BRASIL CONTEMPORÂNEO

Artigo convidado. Editor responsável: Marco Antonio Teixeira
Versão traduzida | DOI: https://doi.org/10.12660/cgpc.v29.90972

QUAL É O FUTURO DA GOVERNANÇA DE CIBERSEGURANÇA NO BRASIL?

What is the future of Brazil's cybersecurity governance?

¿Cuál es el futuro de la gobernanza de ciberseguridad de Brasil?

Luiz Rogério Franco Goldoni[*1,2] | luizrfgoldoni@gmail.com | ORCID: 0000-0001-5257-9470
Karina Furtado Rodrigues[1,3] | karinafrodrigues@gmail.com | ORCID: 0000-0001-9330-6399
Breno Pauli Medeiros[1,2,4] | breno.pauli@gmail.com | ORCID: 0000-0002-9839-5252

[*] Autor correspondente
[1]Escola de Comando e Estado-Maior do Exército, Programa de Pós-Graduação em Ciências Militares, Rio de Janeiro, RJ, Brasil
[2]Laboratório de Poder Cibernético, Rio de Janeiro, RJ, Brasil
[3]Laboratório de Governança, Gestão e Políticas Públicas em Defesa Nacional, Rio de Janeiro, RJ, Brasil
[4]Centro de Tecnologia e Sociedade, Fundação Getulio Vargas, Rio de Janeiro, RJ, Brasil

RESUMO

Em 2023, o Brasil promulgou sua primeira política nacional de cibersegurança. Esta surgiu como resposta a diagnósticos preocupantes, que colocam a segurança da informação e a cibersegurança entre as vulnerabilidades de alto risco da administração pública brasileira, segundo relatório de 2022 do Tribunal de Contas da União (TCU). O que está por vir para a recém-promulgada Política Nacional de Cibersegurança (PNCiber) do Brasil? Nossa análise visa responder a essa pergunta, primeiro desvendando a estrutura de governança cibernética existente que a nova política herdou e, segundo, analisando a estrutura de governança debatida e promulgada pela política atual. Conclui-se que o Brasil fez diversos esforços para securitizar o ciberespaço por meio de uma coleção ampla, porém desconexa, de documentos, cuja maturidade de implementação não está clara, sem que a PNCiber forneça ferramentas de políticas públicas diretas para enfrentar esses desafios.

Palavras-chave: governança, cibersegurança, Brasil, análise de políticas públicas, PNCiber.

ABSTRACT

In 2023, Brazil enacted its first national cybersecurity policy. The policy emerged as a response to worrisome diagnoses, which listed information security and cybersecurity among Brazil's public administration high-risk vulnerabilities, according to a 2022 report from the Federal Court of Auditors. What lies ahead for Brazil's newly enacted Cybersecurity National Policy? Our analysis aims to answer this question by unraveling the existing cyber governance structure that the new policy inherited and by analyzing the governance structure debated and enacted by the current policy. We conclude that Brazil has made several efforts to securitize cyberspace through a broad but disconnected collection of documents; their implementation maturity is unclear, and the Cybersecurity National Policy fails to design straightforward policy tools to address those challenges.

Keywords: *governance, cybersecurity, Brazil, public policy analysis, PNCiber.*

RESUMEN

En 2023, Brasil promulgó su primera política nacional de ciberseguridad. Esta surgió como respuesta a diagnósticos preocupantes, que sitúan la seguridad de la información y la ciberseguridad entre las vulnerabilidades de alto riesgo de la administración pública brasileña, según un informe de 2022 del Tribunal Federal de Cuentas. ¿Qué depara el futuro para la recién promulgada Política Nacional de Ciberseguridad de Brasil? Nuestro análisis busca responder a esta pregunta, primero desentrañando la estructura de gobernanza cibernética existente que la nueva política heredó y, segundo, analizando la estructura de gobernanza debatida y promulgada por la política actual. El desafío es que Brasil ha realizado varios esfuerzos para resguardar el ciberespacio a través de una amplia pero desconectada colección de documentos, cuya madurez de implementación no está clara, y la Política Nacional de Ciberseguridad (PNCiber) no logra diseñar herramientas de políticas públicas directas para abordar esos desafíos.

Palabras-clave: *gobernanza, ciberseguridad, Brasil, análisis de políticas públicas, PNCiber.*

INTRODUÇÃO

O que está por vir para a política de cibersegurança do Brasil? Os esforços do País para proteger o ciberespaço atingiram um marco em 2023 com a promulgação da Política Nacional de Cibersegurança (PNCiber), pelo Decreto Presidencial n. 11.856. A política estabelece metas de segurança cibernética e cria o Comitê Nacional de Cibersegurança (CNCiber), no qual representantes de distintos setores da sociedade podem desenvolver programas e estratégias políticas subsequentes.

O decreto surgiu como resposta a um diagnóstico preocupante. Conforme relatório do Tribunal de Contas da União (TCU, 2022), a segurança da informação e a segurança cibernética são vulnerabilidades de alto risco para a administração pública do País. O relatório revela que 73,1% dos serviços do Governo Federal dependem inteiramente de plataformas digitais; considerados os que dependem delas parcialmente, o percentual sobe para 83,7%. Ademais, 74,6% das organizações públicas não possuem políticas de *backup* estabelecidas e, entre aquelas com tais políticas, 66% não criptografam seus dados. O TCU enfatiza que a legislação brasileira atual não aloca autoridades ou recursos para regular o ciberespaço. O relatório destaca incidentes cibernéticos no Conecte-SUS, no Superior Tribunal de Justiça e na Controladoria-Geral da União. E conclui que o Governo Federal e o setor público em geral carecem de preparação e capacitação suficientes para proteger os bens públicos no ciberespaço.

