que nós criemos resoluções que têm efeito legal, mas que são aprovadas por um comitê que debate isso, então a gente não precisa passar necessariamente por um debate no Congresso Nacional. Dá mais agilidade para um setor que necessita de agilidade, que é o setor da cibersegurança. Essa é a lógica, a lógica também é parecida no caso do Gabinete de Gestão de Cibercrise, onde a única diferença é que nós retiramos os membros da sociedade. Por que? Porque é uma crise cabe ao executor, ao Executivo cuidar dela, ao governo. Não é uma questão mais de Estado, é uma questão de Governo. Aquele governo precisa cuidar daquilo. Ele é que tem os meios e os poderes para fazer as ações necessárias. Então a estrutura é basicamente a mesma, tirando apenas os representantes da sociedade. Aqui nós temos um quadro que mostra a criação das diversas agências do Brasil. Essas 4 marcadas aí, inclusive a última, Agência Nacional de Mineração lá em cima, foram criadas por Medida Provisória. No caso delas era fácil, porque existia, no caso da ANM, por exemplo, o Departamento Nacional de Produção Mineral. Virou-se a chave, transformou-se no Departamento Nacional de Produção Mineral. Tinha pessoas, tinha processos, tinha estrutura já definida para se criar isso. Não é, por exemplo, o caso da ANPD, que não é uma agência mas é uma autoridade que tem uma legislação específica. Não existia a estrutura para virar a chave, então precisou ser criada essa estrutura, e nós vemos uma questão parecida no caso da Agência Nacional de Cibersegurança que nós propomos aqui. Para criá-la, não dá para fazer uma Medida Provisória, mas dá para fazer, por exemplo, um projeto de lei com urgência constitucional. Dá quase na mesma coisa, mas com uma, uma

percepção, uma perspectiva congressual, uma perspectiva legislativa diferente. A nossa proposta de agência com 800 pessoas parece muito ambiciosa para alguns, mas a gente costuma brincar que nós vamos estar no terço inferior ali. Não é uma agência tão ambiciosa assim se nós compararmos com, com outros exemplos que nós temos no Brasil atualmente. Então, embora o número 800 por si só pareça muito grande, ele não é assim tão grande. É importante relevar, observar aqui que o conjunto de recursos, as pessoas ali desenhadas do lado esquerdo da balança, e o conjunto de objetivos e responsabilidades e competências da agência, da política, e do Gabinete de Gestão de Crise, ele foi equilibrado para, para funcionar razoavelmente bem nesse contexto. Qualquer aumento de um ou diminuição de outro implica numa mudança de, de expectativas, então se alguém disser, não. 800 pessoas é muito, a gente só pode dar 600 para vocês. OK. Então o que é que a gente tira das competências? O que é que é menos importante daquela lista de competências que foi colocada ali? Não. Tudo é importante. Bom. Então eu preciso dos 800. Eu não tenho como fazer isso com 600. Pelo menos me mostra como é que seria possível fazer isso, e é para isso que nós estamos tentando ouvir os senhores aqui. Se alguém chegar e disser, não dá para fazer o que vocês estão propondo com 600? Ótimo. Explica para nós, diz como é que a gente põe isso no texto, que a gente vai tentar fazer isso. Essa é a lógica. E, comparando em termos internacionais, o nosso modelo nós citamos que não é o americano, né, mas nós falamos lá do, do francês, o segundo ali, do britânico, o terceiro, e do italiano, que é o quarto. Então nós estamos ali mais ou menos no mesmo número dos italianos. Lembrando que a população da Itália é um terço da brasileira, e em termos de poder de compra comparado à população, à economia italiana é 23% menor do que a brasileira. Então, mesmo se a gente for olhar os números absolutos comparado com, com os italianos, a nossa agência de 800 ela é pequena. 800 para eles é mais do que 800 para nós, traduzindo em outras palavras. Então, nós não estamos aí com nenhuma proposta ambiciosa demais, como os números refletem. Essa aqui é uma estrutura simples. É só uma passagem rápida. Nós temos aqueles, aqueles itens em cinza ali, que são obrigações legais de agências reguladoras, então nós temos que ter esses órgãos, e o roxo, nós temos aí órgãos de assessoramento, uma pequena área de inteligência para monitorar os grupos de hackers, os grupos de, de debate, a Dark Web, etcetera. Os senhores conhecem bem a temática. E ela dispõe de apenas 5 diretorias operacionais, que são aquelas, uma direção geral, uma direção de regulação, uma diretoria de operações, uma diretoria de cibereducação, que é, no meu entendimento, eu venho do meio acadêmico, né? Recentemente. Então é a mais relevante, é aquela que vai de fato surtir efeito no longo prazo, preparar o cidadão para ele se defender, para ele não ficar tão exposto, e uma de administração que não

tem nada demais. Eu não vou incomodá-los com essa, com essa estrutura. Nós temos aqui uma observação importante que os 800 cargos criados são todos eles de nível superior. Nós não criamos cargos de nível médio, e isso tem uma perspectiva muito pragmática. É uma questão meramente de capacidade de absorção e retenção de pessoal. Os cargos intermediários, se nós olharmos, por exemplo, a Associação Nacional dos Analistas de TI reporta que 50% dos analistas de TI do governo foi perdido nos últimos anos. A iniciativa privada tá pagando mais, o governo não tem como competir, as pessoas saem. Então para que nós sejamos minimamente competitivos nesse setor que demanda, existem mais de 300 mil vagas para profissionais de cibersegurança no Brasil atualmente, para nós sermos minimamente competitivos nós temos que trabalhar com os salários mais elevados que o governo puder pagar, então essa é a lógica refletida aí. E na mesma linha, nós temos uma proposta de 300 cargos e funções comissionadas, com um detalhe. Apenas 45, que são os CCEs ali, são cargos de livre nomeação. A proposta de lei que o senhores analizaram aí prevê que, a partir do momento em que o quadro de pessoal da agência for complementado, for preenchido com o pessoal concursado, as FCEs, as funções gratificadas, serão todas por lei, obrigatória agências. Apenas os 45 CCEs, e aí nós estamos falando de superintendências, diretorias e tal poderiam ser preenchidas para, ainda nesse caso permitir uma oxigenação no topo da, da agência. Essa é a nossa perspectiva de implementação. Nós começamos no primeiro ano com 81 pessoas, acrescentamos 132 no segundo ano, levando a 220, 223 (Ininteligível) Bom. Algum erro aí na planilha. Mas, enfim, nós vamos acrescentando os grupos ano a ano, e ela começa no primeiro ano custando 84 milhões e chegando a 594 milhões no último ano. E é aquela pergunta, pô, mas 600 milhões é muito dinheiro, né? É. Vamos lá. A E-Ciber em 2020, ela apontava que o Brasil tinha um prejuízo, e já era uma pesquisa de 2018, foi um dado usado pela E-Ciber, de que nós tínhamos 120 bilhões anuais de prejuízo financeiro causado por ciberincidentes. Cada moedinha dessas aí tá valendo 1 bilhão. É um incidente daquele do INSS que eu mostrei lá no começo para vocês, então esse é o número base. Os números internacionais apontam que nós temos cerca de 85% dos incidentes sendo de baixíssima complexidade. São coisas que um usuário minimamente preparado não, não cairia na armadilha, não estaria sujeito. Isso corresponde a 102 bilhões. O estarrecedor é que o número brasileiro é 93%. Então os 85% são um número mundial, a média mundial. No Brasil o número é 93%. O nosso usuário é menos preparado do que a média mundial. Mas vamos trabalhar com número internacional de 102 bilhões. Digamos que daqui a 5 anos a agência implementada, ela seja capaz de barrar 50% desses 120 milhões de prejuízo. Então nós estamos falando aí de 60 bilhões ao ano. Com a carga tributária nacional, isso corresponde à 24 bilhões em arrecadação. Aqueles 60 bilhões

são 24 bilhões de arrecadação, e a agência custa 0,6 bilhão ao ano. Não precisa fazer uma conta muito significativa para perceber que o investimento, mesmo que a gente não seja capaz de parar 50%, que a gente só pare 20% dos incidentes, já justifica fazer esse investimento. Qual é o ponto, né? O ponto é que se dado é de 2018. Esse número de 120 bilhões é de 2018. E os dados recentes, por exemplo o ransomware cresceu no Brasil, de 2021 para 2022, ele cresceu em 92%. Incidentes de fraude eletrônica bancária, 76%. Incidente de cartão de crédito, 72%. Se nós pegarmos um crescimento de 70%, não vamos considerar o do ransomware de 92%, vamos considerar 70% ao ano de 2018 para cá, o prejuízo em 2023 estimado seria de 1.7 trilhão de reais. Então esses números se tornam desprezíveis. Não daria para ver a meia moeda azul da agência numa escala de 1.7 trilhão aqui. Esse é o exemplo do que eu tenho chamado de custo de não fazer. Mesmo que a agência seja capaz de apenas reduzir em 20% esse crescimento médio de 70% que nós temos ao ano, ao longo de 5 anos isso vai ser responsável por mais de 800 bilhões de economia para o país. Se a agência for capaz de fazer apenas 20%, conter apenas 20% do crescimento, ao invés de crescer 70% ao ano crescer 50% ao ano, essa economia de 20% representa 800 bilhões de reais na economia brasileira ao longo de 5 anos. Uma economia bastante substancial quando a gente tá falando de um custo de 600 milhões, né? Nós estamos falando de alguma coisa acima de mil vezes a menos. Muito obrigado. Passei um pouquinho aqui do tempo previsto. Vamos então, sem mais delongas, passar para os nossos próximos palestrantes. Então eu convido aqui, em nome do Ministério das Relações Exteriores, o nosso estimado Conselheiro Franklin Silva Netto a fazer o uso da palavra.

SR. CONSELHEIRO FRANKLIN NETTO - Um bom dia a todos. Meu nome é Conselheiro Franklin Neto. Eu chefio a Divisão de Segurança e Defesa Cibernética do Ministério. Então veja que ainda, Segurança e Defesa Cibernética, então não fomos nós a origem da, do vazamento para a mudança para Cibersegurança.

NÃO IDENTIFICADO - Com certeza não.

SR. CONSELHEIRO FRANKLIN NETTO - Bom. Eu vou ser bastante breve. Essa aqui é uma audiência pública e temos mais de 100 inscritos, tá? Então em respeito aí a voz do público, eu, como representante de órgão oficial, vou ser, é, bastante resumido aqui na minha fala, mas eu queria abordar dois aspectos. Primeiro é ressaltar a importância e a necessidade dessa política nacional de segurança cibernética porque, do ponto de vista das relações internacionais, a cibersegurança tem sido alçada à uma, uma questão estratégica, tá? Já foi mencionado aqui que o aumento da superfície de ataque a atividade maliciosas

é em função da multiplicação dos, dos dispositivos conectados, em função da necessidade cada vez maior de todos os aspectos da vida dependerem da (Ininteligível), dependerem da internet, e isso também tem se traduzido, do ponto de vista da relação entre Estados, numa necessidade de trazer a questão da segurança cibernética para o centro das preocupações dos Estados. Porque assim como todos os campos da atividade humana têm dependido cada vez mais das tecnologias de informação e comunicação, também o funcionamento do Estado, o funcionamento dos dispositivos democráticos dos Estados, eles também têm dependido dessas, dessas tecnologias, de modo que o Brasil agora tá tratando desse assunto, ele na verdade, ele tá acompanhando um processo e tendências mundiais, né, que todos os países têm tratado essa questão desde uma perspectiva estratégica, tá? Naturalmente que o Ministério fará chegar ao GSI as suas observações e sugestões ao texto da política, mas tem 2 aspectos muito importantes que a política trata, que é a questão, primeiro, dos acordos internacionais, né, que são, é, são aqueles que permitem maior cooperação entre os países, permitem maior contato entre as autoridades, resposta e incidente, e permitem também um outro aspecto importantíssimo. E eu pessoalmente fiquei muito feliz de ver que vai ter uma diretoria sendo criada, Agência Diretoria de Cibereducação, é, porque existe a percepção de que há um gap cada vez maior entre a, as atividades maliciosas e a capacidade de resposta, inclusive no nível cidadão, né? Como nós vimos hoje, aqui, a maioria dos ataques, eles acontecem ao nível individual, né, por uma capacidade, incapacidade pessoal de, é, cuidados, higiene cibernética, cuidado com anexos, cuidado com a necessidade de ter backup pessoal. Então, nós no Ministério também temos estados atentos a isso, e nós sempre ressaltamos a necessidade de cooperação internacional também no campo da educação cibernética, que nós vemos aí, que a criação da, da agência poderá também estabelecer mecanismos de cooperação que permitam uma maior cibereducação no Brasil, né? Então esses são os 2 aspectos que eu mencionarei aqui, tá? De novo, para ser curto. E dizer que o Ministério é, fez uma, um processo interno de consultas. Faremos chegar as nossas sugestões ao texto, e ficamos à disposição aí para discutir com, junto com o GSI esses aspectos mais relativos ao aspecto internacional estratégico da polícia, da política nacional de cibersegurança. Muito obrigado.

SR. MARCELO MALAGUTTI, MESTRE DE CERIMÔNIA - Nós é que agradecemos, Conselheiro Franklin. Temos no MRE um grande parceiro, um grande tradicional parceiro. Muito obrigado. Há um pedido na Doutora Patrícia Peck de uma inversão da pauta porque ela tem que se deslocar para o aeroporto, então nós vamos chamá-la para fazer a sua contribuição. A senhora tem 10 minutos.

SRª DOUTORA PATRÍCIA PECK - Bem. Bom dia a todos. Obrigada, Malagutti, pela gentileza da inversão da pauta. É, primeiramente queria agradecer o convite do Ministro que está aqui com todos. Eu já contribuo com o Estado Brasileiro na temática de cibersegurança há mais de 20 anos, então fico muito feliz de poder tratar dessa temática. É um tema extremamente importante, né, como foi dito, estratégico, emergencial, e a gente tá atrasado, né? O Brasil tá muito atrasado com essa pauta. Eu acho que é importante dar o tom emergencial sobre isso. A pauta de cybersegurança exige conhecimento e preparo técnico específico. Não é qualquer um que entende sobre esse tema. Acho que a gente tem muitas entidades brasileiras, excelentes profissionais que podem ler sobre regulamentação, podem fazer até provas de certificação, mas não são técnicos em cybersegurança. E aí, para isso, como é um tema transversal que alcance afeta todos os setores econômicos, realmente acredito que o melhor caminho é o que está sendo proposto pela política nacional, e é uma forma também de dar o indicativo não só para dentro do país mas para fora, dentro de um diálogo entre todos, né? O cidadão brasileiro está hoje por sua conta e risco. É assim que a gente vive. O Brasil vive uma crise de segurança digital, pelo menos desde 2018 para cá, e só piora. Ela não melhorou em nenhum momento. Em 2019 eu fui convidada pelo Departamento de Estado Norte-americano, o State Department, para representar o Brasil com 28 países em Washington, e o tema era como desenvolver um plano estratégico de 5 anos para tratar sobre como desenvolver uma economia digital, confiável, e segura, considerando 3 pilares, 5G, cloud, nuvem, e inteligência artificial. Voltei para casa deixando lá o plano. Cada um dos países contribuiu com o Estados Unidos. E o que nós fizemos de lá para cá? Quem foi aqui do Brasil depois que me consultou? Com quem eu pude colaborar como expert no assunto? Praticamente ninguém. Hoje estou no Conselho Nacional de Proteção de Dados Pessoais, muito feliz. À convite, na época, indicada. Agora vamos passar por recondição de mandato, por outras indicações, mas infelizmente a própria Autoridade Nacional de Proteção de Dados que foi criada, que é um exemplo, e agora queremos criar outra, é criada no papel mas depois tem dificuldade de autonomia administrativa e orçamentária. Então não adianta a gente ter um plano bonito no PowerPoint e depois não dá orçamento e não conseguir executar na prática, administrativamente falando. Ficar na teoria faz o Brasil virar piada internacional, e a gente tem que ter muito cuidado para não virar piada, né? Ano que vem, eu recebo de novo os 28 países, serei o host dos 28 países, para reatualizar o plano de mais 5 anos, 2024 a 2029. É esperado uma crise em 2029, quando vamos fazer 100 anos da crise de 1929. Essa crise esperada vai ser uma crise digital, uma crise de colapso de energia, de conectividade, de disponibilidade, e vai ser uma crise sanitária de uma nova pandemia. E o que o Brasil está pensando a respeito

disso? Vemos discussões aqui que vão de querer usar assinatura eletrônica com ICP ao invés de migrar direto para reconhecimento facial, cuja OMS, Organização Mundial da Saúde, indica como o melhor protocolo sanitário, inclusive para idoso. Então, a gente realmente precisa conseguir articular esse entendimento, porque em 2030 a gente tem a virada da IA, de superinteligência. Dito isso, né, com toda certeza, para alcançar tração e velocidade, que o Brasil está atrasado, é essencial ter uma Agência Nacional de Cybersegurança de verdade, assim como conseguir de fato viabilizar a Autoridade Nacional de Proteção de Dados, que tem que interagir, ser parceira das mãos e abraçar uma a outra, porque cybersegurança e proteção de dados andam de mãos dadas. Foi assim que a Europa fez quando criou o NIS, e depois o GDPR, senão a gente não dá o salto, né? Já vivemos cyberguerra, Ucrânia e Rússia, e isso alcançou quem não tava na guerra, isso alcançou qualquer país fora do limite com, de território do conflito. Então quando a gente pensa, né, a estratégia de segurança e defesa, 20 anos eu escrevi um artigo, foi publicado num grande jornal chamado Legítima Defesa Digital, que me conferiu poder colaborar com a Escola de Inteligência do Exército, com a Escola Superior de Guerra, com a BIM, com a Polícia Federal, e outras entidades, tudo baseado no artigo 25 do Código Penal que, afinal de contas, viabiliza a resposta à incidentes. Então, claro que privacidade e segurança estão juntas, e a gente não viabiliza a liberdade do indivíduo se não for uma sociedade livre e segura, livre e segura. Dito isso, com toda certeza, a gente tem que ter uma estrutura que possamos proteger de cyberameaças e de cybercrimes, por isso temos colaborado com Legislativo. O Senador Carlos Viana tá com uma proposta de projeto de lei, que já foi protocolado, para criminalizar o sequestro de dados, que é o ransomware. Então extrema importância, como nós estamos na convenção de Budapeste, atualizar o Código Penal e o Código Penal Militar, porque de nada adianta identificar as ameaças e não prender bandido e não reagir, porque senão ele ataca o próximo e ataca o próximo. E hoje nossos bens são digitais. Um patrimônio é digital. Reputação é digital. É muito bom ver uma política nacional escrita de uma forma a contribuir e encerrar lacunas normativas, mas precisamos sim cumprir e atender direitos humanos. Esse é meu papel de colaborar com o Estado Brasileiro desde sempre. Eu não sou de um governo, eu não sou de outro. Eu sou patrimônio intelectual do Brasil. Tô aqui para ajudar, e é assim que a gente deveria fazer para ver se o Brasil avança de verdade, né? Nós temos novos direitos digitais que precisam serviços, já estão na Constituição. Uma agência só funciona com autonomia, orçamento, equipe treinada, capacitação, e tecnologia. O que se não investir em ferramenta, se a gente ficar comprando tecnologia velha dos outros, a gente também não consegue combater bandido que já usa drone e que já usa bot, e já tem inteligência

