PNCiber – Apresentação do Projeto

Este documento explica algumas das opções adotadas na redação do projeto de lei que institui a Política Nacional de Cibersegurança (PNCiber) e o Sistema Nacional de Cibersegurança (SNCiber).

1 DA EXPOSIÇÃO DE MOTIVOS

1.1 Da Urgência e Relevância

Mesmo escrita em 4 folhas, o que a caracteriza como um tanto longa para a média de suas congêneres, a exposição de motivos expõe de forma sucinta um histórico do apontamento da urgente e relevante necessidade de uma Política Nacional de Cibersegurança (PNCiber), de um sistema nacional, e de uma agência que regule as atividades de cibersegurança no país.

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

A proposta abrange e busca congregar não apenas o poder executivo federal, mas também os demais poderes, em todas as esferas (federal, estadual e municipal), bem como o setor produtivo e a academia, norteando (ou "suleando", como preferem alguns) os esforços nacionais em cibersegurança, alinhada com os diagnósticos de diferentes instituições como o Senado Federal, o TCU, o Fórum Econômico Mundial, a FGV e outros não menos importantes e relevantes.

2 DA PROPOSTA "INTEGRADA"

2.1 Uma Política com Seus Instrumentos ("Junto, mas Não Misturado")

Por anos pensou-se em buscar primeiro a implementação de uma Política, para só então se buscar a criação das instituições que concretizariam tal política. Foi apenas recentemente, com a crescente urgência e relevância da temática, que se passou a advogar, e perseguir, uma proposta única, que evitasse a necessidade de uma "serialização" das ações de submissão e aprovação de dois instrumentos, praticamente dobrando o esforço de análise e aprovação pelo Congresso Nacional.

Outrossim, a presente proposta reflete esta opção de concentrar esforços num único instrumento legal. Entretanto, como forma de manter a Política, que tem um propósito mais conceitual, apartada de seu instrumento operacional central, a Agência, esta é criada na forma de um anexo ao projeto de lei.

3 DO MODELO INSTITUCIONAL ADOTADO

3.1 Da Conformidade com as Melhores Práticas Político-Institucionais Mundiais

Nossa proposta incorpora as melhores práticas internacionais à "cultura institucional" brasileira. De forma similar ao ocorrido na Lei Geral de Proteção de Dados (LGPD), amplamente influenciada pela GDPR europeia, nosso modelo central foi aquele proposto pelo Parlamento Europeu, a diretiva NIS2, de dezembro de 2022. Esse modelo pressupõe a existência de um órgão central nacional, no nosso caso a Agência Nacional de Cibersegurança (ANCiber), de um "ente" fiscalizador, na nossa proposta o Comitê Nacional de Cibersegurança (CNCiber) e de um Gabinete de Gerencimento de (Ciber)Crises, que nossa proposta denominou GGCiber.

Mas, embora fundacional para nossa proposta, a NIS2 não é o único documento considerado. Foram analisados ainda o modelo da União Internacional de Telecomunicações (UIT/ONU) e o Modelo de Maturidade proposto pela Universidade de Oxford, adotado pela OEA como referência.

Os conceitos presentes nesses 3 modelos foram, no melhor de nossas capacidades, agregados, debatidos e adaptados à realidade jurídica, política e cultural nacionais.

3.2 Da Opção pelo Modelo de Agência Regulatória

A opção pelo modelo de Agência Regulatória decorre da percepção de que o arcabouço jurídico deste instituto é bem consolidado. Não menos relevante é o fato de que este modelo regulatório é bem acolhido pela cultura institucional, ou "institucionalismo histórico" de nossa sociedade, onde a autonomia confere considerável estabilidade às instituições quanto a eventuais instabilidades políticas ou econômicas. Outros modelos recentemente testados se mostraram frágeis nos quesitos acima mencionados, e foram (ou vêm sendo) gradualmente adaptados para se aproximarem do modelo de agências regulatórias.

3.3 Da Opção pelo Complexo Nacional de Cibersegurança ante as Infraestruturas Críticas (ICs)

Escolhido o modelo jurídico a ser adotado, coube-nos atentar para a transversalidade do cibersegurança, abarcando praticamente todos os setores socioeconômicos das sociedades modernas, o que foi resolvido de uma forma que foi entendida como simples e, por que não, elegante. Essa forma se adequa aos mais modernos conceitos utilizados por grande parte dos países que constituem o "estado da arte" na temática, focando não em "verticais de negócios" ou setores econômicos, mas em "serviços essenciais" para o bom funcionamento da sociedade.

Exemplificando a diferença entre este modelo e aquele das ICs, pautamo-nos por 3 casos nacionais emblemáticos. Primeiro, é senso comum que a capacidade de aplicação da justiça em um território é uma das premissas basilares do conceito de soberania no direito internacional. Ciberincidentes (ou mesmo ciberataques) realizados contra instituições judiciais brasileiras, como o STJ (federal) e o TJDFT (distrital/estadual), apenas para citar dois casos ocorridos aqui em Brasília, inviabilizaram a aplicação da justiça por semanas. Poder-se-ia argumentar que "bastaria acrescentar a justiça" como uma IC para a manutenção do modelo de regramento anterior. Talvez sim, mas provavelmente não.

Recorremos, então, a outro caso emblemático: o Cartão Nacional de Vacinação (ou Certificado Nacional de Vacinação). Um ciberincidente envolvendo o ConecteSUS, sistema do Ministério da Saúde, indisponibilizou a emissão de certificados de vacina em plena pandemia, gerando enormes transtornos para a população por cerca de um mês, limitando um dos direitos humanos mais fundamentais: aquele de ir e vir. Seria o caso de se incluir o Ministério da Saúde como uma IC também? Ou apenas o de se considerar o ConecteSUS como um serviço essencial?

Não é difícil imaginarmos outros casos similares. Em anos recentes, por duas vezes ao menos, a Polícia Federal deixou de emitir passaportes por falta de orçamento para tal. A indisponibilidade do serviço gerou grandes transtornos, e rapidamente foram feitos aportes para o restabelecimento do serviço. Imaginemos, no entanto, que este serviço ficasse indisponível por um mês em decorrência de um ciberincidente, como nos casos do STJ e do ConecteSUS citados há pouco. Seria o caso de se considerar o MRE também como uma infraestrutura crítica?

Por indução, pode-se obter exemplos envolvendo dezenas de serviços de outras instituições que, se consideradas ICs, levariam praticamente todas as instituições a serem consideradas críticas. Parafraseando a máxima popular que diz "onde tudo é prioritário, nada é prioridade", pode-se concluir que "onde tudo é IC, nada é crítico".

Por conseguinte, o modelo proposto foca nos serviços considerados essenciais mais que na vertical em que ele se encontra. Aquele serviço específico deve ter atenção especial de seus gestores e da ANCiber.

De outra parte, como também é senso comum, a gestão de ICs envolve muitos outros fatores além da sua cibersegurança.

Logo, transpondo-se para uma simples lógica de conjuntos, os conceitos de ICs e Serviços Essenciais representam dois conjuntos que não são disjuntos, mas que possuem uma zona de interseção muito menor que qualquer um deles individualmente

3.4 Da Vinculação ao GSI

O modelo institucional brasileiro exige que uma Agência, enquanto autarquia, e assim entidade da Administração Indireta, seja vinculada "ao Ministério em cuja área de competência estiver enquadrada sua principal atividade"[1]. A ANATEL se vincula ao Min. das Comunicações. A ANVISA ao Min. da Saúde. A ANCine ao Min. da Cultura. A ANP, a ANEEL e a ANM ao Min. das Minas e Energia. A ANTAQ e a ANTT ao Min. dos Transportes e a ANAC ao Min. dos Portos e Aeroportos.

A ANCiber, então, tem que ser vinculada a um Ministério. Como se trata de uma questão afeta à segurança nacional, a opção mais adequada é pelo Ministério responsável pelo tema, o GSI. Ainda, desde 2010 o GSI está a cargo da cibersegurança da Administração Pública Federal, o que foi reiterado pela atual administração[2]. Outrossim, acumula tradição e experiência na temática. Por conseguinte, o GSI é o órgão natural de vinculação da ANCiber.

Não obstante, há que se ressaltar que o modelo institucional das Agências Reguladoras concede ampla autonomia administrativa e financeira a elas, tornando-as pouco permeáveis a interferências externas, com seus diretores sabatinados pelo Senado Federal antes de sua nomeação.

4 DA TERMINOLOGIA ADOTADA

4.1 Uma "Língua Viva"

Conquanto todas as línguas faladas sejam "vivas", evoluindo ao longo do tempo, no tocante à cibersegurança ela é ainda mais viva, dinâmica. À medida que o setor avança novos termos são apresentados, enquanto outros inicialmente populares vão sendo abandonados, por serem posteriormente entendidos como errôneos em suas acepções inicialmente utilizadas.

4.2 Os Documentos da União Europeia em Língua Portuguesa

Já em 2016, a primeira versão da diretriz NIS adotava a prática de eliminar o adjetivo "cibernética", em suas flexões de gênero e número – cibernética(s) ou cibernético(s) – substituído pelo prefixo *ciber* associado ao substantivo ao qual se refere. Tal prática, em conformidade com as regras

[1] Decreto-Lei 200, de 25 de fevereiro de 1967, Artigo 4º, Parágrafo Único.

[2] Decreto 11.331, de 01 de janeiro de 2023, Anexo I, Artigo 1º, V.

do Novo Acordo Ortográfico da Língua Portuguesa, é também utilizada pelo Secretário Geral da ONU António Guterres.

Essa abordagem elimina riscos de equívocos pelas complexidades inerentes à língua, como nos casos em que se escreve "segurança e defesa cibernética", onde o adjetivo "cibernética" é aplicável apenas à defesa, deixando o termo segurança em sua acepção mais abrangente, sem qualificação. Para se evitar tal problema, frequente, uma forma seria usar "segurança e defesa cibernéticas". Ou então a adoção do padrão europeu, "cibersegurança e ciberdefesa", tornando clara, inequívoca e não-ambígua a intenção. Dentre os termos correntemente em uso, na NIS2, por exemplo, temos ciberespaço, ciberameaças, ciberataque, ciberatividade, cibercrime, cibercriminalidade, cibercrise, cibersegurança, ciberdefesa, ciberdissuasão, ciber-higiene, ciberproteção e ciber-resiliência, dentre outros.

4.3 Da Padronização do Novo Acordo Ortográfico da Língua Portuguesa

Retornando ao Novo Acordo Ortográfico da Língua Portuguesa, é importante observar que foi feito um enorme esforço, e investimento, pelos países integrantes da Comunidade de Países de Língua Portuguesa (CPLP) para uniformizarmos nossa língua, e não há muito sentido prático em nos distanciarmos dos demais países na forma de redação de documentos oficiais.

4.4 Da Redação Acadêmica e da Prática Profissional

Adicionalmente, a comunidade acadêmica e os praticantes da cibersegurança usualmente adotam a forma das "ciber-coisas" adotada pelos irmãos portugueses, e com considerável frequência adotando a pronúncia anglófona "cyber", mesmo quando leem "ciber". Assim, a realidade se impõe.

4.5 Dos Glossários do GSI e MD

Quanto aos Glossários do GSI e do MD, cumpre observar que ambos são de aplicação restrita, e definidos por meio de portarias de seus respectivos ministérios. Portanto, facilmente ajustáveis quando da existência de uma lei nacional que uniformize a sintaxe e a semântica da redação oficial.

PNCiber – Exposição de Motivos

Este documento apresenta uma exposição de motivos para a urgência e relevância da criação da Política Nacional de Cibersegurança (PNCiber) e do Sistema Nacional de Cibersegurança (SNCiber).

1 ANTECEDENTES

1.1 CPI da Espionagem Eletrônica[1]

Na esteira das denúncias de Edward Snowden sobre espionagem cibernética em larga escala, foi publicado, em abril de 2014, o relatório da CPI da Espionagem Cibernética no Senado Federal, com um diagnóstico bastante denso do panorama da cibersegurança brasileira. No documento, a Comissão indicou que "a escolha do Brasil deveu-se à fragilidade de proteção" dos sistemas e dados e que o incidente se tratou "uma invasão de soberania sem precedentes na história do Brasil".