A PNCiber não é o único esforço para proteger o ciberespaço no País. Desde o início da década de 2000, foram feitos avanços paulatinos e significativos, no que diz respeito às políticas relacionadas ao ciberespaço. Entre 2018 e 2020, foram estabelecidas duas normas cruciais: a Política Nacional de Segurança da Informação (PNSI, Decreto n. 9.637, 2018) e a Estratégia Nacional de Segurança Cibernética (E-Ciber, Decreto n. 10.222, 2020). Essas iniciativas previam um único ator para coordenar e gerir as estruturas nacionais de cibersegurança: o Gabinete de Segurança Institucional da Presidência da República (GSI).

Essas e outras normas que analisaremos estabeleceram uma estrutura de governança ignorada pela maioria dos estudiosos da administração pública brasileira. Prova disso é a ausência de artigos com a palavra-chave "cibersegurança" nas principais revistas de administração pública do País, como *Cadernos Gestão Pública e Cidadania*, *Revista de Administração Pública* e *Administração Pública e Gestão Social*.

Curiosamente, políticas cibernéticas são perfeitas para uma perspectiva de governança em que é crucial ter arranjos institucionais orientados para resolver problemas públicos num contexto no qual as fronteiras de responsabilidade são confusas, onde é necessária uma pluralidade de atores autônomos, tanto de dentro como de fora do Estado, e quando o melhor papel que os governos podem desempenhar é o de orientar e guiar (Milward & Provan, 2000; Peci et al., 2008; Stoker, 1998).

Por conseguinte, esses mecanismos de governança devem ser capazes de definir eficazmente objetivos, atribuir responsabilidades e melhorar a performance geral dessa rede de atores e políticas. Apesar de abundantes, as normas brasileiras são desconexas e possuem maturidade de implementação incerta. O GSI, responsável pela criação e acompanhamento de sua imple-

mentação, não possui capacidade suficiente para fazê-lo sozinho (Goldoni et al., 2023), e por vezes conta com o Exército Brasileiro para realizar algumas de suas atividades. A PNCiber também não conta com recursos financeiros e mão de obra para que saia totalmente do papel, pelo menos por enquanto.

Definimos dois objetivos secundários para compreender o futuro da governança de cibersegurança no Brasil: (i) traçar a governança da cibersegurança existente nas normas anteriores à PNCiber; (ii) avaliar os desafios impostos pela nova política às questões existentes, considerando as disparidades notáveis entre a minuta da PNCiber apresentada no primeiro semestre de 2023 e o decreto posteriormente promulgado.

A próxima seção defende que a governança é crucial para a cibersegurança; a terceira seção investiga a estrutura de governança brasileira relacionada à cibersegurança; a seguinte discute os propósitos e limites da PNCiber, comparando-a com o projeto de lei apresentado meses antes de sua promulgação; a quinta seção apresenta nossas considerações finais.

PORQUE É CRUCIAL ANALISAR A CIBERSEGURANÇA SOB A ÓTICA DA GOVERNANÇA

Governança é um termo polissêmico que pode receber muitos adjetivos, tais como: colaborativa, assimétrica, em rede, participativa, e assim por diante (Ansell & Torfing, 2022; Buta & Teixeira, 2020; Calmon & Costa, 2013). Este artigo parte da perspectiva da governança pública como paradigma da administração pública, onde a governança geralmente engloba processos de tomada de decisão envolvendo atores públicos e privados num esforço combinado para fornecer serviços ou resolver problemas públicos específicos. Esse entendimento alinha-se com a definição de Stoker (1998), que é composta por cinco "proposições":

1. A governança refere-se a um conjunto de instituições e atores pertencentes ou não ao governo.
2. A governança identifica a indefinição das fronteiras e responsabilidades na abordagem das questões sociais e econômicas.
3. A governança identifica a dependência de poder nas relações entre instituições envolvidas na ação coletiva.
4. A governança é sobre redes de atores autônomos e autogovernados.
5. A governança reconhece a capacidade de fazer as coisas, estas que independem do poder do governo para comandar ou usar sua autoridade. Considera o governo capaz de utilizar novas ferramentas e técnicas para orientar e guiar ações (p.16, tradução nossa).

Ademais, a chave para a governança é a mobilização de uma pluralidade de atores capazes de lidar com complexos problemas sociais, o que pode envolver agências do Estado

ou de entidades públicas e privadas. Esse arranjo institucional de resolução de problemas enquadra-se perfeitamente nas políticas de cibersegurança" por "como uma luva na realidade e desafios das políticas de cibersegurança. O porquê é a seguir explorado.

A cibersegurança de um país reside na segurança de uma infinidade de atores. Atores estatais englobam agências que prestam serviços sociais que, se paralisados, podem comprometer políticas públicas fundamentais. Empresas privadas também desempenham papel vital na cibersegurança de um país, especialmente aquelas consideradas de "infraestrutura crítica".