artificial para atacar todo mundo. Então não adianta ter uma equipe que não sabe capturar evidências digitais e não sabe fazer uso dessas evidências depois para levar para o Judiciário e prender bandido, porque quando você prende um bandido digital, você tem que poder fazer cerceamento e cárcere digital, que o cárcere físico não segura um bandido digital de atacar os outros, atacando os celulares dessas pessoas em qualquer lugar do mundo. Então, a gente tem que avançar também na legislação de cumprimento de penas. Então é muito positivo ter um interlocutor único. É muito positivo em efeito internacional, tem um efeito de atrair mais investidores, um efeito de também subir no ranking da OIT, como aqui eu estava conversando com o Arthur Sabbat. Estamos muito juntos, né, Arthur? A ANPD e Conselho tem que tá junto, o Conselho tem que aconselhar a ANPD e vice-versa, não é verdade? Pena que a gente não tem tido muitas reuniões, né? Então a iniciativa tem que ser sincronizadas, a gente tem que ter uma base de dados única de conhecimento, inclusive para poder integrar com o setor privado, porque o setor privado gasta muito dinheiro com segurança privada, e a segurança privada e a segurança pública têm que tá integradas para otimizar esforços, porque a gente está cansado de desperdiçar dinheiro e o crime organizado continuar crescendo, e o cidadão brasileiro abandonado. Então tem alguma coisa errada. É ótimo ter acordos internacionais. Eu mesma comandei o GT2 na ANPD com o Conselho no ano passado de 2022, e a gente estabeleceu contato com mais de 12 países, 12 autoridades, para trabalhar protocolos de educação, para trazer campanha educativa para o Brasil. Só que, infelizmente, por falta de autonomia administrativa, não foi autorizada nenhuma viagem do Presidente da Autoridade Nacional de Proteção de Dados para ir lá assinar esses acordos. Então do que adianta você ser uma autarquia especial, você ser uma autoridade, e não poder fazer uma viagem internacional para assinar um acordo com outro país, com uma outra autoridade? De novo, o Brasil é uma piada. Então, a gente tem que poder olhar todo esse plano maravilhoso que o Malagutti acabou de apresentar e dizer, vamos fazer acontecer? Por que tem a ANPD há 3 anos acontecendo, mas que não conseguiu cumprir tudo isso, então a gente não pode repetir a mesma coisa, e temos que fazer para todos. Então sim, né, é extremamente importante colaborar, né? Ter essas equipes criadas. E aí ao final, é lógico, né, só comentando, a gente tem que alinhar segurança com proteção de dados. Por que? Eu colaborei na Copa da Confederação, na Copa do Mundo, na Copa das Olimpíadas. Na época a discussão era, como fazer a revista digital? Porque todos fazem revista digital nos outros países. É assim que eu descubro se tem ou não uma bomba no estádio. É assim que eu descubro se vai ter ou não um risco numa escola. É assim que eu protejo o protocolo de escola digital segura hoje. Então, eu tenho que usar drones, eu tenho que usar vídeo vigilância, eu tenho que ter o body cam na roupa do

policial, eu tenho que fazer placa na cidades avisando que tem vídeo vigilância, que tem uso de drones. E tudo isso é atendendo o artigo 4, 7, 11, e 23 da LGPD. Então o trabalho de cybersegurança é amarrado com o de proteção de dados. São metas ambiciosas, mas tem como fazer. Muito obrigada.

SR. MARCELO MALAGUTTI, MESTRE DE CERIMÔNIA - Muito obrigado, Doutora. Dando prosseguimento em nome do Ministério da Justiça e Segurança Pública, chamamos a Senhora Estela Aranha, que é assessora especial do gabinete do Ministro.

SRª ESTELA ARANHA - Bom. Bom dia a todos e todas aqui presentes. O Ministério da Justiça tem muitas contribuições nesse debate. Vamos entregar todas as contribuições também por, por escrito para o GSI, mas também a gente quer trazer algumas questões importantes relacionadas, inclusive, ao nosso trabalho e em relação ao trabalho de rede. É, obviamente não vou repetir aqui a relevância e a necessidade desse projeto. Isso é indiscutível. Isso, a necessidade de uma estratégia cybersegurança e a criação de órgãos e a criação do comitê, gerenciamento de crises, isso é indiscutível. Eu queria só trazer um pouco do, em relação à visão do Ministério da Justiça porque além da estratégia, né, de, isso é uma questão que não é somente nessa discussão no Brasil. Todos os países que você apresentou aqui, é, como os Estados Unidos, França, entre outros, eles todos têm uma política de estratégica cybersegurança, mas tem outras áreas de política cibernética que conversam, e muita institucionalidade. São várias instituições, e obviamente a política tem que ser coordenada, mas a execução dessa política, ela depende obviamente de muitos órgãos para poder se conseguir a execução delas. Então, e aí, trazer um pouco dessa discussão dessa interface, e é importante a gente pensar na interface desse sistema proposto com o que a gente já tem existente, inclusive por razões de competências, de atribuições legais ou constitucionais, né? Tem a questão da defesa de cibernética, que, a defesa das infraestruturas críticas, né, que tem tanto o Ministério da Defesa quanto o (Ininteligível) que trabalha, e como é que a gente vai fazer isso. A diplomacia cibernética, o colega do Ministério das Relações Exteriores falou hoje, a questão de segurança cibernética ela é central na geopolítica, ela é central na discussão de guerra e paz, né? Não tem nada mais central que isso. Então, é uma matéria de defesa, é uma matéria de relações exteriores. Inclusive na própria, também de, de relações comerciais, quando a gente está contratando insumos, a grande discussão europeia hoje, por exemplo, o 5G é justamente geopolítica de cyber, de segurança, né? E eu vou trazer um pouco do Ministério da Justiça, que a gente trabalha com segurança digital e combate ao cybercrime, que é uma área. Isso é, enfim, é muito, e vou trazer um pouco também, um colega da Polícia Federal vai falar também, mas eu vou falar aspectos diferentes. Nós

trabalhamos de forma muito coordenadas aqui, e conversei com o Otávio, e o colega vai também, o Otávio é o nosso diretor de cybercrimes lá na Polícia Federal, ele vai trazer um outro aspecto que eu vou trazer. Então essa é a importância, né, da necessidade de como fazer essa coordenação, essa ação, é, colaborativa entre isso, entre esses órgãos. E isso chamou atenção quando nós analisamos o projeto também, que a agência proposta ela tem um papel de regulação e um papel de execução de política. E seria bom também entender um pouco mais, porque eu acho que têm algumas questões de execução de política de cybersegurança que seria interessante, e competência de administração direta, inclusive, né, pela sensibilidade deste tema. Nos chamou pela leitura que nós fizemos, nós fizemos um foco importante na proteção de ativos dos serviços essenciais. No projeto não diz exatamente quais são os serviços essenciais. Acho que seria interessante até estressar isso de alguma forma, na legislação, definir isso. Mas e a outra questão também é a questão, é, que nos chamou atenção da necessidade de ter estruturas flexíveis, uma vez que essas ameaças, elas não são estáticas, elas são imprevisíveis e cada dia mais novas. Então, a questão do Comitê de Crise é uma questão importante, mas ele tem alguns requisitos que seria interessante ter essa abertura para essa imprevisibilidade dessas novas ameaças. Outro ponto super importante que a gente ressalta, que seria o papel central desse, desse novo órgão ou dessa nova instituição é a questão da autonomia. A Autonomia Nacional em relação a cybersegurança, liderar o desenvolvimento tecnológico nesta área e de toda a cadeia de suprimentos digitais. Hoje nós temos problemas de suprimentos digitais, inclusive quando colocou as dezenas de agências relacionadas por causa da infraestrutura, também temos a questão de recursos minerais envolvidos que são essenciais para segurança digital, né, e obviamente também esse desenvolvimento de suprimentos, não só de tecnologia mas como também de sumos básicos, e isso tem que estar central no nosso plano de questão cibernética. E enfim, e ter essa estrutura de modo de que essas novas ameaças que estão desenvolvendo muito rápido com novas tecnologias, até que é a questão que a Professora Patrícia, querida amiga, que a gente ia tomar um café, não conseguiu esses dias, mas vamos conversar aqui, é, traz da inteligência artificial a internet das coisas, cada dia mais na conectividade 5G, e obviamente nós já falou que é uma questão, inclusive, geopolítica na Europa. Uso intensivo de nuvens, inclusive do próprio Governo Federal, entre outras coisas, a dependência digital, né, de tudo e a saída disso, e também todos os potenciais impactos econômicos e sociais de falhas de segurança digitais que continuam aumentando, então é a importância de ter, é, isso. E eu queria trazer um pouco, né, no nosso trabalho do Ministério da Segurança Pública que, enfim, esse debate de cybersegurança, e eu estou chamando de segurança digital e combate a

cybercrime na nossa área, né, de competência e atribuição que é consticional ou legal. É primeiro ressaltar que as ameaças hoje, elas não se envolvem apenas ativos. Se você for ver os planos de cybersegurança nacional, inclusive dos Estados Unidos, da comunidade Europeia, dos países europeus, os principais questões inclusive não são envolvendo ativos, mas a questão de segurança digital. Então, e a gente está trabalhando lá no Ministério da Justiça, uma agenda de segurança digital, estamos, tem colega do MGI, do Ministério de Gestão que está aqui hoje, (Ininteligível) estamos trabalhando na estrutura da Secretaria de Direitos Digitais, justamente para essa agenda política de criar confiança sustentável na economia digital, né? Para apoiar a transformação digital da sociedade com integridade, ética, eficiência, conformidade com a lei, e essa redução dessas vulnerabilidades. E isso não são só aspectos técnicos que estão tratados aqui, mas aspectos econômicos e sociais que envolvem, né, esta segurança cibernética que, para além, obviamente da aplicação da Lei criminal que a gente vai falar aqui, dessa segurança que estamos falando. Então a gente está falando de interferência em processos políticos e democráticos, que isso é central na cybersegurança, muitas vezes com o objetivo da desestabilização. Isso também envolve o trabalho de segurança, nós temos um, desenvolvendo um trabalho integridade do ambiente online, um trabalho de integridade da informação em conjunto até com a Secretaria de Políticas Digitais da SECOM, que faz esse trabalho, e uma, um trabalho de integridade do ambiente online em geral que envolve, inclusive, cidadãos e consumos, né? Isso é muito importante, essas questões. Outras questões que são também importante é a defesa da propriedade intelectual nesse contexto, e as questões relacionadas a vigilância, que eu acho que é colocar aqui. Em relação à questões de cybercrimes e cybersegurança, o Valdemar Latance aqui da Polícia Federal vai falar também. Não vou entrar um pouco, mas a gente tem um papel muito importante da Polícia Judiciária, tanto na Polícia Federal, né? Que tem uma auditoria de cybercrimes, que tem uma área de repressão à fraudes bancárias, é uma área de repressão à pornografia infantil, entre os relacionados, e uma área é de repressão à crimes de alta tecnologia. Aqueelas são áreas plenamente operacionais com resultados, né, então, trabalhando bastante sobre isso e um pouco mais, né? É. A repressão de crimes de alta tecnologia, hoje ele é responsável pelo combate desses crimes de alta tecnologia, tanto pela coordenação quanto os levantamentos iniciais da investigação desses crimes cibernéticos, e subsequente também, eles produz relatórios de análise de crime de alta tecnologia, e identifiquem invasões, né, informáticas de bootnets, extorções digitais, ransomware, mineração clandestina, entre outras coisas. Temos a Base Nacional de Crimes Cibernéticos, que é super importante, projetos como Lunes Cyber Tools e o laboratório de análise de códigos

maliciosos, entre outras coisas, monitoramentos de malware bancário, entre outros ativos. Também o projeto (Ininteligível), também, que é o combate, Ação Coordenada de Combate à Ataques de Ransomware, também é uma atribuição da Polícia Federal. Fora da Polícia Federal, né, temos trabalho do Ministério da Justiça em relação à cooperação jurídica internacional e a internalização da convenção de Budapeste, a Estratégia Nacional de Combate à Corrupção que coordena a rede nacional de laboratório de tecnologia de lavagem de dinheiro, e o Brasil é autoridade, é, o Ministério da Justiça é autoridade central, né, internacional. E também temos o Cyber Lab na Secretaria Nacional de Segurança Pública, que na verdade é uma cor, ela funciona como apoio a todas as delegacias de cybercrime dentro das competências estaduais e faz ações coordenadas, às vezes, as ações nacionais e às vezes trabalhando em relação a isso. Então, só para contar um pouco, né, de outros aspectos relacionados à estratégia de cybersegurança relacionado ao Ministério da Justiça que é muito importante que a gente converse com todo esse projeto, e eu tenho certeza que, que vamos fazer isso. Obrigada.

SR. MARCELO MALAGUTTI, MESTRE DE CERIMÔNIA - Nós é que agradecemos. O Ministério da Justiça foi o segundo Ministério com qual nós conversamos, porque, por uma questão protocolar, o primeiro é a Casa Civil, é aquele que nos autoriza a iniciar o processo e conversar com os demais. E aí o Ministério da Justiça já é o segundo parceiro que teve acesso ao debate e vem nos ajudando. Dando segmento, chamo agora o meu, meu amigo Leonardo Rodrigo Ferreira, Diretor do Departamento de Privacidade e Segurança da Informação da Secretaria de Governo Digital, que vai falar em nome do Ministério da Gestão e Inovação em Serviços Públicos. Leonardo, 10 minutos.

SR. LEONARDO RODRIGO FERREIRA - Bom dia a todos e todas. É, bom dia, Malagutti. Obrigado pelo convite. Já cumprimentando aqui os colegas, né, os cidadãos, né, que nos acompanham de forma online. A ideia que ia trazer um pouco da, dessa visão, tentar usar bem esses 10 minutos aqui que foram disponibilizados para a gente. Primeiro dizer que, né, o Gabinete de Segurança Institucional, né, é um parceiro de longa data, assim como a NPB. Nós somos da Secretaria de Governo Digital do Ministério de Gestão e Inovação e Serviços Públicos, e é bem interessante, é, assim como a Estela gentilmente trouxe aqui, né, as informações sobre o Ministério da Justiça, nós temos uma, uma visão bastante Clara, assim como a Patrícia comentou aqui, a respeito da importância de se trabalhar as temáticas de proteção de dados pessoais em conjunto com as questões de segurança da informação, segurança cibernética. Isso é muito claro para gente, tá, no âmbito do governo digital. Mas quem é o governo digital? O que é o governo digital? Então acho que vale trazer algumas informações aqui, é, para, para fins de contextualização, tá, de todas as

senhoras e senhores, né? Hoje o governo digital, pessoal, é, nós chegamos à marca de 148 milhões de brasileiros que utilizam o nosso acesso gov. Esse único acesso, né, o gov.br nós temos, né, hoje já disponível mais de 4.200 serviços digitais. Então nós temos uma grande infraestrutura crítica, uma grande área prioritária, tá assim, a gente trata com GSI, né, olhamos para essa área de governo digital como a área prioritária, e entendemos que a proteção de dados pessoais em conjunto com as questões de segurança da informação são essenciais, tá, são habilitadores do processo de transformação digital do governo brasileiro. Então é bem interessante a gente fazer uma reflexão, né? O Malagutti trouxe aqui alguns dados. Hoje o Brasil é considerado o segundo país mais digitalizado do mundo, quando você pensa em termos de governo. Estamos atrás da Coreia, né, do Coreia do Sul como foi colocado, e nós avançamos muito nesse último período. Eu poderia trazer alguns fatores que contribuíram para esse avanço, né? A questão da pandemia, né, é um fator relevante, né. Precisamos, né, é fomos forçados, né, a fazer esse movimento para o digital, e a partir disso, né, é um movimento, uma grande reflexão, e nós da secretaria de governo digital temos uma visão bastante otimista, tá, em relação aos avanços, tá, é do governo brasileiro, aos avanços da sociedade brasileira de uma maneira geral. Nesses últimos quatro anos, né, eu vejo vários colegas passando por aqui realmente pontuando preocupações que são bastante relevantes são, são legítimas, né, são comprovados por meio de estatísticas nacionais e internacionais. Porém, nesses últimos quatro anos, nós tomamos uma decisão de sermos habilitadores, sermos, é, viabilizadores dessa transformação digital com ações concretas. Então hoje, tá, eu acho que é importante deixar isso registrado, tá, a Secretaria de Governo Digital conduz junto aos provedores desses 4.200 serviços digitais, como foram, como foi trazido aqui, tá, nós acabamos criando, tá, um programa, o Programa de Privacidade e Segurança da Informação, então trabalhamos conjuntamente a parte de proteção de dados pessoais e segurança da informação para um conjunto de 251 órgãos, tá, hoje do Governo Federal. Têm uns parceiros de primeira hora como Serpro e Dataprev, que são agências, né, que nos apoiam, né, são empresas que nos apoiam nessa tarefa, e hoje já temos diria que dados concretos, tá, que conversam muito pessoal com essa proposta de agência, né? Então eu acho que é muito importante a gente trazer dados concretos, tá, desses avanços nesse, nesse último período, tá, em relação ao nosso programa de privacidade de segurança da informação. Hoje, para vocês terem uma ideia, pessoal, é, nós temos um diagnóstico claro em relação ao nível de maturidade desses órgãos, é, conseguimos ter, é, uma visão clara dos avanços, foi falado que mais uma oportunidade a respeito, né? É, olhando sempre para um conjunto de disciplinas que entendemos ser habilitadores, que vemos refletidos em boa medida aqui nesse projeto de lei. Hoje olhamos para

as questões de governança, de maturidade, metodologia, a parte de tecnologia e pessoas com muita atenção, tá, em relação a essa necessidade de avanço. Então assim, é, desde o primeiro momento, né, fomos procurados pelo GSI. Já, já temos feito, né, várias conversas, tá, já tivemos algumas, já demos algumas boas contribuições, tá, em relação ao atual projeto. Acredito que saímos fortalecidos aqui dessa audiência com várias contribuições da sociedade brasileira, da academia, né, nesse dia de hoje. Dizer, é, Malagutti, que a Secretaria de Governo Digital permanece totalmente à disposição, tá, para continuar invidando esforços no aperfeiçoamento dessa proposta. Nos colocamos à disposição como um case, tá? Hoje, o Governo Digital existe um decreto pessoal, o decreto 11200, que fala do Plano das Infraestruturas Críticas, o Plansic. Hoje existe no Brasil, né, previsto nesse decreto 11200, 7 áreas prioritárias que são consideradas áreas prioritárias, né? Há uma discussão, tá, bem avançada já aqui na Presidência da República, para que o Governo Digital passe a ser considerado um oitava área prioritária, considerando esses números que eu acabei de trazer para vocês. Está muito próximo de se consolidar, e como tal ele precisa ser protegido, né? O Governo Digital precisa ser protegido, e olhamos para isso com muita atenção. Então, acredito que é um momento muito importante de coordenação, né, como ele trouxe como um primeiro pilar de coordenação mas também a necessidade de regulação quando olhamos para a LGPD a 13 709 de 2018, fica muito claro que é uma legislação que obriga, né, órgãos públicos e privados, estados e municípios, há uma envergadura, uma abrangência para todo o Brasil, então sentimos necessidade de termos uma legislação no mesmo patamar para a parte de segurança da informação. Então assim, faz todo sentido quando a gente discute aqui, né, essas questões que foram trazidas aqui pela Estela em relação à essa questão da persecução criminal, né, todas essas preocupações. E só mais a título de colaboração, é, e aí com a visão muito otimista, né, a Estela trouxe 3 áreas da Polícia Federal que têm uma atuação bastante presente nessa área de cybersegurança. Ela falou ali da, existe uma Diretoria de Crimes Organizados, uma diretoria que olha pra parte de cyber, para a área de cybersegurança, e também tem uma área bastante especializado que acaba fazendo todo um trabalho de inteligência voltada para a área de cybersegurança. E é muito comum, pessoal, em bases quinzenais, que a gente interaja com essas agências, né, assim como GSI, né, e outras mais. Então eu acho que é legal externar que existe do nosso lado, né, uma coordenação entre os órgãos de governo assim como o TCU, o CGU, estão todos, né, por vezes nos reunimos, né, e temos discutido essa proposta da agência. Então, queria agradecer mais uma vez da Marcelo, é, agradecer ao Ministro, tá, por essa oportunidade de ter sidos convidados para falar em nome da Secretaria de Governo Digital, do Governo Digital, e dizer que estamos abertos, tá, para

todos os presentes aqui para recebermos sugestões, críticas, né, observações que possam, que possamos, é, amadurecer o nosso processo. Muito obrigado, pessoal. Até mais.