Outro apontamento foi que o Brasil desenvolveu uma dependência crítica de software e hardware para o funcionamento de todos os setores críticos para o país, dentre os quais telecomunicações, transportes, energia, saúde, educação, defesa, comércio, mercado financeiro e radiodifusão.

A Comissão observou que "cada indivíduo é responsável pela proteção ao conhecimento e por sua segurança, enquanto ao Estado compete a defesa dos interesses da sociedade e a proteção aos conhecimentos sensíveis". Mais além, estipulou que "a exemplo de outros países que já implementaram órgãos específicos para a segurança, cabe ao Brasil discutir a possibilidade de **criar uma agência no âmbito da administração pública federal para segurança cibernética**" (grifo nosso). Isso posto, recomendou que, de imediato, o Estado se organizasse para discutir possibilidades que levassem "à **centralização institucional da segurança cibernética na estrutura do governo brasileiro**", concedendo-se a um "órgão governamental específico a atribuição de responsabilidades" sobre o tema da cibersegurança nacional (grifos nossos). A esse órgão caberia a "organização do setor cibernético brasileiro, a responsabilidade de propor políticas e regulamentos voltados para a totalidade da segurança cibernética", excetuando-se os aspectos relacionados à ciberdefesa, "que devem restar ao Ministério da Defesa", mas "tirando proveito dos ganhos sinérgicos da atuação em conjunto".

Dentre as recomendações da douta Comissão ao Poder Executivo, no âmbito da competência dessa Agência, constaram, entre outras:

- Fomento à Pesquisa, Desenvolvimento e Inovação nacionais.
- Fortalecimento de uma indústria nacional de cibersegurança.
- Promoção da cultura de cibersegurança.
- Criação de uma escola ou universidade de cibersegurança.
- Estabelecimento de convênios de cooperação internacional.

O relatório indicou, também, que "a proteção do ciberespaço deve ser encarada de forma estratégica pelo Estado, pois desempenha papel essencial, tanto para a segurança e soberania nacional,

[1] Relatório da CPI da Espionagem Eletrônica, Diário do Senado, Ano LXIX - Sup. "C" ao Nº 51 - quinta-feira, 17 de abril de 2014.

como para a integração cultural e o desenvolvimento econômico", e que "**o país deve discutir e elaborar uma Política Nacional de Segurança Cibernética**" (grifo nosso).

1.2 Estratégia Nacional de Segurança-Cibernética - *e-Ciber*[2]

A despeito da urgência e relevância apontadas pelo Senado, o País pouco avançou na temática desde então. Só em 2020 o Brasil publicou sua primeira Estratégia Nacional de Segurança Cibernética, a e-Ciber, sendo um dos últimos países do G20 a fazê-lo.

A e-Ciber teve o mérito de recolocar a cibersegurança em evidência 6 anos após a CPI da Espionagem, mas foi muito criticada pela sociedade por quatro motivos principais:

- Foi publicada por meio de um Decreto Presidencial, limitando seu alcance à esfera do Poder Executivo federal, contrariando recomendação do Senado por abrangência nacional;
- Foi elaborada sem o suporte de uma Política Nacional de Cibersegurança que apontasse os objetivos políticos pretendidos, outra das recomendações do Senado;
- Não alocou responsabilidades pelas ações propostas, também uma das recomendações da CPI;
- Excluiu explicitamente a ciberdefesa de seu escopo, algo não encontrado em suas congêneres de nenhum outro país, e que, novamente, desconsiderava uma recomendação do Senado.

A despeito de suas limitações, a e-Ciber destacou diversas ações estratégicas importantes para o País, dentre as quais o fortalecimento da governança em cibersegurança, por parte do setor público e do setor privado por meio de um modelo nacional centralizado, refletindo uma das recomendações do Senado de 2014.

A e-Ciber também trouxe dados preocupantes quanto ao ciberespaço brasileiro. Primeiro, ela apontou o Brasil como o 2º país do mundo em prejuízos decorrente de ciberataques. Não obstante sua população seja a 6ª do mundo, e sua economia, em paridade de poder de compra, seja a 7ª ou 8ª. Em 2018, ciberincidentes teriam resultado em perdas de USD 22,5 (vinte e dois bilhões e meio de dólares americanos), ou perto de BRL 120 bilhões (120 bilhões de reais). Não há dados que indiquem que esse valor tenha diminuído desde então. Pelo contrário, Relatório Técnico do Laboratório de Segurança Cibernética da Febraban apontou que os ciberataques nos Brasil aumentaram 94% no primeiro semestre de 2022 em relação ao mesmo período de 2021.

Por fim, a e-Ciber tem vigência para o quadriênio 2020-2023, devendo ser atualizada no início de 2024, sendo importante que tal revisão se baseie numa Política Nacional de Cibersegurança.

1.3 Proposta de Emenda Constitucional 03/2020 do Senado Federal[3]

Concomitantemente, a PEC 03/2020 do Senado Federal, propôs delimitar as competências sobre ciberdefesa e cibersegurança no País, apontando que "em razão da oferta cada vez maior de serviços públicos digitais, é preciso imprimir um sistema de normas cogentes, de aplicação inafastável". Ainda, ressalta que "em tempos de ciberterrorismo, guerra cibernética, aumento dos índices de crimes cibernéticos na sociedade", "inclusive com grave desestabilização social, é preciso

[2] Decreto 10.222, de 5 de fevereiro de 2020.

[3] https://www.congressonacional.leg.br/materias/materias-bicamerais/-/ver/pec-3-2020.

elevar o tema ao nível de prioridade máxima do Estado brasileiro, responsabilidade essa que compete a todos os entes federados e a todos os Poderes republicanos".

Não obstante, talvez o ponto mais relevante dessa PEC seja que a peça exemplifica o entendimento da cibersegurança e ciberdefesa como um tema de Estado, tendo sido assinada por senadores com trajetórias político-partidárias de espectro variadíssimo.

1.4 Relatório da OEA - Modelo de Maturidade[4]

Em agosto de 2020 foi publicada uma avaliação da maturidade da cibersegurança brasileira, baseada no Modelo de Maturidade desenvolvido pela Universidade de Oxford, do Reino Unido.

Com base no relatório das capacidades do Brasil em 2020 e do Reino Unido em 2015, foi possível elaborarmos a tabela comparativa apresentada abaixo.

Estágio	Qtd	BR (2020)	UK (2015)
Formativo	17	71%	14%
Estabelecido	7	29%	62%
Estratégico	0	0%	14%
Dinâmico	0	0%	10%

Depreende-se da tabela que, em 2015, o Reino Unido já tinha cibercapacidades muito mais avançadas do que aquelas apresentadas pelo Brasil em 2020. Entretanto, dados do governo britânico mostram que nesses cinco anos eles investiram em média BRL 1,35 bilhão anualmente, enquanto a média brasileira no mesmo período foi de apenas BRL 15 milhões. É plausível considerar que a diferença de investimentos tenha acentuado ainda mais o débito tecnológico do Brasil.

1.5 Lista de Alto Risco na Administração Pública - TCU[5]

Em junho de 2022, o TCU elaborou a Lista de Alto Risco na Administração Pública, no qual figura a Cibersegurança. Observa o relatório que "segundo o portal do governo digital brasileiro, em 2021, 73,1% dos serviços públicos prestados pelo governo federal já eram totalmente digitais, o que corresponde a 3.598 serviços". Se considerados também aqueles parcialmente digitais, o percentual chega a 86,7%. "Esses números por si só mostram a dimensão dos riscos e o prejuízo que falhas de segurança e indisponibilidade de serviços podem acarretar".

Do relatório consta também que o principal órgão responsável pelo tema, o Gabinete de Segurança Institucional da Presidência da República (GSI/PR), e "o arcabouço normativo vigente, em especial os decretos que orientam a atuação, não alcançam a Administração Pública como um todo, limitando-se, apenas, ao Poder Executivo federal". E que existe, portanto, carência de estrutura (órgão ou entidade) com autoridade ampla; atos normativos que regulem os temas em todo o território nacional, incluindo os setores público e privado; investimentos em segurança da informação e segurança cibernética, áreas de importância estratégica para o país.

[4] Revisão da Capacidade de Cibersegurança da República Federativa do Brasil, Oxford GCSCC/OEA, 2021.

[5] Lista de Alto Risco na Administração Pública, TCU, 2022.

1.6 Relatório da Transição[6]

Em dezembro de 2022, o Gabinete de Transição do governo eleito apontou, em seu relatório final, que o Brasil enfrenta "riscos de segurança cibernética e de apagões na agenda de governo digital".

Nesse contexto, a atual administração determinou, já em seu primeiro dia, a criação da Secretaria de Segurança da Informação e Cibernética (SSIC), composta pelo Departamento de Segurança da Informação e Cibernética (DSIC), o antigo DSI, sinalizando uma elevação do status do tema. Concomitantemente, nomeou-se um Assessor Especial do GSI dedicado à consolidação dos esforços em andamento para a criação de uma proposta inicial da Política Nacional de Cibersegurança.

1.7 Debate no Meio Acadêmico

Sinais da relevância e urgência do tema não vêm apenas da administração pública. Em fevereiro de 2023, na defesa da tese de doutoramento intitulada, "Em Busca de uma Estratégia Nacional de Segurança Cibernética: Marco Legal e Autoridade Nacional de Segurança Cibernética", a Vice-Presidente da Associação Brasileira de Estudos de Defesa (ABED) na gestão 2020-2022, membro da banca, defendeu a proposta de criação de uma "Autoridade Nacional" de cibersegurança contida na tese, e argumentou que talvez fosse o caso dessa "autoridade" ser até mesmo um ministério, dada a relevância da temática para a sociedade brasileira. Argumentos similares foram ouvidos de pesquisadores e empresários do setor presentes ao I Encontro da Rede Nordeste de Estudos Estratégicos e Inovação, realizado em março de 2023 em Pernambuco.

Também em março, a FGV Direito, no Rio de Janeiro, publicou o relatório "Cibersegurança: Uma Visão Sistêmica Rumo a uma Proposta de Marco Regulatório para um Brasil Digitalmente Seguro", na qual apontou que, em 2023, a falta "de uma Agência Nacional de Cibersegurança e de um sistema capaz de preservar a cibersegurança nas suas diferentes dimensões" não é aceitável.

1.8 Relatório de Riscos Globais do Fórum Econômico Mundial de 2023[7]

Em janeiro de 2023 o Fórum Econômico Mundial (WEF) apresentou seu Relatório de Riscos Globais, no qual afirma que "a tecnologia exacerbará as desigualdades, enquanto os riscos da segurança cibernética continuarão sendo uma preocupação constante". O relatório aponta que o "setor de tecnologia estará entre os alvos centrais de políticas industriais mais fortes e maior intervenção estatal".

O WEF apontou também que muitas novas tecnologias "são de propósito geral com aplicações civis, mas também são um multiplicador de força do poder militar, aprimorando as capacidades de armas autônomas, guerra cibernética e capacidades defensivas". Indicou, também, que "novas tecnologias mudarão a natureza da ameaça à segurança nacional e internacional, com aumento de conflitos em vários domínios que obscurecem a definição de guerra convencional. "Crime cibernético generalizado e insegurança cibernética" é um novo elemento na lista dos 10 principais riscos mais graves da próxima década.

[6] Relatório Final, Gabinete de Transição Governamental, 2022.

[7] Global Risks Report 2023, World Economic Forum, 2023.

1.9 Cenário Internacional

Em dezembro de 2022, o Reino Unido atualizou sua Estratégia Nacional de Cibersegurança[8] publicada um ano antes, fundada sobre cinco pilares:

- Fortalecimento do ecossistema cibernético do Reino Unido, aprofundando a parceria entre governo, academia e indústria.
- Construção de um Reino Unido digital resiliente e próspero, reduzindo os riscos cibernéticos às empresas e cidadãos.
- Liderança nas tecnologias vitais para o poder cibernético, com a construção de capacidade industrial e desenvolvimento de estruturas para proteger tecnologias futuras.
- Promoção da liderança e influência global do Reino Unido para uma ordem internacional mais segura, próspera e aberta.
- Detecção, interrupção e dissuasão de adversários.