Consequentemente, as agências reguladoras dos setores de infraestruturas críticas desempenham papel essencial na criação e exigência de medidas de cibersegurança para as empresas, oferecendo-lhes apoio em caso de ciberataques. Se uma empresa ou agência for atacada, deverá ser capaz de identificar e sanar o ataque. No entanto, frequentemente, nem as agências, nem as empresas têm recursos suficientes para manter pessoal de TI altamente treinado. Nesse ponto, torna-se fundamental saber quem pode ajudar e a quem informar o ataque. Ademais, se os ataques forem direcionados a variadas agências e empresas, as ferramentas de comunicação podem ser ainda mais importantes para os identificar e neutralizar.

Assim, se a política encarar os serviços digitais, sistemas de informação governamentais, agências e empresas de maneira compartimentada, sem levar a governança a sério, provavelmente haverá muitas vulnerabilidades, com impactos potencialmente maiores devido à fraca resiliência cibernética (Linkov & Kott, 2019). Logo, as políticas cibernéticas devem considerar todos os cinco princípios de Stoker sobre governança.

A ESTRUTURA DE GOVERNANÇA DA CIBERSEGURANÇA HERDADA PELA PNCIBER

Os esforços para proteger o ciberespaço brasileiro remontam a 2008, quando a defesa cibernética foi considerada um setor estratégico na Estratégia Nacional de Defesa. Após, houve a publicação do Livro Verde de Segurança Cibernética em 2010, que estabeleceu as bases para o desenvolvimento de uma PNCiber (Hurel, 2021).

A década seguinte viu o desenvolvimento da Lei de Crimes Cibernéticos (Lei n. 12.737, 2012) contra invasão e adulteração de computadores, complementada pela Lei n. 12.735 (2012), que criou polícias especializadas para tratar de crimes digitais. Seguiram-se o Marco Civil da Internet (Lei n. 12.965, 2014) e a Lei Geral de Proteção de Dados Pessoais (LGPD, Lei n. 13.709, 2018), que serviram como pilares legislativos para os direitos individuais e a proteção e privacidade de dados *on-line*.

Esforços mais recentes para digitalizar a administração pública brasileira incluíram: a Estratégia Brasileira para a Transformação Digital (E-Digital, Decreto n. 9.319, 2018), o Decreto de Governança e Compartilhamento de Dados (Decreto n. 10.046, 2019) e a Política de Governança Digital (Decreto n. 8.638, 2016). Esta foi substituída pela Estratégia de Governo Digital para 2020-2022 (Decreto n. 10.332, 2020).

A E-Digital é particularmente relevante para a nossa análise. Formulada pelo Ministério da Ciência, Tecnologia, Inovação, propõe melhores práticas para infraestruturas críticas e ciberespaço. Essa ênfase na proteção de infraestruturas críticas foi detalhada por meio da Política Nacional de Segurança de Infraestruturas Críticas (PNSIC, Decreto n. 9.573, 2018), da Estratégia Nacional de Segurança de Infraestruturas Críticas (ENSIC, Decreto n. 10.569, 2020) e do Plano Nacional de Segurança de Infraestruturas Críticas (PLANSIC, Decreto n. 11.200, 2022).

Os riscos cibernéticos são brevemente reconhecidos pelo objetivo estratégico da ENSIC de "incentivar a adoção de recursos e de procedimentos voltados para a segurança cibernética nas infraestruturas críticas" (Decreto n. 10.569, 2020, p. 9). Adicionalmente, a PLANSIC reconhece que deve seguir a E-Ciber (Decreto n. 10.222, 2020) e a Rede Federal de Gestão de Incidentes Cibernéticos (ReGIC, Decreto n. 10.748, 2021), adiante analisados.

Essa estrutura regulatória, que compreende política, estratégia e plano, é replicada em outros documentos nacionais que abordam o tema "ciber". A Política Nacional de Segurança de Infraestruturas Críticas (PNSI), base da governança cibernética do País, foi lançada inicialmente em 2018 e atualizada em 2021. Ela define amplamente segurança da informação como segurança cibernética, defesa cibernética, segurança de dados físicos e confidencialidade, integridade, e garantia de disponibilidade das informações. Alinhado com a E-Digital, a PNSI enfatiza a necessidade de uma política nacional de cibersegurança que reúna os setores público e privado.

