ESCOLA DE COMANDO E ESTADO-MAIOR DO EXÉRCITO

ESCOLA MARECHAL CASTELLO BRANCO

Maj QEM MAX SILVA **ALALUNA**

Modelos de Governança Cibernética nos Estados Unidos da América (EUA) e na Espanha e a sua adequabilidade ao Brasil

Rio de Janeiro

2024

Maj QEM MAX SILVA **ALALUNA**

Modelos de Governança Cibernética nos Estados Unidos da América (EUA) e na Espanha e a sua adequabilidade ao Brasil

Trabalho de Conclusão de Curso apresentado à Escola de Comando e Estado-Maior do Exército, como requisito parcial para a obtenção do título de Especialista em Ciências Militares, com ênfase em Defesa Nacional.

Orientador: Maj Com QEMA LEANDRO KUHN

Rio de Janeiro

2024

A317m Alaluna, Max Silva

Modelos de Governança Cibernética nos Estados Unidos da América (EUA) e na Espanha e a sua adequabilidade ao Brasil. / Max Silva Alaluna. - 2024.

74 f. il. 30 cm.

Orientador : Leandro Kuhn

Trabalho de Conclusão de Curso (Especialização em Ciências Militares) - Escola de Comando e Estado-Maior do Exército, Rio de Janeiro, 2024.

Bibliografia: f. 67 - 75.

1. Governança. 2. Governança Cibernética. 3. Eua; Brasil; Espanha. 4. Capacidades Cibernéticas. 5. Atores Civis De Segurança Cibernética. I Título

CDD 003.5.

Maj QEM MAX SILVA **ALALUNA**

Modelos de Governança Cibernética nos Estados Unidos da América (EUA) e na Espanha e a sua adequabilidade ao Brasil

Trabalho de Conclusão de Curso apresentado à Escola de Comando e Estado-Maior do Exército, como requisito parcial para a obtenção do título de Especialista em Ciências Militares, com ênfase em Política, Estratégia e Administração Militar

Aprovado em 4 de outubro de 2024.

COMISSÃO AVALIADORA

Maj Com QEMA LEANDRO KUHN – Presidente
Escola de Comando e Estado-Maior do Exército

Maj Com QEMA WAGNER DE MATOS SALUSTRIANO – Membro
Escola de Comando e Estado-Maior do Exército

Maj Art QEMA CARLOS EDUARDO DA SILVA LOURENÇO – Membro
Escola de Comando e Estado-Maior do Exército

AGRADECIMENTOS

Ao Major Leandro Kuhn, pela orientação precisa e oportuna, além de todo incentivo e confiança depositados em diversas oportunidades. Seu guiamento proporcionou a realização do trabalho de forma eficiente e constante para conclusão dentro das perspectivas esperadas.

À minha família, que me apoiou sobremaneira tanto na preparação para a realização do Concurso da ECEME quanto no decorrer das atividades para conclusão deste trabalho, inclusive renunciando a diversos momentos de convívio.

A Deus, o qual tem me iluminado e protegido durante toda a caminhada.

RESUMO

O ambiente cibernético tornou-se essencial para a maioria das sociedades modernas. Setores fundamentais da economia, da educação, da saúde e da defesa dos países dependem direta ou indiretamente dessa área. Para que um país esteja preparado para se contrapor às ameaças cibernéticas, ele deve possuir um modelo de Governança Cibernética para atuar de maneira efetiva nesse espaço, o que pode contribuir para o funcionamento das Forças Armadas, dos demais órgãos de segurança do país, bem como as instituições civis e empresas. Este trabalho se alicerça, portanto, por viabilizar uma análise acerca de uma área transversal a todas as áreas do conhecimento, a cibernética, e que representa uma interface com praticamente todos os serviços em uso da sociedade brasileira. Assim, esta pesquisa realiza uma comparação do modelo de Governança Cibernética do Brasil com o da Espanha e dos Estados Unidos da América, países pertencentes ao arco do conhecimento. As estratégias de Governança Cibernética adotada por esses países podem contribuir para que o Brasil possa aperfeiçoar suas abordagens e prover um melhor segurança nessa área.

Palavras-chave: Governança; Governança Cibernética; EUA; Espanha; Brasil; capacidades cibernéticas; atores civis de segurança cibernética.