SR. MARCELO MALAGUTTI, MESTRE DE CERIMÔNIA - Muito obrigado Leonardo. O Leonardo, particularmente, é uma pessoa muito atuante nessa área e é um grande parceiro nosso aqui também. E a Ministra Esther nos recebeu muito carinhosamente lá para debatermos a nossa proposta. Bom. O próximo a falar é o nosso querido amigo Arthur Pereira Sabbat, diretor da ANPD, uma agência irmã com a qual nós temos mantido sempre um relacionamento muito próximo. Sabbat, 10 minutos, por gentileza.

SR. ARTHUR PEREIRA SABBAT - Muito obrigado, Doutor Malagutti. Bom dia a todas, bom dia a todos. Bem. É um grande prazer, em nome da Autoridade Nacional de Proteção de Dados, participar da audiência pública, porque é um projeto que nos interessa sobremaneira. Mas antes de falar nessa parte do interesse da ANPD nesse projeto, vamos falar um pouco. Né, e é claro, sempre difícil falar depois de Patrícia Peck, Estela Aranha, né, Doutor Leonardo, né? Sempre com muita substância, né, e muito conteúdo. Mas o que é que acontece, né? Nós estudamos essa parte também há bastante tempo. Por que o Brasil, ele é, ele é um alvo tão promissor de ataque cibernético? Nós identificamos dentre as, os vários motivos, porque nos encontramos hoje nessa situação, 3 razões principais. Como foi citada, já foram citados aqui pelos que me antecederam, né. Primeiro, porque nós somos um país extremamente digitalizado. Nós fomos atrás de tecnologias, nós nos apropriamos de tecnologias, nós usamos as tecnologias, né, como se fosse aquela, né, aquele banquete em que nós comemos e nos lambuzamos e não nos prestamos atenção devida aos recursos de segurança necessários. Utilizamos, fizemos tudo, e para usar os melhores recursos tecnológicos, mas não nos preocupamos com a segurança que eles deveriam ter e nem com o conhecimento que nós deveríamos demonstrar. Segundo, em virtude do primeiro, temos uma cultura muito reduzida de cybersegurança. Essa, isso tudo tornou o país muito atrativo a cybercriminosos. E o terceiro e último, porque os nossos esforços em âmbito nacional, nossos esforços nacionais, setor público e setor privado em cybersegurança, eles são extremamente difusos, são extremamente fragmentados. Falta-nos uma articulação nacional, que é o que o PL se propõe a oferecer, e essa falta de articulação nacional faz com que aqueles que têm mais recursos se estruturem mais. Aqueles que têm menos recursos vão a culto, missa, oram para dar certo, né, porque, para não ser atacados. E isso tem, né, feito do país um país, um alvo preferencial, até porque os prejuízos não são somente financeiros. Quando nós vamos à vários eventos nacionais sobre segurança cibernética, é claro que o setor produtivo,

ele se preocupa muito com os prejuízos financeiros, se preocupa muito com a parte de reputação e imagem da organização. Isso é extremamente salutar e é correto. Agora, existem outros prejuízos que vêm à cavaleiro dos prejuízos financeiros, são os prejuízos à prestação de serviços públicos quando órgãos públicos são atacados, prejuízo à integridade, mencionado aqui pelo Doutor Malagutti também, integridade das infraestruturas críticas nacionais. Imaginem populações inteiras de certas regiões sem acesso a energia elétrica, sem acesso a água potável por conta de incidentes cibernéticos. São prejuízos à honra e à imagem das pessoas, prejuízos que temos visto de forma crescente a serviços de saúde hospitalares e laboratoriais. Tem furtado, tem feito com que várias, muitas pessoas têm, têm tido protocolos, prontuários, médicos comprometidos, vazados muitas vezes. E é claro que em todos os países, é importante dizer também, em todos os países onde essas iniciativas de, de governança em cybersegurança, então os países onde essas iniciativas deram certo, onde elas funcionaram, sempre. Eu às vezes não gosto de utilizar esses advérbios, sempre, nunca, jamais, tal, mas aí sempre. Sempre o Estado, ele foi o condutor das ações de articulação e quem avocou as principais responsabilidades por articular essas ações nesse sentido. E a Autoridade Nacional de Proteção de Dados é diretamente interessada nesse, nesse projeto de lei. O que é que acontece? Primeiro agradecer por termos sido mencionados tantas vezes no bojo do projeto, porque somos interessados mesmo. Dos 15 a 19 tipos de incidentes cibernéticos que causam mais prejuízo no país, pelo menos um pouco mais da metade envolve comprometimento, violação, vazamento de dados pessoais. E quem são os mais interessados, os maiores interessados na proteção de dados pessoais? Claro, além da ANPD, ANPD é um órgão. Mas quem é o mais interessado? Cada um aqui sentado e cada um que nos assiste. Nós cidadãos somos os mais interessados na proteção de dados pessoais porque somos os titulares desses dados, somos os donos desses dados, e beneficiários últimos de todas essas políticas de proteção de dados pessoais e de segurança cibernética. Somos nós. São nossos os dados que podem vazar, são os nossos dados que podem ser comprometidos, os dados dos nossos parentes, os nossos filhos, esposa e marido. Então, por isso a Autoridade Nacional de Proteção de Dados se coloca à disposição para corroborar com o projeto de lei, o qual já li três vezes, né, e gostei muito, Doutor Malagutti, permita-me dizer que eu gostei muito. Cremos ser essencial que uma agência nacional de cybersegurança se coloque, seja caminho, né, e seja implementada para, mas como nos moldes, aos moldes do que muito bem frisou a Doutora Patrícia Peck, né, que ela, que vamos implementá-la, mas que ela tenha condições para exercer as suas atribuições com correção e com eficácia. Então é isso que nós queremos. É, parabéns pela, pelo projeto de lei. Acredito que, torço para que ele vá à frente, e a ANPD então por fim se coloca

à disposição para corroborar no andamento dessas, dos debates e das discussões sobre o incremento, sobre a, o prosseguimento nas considerações para aprovação do projeto de lei em todas as suas instâncias. O ANPD se coloca à disposição e parabeniza a iniciativa. Muito obrigado.

SR. MARCELO MALAGUTTI, MESTRE DE CERIMÔNIA - Nós é que agradecemos, Sabbat. O Sabbat é conhecido por todo mundo que o conhece como um lorde, um gentleman. É a única pessoa que é capaz de chegar aqui publicamente e dizer que eu coloquei ele para ler um projeto de lei três vezes, e ainda me agradecer por isso. Chamamos agora para representar aqui o Senador Izalci Lucas, o Professor Paulo Barone. Grande tradição como professor, membro do Conselho Nacional de Educação por vários anos, e vai nos brindar aqui com algumas palavras.

SR. PROFESSOR PAULO BARONE - Muito obrigado, Marcelo. Bom dia a todas e todos. Eu gostaria apenas de mencionar que o Senador Izalci Lucas é um dos senadores que mais lida com as questões relacionadas à Ciência e Tecnologia e Inovação. Preside a frente parlamentar nesse tema e sempre apresenta muito interesse por todos os temas que possam se relacionar, não só com a eventual implementação de nova legislação como também contribui muito com o desempenho dos setor Executivo e das organizações da sociedade em torno dessas questões. Então ele me solicitou que comparecesse a essa audiência pública, que examinasse com cuidado a proposição da criação da agência do comitê e de toda a estrutura que teria a incumbência, de dar conta das questões que foram aqui apresentadas relacionadas aos incidentes cibernéticos e a segurança. E ele também se ocupa muito da questão do governo eletrônico. De fato já foi dito aqui, o governo eletrônico brasileiro é bastante presente, ocupa um espaço muito grande na vida brasileira, atende muito ao cidadãos, embora ainda tenha muitos, certamente muitos déficits, talvez um dos quais seja o Sistema de Acesso Unificado, o outro, a certa disjunção das informações, algumas são acessadas por um número do SUS, outras por um número que é o CPF, e coisas do gênero, né? Mas de todo jeito, a presença desta forte, eu diria, característica brasileira, e além disso o fato de que os serviços financeiros no Brasil também têm forte componente eletrônico há muito tempo, tá certo? E o Marcelo sabe, porque trabalhou nisso por bastante, muitos anos. Isso traz ao Brasil uma certa questão de fragilidade já também aqui mencionado. Para a questão Legislativa, é muito importante relacionar o aspecto que o Senador Izalci sempre menciona, que é, não basta discursar mas é preciso também acrescentar recursos a todo, a toda política pública. Não há estratégia que opere sem recursos alocados. Não adianta dialogar apenas. Todo mundo concorda. Ele falou até a respeito da questão do arcabouço fiscal nesses dias, aliás ontem até num evento a que eu compareci

também. O discurso é excelente. Todo mundo apoia a educação, mas na hora de verificar os recursos alocados para a Educação Básica, que é uma característica. aliás é uma política crítica para o Brasil, isso nem sempre funciona da mesma forma. Então é preciso também alocar recursos. Todos os, todas as medidas que forem nessa direção, propostas pelo Governo Federal e submetidos ao Congresso receberão do Senador Izalci a maior atenção, e, com a nossa colaboração, uma análise cuidadosa e um diálogo, uma interlocução cuidadosos que também são apontamentos dele sempre. Ele sempre exige que se dialogue com quem traz a proposição e com outros atores da sociedade que têm contribuições. E por essa razão então eu posso já me colocar à disposição para, a partir do momento em que essa proposta estiver tramitando no Congresso Nacional, a funcionar como interlocutor, como um polo de contato entre todos os cidadãos, todas as organizações da sociedade que têm interesse na questão, para aprimorar, para alongar a discussão, para ouvir outras posições se for o caso, porque um dos mecanismos importantes no Congresso Nacional é a audiência pública, e também para fazer chegar aos interlocutores proponentes do Governo Federal aquelas sugestões que eventualmente requeram maior negociação, porque eventualmente isso pode acontecer até no âmbito da criação de uma nova estrutura organizacional, como é o caso dessa agência reguladora. Então, são essas as exposições que o Senador sempre apresenta, e eu aqui reitero que ele agradece o convite a participação. Mais do que isso, ele se coloca à disposição pessoalmente, e eu aqui o representando em nome da assessoria, faço o mesmo. Muito obrigado. Eu desejo que a audiência seja um sucesso e que o projeto de lei seja aprimorado e chegue ao Congresso já muito mais polido do que certamente é o caso quando nós nos sentamos no grupo técnico, preparando, certamente com muita competência, mas com a possibilidade de ouvir outras vozes. Certamente uma questão tão ampla quanto essa ganha muito mais riqueza e pode se tornar uma ferramenta muito mais importante para proteger não só a soberania nacional em todos os aspectos, mas também a economia brasileira, que sofre muitos prejuízos aqui já apontados também, e a, eu diria assim, o curso da vida corrente das pessoas, que é muito prejudicado muito além das questões da natureza econômica por problemas de natureza já apontada por aqui. Então a atenção ao cidadão, não só como um cidadão de um país tem que ter soberania, de um sistema econômico tem que operar, mas também de tem que ter tranquilidade para o uso das suas, dos recursos tecnológicos das suas possibilidades de antes de uma economia inovadora, de uma sociedade inovadora de serviços públicos inovadores, mas com segurança, com tranquilidade de que isso não implicará para ele em ônus ao invés dos bônus que a tecnologia certamente oferece com muita propriedade. Muito obrigado. Excelente audiência a todos.

SR. MARCELO MALAGUTTI, MESTRE DE CERIMÔNIA - Muito obrigado, Professor Barone, ao senhor e ao Senador Izalci por suas palavras. Fomos brindados aqui com a visita do Senador Rogério Carvalho, que é membro da Comissão de Infraestrutura do Senado. Ele mudou a sua agenda para poder estar aqui presente, e vai fazer o uso da palavra agora. Senador, por gentileza.

SR. ROGÉRIO CARVALHO - Bom dia a todos, a todas. Eu sei que o General Amaro não está aqui, mas, no nome dele, quero cumprimentar a todos os funcionários de carreira, comissionados, todos os Ministérios aqui envolvidos, os representantes das entidades da sociedade civil. E, em nome da minha assessora Thalita, eu quero cumprimentar todas as mulheres aqui presentes. Primeiro, esse é um tema, é, se a gente. Eu sou de formação, eu sou médico, eu sou professor na Universidade Federal de Sergipe, professor da área de medicina da área de saúde pública, e a gente tem duas grandes tecnologias na saúde pública. Não é a clínica que a gente recebe o paciente, a gente recebe a pessoa, e tenta identificar o que é que tá por trás daquela necessidade que leva uma pessoa a um consultório. Então, a gente sabe que tem um problema, a pessoa sente que tem um problema, mas a gente vai atrás para chegar. Qual é a disfunção fisiológica? Qual é a dismorfia, a alteração morfológica? E localizar, e, se for possível, tratar, curar. Senão, a gente acompanhar esse paciente. A outra tecnologia é a da vigilância. A gente trabalha com vigilância epidemiológica, clínica, e sanitária, e não é algo algo simples ou menos relevante do que aquilo. Aliás, se a gente consegue viver 90 anos, se um paciente que descobre que é diabético aos 50 chega aos 85, é porque fazemos vigilância, é porque a gente acompanha este paciente a partir de uma agenda, de uma programação. Então todo mês a gente olha esse paciente e verifica a pressão, verifica os níveis de açúcar no sangue, e vê o estado geral desse paciente. Se tem uma feridinha, trata, trata no começo. Então, isso é vigilância. A gente vai fazendo o trabalho de vigilância e prevenção para que aquele paciente com diabetes, com hipertensão, às vezes cardiopata, que teria pouca perspectiva de vida, consiga sobreviver 20 anos, 15 anos a mais do que as patologias agregadas numa pessoa só não deixaria que ele vivesse. Isso é vigilância. E o mundo caminha para uma, uma total e absoluta digitalização. A inteligência artificial ela é uma questão que não é para daqui a 10 anos, não é para o próximo, o próximo século nem a revolução deste século. É a revolução desta década. O que aconteceu no mundo entre 2010 e hoje é algo sem precedentes na história. A política mudou, a forma de comunicação mudou, as pessoas não se reúnem mais por causa ou em torno de causa e sim em torno de afinidade. Isso gera uma lógica que não é mais, a gente não, não consegue conceber mais a democracia como a gente concebia. A gente tá vinculado e dependente de uma comunicação dirigida que gera uma infocracia. Outro,

outro momento, e foi decorrente de um processo, de um processo de uma revolução tecnológica que vem se dando ao longo dos últimos 30 anos. O mercado de capitais mudou, tudo mudou, a comunicação mudou, tudo mudou em função dessa revolução tecnológica que a captação, ela captura da inteligência transformada em tecnologias que operam o dia a dia. É inexorável. Toda operação do dia a dia estará capturada num pen drive, numa máquina, num servidor. Está em algum lugar. A vida da humanidade e o modo como ela vai se organizar, os serviços, como serão produzidos, todas as informações essenciais de segurança, estratégicas, de empresas e de governos, tudo isso tá capturado e estará dentro e guardado em algum lugar. Então nós estamos falando de algo que é fundamental. Como proteger, em última análise, a vida de todos os brasileiros e do Brasil, e no Brasil? De como proteger o nosso meio ambiente, e como proteger a nossa economia? De como proteger pessoas comuns na garantia dos seus direitos? Nós estamos falando de algo que é muito importante, e eu quero me colocar, algo que não vou entrar. Eu tive, recebi ontem à noite, a minha. Por isso que eu agradeço aqui a Thalita. Ela fez um resumo para mim de todas as etapas do cenário, do que o Reino Unido já fez, do que a União Europeia fez, do que os Estados Unidos já, já fez ou já fizeram. Eu não vou entrar no mérito do que a gente tem para fazer, mas o governo aponta a necessidade de conversar com a sociedade, abrir a importância deste tema numa audiência pública para dizer para todo mundo, nós todos, a sociedade inteira deve estar atenta a necessidade de termos uma regulamentação, e investimento, e acompanhar tudo que importa para nós. Porque a vida, ela está sendo conduzida, guardada, protegida, ou não, se a gente fizer esse monitoramento, essa, porque nós estamos falando de tudo o que envolve a gente, de tudo o que envolve as nossas vidas. Tudo, absolutamente tudo. Até o carro que você guia, do carro que você guia, a privacidade na sua casa, tem algum sistema que está monitorando. Não estamos falando de governo, mas nós estamos falando de tudo. Então, é, eu quero dizer para vocês que o nosso mandato está à disposição, e acho que quanto mais discussões nós fizemos e quanto mais pessoas passarem a defender a necessidade dessa, dessa regulamentação geral, dessa lei, ou desse marco, ou desse, seja lá o nome que dê a essa, a essa formulação de, de um regramento, de uma agência, de uma estrutura para poder gerenciar. Quanto mais a gente envolver as pessoas nisso, mais preciso será e mais eficiente ser, nós teremos, e mais eficácia no, na intenção de nos protegermos e de proteger a sociedade. Então, muito obrigado. Parabéns pela iniciativa, e vamos trabalhar porque a gente já tá atrasado. Obrigado.