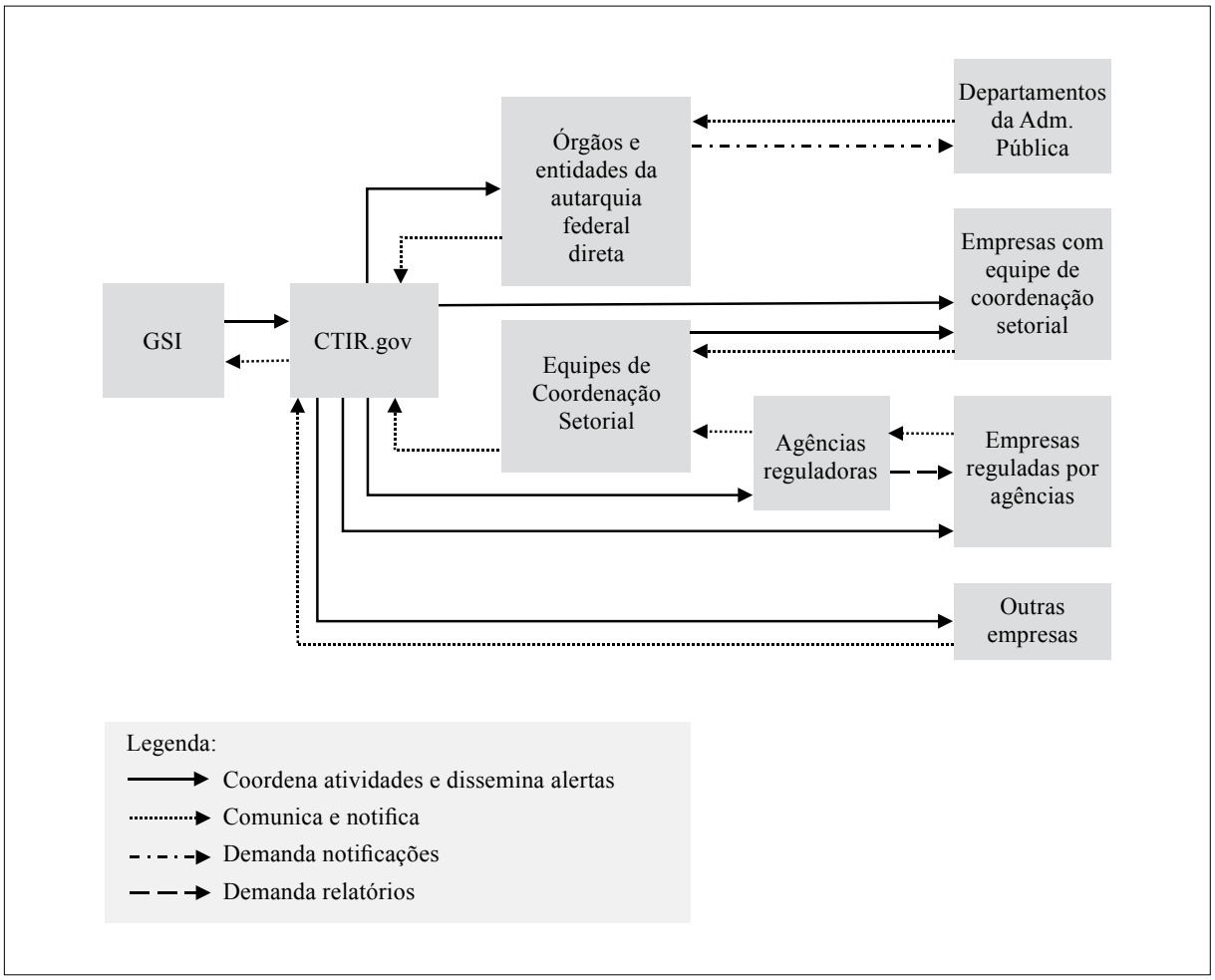
Tal normativa destaca a coordenação entre diversas instituições, adotando uma abordagem *top-down*, com o GSI liderando os esforços de segurança da informação. O documento antecipa o desenvolvimento de uma Estratégia Nacional de Segurança da Informação (ENSI) com módulos que abrangem cibersegurança, ciberdefesa, segurança de infraestruturas críticas, segurança de informações confidenciais e proteção contra vazamentos de dados. Porém, apenas a E-Ciber, válida até 2023, foi publicada.

A PNSI determina o papel do Ministério da Defesa no apoio ao GSI para a cibersegurança, reconhecendo a intersecção entre segurança e defesa cibernética. Em sua versão atualizada de 2021 (Decreto n. 10.641, 2021), a PNSI requer que os entes federais estabeleçam equipes de resposta a incidentes cibernéticos coordenadas pelo CTIR.gov, como parte de uma rede mais ampla de resposta a incidentes. Essa evolução levou à criação da ReGIC, em 2021 (Decreto n. 10.748, 2021), com o objetivo de aprimorar a coordenação entre os órgãos federais para prevenção, tratamento e resposta a incidentes cibernéticos. A ReGIC determina a adesão de entidades da administração pública e estabelece o prazo de 12 meses para implementação integral dessa diretriz.

Embora o termo "governança" esteja ausente na documentação da ReGIC, esta detalha como responder a incidentes cibernéticos, determinando que as agências públicas se reportem às equipes de coordenação do setor ou diretamente ao CTIR.gov. O desenho de rede da ReGIC descreve procedimentos de resposta a incidentes e especifica setores que demandam equipes de coordenação. O artigo 11 obriga o CTIR.gov a coordenar os esforços de resposta a incidentes cibernéticos dos membros da ReGIC, enquanto o artigo 12 atribui às equipes a responsabili-

dade de relatar vulnerabilidades e incidentes que afetem a infraestrutura crítica nacional. Isso estabelece uma governança de rede de cima para baixo, ilustrada na Figura 1.