ABSTRACT

The cyber environment has become essential to most modern societies. Fundamental sectors of the countries' economy, education, health and defense depend directly or indirectly on this area. For a country to be prepared to counter cyber threats, it must have a Cyber Governance model to act effectively in this space, which can contribute to the functioning of the Armed Forces, other security bodies in the country, as well as civil institutions and companies. This work is therefore based on enabling an analysis of an area that cuts across all areas of knowledge, cybernetics, and which represents an interface with practically all services in use in Brazilian society. Thus, this research makes a comparison of the Brazilian Cyber Governance models with those of Spain and the United States of America, countries belonging to the knowledge arc. The Cyber Governance strategies adopted by these countries can help Brazil to improve its approaches and provide better security in this area.

Keywords: *Governance; Cyber Governance; USA; Spain; Brazil; cyber capabilities; civilian cybersecurity actors.*

LISTA DE FIGURAS, QUADROS E TABELAS

SUMÁRIO

1 INTRODUÇÃO

> Todo o fenômeno da guerra cibernética é de tal forma cercado de sigilo governamental que faz os tempos da Guerra Fria parecerem uma época de transparência e abertura. O maior segredo mundial sobre a guerra cibernética é que, ao mesmo tempo em que os Estado Unidos se preparam para uma guerra cibernética ofensiva, eles continuam com políticas que os deixam sem uma defesa efetiva em caso de ataque cibernético. A nação que inventou a nova tecnologia e as táticas para utilizá-la pode não ser a vencedora se seus militares continuarem focados em métodos ultrapassados, vencidos pela inércia e com excesso de confiança em armas obsoletas que aprenderam a amar e considerar superiores (Clarke e Knake, 2015, p. 2).

A Governança é um tema que tem suscitado estudo em diversas áreas do conhecimento pela sua importância e por trazer maior efetividade para as entregas das organizações (Brasil, 2020b). Dentro desse contexto, a área de atuação da Segurança Cibernética tem se valido desse mecanismo para potencializar seu emprego (Espanha, 2023a).

Tanto o tema Governança quanto o tema Segurança e Guerra Cibernéticas (G Ciber) são relativamente recentes, tendo começado a serem desenvolvidos estudos acerca deles somente nas últimas décadas (Clarke e Knake, 2015).

Há diversas definições para governança (Rose-Ackerman, 2017). De acordo com Fukuyama (2013), governança é a capacidade de um governo realizar e fazer cumprir regras e prestar serviços, independentemente da característica democrática ou não desse ente. No entanto, a governança costuma ser usada para sinalizar que há problemas políticos relativos a algum tema, já a boa governança designa todos os tipos de estruturas institucionais responsáveis por promover tanto bons resultados quanto legitimidade pública acerca de determinado assunto (Rose-Ackerman, 2017).

Sobre a Governança, Buta e Teixeira (2020) abordam a matéria com a tendência geral direcionada para a área pública. Nesse sentido, os autores definem que são arranjos os quais permitem a participação de todos os interessados, sob a coordenação do Estado, na solução dos problemas comuns, com o objetivo de entregar de serviços públicos de qualidade e realizar de forma adequada o controle social.

No que tange ao ambiente cibernético, ele encontra-se em plena evolução e demanda constante inovação para alcançar as capacidades necessárias. Nesse sentido, existe a necessidade de se alicerçar em uma gestão de governança mais específica, ou seja, em um ambiente de inovação. Dentro desse contexto:

> a governança dos ambientes de inovação oferece mecanismos para gerenciar de forma eficiente e integrada, com alinhamento de metas, alocação de recursos e atribuição de autoridade, na tomada de decisão para a inovação, oferecendo segurança jurídica a todos os atores do habitat de inovação, construindo, assim, um ambiente de confiança entre os parceiros (Silva e Amaral, 2023).

Além disso, de acordo com Baars *et al.* (2018), a Segurança da Informação deve ser garantida e tratada de forma sistêmica para garantir a continuidade dos negócios e minimizar seus riscos. Nesse contexto, a Segurança Cibernética pode ser conceituada como a arte de garantir a existência e a continuidade de um Estado Nacional de modo a garantir e proteger tanto os ativos de valor informacional quanto as infraestruturas críticas para o funcionamento adequado do país (Brasil, 2017).

Por ser um tema relevante para o país, a Segurança Cibernética vem recebendo atenção, também, do Gabinete de Segurança Institucional da Presidência da República. Esse órgão define o tema da seguinte forma:

> ações voltadas para a segurança de operações, visando garantir que os sistemas de informação sejam capazes de resistir a eventos no espaço cibernético, capazes de comprometer a disponibilidade, a integridade, a confidencialidade e a autenticidade dos dados armazenados, processados ou transmitidos e dos serviços que esses sistemas ofereçam ou tornem acessíveis (Brasil, 2021).