A atualização do documento foi publicada também em japonês, chinês, francês, russo, espanhol e árabe, denotando que o Reino Unido deseja restringir margens de interpretação de um texto escrito apenas em inglês, bem como estender sua influência sobre outras nações.

Em dezembro de 2022, também, o Parlamento Europeu publicou uma nova diretiva de cibersegurança para a União Europeia (2022/2555[9]) conhecida como Diretiva NIS2, que ampliou significativamente o escopo da Diretiva NIS (2016/1148), e restringiu a "margem de apreciação muito ampla relativamente à aplicação das obrigações nela estabelecidas em matéria de segurança e de notificação de incidentes" que os Estados-Membros tinham anteriormente, notadamente no tocante aos Serviços Essenciais.

De outra parte, em março de 2023, os EUA publicaram sua nova Estratégia Nacional de Cibersegurança[10], também alicerçada em 5 pilares:

- Aumentar a segurança intensificando a regulamentação das infraestruturas críticas.
- Buscar interromper e desarticular os agentes de ameaças à segurança nacional dos EUA
- "Moldar as forças do mercado" para impulsionar a segurança e a resiliência
- Exigir que o governo federal "alavanque investimentos públicos estratégicos em inovação, P&D e educação visando resultados economicamente sustentáveis que atendam ao interesse nacional".
- Aproximar os setores público e privado para obter maior visibilidade da atividade adversária e aumentar a velocidade de compartilhamento de inteligência e notificação de riscos e incidentes.

2 CONCLUSÃO

De todo o exposto, fica clara a relevância, bem como a urgência, para o País, da instituição de uma Política Nacional de Cibersegurança (PNCiber) para suprir as lacunas apontadas como necessárias desde ao menos 2014. Se as condições políticas e econômicas nacionais não permitiram a criação dessa

[8] https://www.gov.uk/government/publications/national-cyber-strategy-2022.

[9] Diretiva (UE) 2022/2555 do Parlamento Europeu e do Conselho, de 14 de dezembro de 2022, relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança na União.

[10] https://www.hsdl.org/c/abstract/?docid=875831.

política pública antes, sua ausência em um período em que a digitalização de serviços aumentou significativamente só aumenta a exposição do Brasil às ciberofensas. Portanto, a relevância e a urgência da implementação dessa política são mais presentes do que nunca antes.

Há uma convergência de opiniões, nacionais e internacionais, no sentido de que essa política deve instituir uma Agência Nacional de Cibersegurança, a ANCiber, com competências similares às de suas congêneres em dezenas de nações que constituem o "arco do conhecimento" no âmbito da cibersegurança. No contexto do arcabouço institucional brasileiro, a ANCiber deve ser instituída nos moldes de uma agência reguladora.

Assim sendo, o encaminhamento da proposta formulada trata-se de matéria de máxima urgência e de enorme relevância para a sociedade brasileira.

PROJETO DE LEI Nº XX, DE XX DE XXXXXXXXX DE 2023

Institui a Política Nacional de Cibersegurança e cria o Sistema Nacional de Cibersegurança.

CAPÍTULO I

DA POLÍTICA NACIONAL DE CIBERSEGURANÇA

Seção I

Disposições Gerais

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.

§ 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.

§ 2º Esta Lei estabelece competências relativas à cibersegurança nacional, sem prejuízo às demais competências do Comitê Gestor da Internet no Brasil sobre o modelo de governança da Internet, conforme disposto no Decreto nº 4.829, de 3 de setembro de 2003.

Art. 2 º. A Política Nacional de Cibersegurança é o documento de mais alto nível que orienta a atividade de cibersegurança no País.

Art. 3 º. As ações de ciberdefesa serão coordenadas pelo Ministério da Defesa por intermédio do Sistema Militar de Defesa Cibernética (SMDC).

Parágrafo único. As ações de cibersegurança e de ciberdefesa deverão, sempre que possível, ser planejadas e executadas de forma coordenada pelas instituições competentes.

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;

VII - ciberincidente (ou incidente cibernético): uma ciberofensa combinada ao ciberefeito real ou potencial dela resultante;

VIII - ciberdissuasão (ou dissuasão cibernética): conjunto de ações tomadas com vistas a desencorajar a ação de um potencial perpetrador de ciberofensas;

IX - ciberproteção (ou proteção cibernética): conjunto de medidas para neutralizar ciberofensas e ciberexplorações contrárias ao interesse nacional, podendo ser dos seguintes tipos:

a) passiva: medidas para evitar que as ciberofensas sejam bem sucedidas;

b) ativa: medidas para, uma vez sobrepujadas as proteções passivas, permitir a interrupção da ciberofensa.

X - Ciber-resiliência (ou resiliência cibernética): conjunto de medidas voltadas à redução do impacto dos ciberefeitos, decorrente da compreensão da impossibilidade de se garantir total eficácia das ações de ciberproteção, podendo ser desdobrada em duas vertentes:

a) operação degradada: manutenção da operação dos ciberativos atacados, mesmo que degradada, ou ainda a promoção de sua degradação controlada;

b) recuperação (ou restauração): retorno à operação normal dos ciberativos afetados no mais curto prazo possível.

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.

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

XIII - ciberataque (ou ataque cibernético): conjunto de ações voltadas à utilização das informações obtidas ou não por meio da ciberexploração para causar ciberefeitos;

XIV - cibersegurança (ou segurança cibernética): conjunto de ações voltadas à confidencialidade, integridade, autenticidade e disponibilidade de ciberativos, por meio da:

a) ciberdissuasão;

b) ciberproteção;

c) ciber-resiliência;

d) ciberinvestigação;

e) ciberexploração.

XV - ciberdefesa (ou defesa cibernética): ações coordenadas pelo Ministério da Defesa com a finalidade de:

a) assegurar a cibersegurança de ciberativos de interesse da defesa nacional; e

b) buscar superioridade no domínio cibernético sobre os ciberativos do oponente.

XVI - segurança da informação: ações que objetivam assegurar a confidencialidade, a integridade, a autenticidade e a disponibilidade das informações;

XVII - ciber-risco (ou risco cibernético): possibilidade de ocorrência de um ciberincidente;

XVIII - ciberinspeção (ou inspeção cibernética): ações para identificar ciberameaças.

XIX - ciberlogística (ou cadeia logística cibernética, ou cadeia de suprimentos cibernéticos): o processo de planejar, implementar e controlar a obtenção, o fluxo e o armazenamento eficiente e eficaz de bens, serviços e informações destinados à produção de ciberativos, ou o uso de ciberativos no fluxo de produção de bens e serviços em geral.

XX - mitigação: ações para suavizar, abrandar ou reduzir ciber-riscos e ciberefeitos;

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.

XXII - provedores de serviços essenciais: pessoas físicas ou jurídicas que provejam, operem ou mantenham serviços essenciais, a exemplo de órgãos ou entidades das administrações públicas, concessionários de serviços e operadores nacionais, sejam públicos, privados ou de economia mista.

Seção II

Dos Princípios

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;

II - coordenação, para assegurar a ciberproteção e a ciber-resiliência dos ciberativos que proveem suporte à sociedade brasileira;

III - prontidão tecnológica, para desenvolver cibercapacidades endógenas que garantam o provimento e o acesso ao estado da arte tecnológica, reduzindo o débito tecnológico do país no setor;

IV - autonomia, para afirmar o setor de cibersegurança como fator relevante para a garantia da soberania e dos interesses nacionais;

V - prevenção, para atuar de forma antecipada na identificação e mitigação de ciber-riscos;

VI - desenvolvimento, para afirmar o setor de cibersegurança como fator indutor do desenvolvimento nacional sustentável e duradouro;

VII - integração nacional, para consolidar parcerias entre entes públicos e privados visando assegurar abrangência e efeito sinérgico;

VIII - cooperação internacional, para fomentar o intercâmbio de boas práticas e de alertas sobre ciberameaças e ciberincidentes, o desenvolvimento de cibercapacidades e de medidas de confiança mútua em cibersegurança com outros países, seguindo a tradição universalista das relações exteriores do Brasil;

IX - diligência devida, para assegurar que o País se busque garantir que seus ciberativos não

sejam conscientemente usados para prejudicar outros Estados;

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;

Seção III

Dos Objetivos

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;

II - fomentar a ciberproteção e a ciber-resiliência do Poder Público, dos ciberativos de interesse e da sociedade como um todo;

III - desenvolver na sociedade brasileira a cultura de cibersegurança;

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;

V - promover a autonomia produtiva e tecnológica na área de cibersegurança;

VI - fomentar a participação do Brasil na cadeia produtiva global de produtos e serviços voltados à cibersegurança;

VII - promover o uso ético de ciberativos e das tecnologias a eles associadas no país;

VIII - fomentar o combate ao cibercrime;

IX - promover ações que contribuam para a segurança e para a estabilidade do ambiente digital global; e

X - incrementar a projeção internacional do Brasil e inserir o País em processos decisórios internacionais, para fazer valer os valores e os interesses nacionais.

Seção IV

Das Diretrizes

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.

Seção V

Dos Instrumentos

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.

CAPÍTULO II

DO SISTEMA NACIONAL DE CIBERSEGURANÇA

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.

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.

Seção I

Do Comitê Nacional de Cibersegurança

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.

Art. 14. Compete ao Comitê:

I - propor políticas, diretrizes, estratégias e normas relacionadas à cibersegurança nacional;

II - aprovar, por meio de resolução, os atos normativos concernentes à cibersegurança nacional;

III - recomendar ações a serem realizadas pela ANCiber;

IV - contribuir para a formulação, a execução e a avaliação do Plano Nacional de Cibersegurança;

V - aprovar:

a) a Estratégia Nacional de Cibersegurança;

b) o Plano Nacional de Cibersegurança; e

c) o Complexo Nacional de Cibersegurança.

VI - propor e regulamentar medidas indutoras e linhas de financiamento para fomento da pesquisa e desenvolvimento da cibersegurança nacional;

VII - propor medidas visando o desenvolvimento da cultura de cibersegurança no País;

VIII - propor iniciativas visando a adoção em nível nacional de boas práticas relativas à cibersegurança;

IX - manifestar-se sobre assuntos relacionados à cibersegurança relevantes para a segurança do Estado e da sociedade;

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.

Art. 15. O Comitê Nacional de Cibersegurança será composto por:

I - o Diretor-Geral da ANCiber;

II - um representante do Ministério da Justiça e da Segurança Pública;

III - um representante do Ministério da Defesa;

IV - um representante do Ministério das Relações Exteriores;

V - um representante do Ministério da Fazenda;

VI - um representante do Ministério do Planejamento;

VII - um representante do Ministério da Gestão e da Inovação em Serviços Públicos;

VIII - um representante do Ministério das Comunicações;

IX - um representante do Ministério da Ciência, Tecnologia e Inovações;

X - um representante da Comissão de Ciência, Tecnologia, Inovação, Comunicação e Informática do Senado Federal;

XI - um representante da Comissão de Ciência e Tecnologia, Comunicação e Informática da Câmara dos Deputados;

XII - um representante do Conselho Nacional de Justiça;

XIII - um representante do Conselho Nacional do Ministério Público;

XIV - um representante da Autoridade Nacional de Proteção de Dados;

XV - três representantes de entidades da sociedade com atuação relacionada à cibersegurança;

XVI - três representantes de entidades representativas das infraestruturas críticas;

XVII - três representantes de instituições científicas, tecnológicas e de inovação; e

XVIII - três representantes de entidades representativas do setor empresarial relacionado à área de cibersegurança.

§ 1º O Comitê será presidido pelo Diretor-Geral da ANCiber, que será substituído, em caso de impedimento, pelo seu substituto legal.

§ 2º Os representantes de que tratam os incisos II a XIII, bem como seus suplentes, serão nomeados pelos titulares dos órgãos ou entidades que representarão, para integrarem o Comitê por até 2 (dois) anos, vedada a recondução.

§ 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.

§ 4º 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.

§ 5º O Comitê reunir-se-á ordinariamente, em periodicidade bimestral, mediante convocação de seu presidente

§ 6º O Comitê reunir-se-á extraordinariamente, mediante convocação de seu presidente.

§ 7º A participação no Comitê será considerada prestação de serviço público relevante, não remunerada.