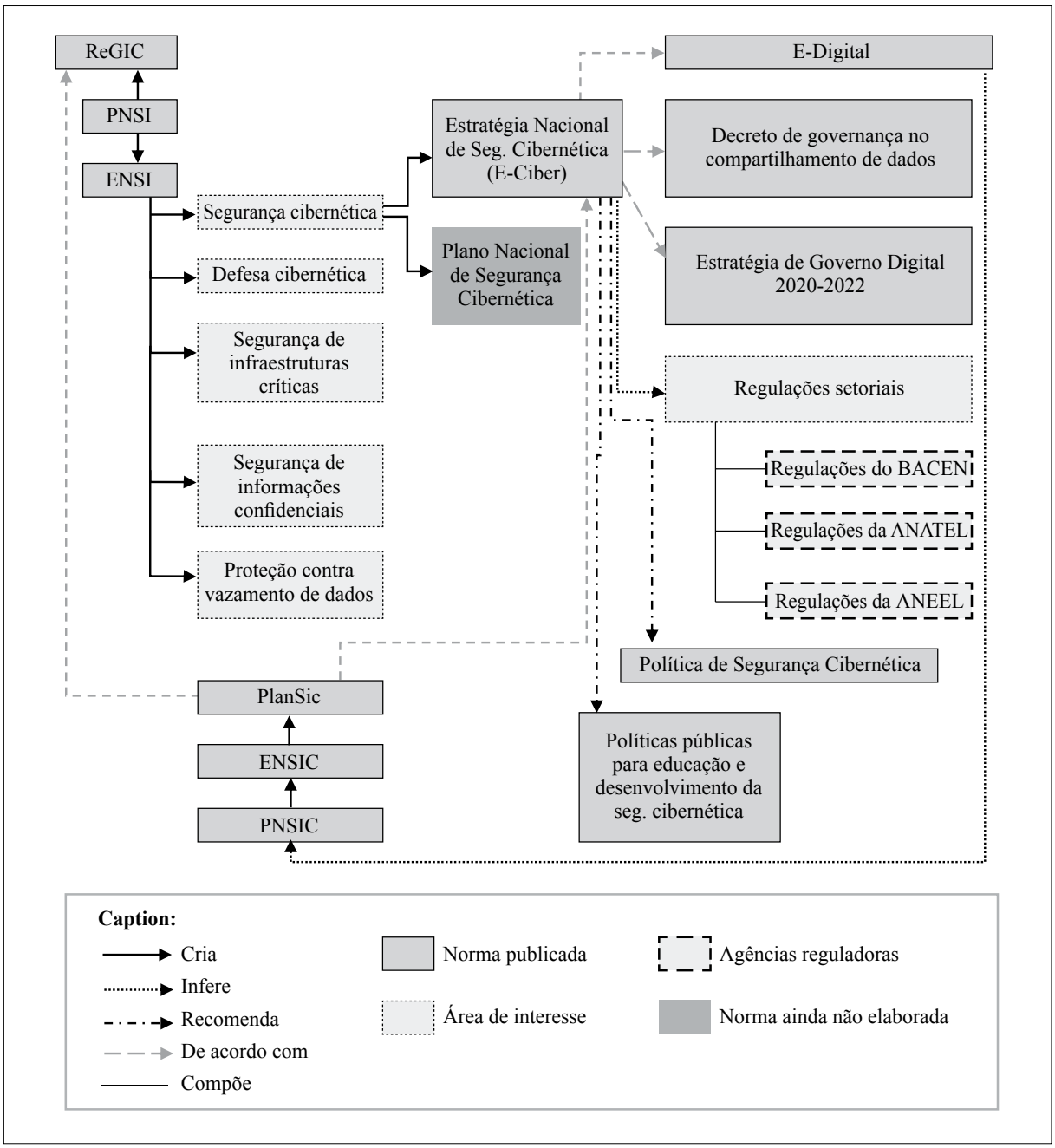
Figura 1 – Estrutura de Governança da ReGIC



Fonte: Adaptado da ReGIC (Decreto n. 10.748, 2021).

As estruturas sobrepostas sustentadas por essas diferentes políticas e estratégias criam um sistema complexo de interação e governança de rede no ciberespaço brasileiro. A Figura 2 mapeia essas relações.

Figura 2 – Conexões entre as Normas de E-governança e Segurança da Informação no Brasil



No nível setorial, e espelhando as exigências da ReGIC, a Agência Nacional de Telecomunicações (ANATEL) (artigo 9º da sua resolução) regulamenta que a notificação dos incidentes cibernéticos mais relevantes deve ocorrer de modo horizontal, entre associados e empresas, bem como verticalmente, para ela própria (Resolução Normativa ANATEL n.740, 2020). No caso

da Agência Nacional de Energia Elétrica (ANEEL), esta deve ser notificada sobre os incidentes cibernéticos mais relevantes, mas sua resolução omite a menção à notificação horizontal (Resolução Normativa ANEEL n. 964, 2021).

Enquanto a E-Ciber recomenda regulamentações setoriais, a ReGIC estabelece planos setoriais para a gestão de incidentes cibernéticos. Estes são obrigatórios e devem ser desenvolvidos por equipes de coordenação setorial. Conforme a ReGIC (artigo 13), o GSI deve divulgar a periodicidade e os elementos essenciais desses planos. Seu Plano Setorial de 2022 estabelece diretrizes para os demais planos setoriais (Portaria GSI/PR n. 120, 2022). Apesar de algumas agências reguladoras, como o Banco Central (BACEN), a ANATEL e a ANEEL, implementarem regulamentações setoriais, estas não foram totalmente alcançadas em todos os setores e agências.

PROMESSAS E REALIDADE DA PNCIBER

Esta seção analisa o que a PNCiber acrescenta à antiga governança cibernética, sabendo que há significativas diferenças entre o que o GSI apresentou em maio de 2023 num projeto de lei e o decreto promulgado em 26 de dezembro de 2023.

A minuta de maio de 2023

O projeto de lei de maio de 2023 publicado pelo GSI previa a criação da Política Nacional de Cibersegurança. A minuta era extensa e abordava o estabelecimento da PNCiber, a criação da Agência Nacional de Cibersegurança (ANCiber), do Comitê Nacional de Cibersegurança (CNCiber) e do Gabinete de Gestão de Crise Cibernética (GSI, 2023).