SR. MARCELO MALAGUTTI, MESTRE DE CERIMÔNIA – Eu, eu não sei se eu agradeço ao Senador, porque ele me deixou apavorado agora. Tô com

calafrios aqui na espinha por causa do tamanho da responsabilidade. Bom. Seguindo a nossa programação, então, eu chamo agora o Senhor Carlos Manoel Baigorri, Presidente da Anatel. Professor, Doutor Baigorri? Bom. Passemos então para o próximo, que será o Doutor Carlos Renato Araújo Braga, diretor da secretaria, o Diretor na Secretaria de Fiscalização e Tecnologia da Informação do Tribunal de Contas da União.

SR. DOUTOR CARLOS RENATO ARAÚJO BRAGA - Muito bom dia a todos. O Tribunal de Contas da União vem a essa audiência pública num chamado do, do Gabine de Segurança Institucional, trazer informações para, aproveitando a transmissão pela internet, esclarecer a sociedade brasileira a importância e o quanto esse tema afeta a todos e a cada um de nós, né, e oferecer um caminho que pode ajudar o governo a aperfeiçoar esse projeto de lei, né? Nós iniciamos com essa fala de que o problema da segurança, reforçando várias falas que vieram antes, né, de que segurança na informação e segurança, e cybersegurança é um problema para ontem, né, no Brasil e no mundo. O Tribunal de Contas da União já vem se debruçando sobre esse tema há algum tempo, então alguns podem estranhar. O que é que o TCU tá falando, tá fazendo numa audiência sobre cybersegurança quando tradicionalmente se fala muito sobre contratos, execução de despesa. Esse é um tema que tá na pauta do TCU, contribuir para a melhoria de todas as políticas públicas. Desde 2020, já existe uma estratégia que está sendo ela, evoluída agora nesse momento, tá, para tratar desse tema, e desde 2020, já foi colocado aqui no início da apresentação de GSI, o TCU apontou esse problema como um problema de alto risco para o país. A lista de alto risco do TCU, ela envolve temas ou problemas que abarcam o montante acima de 1 bilhão de reais. Somente um caso citado aqui pelo Doutor Marcelo atingiu essa cifra ou afeta a vida de mais de um milhão de brasileiros. Como o Doutor Leonardo comentou, cerca de 150 milhões de brasileiros hoje já acessam serviços do Governo Federal, então com certeza esse é um problema que tem que estar na agenda do Estado Brasileiro, né? E atenta a essa, a essa preocupação, o TCU esse ano reformulou a sua estratégia. Na verdade, a atuação em tecnologia da informação já ocorre desde 2006, mas esse ano foi criado uma subunidade específica para tratar desse assunto, né? Uma diretoria específica para avaliar segurança da informação. Bom. Nós vamos falar sobre o que? Sobre o fato de que proteção cibernética ocorre de maneira coletiva e não de maneira individual, e para isso nós temos que ter um articulador, e o articulador tá sendo apresentado nesse projeto de lei que está em discussão hoje aqui. Existem duas oportunidades de melhoria que nós vemos. Nós vamos mostrar o processo pelo qual isso pode ocorrer nesse projeto de lei, e vamos também alertar, fazer um alerta com respeito à multiplicidade de reguladores sobre o mesmo tema, que isso deve

ser um assunto a ser analisado. Bom. Primeiro, eu me servi aqui numa apresentação PowerPoint diferente dos demais, dos que me precederam, para poder trazer à sociedade brasileira uma materialização do que é que é um ataque cibernético, né? A gente fala isso, e isso tá tudo no mundo dos bits, bytes, rolando pelas redes, e a gente não entende o que é que é. Então, nós vamos falar um pouquinho, como é que isso acontece para ver como isso chega na vida de cada um, e para isso eu vou me servir de um exemplo simples. Não é para apresentar isso para os senhores especialistas estão nesse auditório, mas para a sociedade brasileira entender o que é que é um ataque de ransomware, né? E aí entender que esse ataque pode estar saindo do seu celular, pode estar começando pelo seu celular que tá entrando numa rede do Governo na qual tem uma empresa de exportação conectada num determinado sistema, e tem um escritório de contabilidade ligado nessa empresa de importação, né? Então um ataque de ransomware, ele começa com o atacante. E aí a gente tá falando de guerra mesmo, né? Atacante, alguém que vai te invadir. E ele entra por alguma porta alguma, uma porta, por exemplo, que está mais à direita é a do phising, é a do e-mail malicioso. Aquela que a gente, nós, por falta de educação em segurança digital, como já foi mencionado antes, que nós temos baixa maturidade em educação digital, nós clicamos naquele link do e-mail malicioso. E a partir daí, o atacante ganha o que é chamado de foothold, ele ganha um ponto inicial de entrada. Ele entra lá na minha máquina do TCU, se fui eu que cliquei no e-mail, e a partir daí ele começa a fazer uma coisa que as pessoas ficam assustadas, ele começa a andar. Ele começa a andar dentro da rede do TCU, pulando de máquina em máquina se ele invadiu a minha máquina. E, se a minha máquina se conecta nos serviços do governo lá no portal gov, ele pode pular para dentro do portal gov, e se o seu celular estiver conectado lá no portal gov, ele pode pular no seu celular. Ele pode pular para outra empresa que tá pegando o serviço lá no governo, ele pode pular para a prefeitura que tá conectada no sistema do Ministério da Saúde. Esse movimento lateral, ele acontece dentro da organização e fora. Por isso é que ele afeta a vida de todos nós brasileiros, de toda a sociedade brasileira. Por isso é que isso não é um problema do governo, isso é um problema do Estado que tem que ser resolvido de maneira coletiva. E a partir ele procura achar uma conta mais privilegiada, ele procura ter aquele acesso em que ele pode fazer as coisas que ele veio para fazer, destruir criptografar os dados e depois pedir um resgate em Bitcoin, ou simplesmente pegar esses dados e vazar esses dados, como o representante da ANPD falou, os dados pessoais, os dados que têm a nossa vida. Como o Senador mencionou, os dados que trazem a nossa situação de saúde e que eventualmente pode nos expor aí até a riscos à vida, né? Isso é um ataque de ransomware, isso é o que acontece no mundo digital. É contra isso que nós

temos, nós do Estado brasileiro temos que nos proteger, tá? E a defesa nesse momento, ela é feita o que é chamada em camadas. Cada setinha dessa tem que ser bloqueada, então portanto, em cada lugar há um, por onde eu mencionei que os atacantes estão andando, a gente tem que tentar bloquear. Por isso é que tem que haver uma ação de defesa de todos nós em cada celular, em cada empresa, em cada órgão público. Mas essa defesa tem que ser feita de forma coordenada, e a gente já vai falar sobre isso, né? Esse risco ele vai tender a aumentar, porque cada vez mais a gente vai estar interconectado. Uma das, eu falei da porta de entrada do e-mail malicioso, mas tem uma outra porta de entrada que é pelo parceiro, aquele com quem eu me relaciono. E cada vez mais a gente está se relacionando uns com os outros. Negócios com negócios, B2B, Business to Business. Negócios interconectados, B2C. Negócios com clientes, G2C, governo com cidadãos. Todos que confiam uns nos outros no mundo digital, uns vão podendo passar a ser o canal de passagem dos atacantes de um lado para o outro. E isso é inevitável, porque nós queremos transformação digital, nós queremos conexão digital. Nós brasileiros não queremos nós voltar para as filas para sermos atendidos pelas empresas ou pelo governo. A gente quer, cada vez mais, fazer as coisas daqui do nosso celular, então isso é necessário para que o nosso país avance, a cada vez acelere, na verdade, né? Nós já somos o segundo maior e podemos ser o primeiro maior na transformação digital. A gente precisa ter um ambiente de confiança, um ambiente seguro para poder confiar nessas transações. Bom. O que é que o Tribunal de Contas da União já se debruçou e já falou? Sobre a questão da fragmentação da atuação do setor público Federal nesse tema, né? Então, são demonstrados ali alguns normativos, já foi mencionado pelo Doutor Marcelo antes. Algumas iniciativas do Poder Executivo Federal limitadas ao Poder Executivo Federal. Iniciativas do Poder Judiciário limitadas ao Poder Judiciário. Mas na fala anterior minha, eu disse que o problema é de todos nós. Nós temos que ter algo que pegue todos os setores, todos os órgãos públicos de todos os poderes, de todas as esferas, setor público, privado, pessoas jurídicas, e pessoas físicas. Então a gente precisa ter alguém para liderar esse processo no país inteiro, que, na proposta que está sendo colocada, seria aquele comitê e aquela agência, aquela autoridade que tá sendo proposta. Bom. Oportunidades para aperfeiçoar o projeto de lei. O TCU não se debruçou sobre esse tema de avaliação dessa política, né? Existe um processo. Nós como órgãos de controle externo temos um processo de, de avaliação e de validação, de avaliação, melhor dizendo, das políticas públicas, e isso não se desenvolve enquanto a política está sendo gestionada. Não é competência do TCU fazer isso. Mas a gente não pode se furtar a fazer a nossa contribuição. Uma maneira da gente contribuir é mostrar como nós auditaríamos, aliás, melhor, como nós avaliaríamos. Não. Como nós vamos avaliar quando a

política estiver implementada. Na verdade, aquelas, aqueles normativos, aquelas políticas que foram colocadas antes, elas seriam um objeto de avaliação nossa no futuro bem próximo, né? E com essa mudança, e essa avaliação vai ser adiada, e o que é utilizado para ver se uma política pública tá boa ou não, o que é que ela pode melhorar, é um referencial de avaliação de políticas que está publicado no site do Tribunal de Contas da União. Então, uma oportunidade é que o gesta, os elaboradores dessas políticas, de antemão já façam uma autoauditoria nessa política com base nesse próprio guia, né? Esse guia tem um modelo. Esses, esses grupos que estão assinalados são os grupos que se aplicam no estágio atual da política, no estágio de concepção, e já está prevista alguns elementos na implementação que diz respeito à estrutura de governança. Então existem umas tabelas, eu vou dar aqui alguns exemplos, né, inicialmente de coisas que já foram apontados. O que é que é que se descobre passando esse checklist numa política, né? A falta de, clara de objetivos, a definição de indicadores de metas, se existe um modelo lógico para atuação disso, se as estruturas de governança e de gestão estão adequadas. Então, esses são resultados de uma outra política que foi avaliada, a Estratégia de Inteligência Artificial. Então, passando esse checklist nessa proposta de, de política, é possível que o próprio formulador da política consiga identificar a oportunidade de melhoria. E são coisas como essas que estão projetadas aqui agora, que eu vou passar de maneira mais breve, mas esses slides podem ficar disponíveis depois, são as perguntas. Os stakeholders foram identificados, né? Os objetivos estão claros? Como que eu vou acompanhar isso? Como é que eu vou acompanhar se essa política tá dando certo ou não? Isso tá previsto ali dentro? E todos esses elementos são elementos que vão ser fatores críticos de sucesso para essa política dar certo. Existem aqui dentro também aspectos orçamentários, como já foi mencionado antes. Então é o cuidado de se construir algo que vai sair do papel e vai dar certo se tiver esses elementos. E esse modelo é calcado aqui, é o TCU que diz isso, existe um conjunto de fundamentações que estão nesse documento vindos da academia, de modelos de outros países. É uma construção de, de vários pontos de vistas que sinalizam o que é que faz uma política pública dar certo. Uma segunda oportunidade de melhoria que nós vemos é uma discussão, que já foi mencionada aqui, que deve ocorrer. É a criação de uma estrutura nova, né? E existem várias, é, possibilidades de se criar essa estrutura regulatória, vários modelos jurídicos para ela dentro de uma estrutura da administração direta, como uma autarquia simples, como uma autarquia especial, e talvez algum outro modelo que se encaixe dentro do nosso ordenamento jurídico, tá? E uma sugestão tem a ver com o nosso mindset de auditor. Auditor pensa muito assim, se a gente tem que tomar uma decisão, a gente tem que botar no papel uma tabelinha dizendo o que é que dá bom de um lado, o que é que dá bom

do outro, o que é que dá ruim de um lado o, que é que dá ruim do outro. E aí, com base de, numa tabela dessa, objetiva, fica mais fácil de formar convencimento daqueles que têm que tomar a decisão, né? Então essa seria uma outra sugestão da nossa parte. E, por fim, um alerta com respeito à possibilidade de ocorrer fragmentação, duplicidade, e sobreposição devido à multiplicidade de, de agente reguladores, né? Fragmentação, duplicidade, e sobreposição são coisas que acontecem nas políticas públicas com relativa frequência, e isso não necessariamente é uma coisa ruim, né? Então, por vezes a gente tem coisas acontecendo, deixando espaços vazios. Hoje, por exemplo, nós temos isso. Aquelas políticas, elas não tratam de nada do setor privado, então, nitidamente, nós temos uma lacuna a ser preenchida, e há uma certa sobreposição também entre a política que trata de infraestrutura crítica e a atual política que trata de segurança da informação. Isso já foi, inclusive, mostrado ali pelo GSI na apresentação inicial. Então, isso é um alerta. Não quer dizer que isso seja necessariamente ruim, mas hoje nós temos agências que tangenciam o tema de segurança da informação e cibersegurança. A ANPD, a Anatel trata desse assunto, no que diz respeito à regulação da, do sistema de telecomunicações, outras agências reguladoras. Nós temos aí a proposta da criação de uma nova agência para cybersegurança. Existe no Congresso Nacional um projeto para regulamentação da IA, e lá também se prevê uma nova, a criação de uma nova agência. Então há que se ter um cuidado de ver como que essas agências vão trabalhar em coordenação, como foi falado antes, para que a gente não tenha regulações brigando entre si ou falta de regulação. E com isso, aqueles que estão necessitando das orientações são os agentes dessas empresas, as pessoas precisam implementar as medidas de segurança, elas saibam para onde ir e tenham uma orientação única, OK? Então, aqui, um breve cenário do que nós, uma conclusão do que nós falamos, e com isso nós agradecemos a oportunidade de poder contribuir nessa audiência pública. Muito obrigado.

SR. MARCELO MALAGUTTI, MESTRE DE CERIMÔNIA - Muito obrigado ao Carlos Renato. Para vocês terem uma ideia, quando nós vamos escrever uma política pública, existe um guia do, da Casa Civil, mais ou menos umas 230 páginas, que diz assim. Pensem nisso ex-ante, né, antes de começar. Depois tem o outro guia que o Carlos Renato mencionou aqui, que é o ex-post, como eles avaliam. E quando ele fala assim, ah, umas tabelinhas. Bom. Tem uma planilha Excel com umas 42 abas, mais ou menos, pra gente avaliar todos os itens e checar isso tudo. Bom. Boa parte desse trabalho nós já fizemos antes de colocar para a consulta dos senhores aqui, exatamente para evitar essas lacunas, esses gaps, e esses problemas que o Carlos Renato mencionou também. Bom. Dando prosseguimento, nós temos agora o Professor Humberto

Luiz Ribeiro, representando aqui o Departamento de Segurança da Federação das Indústrias do Estado de São Paulo.

SR. PROFESSOR HUMBERTO LUIZ RIBEIRO - Inicialmente, bom dia a todas, a todos. Agradecer a gentileza do convite para nossa manifestação nessa audiência pública. É, verificar que o trabalho também foi muito facilitado pela riqueza dos que me precederam nessa apresentação. Acho que podemos, vários dos temas já foram abordados aqui do nosso interesse. Mas, em primeiro lugar saudar a Presidência da República através do Gabinete de Segurança Institucional pelo endereçamento do tema tão crítico para nossa sociedade. Acho que, inclusive, converge com outros esforços e manifestações que vêm acontecendo, a exemplo do mês passado agora, recente, no Senado Federal na Comissão de Infraestrutura, que por coincidência colocou hoje nessa seção 3 senadores representando essa mesma Comissão de Infraestruturas Críticas, né, endereçando o tema, naquele momento liderado pelo Senador Veneziano Vital do Rego. Uma sessão também bastante rica que aconteceu, e a gente enquanto sociedade civil organizada, já há um primeiro, um primeiro ponto a ser destacado. A convergência entre o Poder Executivo e Legislativo fica claro para nós em relação ao que foi o manifesto aqui, já anteriormente, a essencialidade do tema que nós estamos tratando. Eu sou empresário do setor de cybersegurança, professor no ecossistema da Universidade de Brasília através do Cyberlab, e membro diretor no DESEG da Fiesp. Sobre esse assunto, e também com oportunidade de participações internacionais, né, principalmente através da Universidade Cornell, onde também leciono, ou pesquisador visitante. E trago um ponto preliminar, a consideração sobre quem é o nosso aniversário. Quem são os criminosos? E às vezes há uma visão meio utópica e romântica, e aí, falo isso aqui com muita desenvoltura porque eu trato, e fico muito feliz, inclusive, pela liderança do tema por um profissional do gabarito do Professor Malagutti, que também enfrenta o tema cybersegurança há décadas aqui no ambiente do Distrito Federal e do Brasil, e sabe o que está fazendo. Professor Malagutti, ele reúne as atribuições e as capacidades de uma pessoa que tem vivência no poder público, no setor privado, e também na academia, Então fico muito satisfeito por isso, e juntos sabemos, e acho que, também, a maioria dos senhores, mas para aqueles que estão até online querendo se aculturar um pouco mais, não é mais aquela visão utópica e romântica de, às vezes, um jovem com um computador à frente e que por uma, uma súbita oportunidade consegue invadir o sistemas da NASA, como já aconteceu em casos reais, em filmes, inclusive, retratando, hollywoodianos. Hoje o nosso enfrentamento são organizações criminosas pervasivas globais, artroses, e com um ponto fundamental na grande maioria das vezes. E aí é um desafio, eu vejo aqui,

saúdo os órgãos de segurança pública e de investigação, são discretos. Várias das instituições, eu torço para que nenhuma delas aqui do nosso país, mas várias das instituições globais estão hoje convivendo com o adversário dentro de casa. Há um fato acontecendo globalmente, que é o, a relação Ucrânia e Rússia. Eu acho que os ucranianos hoje estão sofrendo bem o que é a situação de enfrentar o inimigo quando ele está dentro da sua casa. É muito diferente de você enfrentá-lo enquanto ele ainda está no ambiente externo, fora da superfície de ataque que o Professor Malagutti colocou, que o Brasil tem a segunda maior do planeta. Quando ele está fora, eu estou ainda em modo preventivo. Quando ele está dentro, a situação já é outra, a situação de crise, certo? Então nesse ponto, sabendo quem são os adversários, acho que já ilustra que um primeiro ponto, é, de saudação a essa nova proposta que foi colocada, Doutor Malagutti, que é a, uma abordagem não só de combate mas uma abordagem de prevenção ao incidente cibernético. Um outro ponto para nós, muito caro no âmbito da Fiesp, de todo o sistema indústria do Brasil e do setor produtivo como um todo, porque, como muito bem colocado pelo Doutor Renato Braga, estamos tratando um tema que é sistêmico. O governo, setor privado, academia. Nós vivemos no dia a dia das cadeias produtivas num efeito dominó. Se afeta um, a corrente se rompe no elo mais fraco. Todos nós seremos afetados, certo? Mas nesse aspecto, nós convivemos com outros desafios no setor produtivo que é o da neo-industrialização, um deles, é o da neo-industrialização. Precisamos competir na fabricação, na entrega, na produção de serviços, com concorrentes internacionais que, por vezes, têm condições vantajosas, sejam tributárias ou por alguma questão de vocação natural de alguma região, têm condições competitivas bastante agressivas, capacidades elevadas. E a indústria brasileira precisa fazer frente a isso nesse momento de neo-industrialização global. E, nesse momento, a neo-industrialização pressupõe, obviamente, ou a chamada Indústria 40, 4.0 por alguns, pressupõe obviamente a digitalização e obviamente cybersegurança para que a digitalização possa florescer. Então, para nós na indústria, não é um tema sendo tratado especificamente por uma vertical industrial brasileira dos fornecedores de cybersegurança. Não. Ela é cara à todo o setor produtivo nacional. Então, é sobre esse aspecto que trazemos as nossas preocupações, né? Aplaudimos, portanto, o propósito crítico e complexo, o propósito que vem em discussão. Essa sessão, obviamente de nossa parte da Fiesp, aqui, é ainda uma contribuição não-exaustiva, obviamente, preliminar por parte da nossa Federação. Temos todo o entusiasmo e o desejo de engajamento para os próximos passos, Doutor Malagutti, nas ações que vão se suceder a essa sessão, né? Mas apontamos aqui então alguns pontos ainda relevantes. O primeiro é que prevenção no nosso mundo cybersegurança, olhando modelos de maturidade não apenas de tecnologia da informação. Eu falo aqui como