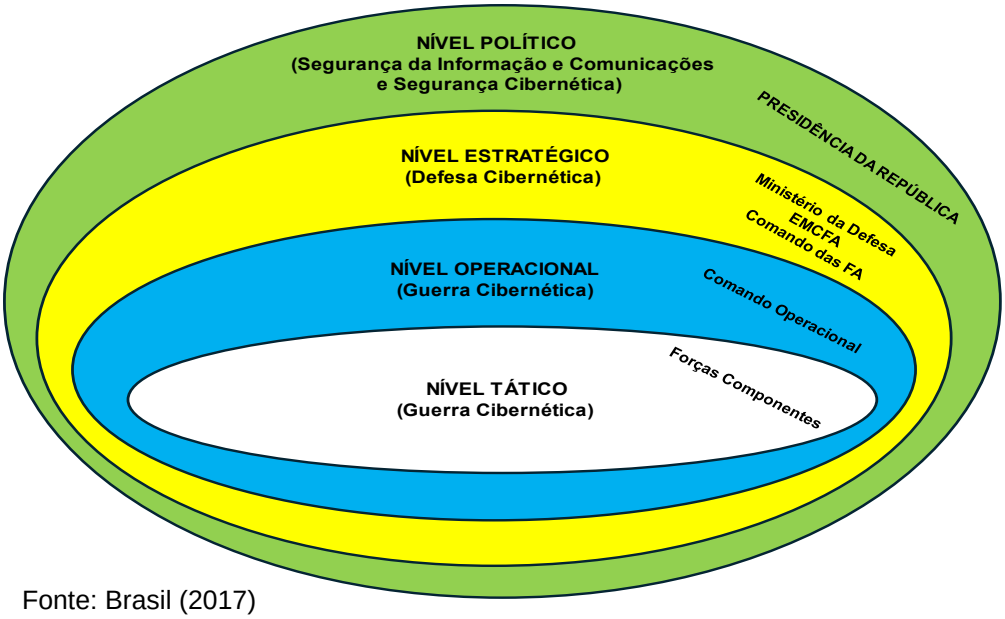
Outro conceito fulcral para o entendimento do tema em estudo é o de G Ciber. De acordo com Clarke e Knake (2015), é um conjunto de ações realizadas por um Estado-nação com a finalidade de executar a invasão de computadores ou de redes de outra nação com o objetivo de causar danos e/ou transtornos.

Ainda nesse diapasão, outro conceito sobre o mesmo tema provém do manual do Exército Brasileiro (EB) no qual aborda o tema:

> corresponde ao uso ofensivo e defensivo de informação e sistemas de informação para negar, explorar, corromper, degradar ou destruir capacidades de C^2 do adversário, no contexto de um planejamento militar de nível operacional ou tático ou de uma operação militar. Compreende ações que envolvem as ferramentas de TIC para

> desestabilizar ou tirar proveito dos sistemas de informação do oponente e defender os próprios Sist Info. Abrange, essencialmente, as ações cibernéticas (Brasil, 2017).

Figura 1 - Níveis de Decisão



Fonte: Brasil (2017)

Vale ressaltar que as ações relativas ao espaço cibernético receberam denominações específicas e seus respectivos responsáveis tanto pela Estratégia Nacional de Defesa (2008) e do Manual de Campanha – Guerra Cibernética EB70-MC-10.232, conforme Figura 1. Outrossim, os níveis de decisão têm as seguintes denominações:

TABELA 01 – Níveis de decisão.

Nível de Decisão	**Denominação**	**Órgão responsável**
Político	Segurança da Informação e Comunicações (SIC) e Segurança Cibernética	Coordenadas pela Presidência da República e abrangendo a administração pública federal (APF) direta e indireta, bem como as infraestruturas críticas da informação inerentes às infraestruturas críticas nacionais

Estratégico	Defesa Cibernética	A cargo do MD, Estado-Maior Conjunto das Forças Armadas (EMCFA) e comandos das Forças Armadas (FA), interagindo com a Presidência da República e a APF
Operacional	Guerra Cibernética	Restrita ao âmbito interno das FA

Fonte: Brasil (2017).

Nessa instância, para que Segurança Cibernética seja efetiva há a necessidade de se estabelecer um modelo de Governança Cibernética bem definido e eficiente. Um modelo é a maneira que as empresas, os órgãos, as instituições ou os países organizam seus processos mais importantes de forma que sejam definidos as dinâmicas, as atribuições e um sistema de avaliação que garanta o funcionamento adequado (Carlotto, 2024).