Quatro das 45 páginas do documento foram dedicadas a uma "Apresentação" e seis, a uma "Exposição de Motivos", onde foram elencadas vulnerabilidades nacionais relacionadas à cibersegurança, baseadas em *rankings* e estudos internacionais e nacionais que destacaram riscos e prejuízos que incidentes cibernéticos causam à economia brasileira. O objetivo era justificar os investimentos necessários para a criação da ANCiber, considerada pelo documento como essencial para o alcance dos objetivos da PNCiber.

A minuta também afirmava que um dos objetivos (GSI, 2023) era "unificar a 'colcha de retalhos' regulatória existente no país" (p. 1). Contudo, uma leitura cuidadosa do documento pode indicar o contrário, pois ele não menciona em nenhum momento a PNSIC ou a PNSI, e a E-Ciber aparece apenas em alguns parágrafos da segunda página da "Exposição de Motivos". A ReGIC é mencionada apenas nominalmente no meio do documento, sem qualquer ênfase. Isso pode apontar para a ineficiência ou substituição das antigas normas e estruturas ou, pior, que elas eram "letra morta".

Os objetivos enumerados no projeto de lei são amplos e ambiciosos. Entretanto, o documento não menciona como seriam alcançados. Há apenas menções a uma futura estratégia nacional de cibersegurança, a um plano nacional de cibersegurança e à ANCiber.

Ademais, conforme Goldoni et al. (2023), o documento é omisso sobre como a ANCiber se relacionaria com as agências reguladoras existentes. "Haveria a supressão de competências nas outras agências? As demais agências reguladoras seriam reguladas pela ANCiber? Poderiam ser responsabilizadas por ela?" (Goldoni et al., 2023). Além disso, como a ANCiber seria financiada?

As respostas a essas questões são vitais para vislumbrar a governança a ser implementada. Principalmente porque a agência aparenta ser a força gravitacional da minuta e, se criada, contaria com 800 novos servidores públicos e com outros 300 cargos comissionados, em um mercado de trabalho carente de pessoal e com difícil retenção, o que demandaria altos salários. Não se sabe o quanto a dificuldade de financiamento contribuiu para a ausência de menção à ANCiber na publicação da PNCiber em dezembro de 2023.

A política promulgada pelo Decreto n. 11.856 (2023)

A política promulgada é bem mais curta que a minuta, totalizando aproximadamente quatro páginas. Foi assinada pelo presidente Lula, em 26 de dezembro de 2023, por meio do Decreto n. 11.856 (2023). Sua publicação via decreto, e não por projeto de lei, sugere que o tema não ganhou a devida relevância no Congresso Nacional.

Em relação aos objetivos, ocorreram poucas, mas significativas, mudanças, como pode ser visto na Figura 3. A remoção da promoção do "uso ético de ciberativos e das tecnologias a eles associadas no país" (objetivo VII do projeto) e a inclusão do desenvolvimento de "regulação, fiscalização e controle destinados a aprimorar a segurança e a resiliência cibernéticas nacionais" (objetivo X da política publicada) se destacam. Nesse ponto, objetivos subjetivos foram substituídos por outros mais concretos (mecanismos de regulação e controle).

Figura 3 – Objetivos da PNCiber

OBJETIVOS APRESENTADOS NA MINUTA	OBJETIVOS NO DECRETO N. 11.856 (2023)
I – garantir a confidencialidade, a integridade, a autenticidade e a disponibilidade dos ciberativos de interesse da sociedade brasileira	I – promover o desenvolvimento de produtos, serviços e tecnologias de caráter nacional destinados à segurança cibernética
II – fomentar a ciberproteção e a ciber-resiliência do Poder Público, dos ciberativos de interesse e da sociedade como um todo	II – garantir a confidencialidade, a integridade, a autenticidade e a disponibilidade das soluções e dos dados utilizados para o processamento, o armazenamento e a transmissão eletrônica ou digital de informações
III – desenvolver na sociedade brasileira a cultura de cibersegurança	III – fortalecer a atuação diligente no ciberespaço, especialmente das crianças, dos adolescentes e dos idosos

(continua)

(conclusão)

Figura 3 – Objetivos da PNCiber

OBJETIVOS APRESENTADOS NA MINUTA	OBJETIVOS NO DECRETO N. 11.856 (2023)
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	IV – contribuir para o combate aos crimes cibernéticos e às demais ações maliciosas no ciberespaço
V – promover a autonomia produtiva e tecnológica na área de cibersegurança	V – estimular a adoção de medidas de proteção cibernética e de gestão de riscos para prevenir, evitar, mitigar, diminuir e neutralizar vulnerabilidades, incidentes e ataques cibernéticos, e seus impactos
VI – fomentar a participação do Brasil na cadeia produtiva global de produtos e serviços voltados à cibersegurança	VI – incrementar a resiliência das organizações públicas e privadas a incidentes e ataques cibernéticos
VII – promover o uso ético de ciberativos e das tecnologias a eles associadas no País	VII – desenvolver a educação e a capacitação técnico-profissional em segurança cibernética na sociedade
VIII – fomentar o combate ao cibercrime	VIII – fomentar as atividades de pesquisa científica, de desenvolvimento tecnológico e de inovação relacionadas à segurança cibernética
IX – promover ações que contribuam para a segurança e para a estabilidade do ambiente digital global	IX – incrementar a atuação coordenada e o intercâmbio de informações de segurança cibernética entre: a) a União, os Estados, o Distrito Federal e os Municípios; b) os Poderes Executivo, Legislativo e Judiciário; c) o setor privado; e d) a sociedade em geral
X – incrementar a projeção internacional do Brasil e inserir o País em processos decisórios internacionais, para fazer valer os valores e os interesses nacionais	X – desenvolver mecanismos de regulação, fiscalização e controle destinados a aprimorar a segurança e a resiliência cibernéticas nacionais
	XI – implementar estratégias de colaboração para desenvolver a cooperação internacional em segurança cibernética

Fonte: Decreto n. 11.856 (2023) GSI (2023, p. 14).