Art. 16. A organização e o funcionamento do Comitê serão regulamentados em ato do Poder Executivo Federal.

Seção II

Da Agência Nacional de Cibersegurança

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.

Art. 18. A ANCiber tem as seguintes competências:

I - atuar como órgão central do Sistema Nacional de Cibersegurança;

II - proteger a soberania e os interesses nacionais no ciberespaço;

III - promover a implementação de ações voltadas à garantia da cibersegurança e da ciber-resiliência do país;

IV - atuar como ponto focal e único ponto de contato do Governo brasileiro no campo da cibersegurança, permitida a delegação, vedada a subdelegação;

V - assegurar a coordenação entre os órgãos e as entidades públicas e privadas envolvidas no campo da cibersegurança em nível nacional;

VI - desenvolver capacidades nacionais de prevenção, monitoramento, detecção, análise e resposta, para detectar e gerenciar ciberincidentes;

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;

VIII - gerir as cibercrises a nível nacional;

IX - desempenhar a função de secretaria-executiva do Comitê Nacional de Cibersegurança;

X - elaborar e submeter à aprovação do Comitê Nacional de Cibersegurança:

a) a Estratégia Nacional de Cibersegurança;

b) o Plano Nacional de Cibersegurança; e

c) o Complexo Nacional de Cibersegurança.

XI - desempenhar a função de secretaria-executiva do Gabinete de Gerenciamento de Cibercrises;

XII - planejar e executar as ações necessárias à implementação e controle da execução das medidas determinadas pelo Comitê Nacional de Cibersegurança;

XIII - gerir o Centro Nacional de Tratamento e Resposta a Ciberincidentes (CTIR.Br), a ser criado na estrutura regimental da ANCiber;

XIV - avaliar e certificar produtos e serviços, no tocante à cibersegurança, diretamente ou por meio de parceiros credenciados pela ANCiber;

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;

XVI - celebrar, a qualquer momento, compromisso com instituições integrantes do Complexo Nacional de Cibersegurança para eliminar irregularidade, incerteza jurídica ou situação contenciosa no âmbito de processos administrativos;

XVII - promover, apoiar e coordenar a realização de ciberinspeções regulares nos ciberativos integrantes do Complexo Nacional de Cibersegurança;

XVIII - promover, apoiar e coordenar ações voltadas à redução de ciber-riscos que envolvam a ciberlogística relativa a serviços essenciais;

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;

XX - propor as ações e definir as prioridades para a cooperação técnica internacional em cibersegurança, em ações conjuntas, combinadas ou compartilhadas com o Ministério das Relações Exteriores;

XXI - promover, apoiar e coordenar a participação nacional em projetos e iniciativas internacionais no campo da cibersegurança e serviços de aplicação relacionados, inseridos nelas o envolvimento de entidades públicas e privadas nacionais, em ações conjuntas, combinadas ou compartilhadas com o Ministério das Relações Exteriores;

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;

XXIII - apoiar o desenvolvimento de habilidades e capacidades industriais, tecnológicas e científicas autônomas, por meio de parcerias com universidades e instituições de pesquisas científicas e tecnológicas, bem como com o sistema produtivo nacional;

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;

XXV - promover o ensino de preceitos básicos de cibersegurança, conhecidos como ciber-higiene, em todos os níveis da educação nacional, com base em convênios especiais com entidades públicas e privadas, em coordenação com o Ministério da Educação;

XXVI - promover a formação, o crescimento técnico e profissional e a qualificação de recursos humanos na área de cibersegurança, inclusive por meio da concessão de bolsas de estudo, de mestrado, de doutorado e de pesquisa, com base em convênios especiais com entidades

públicas e privadas, em coordenação com o Ministérios da Educação e da Ciência, Tecnologia e Inovação;

XXVII - instituir e participar de parcerias público-privadas no território nacional e de consórcios ou fundações com entidades públicas, nacionais e estrangeiras.

XXVIII - elaborar relatórios de gestão anuais acerca de suas atividades, bem como de suas receitas e despesas;

XXIX - ouvir a sociedade em matérias de interesse relevante e prestar contas sobre suas atividades e planejamento;

XXX - arrecadar e aplicar suas receitas

XXXI - realizar auditorias, ou determinar sua realização, no âmbito da atividade de fiscalização de que trata o inciso XV - deste artigo;

XXXII - editar normas, orientações e procedimentos simplificados e diferenciados, inclusive quanto aos prazos, para que microempresas e empresas de pequeno porte, bem como iniciativas empresariais de caráter incremental ou disruptivo que se autodeclarem startups ou empresas de inovação, possam adequar-se a esta Lei;

XXXIII - deliberar, na esfera administrativa, em caráter terminativo, sobre a interpretação desta Lei, as suas competências e os casos omissos;

XXXIV - comunicar às autoridades competentes as infrações penais das quais tiver conhecimento;

XXXV - comunicar aos órgãos de controle interno o descumprimento do disposto nesta Lei por órgãos e entidades da administração pública federal; e

XXXVI - articular-se com as autoridades reguladoras públicas para exercer suas competências em setores específicos de atividades econômicas e governamentais sujeitas à regulação.

Art. 19. A ANCiber organizar-se-á considerando o detalhamento disposto no ANEXO I.

Seção III

Do Gabinete de Gerenciamento de Cibercrises

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.

Art. 21. Compete ao Gabinete:

I - implementar medidas e ações voltadas à mitigação de consequências de ciberincidentes afetos ao Complexo Nacional de Cibersegurança;

II - propor ao Comitê Nacional de Cibersegurança atos normativos concernentes à cibersegurança nacional;

III - recomendar ações a serem realizadas pela ANCiber;

IV - contribuir para a formulação, a execução e a avaliação do Plano Nacional de Cibersegurança;

V - apresentar iniciativas visando à adoção em nível nacional de boas práticas relativas à cibersegurança;

VI - determinar ao Diretor-Geral da ANCiber que notifique o Comitê Nacional de

Cibersegurança, em caráter emergencial, a ocorrência de uma cibercrise considerada relevante.

Art. 22. O Gabinete de Gerenciamento de Cibercrises será composto por:

I - o Diretor-Geral da ANCiber;

II - um representante do Ministério da Justiça e Segurança Pública;

III - um representante do Ministério da Defesa;

IV - um representante do Ministério das Relações Exteriores;

V - um representante do Ministério da Fazenda;

VI - um representante do Ministério do Planejamento e Orçamento;

VII - um representante do Ministério da Gestão e da Inovação em Serviços Públicos;

VIII - um representante do Ministério das Comunicações;

IX - um representante do Ministério da Ciência, Tecnologia e Inovações;

X - um representante da Comissão de Ciência, Tecnologia, Inovação, Comunicação e Informática do Senado Federal;

XI - um representante da Comissão de Ciência e Tecnologia, Comunicação e Informática da Câmara dos Deputados;

XII - um representante do Conselho Nacional de Justiça;

XIII - um representante do Conselho Nacional do Ministério Público; e

XIV - um representante da Autoridade Nacional de Proteção de Dados.

§ 1º O Gabinete será presidido pelo Diretor-Geral da ANCiber, que será substituído, em caso de impedimentos, pelo seu substituto legal.

§ 2º Os representantes de que tratam os incisos II a XIII, bem como seus suplentes, serão designados pelos titulares de seus respectivos órgãos ou entidades de origem, para integrarem o Gabinete por até 2 (dois) anos, permitida uma única recondução, até um período máximo total de 4 (quatro) anos, contínuos ou não.

§ 3º O Gabinete reunir-se-á ordinariamente, em periodicidade bimestral, para reuniões de caráter informativo e consultivo.

§ 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.

§ 5º O Gabinete poderá convidar especialistas ou representantes de instituições relevantes para participarem de suas reuniões, mas esses convidados não terão direito a voto nas deliberações.

§ 6º A participação no Gabinete será considerada prestação de serviço público relevante, não remunerada.

Art. 23. A organização e o funcionamento do Gabinete serão regulamentados em ato do Poder Executivo Federal.

Seção IV

Do Complexo Nacional de Cibersegurança

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.

Art. 25. Os provedores de serviços essenciais com ciberativos incluídos no Complexo são obrigados a cumprir os normativos, medidas e obrigações estipuladas pela ANCiber, no tocante a esses ciberativos visando a garantia da cibersegurança e ciber-resiliência.

CAPÍTULO III

DA ESTRATÉGIA NACIONAL DE CIBERSEGURANÇA

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.

Art. 27. A Estratégia 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 Estratégia será atualizada quadrienalmente.

CAPÍTULO IV

DO PLANO NACIONAL DE CIBERSEGURANÇA

Art. 28. O Plano Nacional de Cibersegurança ("Plano") implementa as determinações da Estratégia Nacional de Cibersegurança.

Art. 29. O Plano deve:

I - estabelecer ações;

II - definir prioridades;

III - estipular prazos;

IV - designar responsáveis e recursos.

Parágrafo único. O Plano será atualizado anualmente.

CAPÍTULO V

DA COOPERAÇÃO INTERNACIONAL

Art. 30. As iniciativas de cooperação técnica internacional em cibersegurança, coerentes com a garantia da soberania e dos interesses nacionais, têm as seguintes finalidades:

I - contribuir para a projeção internacional do Brasil;

II - assegurar o fornecimento e o acesso ao estado da arte tecnológico pertinente ao tema; e

III - assegurar a colaboração do País na busca por uma ordem internacional mais segura, próspera e aberta.

CAPÍTULO VI

DO ENSINO, PESQUISA, DESENVOLVIMENTO E INOVAÇÃO TECNOLÓGICA EM CIBERSEGURANÇA

Art. 31. O Poder Público poderá instituir medidas de incentivo e fomento para atender ao disposto nesta Lei.

Art. 32. O Ministério da Educação promoverá as alterações na legislação necessárias à implementação do ensino de cibersegurança na educação fundamental e média, pública e privada, com o objetivo de tornar a temática obrigatória em disciplinas do currículo escolar, de forma a elevar a percepção dos riscos e a produzir conhecimentos para o desenvolvimento de pessoas e para a qualificação profissional, com ênfase:

I - nas boas práticas de cibersegurança;

II - na ética no uso da internet;

III - na utilização segura de aplicativos

IV - no uso de redes sociais; e

V - na proteção de dados.

Art. 33. As secretarias de educação dos Estados, do Distrito Federal e dos Municípios promoverão as alterações na legislação necessárias à implementação do ensino da cibersegurança, em consonância com o Art. 32 e de acordo com as orientações do Ministério da Educação em relação ao tema.

Art. 34. Fica permitido às instituições oficiais de crédito estabelecer critérios diferenciados de acesso dos beneficiários aos créditos do Sistema Financeiro Nacional para investimentos no fomento ou na concessão de incentivos creditícios destinados a atender às diretrizes desta Lei.

Art. 35. As iniciativas a seguir relacionadas são de interesse nacional e assim consideradas prioritárias para alocação de recursos públicos:

I - programas educacionais voltados à disseminação da cultura de cibersegurança na sociedade, bem como à capacitação e/ou formação de mão-de-obra em cibersegurança; e

II - projetos para ativação de ecossistemas de inovação na área de cibersegurança.

Art. 36. A União, os Estados, o Distrito Federal e os Municípios, no âmbito de suas competências, poderão instituir normativos objetivando conceder incentivos fiscais, financeiros ou creditícios a:

I - empresas e entidades que desenvolvam tecnologia ou forneçam serviços, em território nacional, que contribuam para o incremento da cibersegurança no país; e

II - projetos desenvolvidos pelo setor privado que contribuam para o incremento da cibersegurança no país.

CAPÍTULO VII

DISPOSIÇÕES FINAIS E TRANSITÓRIAS

Art. 37. No prazo máximo de um ano, a contar da entrada em vigor desta Lei, o Poder Executivo Federal:

I - instalará o Comitê Nacional de Cibersegurança;

II - instalará a Agência Nacional de Cibersegurança; e

III - instalará o Gabinete de Gerenciamento de Cibercrises.

Art. 38. Até a regulamentação do Comitê Nacional de Cibersegurança, da Agência Nacional de Cibersegurança e do Gabinete de Gerenciamento de Cibercrises, o Gabinete de Segurança Institucional da Presidência da República será responsável pelas medidas necessárias à implementação das disposições desta Lei.