Por conta deste paradigma, Tribunal de Contas da União (TCU) estabeleceu, também, um conceito de modelo que governança que é “representação clara e pública de como funciona ou deveria funcionar a governança na organização” (Brasil, 2020b). Dessa forma, aquele órgão institui uma forma para o estabelecimento de modelos de governança, o qual consiste na definição de um conjunto de diretrizes, orientações valores, processos e estruturas para que sejam eficazes e alinhadas as atividades de governança (Brasil, 2020b).

Vários países, como por exemplo o Brasil, os Estados Unidos da América e a Espanha, instituíram seu próprio modelo de Governança Cibernética. Um dos exemplos de arcabouço legal sobre o tema no Brasil é a Estratégia Nacional de Cibersegurança do Brasil (E-Ciber) (Brasil, 2020c) como parte da Política Nacional de Segurança da Informação.

Outrossim, os EUA publicaram a “National Cybersecurity Strategy” (USA, 2023a) e a Espanha se valem da “*Estrategia Nacional de Ciberseguridad*” (Espanha, 2019), todos esses documentos como uma parte da Governança Cibernética desses países, os quais, teoricamente, atendem suas peculiaridades e permitem assegurar um posicionamento adequada acerca da matéria.

1.1 PROBLEMA

O modelo de Governança Cibernética instituído no Brasil pode indicar a sua efetividade e a sua adequabilidade, bem como se o país consegue atuar de maneira sistêmica no espaço cibernético. Outros modelos dessa natureza, instituídos em países desenvolvidos, que têm características distintas e que foram criados de forma diferente podem ou não serem aderentes ao Brasil.

Do exposto, o presente estudo pretende trazer luz para identificar em que medida os modelos de Governança Cibernética nos EUA e na Espanha, países do arco do conhecimento, são adequados às necessidades estratégicas brasileiras?

1.2 OBJETIVOS

1.2.1 Objetivo geral

Analisar os modelos de Governança Cibernética nos EUA e na Espanha, países do arco do conhecimento, e verificar se são adequados às necessidades estratégicas brasileiras, bem como se as capacidades cibernéticas ofensivas e defensivas interagem com os setores da sociedade civil.

1.2.2 Objetivos específicos

Para alcançar o Objetivo Geral, foram traçados os seguintes objetivos específicos:

a. Apresentar os conceitos de Governança e Governança Cibernética.

b. Apresentar o funcionamento da Governança Cibernética no Brasil, nos EUA e na Espanha.

c. Comparar os modelos de Governança Cibernética nos países relacionados.

d. Identificar possibilidade de aumento de efetividade no modelo de governança brasileiro, bem como avaliar sumariamente a interação dos setores da sociedade civil com a segurança cibernética.

1.3 DELIMITAÇÃO DO ESTUDO

O presente estudo estará limitado aos modelos atualmente utilizados nos países estudados (Brasil, EUA e Espanha) e disponibilizados em fontes abertas e públicas na rede mundial de computadores. Ao final, este trabalho também buscará sugerir oportunidades de melhoria ao EB.

1.4 RELEVÂNCIA DO ESTUDO

Segundo Goldoni, Rodrigues e Medeiros (2024), o Brasil procurou fazer variados esforços no sentido para securitizar o ciberespaço por meio de uma coleção ampla, porém desconexa, de documentos, cuja maturidade de implementação não está clara. Isso indica que a Governança Cibernética não foi realizada de maneira estruturada e bem definida na sua concepção. Além disso:

> 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. (Goldoni, Rodrigues e Medeiros, 2024)

> 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 (Goldoni, Rodrigues e Medeiros, 2024 apud Kott e Linkov, 2019).

Dessa forma, torna-se importante comparar os modelos de Governança Cibernética do Brasil com países pertencentes ao arco do conhecimento no sentido de possibilitar o aumento de efetividade no modelo de governança do país, o que pode contribuir para o funcionamento das Forças Armadas, dos demais órgãos de segurança do país, bem como as instituições civis e empresas.

O presente estudo se alicerça, portanto, por viabilizar uma análise acerca de uma área transversal a todas as áreas do conhecimento, a cibernética, e que representa uma interface com praticamente todos os serviços em uso da

sociedade brasileira e que pode contribuir na produção acadêmica sobre o tema em questão.

2 REFERENCIAL TEÓRICO-CONCEITUAL

O objetivo deste capítulo é apresentar os principais conceitos acerca do tema em estudo, bem como realizar comentários e interconexões sobre o que se deseja discutir. Na parte que for mais atinente às empresas e corporações (atores que também são relevantes no ambiente cibernético), os conceitos serão direcionados para essa área. Já na parte relativas às normativas legais, serão apresentados conceitos mais aderentes à parte governamental.