Ademais, a política publicada detalhou e desenvolveu objetivos previamente apresentados na minuta: o objetivo I da política engloba os objetivos V e VI da minuta, enquanto os objetivos III e VII da PNCiber desenvolvem ideias contidas no objetivo III da minuta. Outro exemplo notável foi a mudança na redação do objetivo X da minuta, que passou a ser representado pelo objetivo XI da política.

À semelhança da minuta, a PNCiber indica que caberá à Estratégia Nacional de Cibersegurança e ao Plano Nacional de Cibersegurança (ambos instrumentos da PNCiber) implementar

esses objetivos, mas se cala sobre como e quando esses mecanismos serão criados e estabelecidos. Contudo, o documento infere que o instituído CNCiber seria responsável pela implementação e atualização da PNCiber e seus instrumentos.

A importância do CNCiber pode ser medida pelo espaço que lhe é dedicado no texto do Decreto n. 11.856 (2023): quase dois terços. Em 11 de janeiro de 2024, o GSI realizou chamada pública para preenchimento de vagas no CNCiber, relacionadas a representantes da sociedade civil, de instituições científicas, tecnológicas e de inovação, e do setor empresarial. Em 9 de fevereiro, a Portaria GSI n. 6 designou todos os membros do comitê, que já realizou sua primeira reunião.

CONSIDERAÇÕES FINAIS

O Brasil desenvolveu uma miríade de legislações relativas ao seu ciberespaço, embora desconexas e com implementações nebulosas. Nem todas as agências aderiram à ReGIC, assim como nem todos os setores de infraestruturas críticas elaboraram e implementaram normas setoriais de cibersegurança, existindo uma elevada heterogeneidade entre eles. Nesse contexto, a promessa de uma Política Nacional de Cibersegurança surge com a proposta de projeto de lei do GSI.

Apesar das suas aspirações, a Política é um fragmento daquilo que inicialmente se pensava. Permaneceram seus objetivos e a criação do CNCiber. Os mecanismos de governança propostos persistirão? Com pouca ou nenhuma menção à maioria das normas anteriores, como E-Ciber, ReGIC e outras, aguardam-se os passos seguintes da PNCiber.

Dado que a política é excessivamente abrangente, há poucas pistas sobre o que será feito e quais serão os caminhos da E-Ciber e do PNCiber. Ademais, não se sabe se a ANCiber será criada, pois a PNCiber é omissa a esse respeito.

Igualmente, só o futuro dirá qual será o papel do CNCiber: propor e assessorar políticas públicas ou simplesmente endossar o que o GSI pensa e propõe. Dado o contexto histórico anteriormente relatado, só podemos torcer pela primeira opção.

REFERÊNCIAS

Ansell, C., & Torfing, J. (Eds.). (2022). *Handbook on theories of governance*. Edward Elgar Publishing.

Buta, B. O., & Teixeira, M. A. C.. (2020). Governança pública em três dimensões: Conceitual, mensural e democrática. *Organizações & Sociedade*, 27(94), 370-395. https://doi.org/10.1590/S1984-92302008000300002

Calmon, P., & Costa, A. T. M. (2013). Redes e governança das políticas públicas. *RP3-Revista de Pesquisa em Políticas Públicas*, (1), 1-29. https://periodicos.unb.br/index.php/rp3/article/view/11989

Decreto n. 8.638, de 15 de janeiro de 2016. (2016). Institui a Política de Governança Digital no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional. Brasília, DF.

Decreto n. 9.319, de 21 de março de 2018. (2018). Institui o Sistema Nacional para a Transformação Digital e estabelece a estrutura de governança para a implantação da Estratégia Brasileira para a Transformação Digital. Brasília, DF.

Decreto n. 9.573, de 22 de novembro de 2018. (2018). Aprova a Política Nacional de Segurança de Infraestruturas Críticas. Brasília, DF.

Decreto n. 9.637, de 26 de dezembro de 2018. (2018). Institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação, e altera o Decreto n. 2.295, de 4 de agosto de 1997, que regulamenta o disposto no art. 24, caput, inciso IX, da Lei n. 8.666, de 21 de junho de 1993, e dispõe sobre a dispensa de licitação nos casos que possam comprometer a segurança nacional. Brasília, DF.

Decreto n. 10.046, de 9 de outubro de 2019. (2019). Dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados. Brasília, DF.

Decreto n. 10.222, de 5 de fevereiro de 2020. (2020). Aprova a Estratégia Nacional de Segurança Cibernética. Brasília, DF.

Decreto n. 10.332, de 28 de abril de 2020. (2020). Institui a Estratégia de Governo Digital para o período de 2020 a 2022, no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional e dá outras providências. Brasília, DF.