engenheiro que vive de tecnologia da informação no setor privado desde 1995, mas não estamos tratando temas de tecnologia apenas. A tecnologia é apenas uma das pedras fundamentais. Estamos tratando aqui de governança, de resiliência institucional, então, capacidade de gestão vai ser fundamental nos nossos próximos passos de enfrentamento. E para isso, o condão da prevenção já se retrata hoje na literatura acadêmica. Originalmente, lá no MIT, em Boston, produzido, inclusive foi retratado pelo Doutor Malagutti, um dos rankings que o Brasil figurou ali, o 18º lugar do Brasil naquele ranking que foi mostrado em cybersegurança não é 18º entre todos os países, é 18º entre 20 países que são as 20 maiores economias do mundo. Então isso reforça essa relevância que o GSI tem trazido para o tema, Doutor Malagutti. Estamos na capacidade chamada preparedness, que é o tema arco daquele ranking, traduzido de forma ainda livre aqui no Brasil por nós e pelos professores da Fundação Dom Cabral como prontidão cibernética, em 18º entre as 20 maiores economias do mundo, certo? Então, não é apenas prevenção. Existem métricas e métodos para se fazer prontidão. E nesse ponto, reforçar que, através, principalmente, do instrumento de inspeção que eu vi colocado na proposta, o tema prontidão começa a ser abordado pelo, pelo Governo Federal, certo? Então, melhor do que investigação forense, e não que um elimine o outro. A investigação forense, ela é necessária quando o leite já derramou. Mas melhor do que investigar é prevenir através da inspeção, por exemplo. Outros métodos também poderiam ser eventualmente abraçados. Outro ponto que notamos importante aí, fazendo aqui mais uma vez comparativos com modelos de referência internacional, é o tratamento do, do termo negligência ou descaso. Hoje, nós do setor de cybersegurança carecemos na interlocução de governança, carecemos de que o gestor público do outro lado entenda o nível de prioridade que tem que se colocar para esse assunto. E por várias vezes, é a situação como o Senador Rogério Carvalho colocou, por ser médico, ele falou inclusive da vigilância, que é uma abordagem. Ao invés do paciente já entrar infartado no hospital e o médico ter que endereçar um problema super crítico, é melhor que se faça um acompanhamento do nível de colesterol ou do nível, é, de atividade física do paciente, assim por diante. Ou seja, nesse aspecto, o gestor precisa ter o nível de consciência para não ser negligente com o tema. E, eventualmente, temos que discutir que nível de responsabilização temos que ter no arcabouço brasileiro para aqueles que foram negligentes de forma voluntária, proativamente negligente, se é o caso. Outro ponto também, o das métricas. Acho que também o Doutor Braga trouxe uma referência do Ministro Vital do Rêgo, um acórdão importante, que já trouxe uma referência balizadora internacional que é o CIS, CIS7 e CIS8, né, para a métrica, para que o gestor público use como balizador. Existem outros também importantes, dependendo de, do perfil operacional de cada instituição que podem ser adotados, né, mas

o uso das chamadas CVSS, Common Vulnerability Scoring Systems, isso facilita muito o dia a dia e relação entre fornecedores e os usuários do serviço de prontidão cibernética. E, por último, ressaltar aqui, por óbvio, o nível de, de consciência situacional que precisamos ter da sociedade como um todo sobre esse tema, e para isso aplaudir a referência. E eu vi uma área, uma diretoria se eu não me engano, voltada à educação. Nós, inclusive aqui vejo a presença aqui do Professor Rildo, nosso coordenador do SIGOD, Laboratório de Pesquisa Cibernética da Universidade de Brasília, nós aqui temos um papel inclusive de relação em vários níveis de formação. Seja adestramento técnico, seja consciência gerencial, ou seja treinamento específico por áreas, nós temos várias oportunidades para levar até mesmo o nível de consciência da juventude brasileira. Começar lá na escola, talvez de segundo grau, até de primeiro grau, em alguns países já tem acontecido, para que a gente possa prosseguir nessa linha. Portanto, Doutor Malagutti, são alguns temas que trazemos. É uma visão preliminar ainda por parte do nosso grupo da Fiesta. Queremos prosseguir nessa discussão. Entendemos que a sessão de hoje aqui é um marco, mas, mais do que isso, é o início de um caminho para que possamos trilhar juntos, o caminho da prevenção cibernética no nosso Brasil. Muito obrigado a todos. Parabéns a todos.

SR. MARCELO MALAGUTTI, MESTRE DE CERIMÔNIA - Muito obrigado, Humberto. Seguindo aqui temos agora o Professor Luca Belli, representando a Fundação Getúlio Vargas. Professor, 10 minutos, por gentileza. O Humberto passou um pouquinho. Eu vou repreendê-lo depois.

SR. PROFESSOR LUCA BELLI - Bom dia, bom dia. Então, primeiramente queria destacar a grande honra e prazer em ficar aqui com vocês hoje, e a imensa honra de ver o nosso trabalho citado logo no início da apresentação do Doutor Malagutti como uma referência e uma evidência da urgência que o Brasil está enfrentado nesse momento. O trabalho que desenvolvemos na FGV nos últimos anos sobre a cibersegurança, mas mais globalmente, de análise de políticas digitais no âmbito do Centro de Tecnologia da Sociedade, que eu coordeno na FGV do Rio, e também no âmbito de um projeto dedicado que se chama CyberBRICS, que analisa as políticas digitais dos países do bloco BRICS, Brasil, Rússia, Índia, China, África do Sul, justamente porque achamos que isto é muito importante olhar a Europa, os Estados Unidos como fontes de é, sabedoria e progresso. Mas, nessas áreas digitais, é extremamente importante também olhar para outros modelos, justamente pela sofisticação que eles alcançaram os últimos 10 anos, sobretudo China, Rússia. O nosso estudo que foi citado na apresentação do Doutor Malagutti, que se chama Cibersegurança: Uma Visão Sistêmica Rumo a Uma Proposta de Marco Regulatório Para Um Brasil Digitalmente Soberano, é acessível em acesso livre no site, a proposta

da (Ininteligível) ciber à luz desse estudo da nossa pesquisa nos últimos anos. Primeiramente, contextualizamos a complexidade da cibersegurança. Esse é um ponto essencial. A cibersegurança não é simplesmente segurança da informação, não é simplesmente segurança da estrutura, não é simplesmente cibercrime, não é simplesmente cibersegurança das infraestruturas democráticas. É conjunto de todos esses layers, dessas camadas. Então, essencial não somente uma cooperação internacional. Geralmente os ataques chegam do estrangeiro, ou claramente o, as atacante não perpetra o ataque do seu próprio computador, mas, como foi destacado antes, tem uma invasão prévia tipicamente de servidores ou computadores em outras regiões de (Ininteligível) para depois perpetrar o ataque por meio desses computadores invadidos. Então, é essencial de um lado a cooperação internacional, a recente adoção pelo Brasil da convenção de Budapeste do Conselho da Europa, meu antigo empregador é essencial para facilitar essa cooperação internacional, mas essencial é também a compreensão multisectorial. A ideia de criar um comitê de cibersegurança, que também tá no nosso estudo, é essencial. É realmente essencial para facilitar essa cooperação, não somente entres os poderes públicos, mas o setor privado. Quem tem as mãos na massa na cibersegurança há décadas, e academia, os pesquisadores que estudam nesse fenômenos desenvolvem soluções, até para trocar boas práticas. Um ponto que destacamos também no nosso estudo, o diagnóstico técnico e jurídico, ou seja, quais são as vulnerabilidades mais comuns? Mas também quais são as normas que são, que existem em termos de boas práticas e que já foram adotadas no Brasil. O Brasil conseguiu avançar enormemente nos últimos 3 anos por causa, justamente, da adoção de várias regulamentações setoriais. Eu acho que tá no 18, no lugar 18º no ranking das 20 economias, mas também, por coincidência, no ranking da UIT, do Cybersecurity Index da União Internacional de Comunicações. Ele subiu de 50 posições. Então, houve um avanço enorme nos últimos anos por causa dessa consciência da urgência, porém, o que destacamos no nosso estudo é que essa abordagem muito, muito setorial. Ou seja, regulamentação tomada pela Anatel, pela Lanac, pela ANEEL. Essa é uma enorme vulnerabilidade do país, porque a cibersegurança não é enxergada como um conjunto sistêmico mas como setores. Para tomar, retomar aquela metáfora que foi utilizada antes da porta, fechar as portas, não adianta na sua casa ter portas de aço se as janelas estão abertas e ninguém sabe qual janela, qual porta tá aberta ou tá fechada, e ninguém sabe como coordenar. Essa é a função principal de uma agência. Eu parabenizo enormemente o GSI pela essa proposta porque é essencial no país, e o país tem um atraso enorme, não comparado simplesmente com a União Europeia. A ENISA na União Europeia foi criada em 2004, mas também com parceiros, por exemplo, de economias em desenvolvimento como China. A CAC, a

Cyberspace Administration of China, foi criada em 2014. A política de desenvolvimento industrial e digitalização chinesa prevê, desde 2014, digitalização e cibersegurança em conjunto. Esses são duas asas da mesma ave. Fora da metáfora política chinesa, que tem os seus limites, é muito interessante, porque uma ave com uma asa só morre. Uma ave com duas asas vive e sobrevive bem. Então, precisamos considerar a digitalização, que foi muito acelerada nos últimos anos por causa do período pandêmico, como algo cuja condição essencial é a cibersegurança. Aí vou entrar nos comentários muito breve, menos de 5 minutos nas, nos pontos específicos da proposta. Primeiramente, eu acho que, então. Concordamos plenamente com o diagnóstico, não somente a quantidade dos ataques mas também a qualidade, sobretudo por meio de inteligência artificial. Todo mundo fala de inteligência artificial hoje em dia esquecendo que, por exemplo, o ChatGPT facilita a redação de malware. Vamos testemunhar ciberataques sobre esteroides, basicamente, nos próximos anos, e neste momento estamos totalmente despreparados. O uso de deepfake não é simplesmente para compartilhar fake news, é para simular biométricos. Tá sendo usado para simular os seus biométricos e ter acesso, conseguir a invasão de sistemas cujas credenciais são os biométricos, que podem ser simulados muito bem com inteligência artificial. Ao nível da, da criação mesmo da, da ANCiber na proposta, no PM. No PL, desculpe. Um ponto essencial é facilitar a sinergia, a cooperação, e a articulação entre as várias agências. Porém, eu acho esse é uma deficiência da, do atual, da atual versão do texto porque se cria um gabinete e um comitê com participação governamental. Eu acho que se esquece de criar uma inclusão forte das agências reguladoras. Eu não concordo que seria demais trazer todas as agências reguladoras. São 12 no Brasil. 12, 11 oficialmente, 12 contando também ANPD. Então, criar um conselho para, de coordenação, de interação e interagência não seria algo de radicalmente difícil. Isso aí é algo muito inovador. Isso aí é algo que poderia ter sido incluído desde, no comitê mesmo. Um outro ponto que eu achei, talvez, precisarei de um pouco mais, de um pouco mais de detalhes, é, qual seria a, o papel do Comitê Gestorial de Segurança da Informação, que ainda existem no GSI e cuja sucessora, meu velho gabinete, mas esse ponto não é esclarecido muito bem na proposta. Então, poderia até uma superposição de dois órgãos basicamente iguais, então eu sugiro também talvez detalhar como essa sucessão poderia acontecer. Também no artigo 20, eu me dei conta que ao falar do gabinete, a composição do gabinete é principalmente pública, de órgão público, que é absolutamente coerente. Porém, logo no início no artigo 20, se reproduz a mesma formulação do artigo 14 falando que está aberto também à sociedade civil, empresas, e academia. Acho muito (Ininteligível) a essa formulação pode gerar um pouco de confusão. Último ponto que eu queria destacar é a criação do sítio .br, que

também acho um ponto extremamente positivo, ter uma, um centro de reação aos incidentes cibernéticos, porém não é destacado como se articularia com o sítio.gov, que já existe, e também com os outros dois sítio nacionais, que são o cert.br e o Sisa da, opa, desculpa, o Cais da RNP. Eu lembro que esse ponto, aliás, essa confusão que existe no Brasil, que é o único país que tem vários sítios nacionais, foi destacado numa reunião do grupo de segurança da informação, das TIC do BRICS, que foi (Ininteligível) aqui em Brasília. Eu fui convidado pelo Jefferson (Ininteligível), é, há cinco anos. Eu lembro que os parceiros do BRICS destacaram a dificuldade de se coordenar por causa dessa existência de 3 sítios nacionais múltiplos. Aí, uma solução para resolver, e até criar uma coordenação na agência, isso aí é a criação de uma rede nacional de cibersegurança, que destacavam o nosso estudo, no modelo do European Cybersecurity Competence Centre and Network, que foi criado somente o ano passado e que cria, basicamente, uma rede de centros de pesquisa, é, centros acadêmicos, e centros de resposta-ataque para coordenar essa resposta e também para compartilhar boas práticas. Um último ponto, e a necessidade, ao meu ver, e aí eu acho que o Brasil tem realmente a possibilidade de se tornar um pioneiro na definição da cibersegurança. É realmente absurdo constatar, é, algo que é reiterado ao longo do nosso estudo, que o alvo, a principal preocupação da cibersegurança na enorme maioria das políticas, das marcas (Ininteligível) nacionais são os ativos, não as pessoas. Os ativos são essenciais, mas a principal deveria ser o cidadão. Então não custa nada alterar a definição, colocando que a cibersegurança deveria ser o conjunto de ações voltado à garantir a proteção do cidadão e a confidencialidade, a (Ininteligível), e a autenticidade dos ativos. Então, esse é o ponto, que há uma falta enorme de todos os marcos regulatórios precedente. E aí, o Brasil tem a possibilidade de se tornar inovador nessa definição até a nível etimológico. Porquê? O, a proposta coloca muito bem como primeiro princípio o foco no cidadão, e logo depois destaca que (Ininteligível) o cidadão é o elo fraco da segurança, que é verdade. A gente tem a possibilidade de reverter, a gente tem, não a possibilidade, a obrigação de reverter esta tendência, e aí no estudo colocamos justamente a conexão entre a cibersegurança e a soberania digital. Nenhuma população ao mundo é soberana digitalmente se não é, se não for cibersegura, e nenhuma população do mundo é cibersegura se não for soberana digitalmente. Ou seja, se a população, se o cidadão entende como funciona a tecnologia, quais são os riscos, e sabe aproveitar os benefícios, até desenvolvendo a tecnologia. A China inclui no ensino primário a programação desde 2020. Então, precisamos também olhar a outros exemplos para entender as, o valor estratégico da cibersegurança e também os valores estratégicos da pedagogia, não somente nas novas gerações. Precisamos de uma, de um ensino inter, e uma capacitação multigeracional. O problema não

é simplesmente o garoto que pode se tornar com capuche, ciberatacante. O problema somos todos nós. Ninguém aqui recebeu literacia digital como ensino na escola. Ninguém. Então somos todos vulneráveis. Existem 3 tipos de usuário de tecnologia digital. Aqueles que já foram hackeados, aqueles que serão hackeados, e aquele que estão sendo hackeados nesse momento. Ou seja, somos todos e todas vulneráveis. Deve ser uma prioridade nacional investir nas pessoas. Muito obrigado.

SR. MARCELO MALAGUTTI, MESTRE DE CERIMÔNIA - Muito obrigado, Professor. Dando prosseguimento, chamo o Senhor Jefferson Gomes, representante aqui do Serviço Nacional de Aprendizagem Industrial, falando em nome da Confederação Nacional da Indústria.