Há abordagens diversas sobre o tema, inclusive com falta de consenso sobre alguns conceitos e nomenclaturas, como por exemplo o de governança (Rose-Ackerman, 2017). Para aqueles conceitos ainda não apresentados, esse capítulo disponibilizará os conceitos de modo que seja mais fácil a interpretação e o entendimento dessa pesquisa.

A importância deste trabalho se assenta, também, em aspectos relacionados aos conceitos ainda não apresentados. Primeiro, o tema Cibernética é de extrema importância em um mundo conectado (Goldoni, Rodrigues e Medeiros, 2024 apud Kott e Linkov, 2019) no qual as tecnologias digitais se encontram em praticamente todos os processos estratégicos, económicos e industriais da sociedade (Garcia, 2023), conforme Figura 2, sendo tratado em diversos documentos governamentais e objeto de investimentos nas empresas civis.

Segundo, os modelos de governança cibernética nos países desenvolvidos podem revelar suas formas de atuação e apoiar no aperfeiçoamento do setor no Brasil (Garcia, 2023). Terceiro, a sociedade civil, em especial os atores de segurança cibernética podem interagir de maneira mais sinérgica com todo o ecossistema cibernético no país.

O capítulo foi dividido da seguinte forma: inicia-se com os conceitos basilares e apresenta-se, depois, os diversos conceitos relacionados ao ambiente cibernético. Após isso, é apresentada uma tabela sintética com as contribuições de cada um dos artigos utilizados.

Figura 2 - As tecnologias digitais já estão subjacentes a praticamente todos os processos estratégicos, económicos e industriais da sociedade

Fonte: Garcia (2023)

2.1 CONCEITOS BASILARES

Segundo França & dos Santos (2021), “**política** é considerada como integrante da atividade humana em qualquer setor em que se encontre instituído o exercício do poder”. Nesse contexto, a política pode ser conceituada como a atuação no poder ou as abordagens no sentido para influir como o poder é particionado entre as diversas instituições ou entre Estados soberanos, assim deve-se considerar as relações de poder associadas ao exercício do poder tanto em situação estatal quanto não estatal (França e Dos Santos, 2021).

Outro conceito de destaque é a **estratégia**, ela “é o padrão ou plano que integra as principais metas, políticas e sequência de ações de uma organização em um todo coerente” (Mintzberg e Quinn, 2001). Outrossim, Lodi (1969) define estratégia como “a mobilização de todos os recursos da empresa no âmbito nacional ou internacional visando a atingir objetivos a longo prazo”. Já Liddell Hart define como “a arte de empregar forças militares para atingir resultados fixados pela política” (Brasil, 2020a).

Por conta de sua definição ter sofrido variações e evoluções no decorrer da história, desde os tempos de Sun Tzu (Brasil, 2020a), englobando visões tanto militares quanto não militares, para este estudo considera-se estratégia como:

> “a arte e ciência de preparar e aplicar o poder para, superando óbices de toda ordem, alcançar os objetivos fixados pela política”. Arte, por envolver característica pessoais do seu formulador, como experiência, conhecimento, visão e criatividade. Ciência, por se valer de conhecimentos científicos de diferentes áreas (Brasil, 2020a).

Segundo Jean Bodin (2011), em seu livro “Os Seis Livros da República - Livro Primeiro”, **soberania** é o poder absoluto e perpétuo de uma República. Esse conceito é apresentado como o primeiro fundamento do 1º Artigo da Constituição da República Federativa do Brasil de 1988 (Brasil, 1988), isso caracteriza a importância do legislador no termo em questão (Reis, 2008).

2.2 O AMBIENTE CIBERNÉTICO

A importância da governança no setor cibernético se alicerça, também, na seguinte informação: a atividade maliciosa nesse ambiente, muitas vezes, se origina em países que não possuem infraestrutura e governança adequadas (Pawlak, 2016). Consoante ao que dispõem Calderaro e Craig (2020), a tecnologia normalmente evolui de forma mais rápida que a capacidade de se prever o impacto nos sistemas políticos, sociais e econômicos.

A implementação de regulamentos, normas e processos de governança que visam tornar este impacto sustentável costuma ser lenta em relação à evolução tecnológica (Calderaro e Craig, 2020). Logo, existe a necessidade de se instituir, o quanto antes e de maneira eficaz, políticas, estratégias e preparação para atuação no espaço cibernético (Clarke e Knake, 2015).