Art. 39. No prazo máximo de seis meses, a contar da instalação da ANCiber, deverão ser publicados:

I - a Estratégia Nacional de Cibersegurança;

II - o Plano Nacional de Cibersegurança;

III - o Complexo Nacional de Cibersegurança.

Art. 40. No prazo máximo de seis meses, a contar da instalação da ANCiber, as competências atribuídas pelo Decreto 10.748, de 16 de julho de 2021, ao Gabinete de Segurança Institucional da Presidência da República, serão transferidas à ANCiber.

Art. 41. No prazo máximo de seis meses, a contar da instalação da ANCiber, as competências atribuídas pelo Decreto 10.748, de 16 de julho de 2021, ao Departamento de Segurança da Informação e Cibernética da Secretaria de Segurança da Informação e Cibernética do Gabinete de Segurança Institucional da Presidência da República, serão transferidas ao Centro Nacional de Tratamento e Resposta a Ciberincidentes (CTIR.Br) da ANCiber.

§ 1º . A Rede Federal de Gestão de Incidentes Cibernéticos, criada no âmbito do Decreto 10.748, de 16 de julho de 2021, passará a ser denominada Rede Nacional de Gestão de Ciberincidentes.

§ 2º . O Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR Gov) do Departamento de Segurança da Informação e Cibernética da Secretaria de Segurança da Informação e Cibernética do Gabinete de Segurança Institucional da Presidência da República, atuará como equipe de coordenação setorial dos órgãos da Presidência da República

Art. 42. A ANCiber poderá disciplinar, por meio de resolução, o uso de meios eletrônicos para os atos dos processos administrativos da sua área de atuação.

Art. 43. No exercício de suas atividades, a ANCiber poderá:

I - solicitar diretamente ao Ministério do Planejamento e Orçamento a autorização para a realização de concursos públicos e para o provimento dos cargos efetivos autorizados em lei para seu Quadro de Pessoal e as alterações no referido Quadro, observada a disponibilidade orçamentária;

II - celebrar contratos administrativos ou prorrogar contratos em vigor; e

III - conceder diárias e passagens na hipótese de deslocamentos nacionais e internacionais e autorizar afastamentos do País de seus servidores.

Art. 44. Revogam-se todas as disposições em contrário ao disposto nesta Lei.

Brasília, de de 2023; 202º da Independência e 135º da República.

ANEXO I

AGÊNCIA NACIONAL DE CIBERSEGURANÇA

Seção I

Organização e Funcionamento

Art. 1 º. A ANCiber será dirigida por Diretoria Colegiada, composta por um Diretor-Geral e quatro Diretores.

§ 1º O Diretor-Geral da ANCiber exercerá a representação da ANCiber, a presidência da Diretoria Colegiada e o comando hierárquico sobre o pessoal e os serviços, e caber-lhe-á desempenhar as competências administrativas correspondentes e a presidência das sessões da Diretoria Colegiada, sem prejuízo das deliberações colegiadas para matérias definidas no regimento interno.

§ 2º A estrutura organizacional da ANCiber será definida em decreto e contará com Procuradoria, Ouvidoria, Corregedoria, Auditoria e unidades administrativas.

Art. 2 º. Os membros da Diretoria exercerão mandatos de cinco anos, não coincidentes, permitida uma única recondução.

Art. 3 º. Os membros da Diretoria Colegiada ficam impedidos de exercer atividade ou de prestar qualquer serviço no setor regulado pela ANCiber, pelo período de seis meses, contado da data de exoneração ou do término de seus mandatos, assegurada a remuneração compensatória.

Art. 4 º. É vedada a indicação para a Diretoria Colegiada:

I - de Ministro de Estado, Secretário de Estado, Secretário Municipal, dirigente estatutário de partido político e titular de mandato no Poder Legislativo de qualquer ente federativo, ainda que licenciados dos cargos;

II - de pessoa que tenha atuado, nos últimos seis meses, como participante de estrutura decisória de partido político;

III - de pessoa que tenha participação, direta ou indireta, em empresa ou entidade que atue no setor sujeito à regulação exercida pela ANCiber;

IV - de pessoa que se enquadre nas hipóteses de inelegibilidade previstas no inciso I do caput do art. 1º da Lei Complementar nº 64, de 18 de maio de 1990; e

V - de membro de conselho ou de diretoria de associação, regional ou nacional, representativa de interesses patronais ou trabalhistas ligados às atividades reguladas pela ANCiber.

Parágrafo único. A vedação prevista no inciso I do caput deste artigo estende-se também aos parentes consanguíneos ou afins até o terceiro grau das pessoas nele mencionadas.

Art. 5 º. Ao membro da Diretoria Colegiada é vedado:

I - receber, a qualquer título e sob qualquer pretexto, honorários, percentagens ou custas;

II - exercer outra atividade profissional, ressalvado o exercício do magistério, se houver compatibilidade de horários;

III - participar de sociedade simples ou empresária ou de empresa de qualquer espécie, na forma de controlador, diretor, administrador, gerente, membro de conselho de administração ou conselho fiscal, preposto ou mandatário;

IV - emitir parecer sobre matéria de sua especialização, ainda que em tese, ou atuar como consultor de qualquer tipo de empresa;

V - exercer atividade sindical;

VI - exercer atividade político-partidária; e

VII - estar em situação de conflito de interesse, nos termos da Lei nº 12.813, de 16 de maio de 2013.

Art. 6 º. A organização e o funcionamento da Diretoria Colegiada serão estabelecidos na estrutura regimental da ANCiber.

Art. 7 º. Compete à Diretoria Colegiada:

I - exercer a administração da ANCiber;

II - editar as normas sobre matérias de competência da ANCiber; e

III - decidir, em última instância, na esfera da ANCiber, sobre as matérias de sua competência, exceto nas hipóteses em que o regulamento ou resolução da ANCiber estabelecer o Diretor-Geral como última instância recursal.

§ 1º A Diretoria Colegiada deliberará por maioria absoluta de seus membros, e caberá ao Diretor-Geral, além do voto ordinário, o voto de qualidade.

§ 2º O regimento interno da ANCiber estabelecerá a competência da Diretoria Colegiada, do Diretor-Geral, dos Diretores e de outras autoridades da ANCiber para a prática dos atos atribuídos por esta Lei, inclusive quanto ao processamento e à decisão de recursos administrativos.

Art. 8 º. Os atos normativos da ANCiber que afetarem, de forma substancial e direta, direitos de agentes econômicos do setor por ela regulado deverão ser acompanhados da exposição formal dos motivos que os justifiquem e ser submetidos à consulta ou à audiência pública.

Art. 9 º. A ANCiber, por meio de resolução, disporá sobre os processos administrativos em seu âmbito de atuação, notadamente sobre:

I - requisitos e procedimentos de fiscalização dos procedimentos de cibersegurança aplicáveis ao país;

II - regras e procedimentos de aplicação de medidas acautelatórias e sanções administrativas;

III - hipóteses e critérios para a apresentação de garantias financeiras ou a contratação de seguros para cobertura dos ciber-riscos; e

IV - hipóteses e critérios para realização de consulta pública e audiência pública para os atos normativos da ANCiber.

Art. 10. As sessões deliberativas da Diretoria Colegiada, afetas às atividades de cibersegurança, serão públicas e terão suas datas, pautas e atas divulgadas.

Parágrafo único. Nas sessões da Diretoria Colegiada, de que trata o caput deste artigo, é assegurada a manifestação da Procuradoria da ANCiber, das partes envolvidas no processo e de terceiros interessados, na forma estabelecida no regulamento da ANCiber.

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.

§ 1º Regulamento disporá sobre o conteúdo e a metodologia da análise de impacto regulatório, os quesitos mínimos a serem objeto de exame, os casos em que será obrigatória sua realização e aqueles em que poderá ser dispensada.

§ 2º A Diretoria Colegiada da ANCiber manifestar-se-á, em relação ao relatório de AIR, sobre a adequação da proposta de ato normativo aos objetivos pretendidos, e indicará se os impactos estimados recomendam a sua adoção e, quando for o caso, os complementos necessários.

§ 3º A manifestação de que trata o § 2º deste artigo integrará, juntamente ao relatório de AIR, a documentação a ser disponibilizada aos interessados para a realização de consulta ou de audiência pública, quando a Diretoria Colegiada decidir pela continuidade do procedimento administrativo.

§ 4º O regimento interno da ANCiber disporá sobre a operacionalização da análise de impacto regulatório.

§ 5º Nos casos em que não for realizada a AIR, deverá ser disponibilizada, no mínimo, nota técnica ou documento equivalente que fundamente a proposta de decisão.

Art. 12. A ANCiber disporá sobre os procedimentos a serem adotados para a solução de conflitos entre agentes da atividade de cibersegurança, com ênfase na conciliação e na mediação.

Art. 13. A ANCiber assegurará a necessária ligação com os demais órgãos da administração pública federal aos quais a lei confere competência no campo da cibersegurança.

Art. 14. Em âmbito internacional, a ANCiber manterá relações com organismos, instituições e órgãos competentes e monitorará questões em sua esfera institucional de autoridade competente para a cibersegurança, exceto em áreas nas quais a lei confere poderes específicos a outros órgãos da administração pública federal.

Art. 15. No tocante ao Art. 13 e ao Art. 14 o vínculo com a ANCiber é assegurado para garantir posições nacionais unitárias condizentes com as políticas de cibersegurança definidas pelo Estado brasileiro.

Art. 16. A ANCiber poderá estipular acordos de cooperação que definam modalidades de colaboração com a Autoridade Nacional para Proteção de Dados e outras instituições que atuem na regulação do ciberespaço.

Art. 17. A ANCiber poderá promover, desenvolver e financiar projetos e iniciativas específicas, inclusive aquelas que visam promover a transferência tecnológica de resultados de pesquisa no campo.

Art. 18. A fixação das dotações orçamentárias da ANCiber na Lei Orçamentária Anual e sua programação orçamentária e financeira de execução não sofrerão limites nos seus valores para movimentação e empenho.

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.

Art. 20. A ANCiber submeterá anualmente ao Ministério do Planejamento e Orçamento a sua proposta de orçamento, para inclusão na lei orçamentária anual a que se refere o § 5º do art. 165 da Constituição Federal.

§ 1º A ANCiber fará acompanhar as propostas orçamentárias de um quadro demonstrativo do

planejamento plurianual das receitas e despesas, visando ao seu equilíbrio orçamentário e financeiro nos cinco exercícios subsequentes.

§ 2º A lei orçamentária anual consignará as dotações para as despesas de custeio e capital da ANCiber, relativos ao exercício a que ela se referir.

Art. 21. Constituem receitas da ANCiber:

I - as dotações, consignadas no orçamento geral da União, os créditos especiais, os créditos adicionais, as transferências e os repasses que lhe forem conferidos;

II - as doações, os legados, as subvenções e outros recursos que lhe forem destinados;

III - os valores apurados na venda ou aluguel de bens móveis e imóveis de sua propriedade;

IV - os valores apurados em aplicações no mercado financeiro das receitas previstas neste artigo;

V - os recursos provenientes de acordos, convênios ou contratos celebrados com entidades, organismos ou empresas, públicos ou privados, nacionais ou internacionais;

VI - o produto da venda de publicações, material técnico, dados e informações, inclusive para fins de licitação pública.

VII - taxas de fiscalização;

VIII - taxas de certificação de produtos e serviços de cibersegurança;

IX - o produto dos emolumentos, preços ou multas;

X - os valores apurados na venda ou locação de bens;

XI - quantias recebidas pela aprovação de laudos de ensaio de produtos e pela prestação de serviços técnicos por órgãos da ANCiber; e

XII - rendas eventuais.

Art. 22. Constituem o patrimônio da ANCiber os bens e os direitos:

I - que lhe forem transferidos pelos órgãos da Presidência da República;

II - que venha a adquirir ou a incorporar.

Seção II

Quadro de Pessoal

Art. 23. A Lei nº 10.871, de 20 de maio de 2004, passa a vigorar com as seguintes alterações:

"Art. 1º. .....

.....