SR. JEFFERSON GOMES - Obrigado. Bom. Antes de tudo, boa tarde ou boa, bom dia a todas e bom dia a todos. Professor Luca Belli, maravilhosa a sua explanação. Muito boa. Parabéns. Eu gostaria só de colocar a Confederação Nacional da Indústria, é, enfatizando a sua apresentação. Em todos os pontos o senhor foi muito preciso, e o senhor sabe que na, cada corporação, cada empresa tem as suas próprias, os seus próprios regramentos. Mas, basicamente, elas dividem. Ah, perdão. Deixe eu cumprimentar também o Professor Malagutti. Obrigado pela oportunidade. E aqui, em nome do meu colega Humberto, cumprimentando todos os colegas da indústria aqui, nacional. Mas professor, todas empresas têm os seus próprios regulamentos, seus regramentos. Entendimento dos riscos e benefícios, fundamentalmente, porque quem tá na empresa hoje nesse level não é nativo digital. Inclusive nós trabalhamos com o Fórum Econômico Mundial em inúmeros projetos, e 75% dos projetos de transformação, de transformação digital então sendo aplicados no mundo neste exato momento falham, e as falhas acontecem por três motivos. Um motivo. Vários motivos, mas 3 motivos clássicos. Um motivo, necessariamente, a ausência de conhecimento de utilização. O outro é a ausência de utilização de metodologias ágeis, porque tudo que o senhor falou tem que ser ágil. A gente não pode usar os mesmos mecanismos que a gente chama de lin, porque a gente tem que utilizar modelos muito rápidos para mudar a direção. E o terceiro fator, a ausência de conhecimento do C-level. Um programa de extensão de formação não somente para as pessoas que não tomam decisões e são usuários tecnológicos, mas fundamentalmente para as pessoas que tomam decisões é emergencial. E aqui, é, Professor Malagutti, eu gostaria de colocar na nossa proposição, fundamentalmente, a disponibilização do Sistema Indústria para quaisquer dos seus projetos, que sejam colocados para tentar avaliar todas as possibilidades de implementações que serão necessárias. Então, em termos práticos, o Sistema Indústria criou o ato simplórios há 10 anos, dentro do Serviço Nacional de Aprendizagem Industrial,

que tem 82 anos. Formou mais de 80 milhões de brasileiros para a indústria nacional, ele formou há 10 anos uma rede de institutos em parceria com o BNDES, e montou 26 institutos de inovação pelo Brasil afora. Isso, há 10 anos, tinham 4 pilares. Um pilar clássico, Brasil, né, uma industrialização hoje, mas fundamentalmente dependência energética de sempre, uma área de, é, especificamente para renovação energética. Um segunda área específica era de biotecnologia, uma terceira área de economia circular, e a quarta área específica para transformação digital. E um dos módulos de transformação digital era cybersegurança, isso em 2012. É, isso muito claramente, porque todas as empresas. A gente tem esses dados. Ou você vai ser, ou você será, ou você já foi, ou você está sendo agora. Só no Estado de Santa Catarina, da qual eu sou natural. No Estado de Santa Catarina nós fizemos uma pesquisa, que mais de 90% das indústrias catarinenses, que tem todos os, tem mais de 20 setores industriais, especialmente 21 setores industriais, 90% das empresas já foram hackeadas, hoje, nesse exato momento. Bom. Então, quando nós pensamos em montar essas estruturas, claramente nós montamos, mas com uma visão bem clássica. A gente faz pesquisa, obviamente tem que fazer pesquisa, mas nós temos que trabalhar em missões, e missões, especificamente, a gente considera o seguinte ponto. Nós precisamos desenvolver tecnologias e entender se isso pode ser escalável, se isso pode ser perene, contínuo, ao longo do tempo, e se isso pode ser sustentável, que pare em pé. Fundamentalmente para em pé em todos os contextos, social, ambiental, mas o, a questão financeira também seja de interesse. E consequentemente, se você consegue desenvolver (Ininteligível) provas de conceitos que fazem isso, com essas tecnologias nós imaginamos o que tem que ser feito em termos de infraestrutura, formação de pessoas, desenvolvimento de novos negócios. E aí, se você tem possibilidade de infra, gente, e negócios, quais são as características que você deve compor para legislações e regulações. Então, necessariamente nesse ponto, em termos práticos, uma na área que foi, que foi colocada como importante era área de Indústria 4.0. Não sei se todos estão familiares, familiarizados com o termo Indústria 4.0, mas ela surge em 2013 no governo germânico por um fenômeno muito interessante. Não é para amplificar a capacidade de tecnologia, simplesmente, mas porque duas grandes corporações germânicas tinham sido hackeadas. Duas grandes corporações. E, basicamente, lá é colocado, bom. Se nós vamos trabalhar com tecnologias exponenciais que estão na ponta, linguagem de baixo nível, sensor, sensores ligados na máquina, e linguagem de alto nível, todo o sistema de comunicação entre as plantas industriais, facilmente estamos vulneráveis. Foi criado o modelo de Industria 4.0 baseado na cybersegurança, e obviamente que depois você vai tentando aplicar questões de produtividade. Resultado prático, é, o que é colocado por vários

setores industriais, perdão. Vários países hoje, e o Brasil não foge à regra, Professor Malagutti, é que o tema coleta em armazenamento é vulnerável. Coleta em armazenamento é vulnerável porque todos os dispositivos de baixo nível, que são aquele sensor que tá na ponta do seu automóvel, seja para homework, seja para ambientes industriais, é a mesma coisa nesse aspecto. Mas o sensor que tá colocado na ponta daquela máquina, ele tá capturando dados e ele tá também sendo vulnerabilizado, mas também todos os sistemas de comunicação entre a cadeia de valor. Então, em termos práticos, vulnerabilidades de sistemas IOT é uma coisa importante. A gente vem desenvolvendo alguns programas, por exemplo, um framework para, por exemplo, o setor elétrico para a definição de protocolos e sistemas seguros de forma bem transversal, e também para questões de criptografia no setor elétrico, autenticação integrada. São, vários projetos estão sendo feitos. Nossos principais parceiros estrangeiros hoje são os Estados Unidos da América, em vários projetos com vários universidades específicas, mas a questão de armazenamento também é uma área estratégica entre coleta de, uma vez que você coletou, como você vai armazenar? Hoje, grande parte das nossas empresas estão trabalhando com dados e com empresas especialistas, e os dados de empresas especialistas. Vocês conhecem Google, vocês conhecem, é, Azure, vocês conhecem um conjunto de corporações. Qual é a nossa capacidade de monitorar e controlar em tempo real esses nossos dados? Bom. Se você encara que coleta e armazenamento é importante para ser estudado dentro de todas as possibilidades, uma outra lógica nossa, também, é processamento, processamento de dados. E aí quando você entra em processamento de dados, também tá vulnerável, porque você vai processar na borda, você vai processar na chamada fog, que são nas redes de servidores, você vai processar na nuvem. Como é isso? O meu colega, é, Humberto vive disso, né, Humberto? Sabe que, que basicamente, nós estamos, é, muito prejudicados em termos porque essas tecnologias são extremamente rápidas, e o hype é muito intenso. Eu trabalho, eu sou professor lá do Instituto Tecnológico da Aeronáutica, lá o ITA, e eu trabalho na área de inteligência artificial. Para vocês terem uma ideia, hoje nós temos 6, 5, 7 algoritmos muito interessantes somente para a visão, para verificar se você é essa pessoa especificamente. Mas se eu for olhar o hype que tá vindo para os próximos 3 anos, eu tenho mais de 30 tipos distintos de algoritmo chegando. Como é que você consegue manter a latência de conhecimento com tudo chegando? Então, poxa vida, é importante, é vulnerável, e a gente tem que criar protocolos para isso. E finalmente, finalmente é a questão de educação do usuário, e é aí que estão essas questões de riscos e benefícios bem colocado pelo professor, mas são coisas básicas, desde o e-mail até o uso de um app. Bom. Isso posto, o Sistema Indústria se preparou, e hoje, por exemplo, na Bahia, nós temos uma

planta piloto. Se vocês quiserem testar modelos, nós temos uma planta piloto industrial, é, extremamente flexível, não só para produção, não para produção contínua, flexível, onde todos os objetos lá são, quero hackear suas máquinas. É uma planta somente para isso. Nós temos em Santa Catarina, também, no Instituto de Sistemas Embarcados, em que uma parte do Instituto de Sistemas Embarcados é somente para cybersegurança. A gente acabou de lançar um satélite, é, tempos atrás, um ano, um satélite. Finalmente, finalmente nós temos um instituto de sistemas de desenvolvimento de sensores que fica no Rio Grande do Sul, também só para vulnerabilização de sensores. O que mais se faz é testar isso. E finalmente, o nosso Instituto somente de TIC, que fica lá no Porto Digital lá em Pernambuco, também uma boa, bem preparada. Enfim, eu coloco todos os nossos institutos, todas as nossas estruturas do Sistema Indústria. Nós investimos 3 bilhões de reais na montagem dessas, dessas capex todos. Temos mais de mil pesquisadores, são mais de, são mais de 2.600 projetos executados, somando um total de mais de 2 bilhões e meio de projetos de pesquisa. Hoje são as principais unidades da Embrapii. Muito obrigado. Tenham todos um bom dia.

SR. MARCELO MALAGUTTI, MESTRE DE CERIMÔNIA - Bom. Como vocês perceberam, nós professores estamos nos preparando (Ininteligível) um compromisso de última hora e vai ser representado pelo Senhor João Zanon, que é assessor da Superintendência de Planejamento e Regulação.

SR. JOÃO ZANON - Primeiro, obrigado, pessoal. É, obrigado pelo convite da Anatel, tá participando. Infelizmente, o Presidente Baigorri não foi, não é possível para ele estar participando. Ele teve uma reunião urgente com o Ministro, e aí eu, o João Zanon, vou tá falando em nome da agência. Eu sou assessor na Superintendência de Planejamento e Regulamentação, né, que é uma das áreas muito engajadas nesse tema, né? Como já foi falado bastante, né, o tema de cybersegurança é um tema extremamente importante não só para o Brasil como para agência, né? Um tema que a Anatel, ela é engajada há muitos anos, né? Se tomar alguns exemplos, né, desde 2014 a gente tem um grupo de infraestrutura crítica que a Anatel vem participando e coordenando. 2020, a gente teve um novo regulamento sobre cybersegurança e a criação do GT-Ciber, que é um grupo de trabalho onde eu acredito que vários os senhores participam muito ativamente, né, acompanhado pelo Gustavo e pela Vanessa, onde a gente tem colaboração entre todos os agentes envolvidos, né, para ter troca de informações, né, notificação de acidentes, né, definião de melhores práticas. Então é um tema de extrema importância e relevância para a agência. Não por isso, né, que a gente não poderia recusar esse convite, estar participando dessa discussão. É, por óbvio, né, esse é um tema transversal onde a colaboração entre todos os agentes é de extrema relevância, né? Se

você pega, é, todas as iniciativas que a gente teve até o momento da agência, a gente sempre pautou pelo diálogo, pelo consenso, pela discussão. E eu acredito, né, que a iniciativa que está sendo tomada aqui, vai no mesmo sentido, né? E a gente parabeniza, né, a Anatel, essa iniciativa. É, a Anatel, como a gente disse, não só a nível nacional como internacional, é muito interessada nesse tema. Pegando dois exemplos recentes, né, a gente teve, ano passado o Pleno Potenciáveis, né, conferência de mais alto nível da UIT. A gente teve duas resoluções extremamente relevantes. A resolução 130 sobre cibersegurança onde o Brasil é capitaneou, inclusive, uma parte dessa discussão onde grande parte dos nossos interesses pôde, de certa forma, ser discutido, representado, e também a resolução sobre Inteligência Artificial, uma nova resolução que foi aprovada na UIT, e que também, por suposto, toca esse tema, né? Na verdade, cibersegurança toca todos os temas de vanguarda, então, cada vez mais importante essa iniciativa. Quando a gente fala em 5G, então, tem convergência das redes, redes orientadas a pacotes, internet das coisas. Então, você tem vários verticais onde, necessariamente, os dados são necessários, como já foi citado aqui, e, por consequência, a proteção desses dados. Não por isso, né, é importante o envolvimento de todas as, as entes de governo e uma uma coordenação de alto nível, né, com uma política de governo, um órgão dedicado para isso. E, novamente, a gente parabeniza a iniciativa. Sobre as contribuições, a agência tá analisando com muito cuidado e carinho o documento, né, a minuta, e em tempo a gente vai estar devolvendo, né, os nossos comentários para que a proposta possa ser aprimorada. Bem. Muito rapidamente, é isso. Agradeço novamente.

SR. MARCELO MALAGUTTI, MESTRE DE CERIMÔNIA - Agradecemos. A Anatel é parceira de primeira hora conosco. A Vanessa que o, que o João citou aqui, é colega nossa, atuante no ComDCiber, no Guardião Cibernético, o nosso exercício anual há muitos anos. E foi uma das primeiras pessoas a ter a oportunidade de olhar, ela. O Sabbat, que falou que leu 3 vezes, a Vanessa também leu outras 3 vezes. É, então assim, a Anatel tem sido uma grande parceira nossa nessa iniciativa. Bom. Agora eu chamo o Senhor Valdemar Latance Neto, Chefe do Serviço de Análise de Dados de Inteligência Policial da Polícia Federal.

SR. DELEGADO VALDEMAR LATANCE NETO - Alô. Ops. Bom dia a todas e a todos. Meu nome é Valdemar. Eu sou delegado da Polícia Federal, Chefe do Serviço de Análise e Inteligência Policial da Diretoria de Combate à Crimes Cibernéticos, e em nome da qual eu falo nessa manhã. Em harmonia com o que disse antes o nosso parceiro, o Leonardo, e também o Ministério da Justiça por meio da brilhante intervenção da Doutora Estela Aranha. Eu queria registrar, primeiramente, a presença do diretor da DCIBER, o Doutor Otávio, o

Coordenador Geral de Combate a Crimes de Alta Tecnologia e o seu substituto, os peritos criminais federais Herman e Flávio, tudo a mostrar a relevância que a Polícia Federal dá à esse evento. Agradeço ao GSI pela hospitalidade e saúdo pela realização dessa importantíssima audiência pública que representa a concretização do princípio democrático, possibilitando um debate aberto e plural desse tema, que afeta a sociedade integralmente, como vimos aqui nos, nas intervenções que me antecederam. O debate aqui é sobre o projeto de lei que busca instituir, então, a política nacional de cibersegurança, o sistema nacional composto por uma agência, pelo comitê, e pelo gabinete de gerenciamento de cibercrises. As finalidades principais do projeto são, resumidamente, unificar a colcha de retalhos regulatória do Brasil, diminuir o débito tecnológico nacional, e ampliar a participação brasileira na cooperação internacional sobre a temática. É impossível discordar dessas finalidades. Porém, com o devido respeito, o PL demanda alguns ajustes. Nada de anormal, por se tratar de um projeto cujas discussões estão apenas começando. Para não me alongar demasiadamente, eu vou focar minha intervenção na finalidade de ampliar a cooperação internacional na cyber segurança, na importância de integração entre as instituições públicas e privadas, e no papel da Polícia Federal no Sistema Nacional de Cybersegurança. É, o projeto prevê como princípio na Política Nacional de Cybersegurança no artigo quinto, inciso 8, a cooperação internacional. E aqui nesse ponto, há anos a Polícia Federal tem destaque mundial em intercâmbio de informações com autoridades policiais estrangeiras sobre crimes cibernéticos. Incontáveis operações policiais foram feitas graças à cooperação internacional. A instituição construiu, portanto, um sólido conhecimento sobre várias espécies de cybercrimes, modos de atuação, melhores formas de preservação e coleta de prova, entre outras atividades que poderiam contribuir nas atividades dos órgãos do Sistema Nacional de Cybersegurança. E aí eu digo, poderiam porque a PF não foi expressamente incluída no Sistema Nacional, especialmente no comitê e no Gabinete de Gerenciamento de Crises. Respeitosamente, não há razões constitucionais nem legais para essa exclusão, né? Ao contrário, o exame sistemático da Constituição Federal e da legislação nacional sugere que a Polícia Federal integra o Sistema Nacional de Cybersegurança em posição separada da vaga disponibilizada ao Ministério da Justiça e Segurança Pública, que possui outras várias temáticas de extrema relevância. Isso porque a responsabilização de quem comete atos ilícitos como cyberofensa, cybercrime, cyberataque, nas definições trazidas pelo próprio PL no artigo quarto demanda apuração, né? Responsabilização demanda primeiro a apuração por meio da investigação policial, que é uma atividade regulamentada na Legislação Processual Penal e com finalidade de reconstruir os possíveis fatos criminosos por meio de provas válidas, que respeitem fielmente os limites legais e

constitucionais, como o extenso rol de direitos individuais que estão previstos na Constituição. É o nosso trabalho. Nos casos de crimes transnacionais, a Polícia Federal, a Constituição Federal atribui à Polícia Federal o exercício com exclusividade das funções e Polícia Judiciária na União conforme o artigo 144, parágrafo primeiro, inciso 4, incluindo aí as infrações penais em detrimento de bens e serviços da União, e que tenham repercussão internacional. Então, na hipótese de acontecer um ataque cibernético contra uma estrutura crítica gerenciada pelo Governo Federal, caberia a Polícia Federal investigar o caso e esclarecer como os fatos ocorrendo, ocorreram. Aproveitando até a apresentação anterior aqui, aquele caso do INSS de 1 bilhão é investigado pela Polícia Federal. Até a própria, a própria manchete da imprensa trazia o nome lá, Polícia Federal. Então, ainda nesse exemplo aventado, né, a Polícia Federal necessariamente teria de ser acionada. Não. Perdão. Assim, supondo então, ainda, né, naquele meu exemplo, que a gravidade do caso exigisse o acionamento do Gabinete de Gerenciamento de Crises, a Polícia Federal não faria parte da ação nos termos do texto original do projeto de lei. Óbvio, né? Então além das razões constitucionais, razões práticas também apontam a pertinência da integração da instituição responsável pela apuração dos fatos criminosos no Sistema Nacional de Cybersegurança, né? É, nesse exemplo, né, a Polícia Federal seria acionada e imediatamente começaria investigação. Uma PF não faz parte do comitê. Perdão. Do Gabinete de Gestão de Crises, ficaria aberta a possibilidade de serem adotadas providências contraditórias pela PF e pelo gabinete, né? Então, em vez de integração, haveria sobreposição de ações estatais com a possibilidade de se chocarem, em prejuízo da necessária eficiência estatal que também é exigida no artigo 37 da Constituição. Além disso, né, a participação da Polícia Federal é imprescindível na elaboração de eventuais regras sobre a preservação e coleta de dados que serão fundamentais para cyberinvestigação, e também nas normas sobre a necessidade de comunicação de incidentes cibernéticos às autoridades policiais, um tema relevantíssimo. Informar, a obrigação de informar as autoridades policiais. Embora o PL tenha reservado uma vaga para o membro do Ministério da Justiça e da Segurança Pública, esse ponto, na nossa opinião, merece ser discutido, tendo em vista a existência de diversos órgãos dentro da estrutura do Ministério da Justiça. E o governo atual elegeu algumas prioridades, e o combate aos crimes cibernéticos é uma delas, tanto que dentro da Polícia Federal foi criada a Diretoria de Combate aos Crimes Cibernéticos, que era algo que era, parecia óbvio há muito tempo, mas ninguém nunca fez. E finalmente o governo elegeu isso como prioridade e criou a DCIBER, a demonstrar como esse tema é prioritário para o governo. É, o, a eficiência, né, de todo esse sistema de proteção que o PL pretende construir no cyberespaço depende da aplicação, na medida legal, de sanções aos que

ousarem cometer crimes. Vários também que me antecederam disseram isso. Se os criminosos não forem punidos, a sensação de impunidade levará ao aumento das infrações penais, que já é, aqui, enorme, como também já disseram. A cyberinvestigação que tá no artigo quarto, inciso 11 do projeto de lei, portanto, é atividade essencial para manutenção da cybersegurança, que tá no mesmo artigo quarto, inciso 9, tanto que o artigo 6, 8 do projeto de lei consagra como objetivo do plano fomentar o combate ao cybercrime. Diante do exposto, a Polícia Federal defende, com devido respeito, a inclusão de um inciso no artigo 15 e outro no artigo 22 com a inscrição, um representante da Polícia Federal, para que também integremos o Comitê e o Gabinete de Gerenciamento de Cybercrimes. Concluindo, né, diante das circunstâncias nacionais no Sistema Nacional de Cybersegurança, a Polícia Federal deveria integrar o Comitê Nacional de Cybersegurança e o Gabinete de Gerenciamento de Cybercrimes sem prejuízo do outro indicado pelo Ministério da Justiça e da Segurança Pública responsável por outras áreas temáticas também relevantes na composição desses novos órgãos. Agradeço novamente pela oportunidade e pela atenção. Muito obrigado.