A governança costuma tratar processos de tomada de decisão com a participação de atores públicos e privados em um esforço combinado para fornecer serviços ou solucionar problemas públicos de natureza específicos (Goldoni, Rodrigues e Medeiros, 2024). Savaş & Karataş (2022) indicam que a governança garante que as necessidades, condições e opções das partes interessadas sejam equilibradas. Nesse diapasão, ela também permite uma determinação da gestão e administração na tomada de decisões e priorização, ao passo que viabiliza uma avaliação de necessidades para alcançar objetivos institucionais comuns. (Savaş e Karataş, 2022).

Vale ressaltar que a definição de Espaço Cibernético demonstra a amplitude e o alcance da área de atuação desse ambiente (Malatji e Matli, 2023) ele é:

> um domínio global dentro da dimensão informacional do ambiente operacional que consiste em uma rede interdependente de infraestruturas de Tecnologia da Informação e Comunicações (TIC) e de dados, incluindo a internet, redes de telecomunicações, sistemas de computador, processadores embarcados e controladores (Brasil, 2017).

Nesse contexto, o Brasil, os Estados Unidos da América e a Espanha têm envidado esforços no sentido de criarem suas políticas e estratégias nacionais para atuação efetiva no espaço cibernético. As políticas de defesa são o direcionador de mais alto nível para o planejamento de ações destinadas à defesa do País, focadas nas ameaças externas e no estabelecimento de objetivos para o preparo e o emprego das expressões do Poder Nacional, em favor da Defesa Nacional (Brasil, 2020d; Brasil, 2017).

2.3 REVISÃO BIBLIOGRÁFICA

A revisão bibliográfica deste trabalho foi baseada em um conjunto de publicações que abrange o referencial teórico a ser utilizado acerca do tema Governança Cibernética. A síntese das publicações para essa revisão encontra-se na Tabela 2.

TABELA 02 – Síntese da revisão bibliográfica.

Título	Autor(es)	Ano	Contribuição
What does 'Governance' Mean?	Rose-Ackerman	2017	Apresenta um estudo sobre governança e explicita que esse termo é difuso e variado
Qual é o futuro da governança de cibersegurança no Brasil?	Goldoni, Rodrigues e Medeiros	2024	Apresenta um panorama da Governança Cibernética no Brasil e expõe a situação atual dessa área no país
Cyber resilience of systems and	Kott e Linkov	2019	Introduz os conceitos fundamentais de resiliência

networks			cibernética
Key Factors for a Cybersecurity and Cyberintelligence Policy in Brazil	Garcia	2023	Estudo que mapeia a situação atual da capacidade cibernética nacional brasileira e identifica os vetores promissores para o seu desenvolvimento
O sentido da política como vocação em Max Weber	França e Dos Santos	2021	Apresenta o conceito de política e sua relação com o poder e o Estado soberano
O processo da estratégia	Mintzberg e Quinn	2001	Obra clássica sobre o tema estratégia, com ênfase em seu conceito e abordagens voltadas à administração estratégia em empresas
Estratégia de negócios: planejamento a longo prazo	Lodi	1969	Obra histórica e seminal sobre o planejamento e estratégia de negócios em empresas
Manual de Fundamentos ESTRATÉGIA (EB20-MF-03.106), 5ª Edição	Estado-Maior do Exército	2020	Manual que orienta o estudo e a aplicação da Estratégia no âmbito do Exército Brasileiro, a partir das orientações do Ministério da Defesa
Os Seis Livros da República - Livro Primeiro	Bodin	2011	Reforça que a soberania é poder absoluto e perpétuo de uma República.
Constituição da República Federativa do Brasil de	Brasil	1988	Apresenta a soberania como o princípio fundamental e de relevância para a República Federativa do Brasil

1988			
"Todo o poder emana do povo": o exercício da soberania popular e a constituição de 1988	Reis	2008	Apresenta uma abordagem epistemológica acerca do poder soberano do povo em relação à formulação de leis e sua disposição na Carta Magna
Capacity Building in Cyberspace as an Instrument of Foreign Policy	Pawlak	2016	Apresenta a importância de um ambiente cibernético seguro para o impacto positivo do desenvolvimento humano
Transnational governanceof cybersecurity: policy challenges and global inequalities in cyber capacity building	Calderaro e Craig	2020	O artigo discute os principais fatores que explicam os esforços dos Estados para melhorar a sua capacidade cibernética. Além disso, o estudo indica que a regulamentação e a governança na área tecnológica costumam ser mais lenta que o seu progresso
Guerra Cibernética: A próxima ameaça a segurança o que fazer a respeito.	Clarke e Knake	2015	Obra clássica sobre Guerra Cibernética e ameaças de segurança nesse ambiente. Apresenta-se um panorama acerca das ações de Defesa e Guerra Cibernética e sua influência nos EUA
Cyber governance	Savaş e Karataş	2022	O estudo traça um panorama sobre a governança