Decreto n. 10.569, de 9 de dezembro de 2020. (2020). Aprova a Estratégia Nacional de Segurança de Infraestruturas Críticas. Brasília, DF.

Decreto n. 10.641, de 2 de março de 2021. (2021). Altera o Decreto n. 9.637, de 26 de dezembro de 2018, que institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação, e altera o que regulamenta o disposto no art. 24, caput, inciso IX, da Lei n. 8.666, de 21 de junho de 1993, e dispõe sobre a dispensa de licitação nos casos que possam comprometer a segurança nacional. Brasília, DF.

Decreto n. 10.748, de 16 de julho de 2021. (2021). Institui a Rede Federal de Gestão de Incidentes Cibernéticos. Brasília, DF.

Decreto n. 11.200, de 15 de setembro de 2022. (2022). Aprova o Plano Nacional de Segurança de Infraestruturas Críticas. Brasília, DF.

Decreto n. 11.856 de 26 de dezembro de 2023. (2023). Institui a Política Nacional de Cibersegurança e o Comitê Nacional de Cibersegurança. Brasília, DF.

Gabinete de Segurança Institucional da Presidência da República. (2022). *Portaria gsi/pr nº 120, de 21 de dezembro de 2022.* https://in.gov.br/en/web/dou/-/portaria-gsi/pr-n-120-de-21-de-dezembro-de-2022-452767918

Gabinete de Segurança Institucional da Presidência da República. (2023). *PNCiber – Apresentação do projeto*. https://www.gov.br/gsi/pt-br/ssic/audiencia-publica/PNCiberAudienciaPublicaProjetoBase.pdf

Goldoni, L., Rodrigues, K. & Oliveira, T., Jr. (2023, junho 8). O urgente debate sobre a proposta de Política Nacional de Cibersegurança. *Estadão*. https://www.estadao.com.br/

Hurel, L. M. (2021). *Cibersegurança no Brasil: Uma análise da estratégia nacional*. Instituto Igarapé. https://igarape.org.br/wp-content/uploads/2021/04/AE-54_Seguranca-cibernetica-no-Brasil.pdf

Lei n. 12.735, de 30 de novembro de 2012. (2012). Altera o Decreto-Lei n. 2.848, de 7 de dezembro de 1940 - Código Penal, o Decreto-Lei n. 1.001, de 21 de outubro de 1969 - Código Penal Militar, e a Lei n. 7.716, de 5 de janeiro de 1989, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências. Brasília, DF.

Lei n. 12.737, de 30 de novembro de 2012. (2012). Dispõe sobre a tipificação criminal de delitos informáticos. Brasília, DF.

Lei n. 12.965, de 23 de abril de 2014. (2014). Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF.

Lei n. 13.709, de 14 de agosto de 2018. (2018). Dispõe sobre Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF.

Kott, A., & Linkov, I. (Eds.). (2019). Cyber resilience of systems and networks (Vol. 1). New York, NY: Springer International Publishing.

Milward, H. B., & Provan, K. G. (2000). Governing the hollow state. *Journal of Public Administration Research and Theory*, *10*(2), 359-380. https://doi.org/10.1093/oxfordjournals.jpart.a024273

Peci, A., Pieranti, O. P., & Rodrigues, S. (2008). Governança e New Public Management: Convergências e contradições no contexto brasileiro. *Organizações & Sociedade*, *15*, 39-55. https://doi.org/10.1590/S1984-92302008000300002

Portaria GSI/PR n. 120, de 21 de dezembro de 2022. (2022). Aprova o Plano de Gestão de Incidentes cibernéticos para a administração pública federal. Brasília, DF.

Resolução n. 740, de 21 de dezembro de 2020. (2020). Aprova o Regulamento de Segurança Cibernética Aplicada ao Setor de Telecomunicações. Brasília, DF.

Resolução Normativa Aneel n. 964, de 14 de dezembro de 2021. (2021). Dispõe sobre a política de segurança cibernética a ser adotada pelos agentes do setor de energia elétrica. Brasília, DF.

Stoker, G. (1998). Governance as theory: Five propositions. *International Social Science Journal*, *50*(155), 17-28. https://doi.org/10.1111/1468-2451.00106

Tribunal de Contas da União. (2022). *Lista de alto risco da administração pública federal: Segurança da informação e segurança cibernética*. Brasília, DF. https://sites.tcu.gov.br/listadealtorisco/seguranca_da_informacao_e_seguranca_cibernetica.html

NOTA

Este artigo teve apoio da Fundação Carlos Chagas de Amparo à Pesquisa do Estado do Rio de Janeiro – Programa Jovem Cientista do Nosso Estado [E-26/201.423/2022]

CONFLITOS DE INTERESSE

Os/as autores/as não têm conflitos de interesse a declarar.

CONTRIBUIÇÃO DE AUTORIA

Luiz Rogério Franco Goldoni: Conceituação, curadoria de dados, análise formal; Investigação; Administração de projetos; Supervisão; Validação; Visualização; Redação – rascunho original; Redação – revisão e edição.

Karina Furtado Rodrigues: Conceituação; Análise formal; Aquisição de financiamento; Investigação; Metodologia; Administração de projetos; Recursos; Supervisão; Validação; Visualização; Redação – rascunho original; Redação – revisão e edição.

Breno Pauli Medeiros: Conceituação, curadoria de dados; Investigação; Visualização; Redação – rascunho original; Redação – revisão e edição.