SR. MARCELO MALAGUTTI, MESTRE DE CERIMÔNIA - Delegado, já de pronto, eu asseguro para o senhor que o senhor tem o meu voto para incluir a Polícia Federal nessas duas instâncias. Eu sou o único decisor, mas o meu voto você já tem. Bom. É, isso posto, agora nós terminamos a última intervenção de convidados e abrimos (Ininteligível) voltamos a palavra aqui aos demais interessados aqui presente, que por acaso tenham interesse. Venha, por favor. Dirija-se. A senhora em seguida. É, dirija-se ali ao púlpito, por gentileza. Venha. OK. Eu peço àqueles que forem fazer o uso da palavra que identifiquem seu nome, seu, seu órgão de origem ou aquele que representam, ou, como cidadãos, todos estão livres para fazer seus comentários. Observação. É, o nosso controle de tempo está aqui na frente, na primeira fila. Nós estamos dando 3 a 5 minutos para cada um dos interessados, para não alongarmos demais a conversa.

SR. BRENO - Bom dia a todos. Meu nome é Breno. Represento a ABRINT. A ABRINT é a Associação Brasileira de Provedores de Internet e Telecomunicações, representa os provedores regionais de internet, que são, na sua maioria, pequenas e médias empresas de todo o Brasil, que somadas, em conjunto, são responsáveis por 52% dos acessos de internet banda larga fixa no Brasil. Nossa associação tem dado grande atenção ao tema da cybersegurança, com apoio contínuo às atividades do Cyberlab no Ministério da Justiça, por exemplo, e com esforços para a criação da cultura cyber no mercado de provedores, com projetos próprios, e abrindo espaço para o GSI em nosso encontro nacional realizado no final de maio, em São Paulo. Aqui, já

agradecendo novamente a participação do Marcelo. Nesse sentido, a ABRINT apoia e reconhece a importância da Política Nacional de Cybersegurança e do Sistema Nacional de Cyber Segurança. Está certa de que há espaço para aprimoramento estrutural e comportamental. Do ponto de vista estrutural, a ABRINT concorda com a criação de uma agência reguladora na qualidade de entidade autárquica vinculada ao GSI, e recebe com satisfação seus padrões mínimos operacionais. Porém, a ABRINT discorda do endereçamento dado a busca de transversalidade da cybersegurança, seja em razão da ausência ainda de definições claras sobre defesa e segurança, seja em função do aparente afastamento das infraestruturas críticas do universo cyber. Já do ponto de vista comportamental, a preocupação da ABRINT se estende além do diálogo institucional e alcança o respeito às competências das outras agências reguladoras. Compartilhar iniciativas é relevante e necessário, mas não se pode deixar de lado as competências setoriais. A conquista de uma soberania digital passa pela clareza e positivação desta delimitação de competências setoriais, sobre o risco da novidade suprimir, suprimir estruturas e comportamentos já regulados, com destaque especial à regulação pela Anatel, referência digna de destaque pelo seu equilíbrio e força. Muito obrigado.

SR. MARCELO MALAGUTTI, MESTRE DE CERIMÔNIA – Por gentileza.

SRª VANESSA FUSCO - Bom dia a todos e todas. Meu nome é Vanessa Fusco. Sou promotora de justiça, membro colaboradora dos Conselho Nacional do Ministério Público, e coordenadora do grupo responsável pela elaboração do Plano de Segurança Cibernética do Ministério Público Brasileiro. Então eu quero agradecer ao convite, ah, do GSI para a nossa participação. Temos participado ativamente do Exercício do Guardião Cibernético. Eu gostaria de fazer rapidamente algumas referências aos, à fala dos meus antecessores, principalmente dos professores, né, Luca Belli, também, é, da empresa, das empresas, da indústria, e finalmente da Polícia Federal, que é realmente quem faz a nossa, que onde nós recebemos efetivamente a investigação e que damos prosseguimento a este sistema de percepção penal. O Ministério Público Brasileiro, é, eu vou falar rapidamente, ele só se despertou a partir da pandemia, dessa necessidade, é, de efetivamente tratar, tanto no âmbito interno, como com a criação da política, quanto também para sensibilizar, recapacitar os seus membros, é, e servidores da necessidade da proteção, da segurança da informação, e também da segurança, por consequência, da segurança cibernética. Apesar de Minas Gerais, nós termos desde do ano de 2008 a primeira Promotoria de Justiça de Combate aos Crimes Cibernéticos do Brasil. Eu tive a honra de iniciar e por isso estou nesse tema até hoje. Nós não tínhamos ainda, de maneira sistêmica, essa ideia de se fazer de uma maneira estratégica que o Ministério Público se dedicasse a esta, a este tema, como

deveria. E finalmente então, estamos agora nesse, e terminando essa política, é, o TCU muito bem disse que nós estavas em estudo, né, e eu me senti aí provocada em falar, porque o estudo, é, sou eu que estou lá liderando ali a, a duras penas, enfim, essa missão de fazer esse plano estratégico. Mas o que eu gostaria de trazer como contribuição, primeiro é de agradecer, é, que nós fomos também contemplados em estar, é, participando do comitê e também da Gestão de Cibercrises. Somos atores, como disse aqui a Polícia Federal, é, muito importante, principalmente, é, para assegurar a percepção penal do cibercriminosos, tendo em vista a questão da cadeia de custódia, que tem que começar já lá, na coleta da prova, para que cheguemos lá no Ministério Público e nós possamos fazer, é, ter sucesso na ação penal para a condenação do cibercriminosos. Também para nós, eu sou também responsável pela inteligência no Ministério Público de Minas Gerais e no GNCOC. Sabemos que, é, há uma gama de cibercriminosos que tratam, é, hoje se dedicam a essas atividades via internet, e nós efetivamente temos que estar preparados para isso. A minha palavra é só para dizer que nós concordamos também com a necessidade de haver a sensibilização da alta administração, é, dos gestores, né? E é o que nós estamos fazendo junto ao Conselho Nacional dos Procuradores Gerais, é, quem engloba tantos ramos como as unidades do ministério público para que nós possamos também, como o setor público e como órgão indispensável é o funcionamento da Justiça, que nós também possamos fazer a nossa parte, integremos esse sistema e essa luta, é, contra o cibercriminosos e para uma eficaz política de cibersegurança que tire o nosso Brasil na área da cibersegurança, desse atraso na estratégia. É, para os senhores terem uma ideia, se os senhores virem aí no Observatório da Cibersegurança das Américas, da OEA, né, Trinidad Tobago, desde 2013, tem uma estratégia de segurança, e nós só em 2020 que conseguimos construir a duras penas a nossa. E espero agora, não mais por decreto, mas sim por um, uma participação ampla que começa, que começa hoje, aqui nessa audiência pública. Muito obrigada. Estamos à disposição também para contribuir. Até logo.

SR. MARCELO MALAGUTTI, MESTRE DE CERIMÔNIA - Muitíssimo a Doutora Vanessa, sempre contribuindo aqui com as nossas iniciativas. Por gentileza, vão se aproximando conforme o interesse.

SR. IVANILDO - Bom. Boa tarde, né? Já, já passamos do meio-dia. Meu nome é Ivanildo. Eu sou policial rodoviário federal, mas estou aqui não representando minha instituição, mas como cidadão, porque é um tema que, que afeto a mim. Gostaria de parabenizar o GSI pela iniciativa. Fiquei feliz em, em saber que teremos respostas das nossas contribuições. Particularmente, eu enviei 5 páginas de contribuição ontem até 1 da manhã, então fiquei muito

satisfeito e muito ansioso para ver o que foi indeferido, a motivação que foi dada. É, parabenizar o colega da FGV e o da CNI. Fiquei feliz em ver que muitas das minhas contribuições coincidem com o que vocês falaram, e apenas um eu queria trazer aqui com relação ao comitê, que o colega da Polícia Federal abordou, é, e ao gabinete. Acho sim que órgãos devem representados ainda como a Polícia Federal. Minha ressalva é apenas que seja dado o espaço para o especialista. No caso se o Delegado for especialista na área, também, mas mais para o perito, eles têm uma área específica sobre isso. E senti falta, no projeto, de uma referência específica sobre os critérios de entrada no comitê. Você viu os órgãos, mas, é, nós temos a experiência aqui no Brasil de um comitê ser composto de pessoas, muitas vezes, que não têm conhecimento na área, e segurança você não faz sem conhecimento, sem informação, sem experiência. Então, uma das minhas sugestões foi exatamente inserir uma experiência comprovada, ou uma formação, ou uma defesa, ou uma causa, ou uma reputação ilibada. Né, ilibada não. Uma reputação na área, é, de modo que o Comitê e o Gabinete de Cybercrise não fiquem refém das informações que chegam, e sejam convencidas, assim como posso atuar de forma mais efetiva, com relação à ideia de educação, a programática na educação infantil. Achei nobre a inserção, porém ela não resolve o problema hoje. Nós temos iniciativa. É uma pena que o colega da, do MGI não está aqui, mas é um órgão que teve iniciativas fortes nos últimos 3 anos, e nós precisamos de capacitações e treinamentos para os órgãos de administração pública, visando fechar essa brecha. Os atacantes, eles não descansam, e a gente não pode descansar também. Era isso. Muito obrigado.

SRª CAROLINA - Olá, bom dia. Boa tarde todos e a todas. Meu nome é Carolina. Sou advogada e pesquisadora do GETIS. É um grupo de estudos em tecnologia e informação e sociedade da Universidade Federal de Fortaleza. Agradeço em nome do GETIS e do LABID a oportunidade de trazer algumas considerações para essa audiência. Bom. Para ser bem breve, é, a minha fala vai destacar alguns pontos de reflexão e sugestão, é, muito no intuito colaborativo, né, como todos aqui fizemos, e as demais contribuições serão enviadas por e-mail. Bom. O primeiro ponto refere-se à Agência Nacional de Cybersegurança, e a nossa observação é que as suas competências, elas devem ser pensadas de modo que haja convergência com as funções da ANPD, da ANATEL, e demais agências reguladoras já existentes, a fim de evitar o conflito e supressão de competências. Isso também foi bem abordado aqui, e a gente corrobora com, com essa necessidade. Sobre os amplos poderes de prevenção aos cyberincidentes que estão previstos no inciso sexto do artigo 18. Cidade. Isso é importante porque, para garantir ao cidadão que não haverá um monitoramento ou uma utilização de Poder com fins desvirtuados. Aí

também entra, né, uma pauta nossa de promover a cripto, a criptografia como ferramenta de proteção dos Direitos Humanos digitais. Outro ponto é sobre o inciso 29 do Artigo 18, é, que fala sobre ouvir a sociedade, né? Então, ouvir a sociedade realmente não deve ser um ponto secundário, pois há um interesse relevante de diversos setores. Então a nossa sugestão, que não ficou muito claro, seria, como que a sociedade será ouvida? Por audiência pública? Por manifestação escrita, pela plataforma Mais Brasil? É preciso que isto esteja melhor definido em lei para que essa possibilidade não caia em desuso e vire uma letra morta. E sobre as matérias de interesse relevante quanto a esse ponto, o que será considerado como matéria de interesse relevante para que a sociedade seja ouvida? É importante que isso também esteja bem definido. O segundo ponto refere-se ao Comitê Nacional de Cybersegurança. A sugestão do, é que deve-se incluir também uma cadeira para representantes da sociedade que atuem na defesa dos Direitos Humanos no âmbito digital, e também repensar a forma de nomeação dos setores não-governamentais para que haja a preservação do multisetorialismo, estabelecendo que as indicações não se dêem apenas pelo Poder Executivo, mas que haja uma forma mais deliberativa para dar melhor representatividade a esses setores. Sobre o funcionamento desse comitê, como se dará a estrutura deliberativa de aprovação? Será por votos de maioria dos integrantes, por voto qualificado, por consenso? Um terceiro ponto refere-se ao Gabinete de Gerenciamento de Cybercrises. Há a necessidade de incluir o Ministério dos Direitos Humanos como uma forma de contrapeso. Isso se dá pela preocupação de que não tenham condutas autoritárias e excesso de estatais que ocasionem um técnico, um techno-autoritarismo. O quarto e último ponto refere-se ao complexo, Complexo Nacional de Cybersegurança. O questionamento é, quem vai compor esse complexo? Além disso, se novas normas reguladoras serão criadas, é preciso que haja uma cooperação com os demais entes normatizadores e fiscalizadores setoriais como a ANATEL, a ANPD, e outros aqui já mencionados também, é, porque senão onde ficaria a hierarquia? Em um conflito de normas, quem resolverá? Por fim, tendo em vista que as pessoas humanas representam um dos pilares da cybersegurança, sugere-se que a redação seja elaborada levando em conta os princípios da linguagem acessível, inclusiva e simples, visando a promoção da cidadania e do acesso à informação para todos os cidadãos. Essa é a nossa contribuição. Muito obrigado.

SR. RODRIGO AZEVEDO GRECO - Boa tarde a todos e a todas. Meu nome é Rodrigo Azevedo Greco. Sou advogado. Não tô representando ninguém, tô aqui na qualidade de cidadão. Queria começar parabenizando na pessoa do Doutor Malagutti, a iniciativa e a transparência do processo com a qual a Presidência da República e o GSI tem conduzido essa matéria. Tenho 5 rápidos

comentários. Na verdade, são mais dúvidas, e fico aqui para a reflexão de vocês. O primeiro é uma suposta competência normativa do comitê. O senhor falou que o comitê teria uma função de supervisão das atividades da agência, e, mas eu vi que aqui no artigo 14, inciso 2, ele tem uma competência para aprovar, por meio de resolução, atos normativos concernentes a cybersegurança. Eu fiquei na dúvida como essa competência normativa seria exercida pelo comitê, com a matéria, se não tem um conflito interagência, como separar essas competências normativas. Segundo ponto diz respeito ao escopo dos produtos e serviços que estariam sendo avaliados pela agência. No Artigo 18, inciso 14, quando trata da competência da agência, diz que compete a agência avaliar produtos e serviços, vírgula, no tocante a cybersegurança. Mas o anexo 1, artigo 21, inciso 8º, quando trata das receitas da agência, lista dentre elas as taxas de certificação de produtos e serviços de cybersegurança. Ao meu ver são conceitos distintos. Então, eu vi um produto de cybersegurança seria por exemplo um firewall. Mas quando você fala de produtos e serviços, vírgula, no tocante à cybersegurança, você tem um universo muito maior de produtos e serviços, né? Por exemplo, um eletrodoméstico que esteja conectado à internet, né, uma Smart TV, pode ser alvo de ataque, se tornar um bot por ataque de DDoS. Então eu não sei de qual universo que vocês estão falando, tratando, ou se são universos realmente distintos. O universo menor que seria certificado, que seriam produtos e serviços de cyber, mas a variação sobre um universo maior que seriam produto de serviços no tocante a ANCiber. Terceiro ponto é, quando se fala de cobrança de taxas, fato gerador, contribuinte, valor, tem que estar previstos em lei. Eu não encontrei isso na, no projeto. Eu não sei se vai ser feito uma, num outro projeto de lei, prevendo e regulando a cobrança das, dessa taxa. Ainda no tema de certificação de produtos, a Anatel, hoje, ela já certifica equipamentos de telecomunicações, inclusive levando em consideração aspectos relacionados a cybersegurança. A dúvida que fica é se a ANCiber estaria propondo requisitos novos que deveriam ser levados em consideração pela Anatel no processo de certificação que ela conduz, ou se os produtos estariam sujeitos a uma dupla certificação pela Anatel e pela, e pela ANCiber. E por fim, no anexo 3 do decreto que trata da estrutura da agência, é atribuído contato das competências do órgão de inteligência, uma delas é a subsidiar ou produzir conhecimento que subsidi o processo decisório da ANCiber, em especial aquele relacionado às análises de pedidos de autorizações, processos de revogação, e cancelamento de registros dos agentes regulados pela agência. Isso é algo que eu não encontrei no projeto de lei, e eu não entendi que registro é esse que os agentes regulares têm que fazer perante a agência. Isso tá só no decreto, não tá na lei. Fiquei com essa dúvida. De depois pudesse ser esclarecido, eu agradeço. Muito obrigado.

SR. ANTOVANI - Bom dia a todos. É, meu nome é Antovani. Sou Gerente de Relações Governamentais da ABINI, Associação Brasileira da Indústria Elétrica e Eletrônica, e em nome do meu Presidente, Humberto Barbato, a gente gostaria de cumprimentar o GSI e a secretaria por essa importante iniciativa de criar, de estudar essa nova Política Nacional de Segurança Cibernética, né, que deverá ser então enviada para o Congresso Nacional. A ABINI tem cerca de 400 indústrias associadas. É, nós produzimos, vou brincar aqui, nós fabricamos a máquina do crime, né? Porque é do celular, é do computador, é do tablet, né, é da rede da fibra ótica que as pessoas se aproveitam, que o crime não se aproveita para entrar no sistema e fazer o que a gente está discutindo aqui fora, mas de tentar impedir isso, né? Então, nós trabalhamos tudo, toda essa área dos produtos da tecnologia da informação e da comunicação, e por isso que é importante nós entendermos que é importante a nossa participação. Já tivemos isso. A ABINI teve uma contribuição muito importante na definição da política do 5G, né? Sabe que havia uma disputa no mundo, os Estados Unidos de um lado, a China, né, fabricantes da China de outro, etcetera e tal. E a gente conseguiu, imaginamos com a nossa simplicidade, contribuir, demonstrando que nós tínhamos toda uma rede instalada no país, né, que trabalhava com, de certa forma, com as duas, com os dois equipamentos, e que não era possível você fazer alguma coisa de maneira exclusiva. Então a gente imagina que, da mesma forma que a gente conseguiu contribuir nessa questão do 5G, a gente costuma fazer isso em todas as audiências públicas que a gente é chamado. Por exemplo, há poucos dias nós participamos de um workshop, a Anatel também tem uma política de rede de telecomunicações, e a gente tem conseguido, como uma indústria, participar e contribuir nessa, nessa formulação dessas políticas, né? Então a gente, mas a gente ao mesmo tempo que tem essa capacidade de contribuir, a gente tem um problema que eu queria colocar aqui. Nós temos 11 setores nessa indústria, nós temos 123 grupos de trabalho, então a gente se mostra assim como uma certa lerdeza, diria assim, né, e talvez, quando eu ouvi aqui no começo, o GSI comunicou que a gente tem até a meia-noite de hoje para apresentar essa sugestão. Então vamos lá. Provavelmente, nós não teremos condições (Ininteligível) com muita coisa hoje, mas ao final, eu vou apresentar a nossa solução que a gente acha que a gente pode contribuir, e da forma como a gente pensa em fazer isso, tá certo? A ABINI e os seus associados têm uma larga experiência nos processos de averiguação, de conformidade, e certificação de equipamentos, na aplicação de normas e padrões nacionais e internacionais, e referências de boas práticas do tema da segurança cibernética, onde certamente nós poderíamos contribuir de maneira relevante na discussão e decisão referente a essa Política Nacional de Segurança Cibernética. Contemplando a experiência das nossas indústrias e o

compartilhamento de informações, e o entendimento sobre esse importante ecossistema no Brasil, com o objetivo de auxiliar os estudos e debates sobre esse tema. E ela pode dizer então que, em nome desses 400 associados e desses 11 grupos de trabalho, que a gente ia pedir uma prorrogação dos 30 a 40 dias para poder apresentar. Tendo em vista essa dificuldade que a gente tem com relação ao tema. Peço desculpa, é que eu tô tomando remédio para minha sinusite que tá me deixando sem saliva aqui, tá? Mas e, tendo de vista essa questão, a gente vai fazer esse estudo, tá? A gente sabe que esse projeto ou medida provisória, ela vai passar para o Congresso Nacional. Então de toda forma, fechado isso tudo a gente repassa para vocês informalmente, e depois, no Congresso, a gente acredita que a gente pode contribuir então no aperfeiçoamento, na melhoria, se possível, dessa proposta. Muito obrigado.