XXI - Especialista em Cibersegurança, composta por cargos de Especialista em Cibersegurança, de nível superior, com atribuições voltadas às atividades inerentes à regulação, fomento e fiscalização da cibersegurança, ao acompanhamento dos desenvolvimentos da cibersegurança brasileira e internacional, à implementação da política nacional de cibersegurança, ao estímulo do desenvolvimento e implementação de ferramentas, processos e técnicas de cibersegurança, à promoção e ao fomento do desenvolvimento de pesquisas científicas e tecnológicas, direcionadas à cibersegurança e ao exercício das competências a cargo da Agência Nacional de Cibersegurança;

XXII - Técnico em Cibersegurança, composta por cargos de Técnico em Cibersegurança, de nível

intermediário, com atribuições voltadas ao suporte e ao apoio técnico especializado às atividades desenvolvidas pelos Especialistas em Cibersegurança e ao exercício das competências a cargo da Agência Nacional de Cibersegurança.

Art. 1º. São atribuições específicas dos cargos de nível superior referidos nos incisos I a IX, XIX e XXI do art. 1º desta Lei: (NR)

.....

Art. 2º. São atribuições comuns dos cargos referidos nos incisos I a XVI, XIX a XXII do art. 1º desta Lei: (NR)

.....

Parágrafo único. No exercício das atribuições de natureza fiscal ou decorrentes do poder de polícia, são asseguradas aos ocupantes dos cargos referidos nos incisos I a XVI e XIX a XXII do art. 1º desta Lei as prerrogativas de promover a interdição de estabelecimentos, instalações ou equipamentos, assim como a apreensão de bens ou produtos, e de requisitar, quando necessário, o auxílio de força policial federal ou estadual, em caso de desacato ou embaraço ao exercício de suas funções. (NR)

Art. 15. .....

I - vencimento básico e Gratificação de Desempenho de Atividade de Regulação - GDAR para os cargos a que se referem os incisos I a XVI e XIX a XXII do art. 1º desta Lei; (NR)

.....

Art. 15-A. A partir de 1º de janeiro de 2014, a estrutura remuneratória dos cargos a que se referem os incisos I a XVI e XIX a XXII do caput do art. 1º constitui-se de: (NR)

.....

Art. 16. Fica instituída a Gratificação de Desempenho de Atividade de Regulação - GDAR, devida aos ocupantes dos cargos a que se referem os incisos I a XVI e XIX a XXII do art. 1º desta Lei, quando em exercício de atividades inerentes às atribuições do respectivo cargo nas Agências Reguladoras referidas no Anexo I desta Lei, observando-se a seguinte composição e limites: (NR)

.....

Art. 17. O titular de cargo efetivo referido nos incisos I a XVI e XIX a XXII do art. 1º desta Lei, em exercício na Agência Reguladora em que esteja lotado, quando investido em cargo em comissão ou função de confiança fará jus à GDAR, nas seguintes condições: (NR)

.....

Art. 18. O titular de cargo efetivo referido nos incisos I a XVI e XIX a XXII do art. 1º desta Lei que não se encontre em exercício na entidade de lotação, excepcionalmente, fará jus à GDAR nas seguintes situações: (NR)

....."

Art. 24. Ficam criados, no Quadro de Pessoal da Agência Nacional de Cibersegurança os seguintes quantitativos de cargos, para provimento gradual:

I - quinhentos e cinquenta cargos de Especialista em Cibersegurança; e

II - duzentos e vinte e cinco cargos de Analista Administrativo.

Parágrafo único. Altera-se o ANEXO I da Lei nº 10.871, de 20 de maio de 2004, para incluir a Agência Nacional de Cibersegurança (ANCiber) como Autarquia Especial com os cargos e quantitativos

estipulados no caput deste artigo.

Art. 25. Ficam criados vinte e cinco cargos de Procurador Federal a serem alocados à Agência Nacional de Cibersegurança, para provimento gradual.

Parágrafo único. Altera-se o ANEXO II da Lei nº 10.871, de 20 de maio de 2004, para incluir a Agência Nacional de Cibersegurança (ANCiber) como Autarquia Especial com os cargos e quantitativos estipulados no caput deste artigo.

Art. 26. As carreiras criadas no Art. 23 são estruturadas conforme suas congêneres discriminadas na Lei nº 10.871, de 20 de maio de 2004.

§ 1º . Altera-se o ANEXO III da Lei nº 10.871, de 20 de maio de 2004, para incluir os cargos de Especialista em Cibersegurança e Técnico em Cibersegurança na coluna CARGOS, com os números 21 e 22, respectivamente.

§ 2º . Altera-se o ANEXO IV da Lei nº 10.871, de 20 de maio de 2004, para incluir o cargo de Especialista em Cibersegurança na coluna CARGO.

§ 3º . Altera-se o ANEXO V da Lei nº 10.871, de 20 de maio de 2004, para incluir o cargo de Técnico em Cibersegurança na coluna CARGO.

§ 4º . Altera-se a Tabela A "valor do ponto da GDAR para os cargos de Nível Superior" do ANEXO VI da Lei nº 10.871, de 20 de maio de 2004, para incluir o cargo de Especialista em Cibersegurança na coluna CARGO.

§ 5º . Altera-se a Tabela B "valor do ponto da GDAR para os cargos de Nível Intermediário" do ANEXO VI da Lei nº 10.871, de 20 de maio de 2004, para incluir o cargo de Técnico em Cibersegurança na coluna CARGO.

Art. 27. O provimento gradual a que se referem o Art. 24 e o Art. 25 desta Lei dar-se-á em até 5 (cinco) anos, conforme quantitativos dispostos no ANEXO I.

Art. 28. A Lei nº 13.848, de 25 de junho de 2019, passa a vigorar com as seguintes alterações:

"Art. 2º. .....

.....

XII – a Agência Nacional de Cibersegurança (ANCiber). (NR)"

Art. 29. A Lei nº 11.890, de 24 de dezembro de 2008, passa a vigorar com as seguintes alterações:

"Art. 154. .....

.....

XLI - Especialista em Cibersegurança, integrante da carreira de Especialista em Cibersegurança;

XLII - Técnico em Cibersegurança, integrante da carreira de Técnico em Cibersegurança.

.....

Art. 157. .....

I - para as carreiras de que tratam os incisos I, II e XVI a XLII do caput do art. 154;" (NR)

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.

Art. 31. Com fulcro no disposto no artigo 2º, inciso VI, alínea "i" da Lei 8.745, de 9 de dezembro de 1993, fica a Agência Nacional de Cibersegurança autorizada a contratar profissionais temporários para o preenchimento de seu quadro de pessoal, limitada aos quantitativos anuais dispostos no ANEXO II.

Seção III

Quadro de Cargos em Comissão

Art. 32. Ficam criados, na estrutura organizacional da Agência Nacional de Cibersegurança, os seguintes cargos e funções em comissão:

I - um CD-I;

II - quatro CD-II;

III - quatro CCE-16;

IV - seis FCE-16;

V - quatro CCE-15;

VI - seis FCE-15;

VII - oito CCE-14;

VIII - doze FCE-14;

IX - oito CCE-13;

X - doze FCE-13;

XI - oito CCE-12;

XII - doze FCE-12;

XIII - oito CCE-11;

XIV - doze FCE-11;

XV - vinte FCE-10;

XVI - vinte e cinco FCE-9;

XVII - vinte e cinco FCE-8;

XVIII - quarenta FCE-7;

XIX - quarenta FCE-6; e

XX - quarenta e cinco FCE-5.

§ 1º Os cargos CD-I e CD-II são, respectivamente, de Diretor-Geral e de Diretor.

§ 2º A estrutura de cargos em comissão da Agência Nacional de Cibersegurança será regida pelas disposições da Lei nº 14.204, de 16 de setembro de 2021, e pelo disposto nesta Lei.

§ 3º No tocante à ANCiber, o disposto no artigo 13, inciso III, da Lei 14.204 de 16 de setembro de 2021 somente será válido após o preenchimento do quadro de pessoal da Agência.

Seção IV

Primeira Diretoria

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:

I - o Diretor-Geral nomeado com mandato de cinco anos;

II - um Diretor nomeado com mandato de quatro anos;

III - um Diretor nomeado com mandato de três anos;

IV - um Diretor nomeado com mandato de dois anos; e

V - um Diretor nomeado com mandato de um ano.

§1º Na hipótese de vacância no curso do mandato, o Diretor-Geral ou o Diretor nomeado em substituição ocupará o cargo pelo prazo remanescente para o fim do mandato.

§2º Os integrantes da primeira Diretoria da Agência Nacional de Cibersegurança, previamente aprovados pelo Senado Federal, serão nomeados na mesma data de entrada em vigor do ato do Poder Executivo que aprovar o regulamento e a estrutura regimental da Agência Nacional de Cibersegurança.

ANEXO II

EVOLUÇÃO DO QUADRO DE PESSOAL DA AGÊNCIA NACIONAL DE CIBERSEGURANÇA

Item	**Ano I**	**Ano II**	**Ano III**	**Ano IV**	**Ano V**
No Ano	**81**	**121**	**160**	**200**	**238**
Acumulado	**81**	**202**	**362**	**562**	**800**

DECRETO Nº XX, DE XX DE XXXXXXXXX DE 2023

Instala o Comitê Nacional de Cibersegurança, o Gabinete de Gestão de Cibercrises, a Agência Nacional de Cibersegurança, e aprova suas Estruturas Regimentais.

O PRESIDENTE DA REPÚBLICA, no uso da atribuição que lhe confere o art. 84, caput, incisos IV e VI, alínea "a", da Constituição, e tendo em vista o disposto nos na Lei nº XX.XXX, de XX de XXXXXX de 2023,

DECRETA :

Art. 1 º. Ficam instalados o Comitê Nacional de Cibersegurança (CNCiber), a Agência Nacional de Cibersegurança (ANCiber), e o Gabinete de Gestão de Cibercrises (GGCiber), criados pela Lei nº XX.XXX, de XX de XXXXXX de 2023.

Art. 2 º. Fica aprovada a Estrutura Regimental do CNCiber, na forma do Anexo I.

Art. 3 º. Fica aprovada a Estrutura Regimental do GGCiber, na forma do Anexo II.

Art. 4 º. Fica aprovada a Estrutura Regimental da ANCiber, na forma do Anexo III.

Art. 5 º. O Diretor-Geral da ANCiber publicará, no Diário Oficial da União, no prazo de sessenta dias, contado da data de entrada em vigor deste Decreto, o regimento interno para detalhar as unidades administrativas integrantes da Estrutura Regimental da ANCiber, suas competências e as atribuições de seus dirigentes.

Parágrafo único. O regimento interno conterá o Quadro Demonstrativo dos Cargos em Comissão da ANCiber.

Art. 6 º. O Diretor-Geral da ANCiber publicará, no Diário Oficial da União, no prazo de sessenta dias, contado da data de entrada em vigor deste Decreto, relação nominal dos titulares dos cargos em comissão a que se refere o Anexo IV, que indicará, inclusive, o número de cargos vagos, suas denominações e seus níveis.

Art. 7 º. A partir da data da entrada em vigor deste Decreto, fica a ANCiber investida no exercício pleno de suas atribuições.

Art. 8 º Este Decreto entra em vigor em XX de XXXXXXXX de 2023.

Brasília, de de 2023; 202º da Independência e 135º da República.

ANEXO I

ESTRUTURA REGIMENTAL DO COMITÊ NACIONAL DE CIBERSEGURANÇA

Art. 1 º. Fica instalado o Comitê Nacional de Cibersegurança, 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.

Art. 2 º. As competências do Comitê Nacional de Cibersegurança são aquelas estabelecidas no Art. 14 da Lei nº XX.XXX, de XX de XXXXXX de 2023.

Art. 3 º. A composição do Comitê Nacional de Cibersegurança é a determinada pelo Art. 15 da Lei nº XX.XXX, de XX de XXXXXX de 2023.

§ 1º Cada membro do Comitê Nacional de Cibersegurança terá um suplente, que o substituirá em suas ausências e impedimentos.

Art. 4 º. O quórum de reunião do Comitê Nacional de Cibersegurança será de dois terços dos membros e o quórum de aprovação será de maioria simples dos membros.

Art. 5 Parágrafo único. Além do voto ordinário, o Presidente do Comitê Nacional de Cibersegurança terá o voto de qualidade em caso de empate.