studies in ensuring cybersecurity: an overview of cybersecurity Governance			cibernética e a sua importância para a o aumento da capacidade de segurança cibernética
The Potential Benefits and Challenges of a BRICS+ Agency for Cybersecurity Intelligence Exchange	Malatji e Matli	2023	O estudo realiza o diagnóstico que as nações pertencentes ao BRICS carecem de uma estrutura coesa de segurança cibernética para o intercâmbio de informações e propõe uma agência dedicada ao compartilhamento e à análise de informações de segurança cibernética
Estratégia Nacional de Defesa. Política Nacional de Defesa	Ministério da Defesa	2020	PND e END os quais são os direcionadores de alto nível para a Defesa Nacional do Brasil. Nessa atualização, o Espaço Cibernético recebe destaque com o objetivo de garantir a soberania nacional. Além disso, define o Setor Cibernético como um dos três Setores tecnológicos essenciais para a Defesa Nacional
Manual de Campanha – Guerra	Estado-Maior do Exército	2017	Manual que orienta a atuação do Exército Brasileiro no quesito Guerra Cibernética

Cibernética (EB70-MC-10.232), 1ª Edição			em prol da Defesa Nacional do Brasil

Fonte: O autor (2024).

3 METODOLOGIA

Este capítulo tem por finalidade apresentar a metodologia utilizada para o desenvolvimento deste trabalho de pesquisa. Como primeira etapa, foram realizadas reuniões com o orientador e com os outros alunos do primeiro ano do Curso de Comando e Estado-Maior (CCEM) da ECEME acerca do tema Governança Cibernética nos países do “arco do conhecimento” (tema integrante do Plano de Desenvolvimento da Doutrina Militar Terrestre 2024, EB-P-10.001) para delimitação dos países a serem estudados. Para este trabalho foram definidos como focos de pesquisa os EUA, a Espanha e o Brasil.

Definida a delimitação geográfica para a pesquisa, foram realizadas buscas de artigos científicos, de dissertações de mestrado, de teses de doutorado, de documentos, de legislações brasileiras, dos EUA e da Espanha que tratam da governança cibernética ou que pudessem de alguma forma apoiar no trabalho.

A fim de atingir os propósitos deste Capítulo, os seguintes tópicos serão apresentados: desenho da pesquisa, estratégia de pesquisa e coleta de dados, tratamento de dados e limitações do método.

3.1 DESENHO DA PESQUISA

A organização e estruturação de trabalhos acadêmicos, em especial do tipo monografia, podem se assentar nas normas definidas pelas próprias instituições de ensino superior ao qual o aluno está inserido. Nesse sentido, a ECEME confeccionou manual próprio para padronizar o projeto de pesquisa, o Manual Escolar para a Elaboração de Projetos de Pesquisa - ME 21-259 (Brasil, 2012).

De acordo com o manual supracitado, a classificação metodológica para a realização desta pesquisa científica é: qualitativa, uma vez que contempla a

subjetividade e demanda uma procura profundada para entender os fenômenos, a história e as análises de documentos; explicativa, pois busca tornar o tema inteligível justificando os motivos; documental, porque é realizada a partir de documentos de órgãos públicos e privados, como decretos, portarias, manuais, relatórios etc; e bibliográfica, pois baseia-se em material publicado como livros, artigos científicos, dissertações e outros documentos.

3. 2 ESTRATÉGIA DE PESQUISA E COLETA DE DADOS

O referencial teórico-conceitual foi capaz de esclarecer as diversas fontes de consulta para a preparação deste trabalho, de modo que na busca do material foi possível identificar a disperção do material a ser coletado.

Assim, relativamente aos artigos científicos, às dissertações e às teses, a pesquisa buscou utilizar tanto os trabalhos seminais acerca do tema governança, segurança cibernética e governança cibernética quanto aqueles que trazem informações atualizadas, ou seja, no estado da arte sobre o tema ou que foram publicados nas últimas duas décadas (período no qual o tema cibernética tornou-se mais relevante no cenário mundial).

Sobre a documentação, foram buscados portaria e manuais do Exército Brasileiro, leis e decretos brasileiros e dos países definidos para o estudo (EUA e Espanha). Além disso, foram identificados sítios eletrônicos que realizam relatórios periódicos sobre a governança cibernética de diversos países, inclusive os estudados. Esse compêndio documental também é utilizado para a pesquisa.