SR. PAULO EMERSON - Boa tarde a todos. Meu nome é Paulo Emerson. Eu sou representante da ANPPD regional do Distrito Federal, e na ANPPD da nacional sou Vice-Diretor do comitê público e também sou membro da Rede Governança Brasil. Antes de tudo, agradecer as sábias palavras do nosso Professor, ai, meu Deus, Luca Belli. A gente que trabalha com privacidade, nós buscamos muito que o cidadão seja representado, que a pessoa, que o indivíduo seja representado. E infelizmente, no nosso país ainda não foram feitas as devidas exceções para as políticas públicas para educação, na área da privacidade e na área da segurança cibernética. E é importante eu estar falando aqui uma, algo que eu acho que é crucial para dentro da política. Por mais que eu tenha os comitêres gestores, por mais que eu tenha a estrutura da política sendo estruturada, nós não temos menção sobre como a operação vai acontecer. A governança para execução de um cenário de crise, é obrigatório que a gente tenha cadeia de custódia muito rápida, muito eficiente, e eficaz, porque o crime já aconteceu. Nós não temos mecanismos de congelamento do crime cibernético, que é algo que é crucial, porque nós temos um Judiciário letárgico. Não é porque o Judiciário não quer atuar. É porque infelizmente nós não temos braços operacionais suficientes que andem na velocidade do crime cibernético. Então é, essa é uma colocação que a gente precisa ter muita assertividade, e, preferencialmente, começa na primeira propositura da política, e não depois, porque se acontecer depois, o que é que vai acabar acontecendo? Vai ficar dentro de uma lacuna do esquecimento. Nós temos uma responsabilidade quando a gente constitui uma empresa dentro da sociedade brasileira, é responsabilidade objetiva direta. Nós temos a obrigação de proteger os dados dos nossos negócios. Nós temos a obrigação de proteger os nossos negócios. Nós temos obrigação de proteger a soberania nacional, não somente o governo. E, professor, agradeço muito o trabalho da GSI. Muitos não conhece o trabalho que vocês exercem no decorrer de vários anos,

que não é um gabinete que foi construído agora. E a gente pretende poder ajudar tecnicamente, cientificamente, que é o papel que a nossa associação pode fazer é essa. Dentro da Rede Governança Brasil, nós atuamos em todos os municípios brasileiros, então nós temos a realidade da pessoa que não tem a internet disponível. Não adianta eu falar de 2G, 3G, 4G, 5G. Nós temos aqui, na nossa capital federal, situações de escolas públicas que não têm o cabeamento de fibra ótica para chegar na internet, assim como nós temos locais aqui que têm uma internet de 10 GB dentro da infovia. E temos uma outra situação que é importante destacar, é, não na parte política mas na parte econômic. O único país que fabrica, hoje, semicondutor é a China e um pedacinho que tá lá perto da China. Como que a gente vai fazer essa diferenciação do plano de continuidade no sistema de gestão de continuidade de negócio na estrutura do plano de continuidade, no Sistema de Gestão de Continuidade de Negócio do nosso país? Porque não adianta eu chegar aqui e dizer que eu tenho internet, que eu tenho estrutura tecnológica, cibernética, eu não posso ter serviço parado e com desastres acontecendo. Isso tem que acabar. Agradecemos o nosso apresentação e agradeço muito ao senhor, Professor.

SR. IGOR MORAES - É, bom dia a todos. Deixa eu me apresentar primeiro. Eu me chamo Igor Moraes. Eu sou professor do Instituto de Computação da Universidade Federal Fluminense, é, trabalho no tema desde 2001 quando eu comecei minha iniciação científica. Na época o objetivo era, quem conseguia invadir o laboratório de pesquisa vizinho para mostrar que era mais capacitado. Hoje em dia, eu acho que eu faço coisas um pouquinho mais interessante do que isso (Ininteligível). Mas enfim. Hoje eu tô aqui representando a Sociedade Brasileira de Computação, a SBC. Eu coordeno uma das comissões especiais da SBC, a Comissão Especial em Segurança da Informação em Sistemas Computacionais. Dentre as, as coisas que a SBC faz, não é, que é a (Ininteligível) na área, no Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais, debate ideias, traz pescadores de universidades renomadas do exterior para debater esses temas. Então o meu papel aqui hoje é colocar toda a capacidade técnica do, dos docentes e dos profissionais que trabalham nessa área na comunidade de segurança da informação em sistemas de computacionais, filiados SPC, à disposição do GSI para colaborarem na composição do comitê previsto no projeto de lei ou em outros temas relacionados ao projeto de lei. É, a gente tem algumas sugestões técnicas, mas isso eu faço por e-mail. Muitas delas já foram comentadas aqui sobre a questão da, da governança, sobre a questão de, como o Luca falou, de ter múltiplos centros de tratamento de incidentes da RNP ou do Cert, ou (Ininteligivel). Enfim. E a gente já faz alguns conselhos, né? Então a SBC já

tem um representante no Conselho da Nacional de Proteção de Dados. A gente faz parte também do Conselho de Diretor da RNP, do Conselho, é, tem conselheiros que representa o SBC no CGI, então é uma atividade que, que a sociedade já faz há bastante tempo e que trata, é, desse tema há bastante tempo. É, e um ponto que a gente pode contribuir, mais especificamente, é justamente essa questão da segurança. Da, da educação e cibersegurança, né? Primeiro eu queria parabenizar Marcelo e ao GSI porque a gente ficou muito feliz de, ao ler o projeto ter várias menções à academia, ao ensino, a pesquisa, e o desenvolvimento, e por muitas vezes a gente é relegado a, deixado de lado, né? E isso a gente ficou muito contente ao ler o documento, e aí foi, a gente ficou mais instigado ainda a saber como é que a gente pode ajudar, e a política nacional de cibersegurança. E uma das coisas que a gente está trabalhando, e essa é, para daqui a alguns meses isso vai estar pronto, é, a Comissão Especial junto com a diretoria da SBC trabalhou no referencial de um curso de graduação em cibersegurança. Então, esse referencial já tá pronto. Ele passou por um processo de 2 anos de maturação, de desenvolvimento. É, durante 2 meses, no final do ano passado e início desse ano, né, até o final de fevereiro, ele ficou aberto para uma audiência, para audiência pública. Então, foram recebidos vários comentários que a Comissão de Educação da SBC levou em consideração, e agora tá em fase final de regulamentação pela Diretoria da SBC, e o objetivo é fazer com que ele faça parte do, da DCN, né, das, se torne uma diretriz curricular do MEC, e esse esse referencial possa servir de base para cursos de graduação, de bacharelado em cibersegurança. Então essa é uma área que a gente pode contribuir, aproveitando a transparência ali. É uma contribuição grande da, da comunidade de segurança da Seseg da SBC. Então, queria novamente deixar aqui a, o nosso conhecimento técnico, né, que é a melhor arma que a gente tem para combater a cibersegurança já disponível ao GSI, a quem tiver interesse também de contribuir à Seseg. Muito obrigado e bom dia a todos.

SR. JEFFERSON NASSIF - Uma boa tarde a todos. Meu nome é Jefferson Nassif. Eu sou chefe da Assessoria Internacional do Ministério das Comunicações. O Ministério das Comunicações deve fazer apresentação de suas contribuições formalmente, então falo aqui mais na qualidade de um estudioso do assunto, e a experiência de quem passou pela relatoria da CPI, né, do Snowden em 2014, depois colaborou para a Resolução de Segurança Cibernética da Anatel, e depois aqui também, no próprio Departamento de Segurança da Informação em 2019, escrevendo a Estratégia de Segurança Cibernética E-Ciber. É, primeiro parabenizo pela iniciativa, Malagutti. É excelente podermos estar aqui discutindo abertamente esse tema tão, tão importante, e por algumas inovações, inclusive esse glossário, que realmente

vai trazer luz sobre assuntos e dúvidas que pairavam o tempo em que estavam aqui em 2019, a começar pelo uso da palavra segurança cibernética ou segurança da informação. Havia muita disputa sobre qual termo deveríamos usar naquele tempo, e é bom que a palavra segurança cibernética tenha sido aquela escolhida, porque realmente, na minha opinião, é a mais adequada. Então, parabéns mais uma vez pela, pela estrutura que foi desenhada para, para política nacional, pela, pela ideia de construção da, da Agência Nacional de Segurança Cibernética, que também já era uma previsão que depois foi excluída da Estratégia de Segurança Cibernética. Bem. Meus são uns 5 ou 6 contribuições, bem rapidamente. Primeiro, com relação aos princípios, na sessão 2, no artigo quinto, acho importante que seja incluído os conceitos relacionados à proteção dos Direitos Humanos, fundamentais ali, logo no começo do texto. Com relação à sessão no artigo 14 inciso em seu segundo, é, também conhecido com o colega que me antecedeu, com relação ao papel opinativo e consultivo desse comitê. Não deve ter, na minha opinião, um papel normativo, que é, esse papel normativo deverá caber exclusivamente a Agência Nacional de Segurança Cibernética, e assim você evita sobreposição de atribuições. É, existe uma menção muito importante a análise de impacto regulatório. A qual concordo. Ação internacional, o artigo primeiro da sessão primeiro, parágrafo segundo, é, isso ao longo do texto da avaliação de vocês acertadamente confere uma atribuição importante a cooperação internacional, mas essa importância não está devidamente, é, preenchida, desenhada na estrutura da Agência Nacional de Segurança Cibernética. Entendo pois que deve haver uma diretoria internacional específica para tratar desse assunto, extremamente importante. Com relação a certificação dos produtos, também já, já foi precedido nesse ponto, mas expresso mesmo assim, pode haver aqui um conflito de competências com a Anatel porque a atribuição de certificação de produtos de telecomunicações cabe a Agência Nacional de Telecomunicações. Valeria a pena detalhar, especificar melhor o que caberá, com relação a certificação de produtos pela ANCiber, se vai ser de produtos ou de serviços, e mesmo assim valeria a pena ainda analisar melhor o que é certificação de serviços, já que existe certa polêmica com relação a certificação de software. E por último as taxas de fiscalização, né? Também fui precedido. É importante deixar ressaltado que deve haver uma previsão legal, um instrumento específico tal como a taxa de fiscalização que na Anatel é chamada de Fistel. Existe uma tabela específica, uma lei específica determinando quais são essas taxas, e que dará a previsibilidade para os administrados. Muito obrigado.

SRª ANDRÉIA VATINÊ - Bom dia a todos. Meu nome é Andréia Vatinê. Estou aqui representando o grupo Thales e também a Omnisys, que é uma empresa

subsiária da Thales brasileira aqui no Brasil. Acho que primeiramente eu gostaria de agradecer, é, um orgulho ver que essa iniciativa que traz né, a gente vai trabalhar nessa política, mas estamos aqui todos. Tem, né, a gente vê a entidades do governo, iniciativas privadas. Eu acho que juntos somos mais fortes, então, acho que para fazer acontecer, estamos no caminho certo. Aqui a minha pergunta, principalmente com relação na minuta, consta a criação, é, do Comitê Nacional de Cibersegurança, no caso, né? E nessa, nesse, na parte da minuta é comentado que teremos diversos representantes, né, de vários mistérios, também de empresas privadas. Eu acho que faz falta algum tipo de informação voltado aos critérios. Então quais são os critérios, por exemplo, para uma empresa privada participar? E além disso, eu percebi que foram elencados, assim. Deve ter uma limitação de pessoas, obviamente, até porque são diversos grupos envolvidos. Mas acho que no caso da iniciativa privada, por exemplo, nós na Thales, a gente tem serviços, por exemplo, de proteção de dados, serviço de soluções de defesa. Aqui se falou muito em iniciativas de ciberseguranças, de políticas nacionais, da Europa, dos Estados Unidos. Mas até do lado, né, do Brasil, na Colômbia, em outros países da América Latina, a gente tem trabalhado também nessas iniciativas, e eu vejo que a participação de empresas privadas podem agregar com os aprendizados, né, lições aprendidas, com as boas práticas que a gente tem trabalhado, né, as tendências do mercado. Então, basicamente, esse é o meu comentário. Agradeço a todos. Obrigada.

SR. MARCELO MALAGUTTI, MESTRE DE CERIMÔNIA - Na Linha do que tava explicado nas regras, de que nós poderíamos responder perguntas, a colega fez uma pergunta. A questão da representação, da forma de representação ainda não tá muito bem definida porque isso depende um pouco de uma decisão presidencial, eu diria. Tipicamente, os nossos conselhos e comitês, eles têm uma indicação feita pelo Executivo. Nós inovamos um pouco no caso do CNCiber, do nosso Comitê Nacional, onde cada órgão pode designar a pessoa que pretende que deseja, que represente aquele órgão. A não ser no caso da, do grupo laranja ali, que é o grupo da sociedade civil, onde nós temos lá em cima, se eu estou conseguindo ler direito, as empresas. E aí, seria, por exemplo, o caso da Thales se candidatar, seria naquele grupo. Nós temos pesquisa, tecnologia, que seria basicamente a academia, centro de pesquisa, Sociedade Brasileira de Computação. Depois nós temos um outro grupo (Ininteligível) críticas, na hora de, por exemplo a Anatel, ANEEL, e qualquer outro representante de infraestruturas críticas. E por fim, nós temos, como eu disse, os órgãos como o CERT.br, como o CGI, como a RNP, etcetera. Então são grupos distintos com representações distintas, mas infelizmente nós não temos como fazer uma previsão legal agora de como vai ser a nomeação, a

candidatura, a concorrência. Eu citei a pouco aqui, o Professor Barone fez parte do Conselho Nacional de Educação. O Conselho Nacional de Educação eu conheço bem a estrutura. Eles têm um conjunto de regras de indicação em que as instituições de ensino superior ou de ensino fundamental indicam as pessoas, forma-se uma lista, e o presidente nomeia. Então assim, esse é um processo, eu tô usando como exemplo, mas é um processo comum para os demais comitês. Chega digamos uma lista tríplice, aqui no caso tem que ser um pouco maior porque são 3 dos membros, mas chega uma lista e o presidente escolhe e nomeia as pessoas que ele entende que, para aquele momento político do país e tal, é, são as pessoas adequadas. Nesse momento, a gente não tem como avançar para responder a sua pergunta. É, pois não.

SR. ZÉ BALAS - Boa tarde, senhoras e senhores, e também os que estão nos vendo no YouTube. Eu me chamo Zé Balas. Eu sou da secretaria de governo. Tô representando o secretário de José Humberto, e o Governo do Distrito Federal de uma certa forma. Agradeço todo mundo que está aqui, né, fazendo essa união de esforços aí para uma coisa que a gente está bastante atrasado em relação ao mundo, e é uma ameaça real e constante aí. Não é mais ficção. Eu vim falar sobre a importância de incluir a juventude que tem conhecimentos na área de programação e de tecnologia muito avançados, certo? Vivemos em uma era digital onde a cybersegurança é um desafio constante. Precisamos aproveitar o potencial desses jovens que possuem expertise e visão única sobre o mundo virtual. A juventude pode trazer soluções inovadoras, identificar vulnerabilidades, e desenvolver medidas preventivas para proteger nossos sistemas e dados. Para isso, é fundamental criar oportunidades de aprendizado e colaboração, como feiras e hackatons, onde eles possam compartilhar conhecimentos e trabalhar em conjunto. Também devemos investir em programas de educação e treinamento, adaptando os currículos, currículos escolares e fornecendo recursos adequados. Ao incluir essa juventude na cybersegurança, fortaleceremos nossas defesa contra ameaças virtuais e criaremos um ambiente mais seguro para a inovação e proteção digital. Devemos apoiar e incentivar essa inclusão, promovendo a colaboração entre jovens talentosos e as organizações responsáveis pela segurança cibernética. E junto a gente pode construir esse futuro, estar mais preparado para os desafios emergentes. Só isso. Muito obrigado.

SR. MARCELO MALAGUTTI, MESTRE DE CERIMÔNIA - Novamente, no contexto da resposta, é só observar que o canto inferior aqui direito prevê uma gerência específica na diretoria desse tipo de educação, para a realização de exercícios e simulações entre os quais hackatons e equivalentes.

SR. RODRIGO ROSA - É, boa tarde a todos. Eu me chamo Rodrigo Rosa. Sou Gerente de Defesa Cibernética da Petrobras. Venho aqui representar a Petrobras nesse, nesse processo, parabenizar o GSI, e colocar a Petrobras à disposição. Nós já colaboramos com o GSI na troca, né, de informações sobre incidentes cibernéticos, né, compartilhamento de inteligência. Lideramos uma rede aí que roda sobre o MISP, né, que é uma plataforma chamada Malware Information Sharing Platform, trocando uma série de sensores, né? A Petrobras investe bastante em sensores no ecossistema de defesa cibernética, e a gente tem essa cultura de compartilhar. Então, é, o papel fundamental da, do GSI, puxando, né, esse trabalho, e nos colocamos aqui, enfim, a disposição. Somos filiados ao FIRST assim como o CTIER, né, o Fórum Mundial de Times de Resposta de Incidente, e venho colocar aqui a gente como, além de manifestar o interesse institucional da companhia, né, em participar inclusive aí numa das cadeiras como infraestrutura crítica. Obrigado.

SR. MARCELO MALAGUTTI, MESTRE DE CERIMÔNIA - A palavra está franqueada. Se mais alguém quiser fazer sua contribuição, sua manifestação, senão vou apenas repetir aqui. Estamos recebendo sugestões até às 23:59 de hoje. Eu não posso, é, atender diretamente aqui o pedido que foi feito de conceder mais prazo. Não tenho competência, não tenho autonomia para fazer isso sozinho, mas posso assegurar que todas as contribuições que chegarem, mesmo que cheguem um pouco depois disso, nós vamos tentar encaixar no nosso processo, é, de respostas dentro da medida do possível, se nós tivermos braços e pernas suficientes para darmos conta disso tudo dentro do prazo legal. É, não havendo mais nenhuma intervenção, nenhuma manifestação de algum outro interessado, é, coube a mim aqui a tarefa de considerar encerrada essa audiência e agradecer novamente, muitíssimo, a contribuição, a dedicação dos senhores aqui. Já estamos uma hora avançada. Todo mundo já com fome. Mas do meu ponto de vista, participando do processo, considero que foi extremamente gratificante, extremamente produtivo a participação dos senhores e senhoras. Todas as contribuições aqui vão nos ajudar, certamente, a melhorar bastante o nosso projeto. Muito obrigado. E, como dizem os jovens, tamo junto.