Art. 6 º. Serão convidados a compor o Comitê Nacional de Cibersegurança, sem direito a voto:

I - um membro de Ministério Público Estadual, indicado pelo Conselho Nacional de Procuradores-Gerais;

II - um membro do Ministério Público Federal, indicado pelo Procurador-Geral da República; e

III - um membro da Defensoria Pública, indicado pelo Colégio Nacional dos Defensores Públicos Gerais.

Art. 7 º. A Secretaria-Geral da Agência Nacional de Cibersegurança exercerá a função de Secretaria-Executiva do Comitê Nacional de Cibersegurança.

Art. 8 º. O Comitê Nacional de Cibersegurança poderá instituir comissões especiais com a finalidade de realizar tarefas e estudos específicos destinados à cibersegurança na ordem econômica constitucional brasileira.

Art. 9 . As comissões especiais:

I - serão compostas na forma de ato do Comitê Nacional de Cibersegurança;

II - não poderão ter mais de sete membros;

III - terão caráter temporário e duração não superior a um ano; e

IV - estarão limitadas a cinco operando simultaneamente.

Art. 10. Os membros do Comitê Nacional de Cibersegurança e das comissões especiais que se encontrarem no Distrito Federal reunir-se-ão presencialmente ou por videoconferência e os membros que se encontrem em outros entes federativos participarão da reunião por meio de videoconferência.

Art. 11. É vedado aos membros a divulgação de discussões em curso no Comitê Nacional de Cibersegurança sem a prévia anuência de seu Presidente.

ANEXO II

ESTRUTURA REGIMENTAL DO GABINETE DE GERENCIAMENTO DE CIBERCRISES

Art. 1 º. Fica instalado o Gabinete de Gestão de Cibercrises, 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.

Art. 2 º. As competências do Gabinete de Gestão de Cibercrises são aquelas estabelecidas no Art. 21 da Lei nº XX.XXX, de XX de XXXXXX de 2023.

Art. 3 º. A composição do Gabinete de Gestão de Cibercrises é a determinada pelo Art. 22 da Lei nº XX.XXX, de XX de XXXXXX de 2023.

§ 1º Cada membro do Gabinete de Gestão de Cibercrises terá um suplente, que o substituirá em suas ausências e impedimentos.

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.

Art. 5 Parágrafo único. Além do voto ordinário, o Presidente do Gabinete de Gestão de Cibercrises terá o voto de qualidade em caso de empate.

Art. 6 º. Serão convidados a compor o Gabinete de Gestão de Cibercrises, sem direito a voto:

I - um membro de Ministério Público Estadual, indicado pelo Conselho Nacional de Procuradores-Gerais;

II - um membro do Ministério Público Federal, indicado pelo Procurador-Geral da República; e

III - um membro da Defensoria Pública, indicado pelo Colégio Nacional dos Defensores Públicos Gerais.

Art. 7 º. A Secretaria-Geral da Agência Nacional de Cibersegurança exercerá a função de Secretaria-Executiva do Gabinete de Gestão de Cibercrises.

Art. 8 . Os membros do Gabinete de Gestão de Cibercrises que se encontrarem no Distrito Federal reunir-se-ão presencialmente ou por videoconferência e os membros que se encontrem em outros entes federativos participarão da reunião por meio de videoconferência.

Art. 9 . É vedado aos membros a divulgação de discussões em curso no Gabinete de Gestão de Cibercrises sem a prévia anuência de seu Presidente.

ANEXO III

ESTRUTURA REGIMENTAL DA AGÊNCIA NACIONAL DE CIBERSEGURANÇA

CAPÍTULO I

DA NATUREZA, FINALIDADE, SEDE E COMPETÊNCIA

Art. 1 º. A Agência Nacional de Cibersegurança - ANCiber, autarquia sob regime especial, com sede e foro no Distrito Federal, personalidade jurídica de direito público e autonomia patrimonial, administrativa e financeira, nos termos da Lei nº XXXX, de XX de XXXXX de 2023, vinculada ao Gabinete de Segurança Institucional da Presidência da República, tem por finalidade promover o desenvolvimento, a regulação e a fiscalização das atividades de cibersegurança no País.

Art. 2 º. As competências da ANCiber são aquelas determinadas no Art. 18 da Lei nº XX.XXX, de XX de XXXXXX de 2023.

CAPÍTULO II

DA ESTRUTURA ORGANIZACIONAL

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.

Art. 4 º. A ANCiber será dirigida pela Diretoria Colegiada, composta por um Diretor-Geral e quatro Diretores.

§ 1º O Diretor-Geral e os demais Diretores terão mandatos de cinco anos, não coincidentes, permitida uma única recondução, observadas as disposições da Lei nº 9.986, de 18 de julho de 2000, e da Lei nº 13.575, de 2017.

§ 2º A Diretoria Colegiada designará um de seus integrantes para assumir a Direção Geral nas hipóteses de vacância, ausências eventuais e impedimentos legais do Diretor-Geral.

§ 3º O termo inicial de todos os mandatos será a data de publicação do ato de nomeação dos primeiros membros da Diretoria Colegiada.

§ 4º O termo inicial de que trata o § 3º prevalecerá para cômputo da duração dos mandatos, mesmo que as nomeações e as posses subsequentes venham a ocorrer em datas diferentes.

§ 5º Na hipótese de vacância no curso do mandato, o Diretor-Geral ou o Diretor nomeado em substituição ocupará o cargo pelo prazo remanescente do mandato.

Art. 5 º. O Procurador-Chefe será nomeado após indicação do Advogado-Geral da União, nos termos do § 3º do art. 12 da Lei nº 10.480, de 2 de julho de 2002.

Art. 6 º. O Ouvidor será nomeado pelo Diretor-Geral, após indicação da Diretoria Colegiada

Parágrafo único. O Ouvidor terá mandato de três anos, vedada a recondução.

Art. 7 º. O Auditor Chefe será nomeado pelo Diretor-Geral, após indicação da Diretoria Colegiada e apreciação do Ministério da Transparência e Controladoria-Geral da União.

Art. 8 º. O Corregedor será nomeado pelo Diretor-Geral para mandato de dois anos, após indicação da Diretoria Colegiada e apreciação do Órgão Central do Sistema de Correição.

Art. 9 º. O Executivo de Inteligência será nomeado pelo Diretor-Geral, após indicação da Diretoria Colegiada e apreciação do órgão central do Sistema Brasileiro de Inteligência.

CAPÍTULO III

DAS COMPETÊNCIAS DAS UNIDADES

Art. 10º. À Diretoria Colegiada compete:

I - exercer a administração da ANCiber;

II - editar as normas sobre matérias de competência da ANCiber;

III - decidir, em última instância, na esfera da ANCiber, sobre as matérias de sua competência, exceto nas hipóteses em que norma da ANCiber estabeleça o Diretor-Geral como última instância recursal;

IV - deliberar sobre a alteração dos quantitativos e a distribuição dos cargos comissionados executivos e funções comissionadas executivas, observados os valores de retribuição correspondentes e desde que não acarrete aumento de despesa;

V - aprovar o planejamento estratégico da ANCiber para ciclos plurianuais compatíveis com os seus macroprocessos, que contemplará objetivos estratégicos, metas, indicadores de resultados e padrões de desempenho;

VI - aprovar a política de gestão de integridade, de riscos e de controles internos;

VII - aprovar a proposta orçamentária anual da ANCiber a ser encaminhada ao Gabinete de Segurança Institucional da Presidência da República;

VIII - aprovar a requisição de servidores e empregados de órgãos e de entidades da administração pública;

IX - decidir sobre procedimentos administrativos de fiscalização da atividade de cibersegurança;

X - aprovar relatório anual de atividades da ANCiber; e

XI - aprovar o regimento interno da ANCiber.

Art. 11. As decisões da Diretoria Colegiada serão tomadas pelo voto da maioria absoluta de seus membros, e caberá ao Diretor-Geral, além do voto ordinário, o voto de qualidade.

§ 1º As decisões da Diretoria Colegiada serão registradas em atas que ficarão disponíveis para conhecimento geral.

§ 2º Os atos normativos da Diretoria Colegiada serão publicados no Diário Oficial da União e no sítio eletrônico da ANCiber.

§ 3º As reuniões da Diretoria Colegiada relacionadas às atividades de cibersegurança serão públicas e terão suas datas, pautas e atas divulgadas no sítio eletrônico da ANCiber.

§ 4º Nas reuniões da Diretoria Colegiada de que trata o § 3º, será assegurada a manifestação da Procuradoria Federal Especializada, das partes envolvidas no processo e de terceiros interessados.

Art. 12. À Secretaria-Geral compete:

I - assistir o Diretor-Geral na representação institucional da ANCiber;

II - preparar o despacho de expediente do Diretor-Geral e ocupar-se das relações públicas da ANCiber;

III - efetuar o acompanhamento da tramitação dos atos legais de interesse da ANCiber; e

IV - providenciar a publicação oficial e a divulgação das matérias relacionadas com a área de atuação da ANCiber.

V - prestar apoio técnico e administrativo:

a) à Diretoria Colegiada;

b) ao Comitê Nacional de Cibersegurança; e

c) ao Gabinete de Gestão de Cibercrises.

Art. 13. À Procuradoria Federal Especializada junto à ANCiber, órgão de execução da Procuradoria-Geral Federal, compete:

I - representar judicial e extrajudicialmente a ANCiber, observadas as normas estabelecidas pela Procuradoria-Geral Federal;

II - orientar a execução da representação judicial da ANCiber, quando sob a responsabilidade dos demais órgãos de execução da Procuradoria-Geral Federal;

III - exercer atividades de consultoria e assessoramento jurídicos no âmbito da ANCiber e aplicar, no que couber, o disposto no art. 11 da Lei Complementar nº 73, de 10 de fevereiro de 1993;

IV - auxiliar os demais órgãos de execução da Procuradoria-Geral Federal na apuração da liquidez e certeza dos créditos, de qualquer natureza, às atividades da ANCiber, para inscrição em dívida ativa e cobrança;

V - zelar pela observância da Constituição, das leis e dos demais atos emanados dos Poderes Públicos, sob a orientação normativa da Advocacia-Geral da União e da Procuradoria-Geral Federal;

VI - coordenar e supervisionar, técnica e administrativamente, suas unidades descentralizadas; e

VII - encaminhar à Advocacia-Geral da União ou à Procuradoria-Geral Federal, conforme o caso, pedido de apuração de falta funcional praticada por seus membros.

Art. 14. À Ouvidoria compete:

I - receber e encaminhar à Diretoria Colegiada reclamações, críticas e comentários sobre a atuação da ANCiber e acompanhar o tratamento e a efetiva conclusão das manifestações;

II - estabelecer canais de atendimento e de comunicação com a sociedade, com vistas à internalização das demandas para a melhoria dos serviços da ANCiber;

III - promover as ações necessárias à apuração da veracidade das reclamações e das denúncias, e solicitar as providências necessárias ao saneamento de eventuais irregularidades;

IV - zelar pela qualidade e pela tempestividade dos serviços prestados pela ANCiber;

V - atuar como ponto focal único para o trato do e-SIC; e

VI - elaborar relatório anual das atividades da Ouvidoria e encaminhá-lo à Diretoria Colegiada, que poderá manifestar-se em vinte dias.

§ 1º O Ouvidor terá acesso a todos os processos da ANCiber necessários à avaliação das reclamações e das denúncias.

§ 2º Os relatórios anuais do Ouvidor não terão caráter impositivo e caberá à Diretoria Colegiada, em última instância, deliberar a respeito dos temas relacionados ao setor de atuação da ANCiber.

§ 3º Transcorrido o prazo para manifestação da Diretoria Colegiada, o Ouvidor deverá encaminhar o relatório anual, acompanhado da manifestação da Diretoria Colegiada, se houver, ao titular do ministério a que a ANCiber estiver vinculada, à Câmara dos Deputados, ao Senado Federal e ao Tribunal de Contas da União, divulgando-os no sítio da ANCiber.

Art. 15. À Auditoria Interna compete:

I - realizar auditorias, independentes e objetivas, incluídas as atividades de acompanhar, analisar, proceder a levantamentos e comprovações metodologicamente estruturadas sobre a integridade, a adequação, a eficácia, a eficiência e a economicidade dos processos, dos sistemas de informações e de gerenciamento de riscos, com o objetivo de contribuir para o fortalecimento da gestão orçamentária, financeira, administrativa, contábil, técnica e patrimonial, e o aprimoramento dos controles internos;

II - elaborar relatório das auditorias realizadas e propor medidas preventivas e corretivas dos desvios detectados, se for o caso, encaminhando-o à Diretoria Colegiada; e

III - consolidar as informações requeridas pelos órgãos de controle interno e externo.

Art. 16. À Corregedoria compete:

I - exercer as atividades de órgão seccional do Sistema de Correição do Poder Executivo federal-SISCOR;

II - planejar, dirigir, orientar, supervisionar, avaliar e controlar as atividades de correição no âmbito da ANCiber;

III - instaurar, de ofício ou por meio de representações e denúncias, de sindicâncias, inclusive as patrimoniais, de processos administrativos disciplinares e de demais procedimentos correcionais para apuração de responsabilidade por irregularidades praticadas na ANCiber;

IV - decidir sobre o arquivamento de denúncias e representações;

V - encaminhar para julgamento pela Diretoria Colegiada os processos administrativos disciplinares que possam implicar a aplicação de penalidades de sua competência; e

VI - exercer as demais competências previstas no art. 5º do Decreto nº 5.480, de 30 de junho de 2005.

Art. 17. À Inteligência compete:

I - assessorar o Diretor-Geral e os demais Diretores nas áreas de inteligência e contrainteligência, na tomada de decisões de caráter estratégico;

II - integrar atividades de inteligência de cibersegurança e ciberdefesa, voltadas para as áreas de atuação da ANCiber, em consonância com os órgãos de inteligência federais e estaduais;

III - produzir conhecimento que subsidie:

a) o processo decisório da ANCiber, em especial aquele relacionado às análises de pedidos de autorizações, processos de revogação e cancelamentos de registros dos agentes regulados pela Agência;

b) ações de órgãos de segurança pública e de defesa destinadas a neutralizar, coibir, inibir e reprimir atos ilícitos relativos ao setor regulado pela ANCiber;

c) o planejamento e a execução das medidas relacionadas à cibersegurança, de dados, de conhecimentos, de bens patrimoniais e de servidores politicamente expostos; e

d) a tomada de decisão por meio do acompanhamento da dinâmica da cibersegurança nacional e internacional;

IV - planejar, propor e executar operações integradas com outros órgãos da administração pública e apresentar quando necessário, medidas corretivas a serem aplicadas à ANCiber;

V - acompanhar o monitoramento interno de segurança; e

VI - propor medidas de controle do acesso do público externo aos prédios da ANCiber e em eventos promovidos pela Agência.

VII - representar a ANCiber junto ao Sistema Brasileiro de Inteligência (Sisbin) na troca de informações e conhecimentos de Inteligência.

Art. 18. Às Superintendências compete planejar, organizar, executar, controlar e avaliar os processos organizacionais e operacionais da ANCiber.

CAPÍTULO IV

DAS ATRIBUIÇÕES DOS DIRIGENTES

Art. 19. São atribuições do Diretor-Geral:

I - representar a ANCiber;

II - exercer a gestão administrativa no que se refere a pessoal e serviços e coordenar as unidades administrativas;

III - presidir as sessões da Diretoria Colegiada;

IV - firmar acordos, contratos, convênios, ajustes e outros instrumentos congêneres, conforme decisão da Diretoria Colegiada;

Parágrafo único. O Diretor-Geral poderá delegar atos de gestão administrativa.

Art. 20. São atribuições dos membros da Diretoria Colegiada:

I - cumprir e fazer cumprir as disposições regulamentares previstas.

II - zelar pelo cumprimento dos planos e dos programas da ANCiber;

III - praticar e expedir os atos de gestão administrativa no âmbito de suas atribuições delegadas, observado o Regimento Interno; e

IV - executar as decisões adotadas pela Diretoria Colegiada.

Art. 21. Ao Chefe de Gabinete, ao Secretário-Geral, ao Procurador-Chefe, ao Ouvidor, ao Auditor-Chefe, ao Corregedor, ao Executivo de Inteligência, aos Superintendentes e aos Gerentes incumbe planejar, dirigir, coordenar e orientar a execução das atividades das respectivas Unidades e exercer outras atribuições que lhes forem cometidas em Regimento Interno.

CAPÍTULO VI

DISPOSIÇÕES FINAIS

Art. 22. 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:

I - o Diretor-Geral com mandato de cinco anos;

II - um Diretor nomeado com mandato de quatro anos;

III - um Diretor nomeado com mandato de três anos;

IV - um Diretor nomeado com mandato de dois anos; e

V - um Diretor nomeado com mandato de um ano.

§ 1º Na hipótese de vacância no curso do mandato, o Diretor-Geral ou o Diretor nomeado em substituição ocupará o cargo pelo prazo remanescente para o fim do mandato.

§ 2º Os integrantes da primeira Diretoria da Agência Nacional de Cibersegurança, previamente aprovados pelo Senado Federal, serão nomeados na mesma data de entrada em vigor do ato do Poder Executivo que aprovar o regulamento e a estrutura regimental da Agência Nacional de Cibersegurança.

§ 3º Os integrantes da primeira Diretoria da ANCiber nomeados em conformidade com o § 2º deliberarão em reunião da Diretoria Colegiada sobre a designação dos Diretores a cada uma das Diretorias instituídas pelo regimento interno.

Art. 23. A ANCiber disponibilizará ao Gabinete de Segurança Institucional da Presidência da República as informações relativas ao setor de cibersegurança e às suas atividades, com vistas a subsidiar a formulação de políticas públicas.

Art. 24. A Diretoria Colegiada estabelecerá, no prazo de cento e oitenta dias, contado da data de entrada em vigor deste Decreto, os critérios para ocupação dos cargos e funções em comissão da ANCiber, que considerarão, como parâmetro, os requisitos para ocupação de cargos e funções em comissão na administração pública federal.

Nota Técnica SSIC/GSI nº 01/2023

Assunto: Proposta de Projeto de Lei de criação da Política Nacional de Cibersegurança

Sumário Executivo

Esta nota técnica busca mensurar o impacto sobre as contas públicas brasileiras do Projeto de Lei de iniciativa do GSI, visando a criação da Política Nacional de Cibersegurança.

Referido projeto cria um Comitê Nacional de Cibersegurança (CNCiber) e um Gabinete de Gerenciamento de Cibercrises (GGCiber) cuja participação é não remunerada, de sorte que não apresentam impacto significativo nas contas públicas.

O maior impacto decorre da criação da Agência Nacional de Cibersegurança (ANCiber) cujo modelo adotado é aquele de uma agência reguladora, inicialmente prevista para contar com 800 (oitocentos) servidores quando atingido seu efetivo integral, planejado para ser alcançado ao final de 5 (cinco) anos contados de sua instalação pelo Poder Executivo. Esse impacto é analisado a seguir.

Anexo I, Artigos 24 e 25

O artigo 24 cria 550 (quinhentos e cinquenta) cargos de Especialista em Cibersegurança. Referida especialidade foi criada no Art. 23, sendo equiparada aos cargos de especialistas das demais Agências Reguladoras já existentes na Administração Pública Federal.

Em se tratando de uma nova carreira, quando da realização de concurso público os admitidos iniciarão no primeiro nível desta, e passarão por progressões ao longo dos anos de implantação da Agência.

O artigo 24 cria também 225 (duzentos e vinte e cinco) cargos de Analista Administrativos, uma carreira já existente na legislação atinente às Agências Reguladoras.

De sua parte, o artigo 25 cria 25 (vinte e cinco) cargos de Procurador Federal.

Os cálculos aqui realizados levam em conta as progressões de carreira e também o quantitativo de pessoal previsto para cada ano de implantação. O cômputo considera também encargos sociais sobre os subsídios nominais.

Item	Ano 1	Ano 2	Ano 3	Ano 4	Ano 5
Pessoal no Ano	81	121	160	200	238
Pessoal Acum.	81	202	362	562	800
Subsídios	30.800.443,92	77.763.657,36	141.210.153,36	221.864.732,16	319.657.316,88

Observa-se que o quantitativo total de 800 (oitocentos) servidores coloca a ANCiber como do mesmo tamanho da ANEEL e um pouco menor que a ANP, muito menores que suas congêneres ANAC, ANVISA e ANATEL, por exemplo.

Em termos comparativos internacionais, a ANCiber proposta é significativamente menor que suas congêneres norte-americana (NSA e CISA), britânica (NCSC) e francesa (ANSSI), e similar à italiana (ACN).

Anexo I, Artigos 32

O artigo 32 cria 45 (quarenta e cinco) cargos (CD e CCE) e 255 (duzentas e cinquenta e cinco) funções (FCE), conforme tabela abaixo.

Função	Descrição	CCE	FCE
CD-I	Cargo Comissionado de Direção I	1	0
CD-II	Cargo Comissionado de Direção II	4	0
CCE/FCE-16	Cargo/Função Comissionado Executivo 16	4	6
CCE/FCE-15	Cargo/Função Comissionado Executivo 15	4	6
CCE/FCE-14	Cargo/Função Comissionado Executivo 14	8	12
CCE/FCE-13	Cargo/Função Comissionado Executivo 13	8	12
CCE/FCE-12	Cargo/Função Comissionado Executivo 12	8	12
CCE/FCE-11	Cargo/Função Comissionado Executivo 11	8	12
CCE/FCE-10	Cargo/Função Comissionado Executivo 10	0	20
CCE/FCE-09	Cargo/Função Comissionado Executivo 9	0	25
CCE/FCE-08	Cargo/Função Comissionado Executivo 8	0	25
CCE/FCE-07	Cargo/Função Comissionado Executivo 7	0	40
CCE/FCE-06	Cargo/Função Comissionado Executivo 6	0	40
CCE/FCE-05	Cargo/Função Comissionado Executivo 5	0	45
Total		45	255

Para tal conjunto de cargos e funções estimou-se o custo abaixo, considerando-se também os encargos sociais aplicáveis e o quantitativo de pessoal previsto para cada ano de implantação.

Item	Ano 1	Ano 2	Ano 3	Ano 4	Ano 5
Pessoal no Ano	81	121	160	200	238
Pessoal Acum.	81	202	362	562	800
Funções	19.583.069,57	31.882.512,24	36.820.265,38	36.820.265,38	36.820.265,38

Custo Total Estimado

Considera-se que o custo de pessoal não pode ultrapassar 60% (sessenta por cento) do orçamento total da agência.

Outrossim, o custo total da agência, quando plenamente instalada, a partir de seu quinto ano de existência, é estimado para pouco menos de 600 milhões de reais anuais, conforme demonstrado na tabela a seguir.

Item	Ano 1	Ano 2	Ano 3	Ano 4	Ano 5
Pessoal no Ano	81	121	160	200	238
Pessoal Acum.	81	202	362	562	800
Subsídios	30.800.443,92	77.763.657,36	141.210.153,36	221.864.732,16	319.657.316,88
Funções	19.583.069,57	31.882.512,24	36.820.265,38	36.820.265,38	36.820.265,38
Pessoal	50.383.513,49	109.646.169,60	178.030.418,74	258.684.997,54	356.477.582,26
Custeio & Investimento	33.589.008,99	73.097.446,40	118.686.945,82	172.456.665,02	237.651.721,50
Total	83.972.522,48	182.743.616,00	296.717.364,56	431.141.662,56	594.129.303,76

De outra parte, estimativas de consultorias internacionais apontam que as perdas financeiras com ciberofensas no Brasil em 2023 podem ultrapassar os USD 100 bilhões (cem bilhões de dólares americanos), valor próximo a BRL 500 bilhões (quinhentos bilhões de reais). E esse valor cresce a cada ano. Isso faz com que o custo da ANCiber completa, após o quinto ano de sua instalação, seja cerca de 0,1% (um décimo por cento) do prejuízo previsto para o país este ano. Considerando-se que quase 90% (noventa por cento) dessas ciberofensas são de baixa complexidade, se a ANCiber puder ajudar a reduzir em apenas 10% as perdas projetadas, ela ainda custará menos de 10% da economia que trará ao país.