Um dado importante a ser destacado é que a pesquisa se baseou, também, em documentação pública localizada em plataformas disponíveis, como por exemplo os Periódicos da Capes, sítios *web* de Universidades públicas brasileiras, de órgãos públicos brasileiros, bem como outros sítios *web* da rede mundial de computadores.

3.3 TRATAMENTO DOS DADOS

Para a realização desta pesquisa serão utilizados os seguintes métodos e técnicas de tratamento de dados, conforme (Brasil, 2012): análise de conteúdo e o comparativo.

Relativamente à análise de conteúdo, foram realizados estudos nos

documentos identificados como importantes para o desenvolvimento da pesquisa. Já sobre a técnica comparativa, foram exploradas as similaridades e diferenças dos modelos de governança cibernética em cada um dos países estudados com o objetivo de verificar a adequabilidade dos modelos de Governança Cibernética dos EUA e da Espanha serem utilizados no Brasil.

3.4 LIMITAÇÕES DO MÉTODO

Cabe ressaltar que um fator dificultador da pesquisa é a existência de legislação esparsa sobre a governança cibernética nos países estudados, o que pode gerar uma pesquisa que não garante a completude dos dados necessários para o trabalho realizado.

Outrossim, além da não garantia da completude documental, a legislação e manuais disponíveis dos EUA e da Espanha, e até mesmo do Brasil, podem não estar em sua versão mais atualizada, gerando um modelo comparativo que não se encontra plenamente caracterizado com o tempo mais recente. No entanto, o material pesquisado e utilizado é suficiente para alcançar os objetivos deste trabalho de pesquisa científica.

4 CRONOGRAMA

TABELA 03 – Cronograma de preparação das atividades de pesquisa no CDEM 2024

	FEV	MAR	ABR	MAIO	JUN	JUL	AGO	SET	OUT	NOV
Elaboração do Projeto de Pesquisa (T1)										
Pesquisa Bibliográfica (Revisão de Literatura)										
Elaboração da Introdução e Referencial Teórico (T2)			26							
Elaboração da Metodologia (T3)					14					
Coleta de Dados (artigos, dissertações, teses, manuais, decretos, leis, relatórios etc)										
Tratamento de Dados (Anl de Conteúdo, Revisão Sistemática...)										
Elaboração do Artigo Científico/Opinião										
Depósito do Artigo Científico/Opinião (Moodle)						26				
Elaboração da Análise e Discussão dos Resultados e Considerações Finais										
Retificação do Artigo Científico/Opinião										
Submissão do Artigo ao periódico										
Revisão da Monografia										
Preparação de Documentação para Depósito										
Depósito								9		
Retificação das Observações da Banca Examinadora									4	
Preparação da Apresentação										
Apresentação dos Resultados										12

Fonte: O autor (2024).

5 A GOVERNANÇA CIBERNÉTICA NA ESPANHA

Este capítulo tem o objetivo de descrever como funciona a Governança Cibernética na Espanha. Além disso, destina-se, também, a esclarecer como foram estabelecidos e implementados os arcabouços basilares para a sua consecução**.**

5.1 UMA VISÃO DA GOVERNANÇA NA ESPANHA

De modo geral, a governança tem se mostrado como um termo ambíguo, possui diversos significados e frequentemente está relacionado a questões políticas e/ou estratégicas (Rose-Ackerman, 2017). Já a Governança Cibernética, tema específico dessa pesquisa, é uma das vertentes da governança em um país. No entanto, antes de se abordar a Governança Cibernética propriamente dita, apresentaremos conceitos gerais sobre o tema mais geral na visão espanhola e a seguir será abordado o tema mais específico.

Nesse contexto, o conceito de governança pode ser relativamente diferente de país para país. Nesse sentido, buscou-se a definição de governança em fontes da Espanha para melhor apresentar o seu significado naquele local.

Assim, de acordo com o dicionário da língua espanhola disponibilizado pela Real Academia Espanhola (instituição fundada em 1714 e responsável oficial pela tutela da língua castelhana) governança pode ser definida como a arte ou a forma de governar para alcançar um desenvolvimento socioeconômico e institucional proporcionando um equilíbrio saudável entre o Estado, a sociedade civil e a economia de mercado (RAE, 2001).

Além do significado do dicionário, este estudo traz o significado de governança para os órgãos públicos espanhóis. Nesse sentido, a governança representa uma mudança de paradigma nas relações administrativas, promovendo a adoção de políticas públicas com a participação de diferentes setores públicos e privados (Espanha, 2022). Outrossim, no âmbito da Administração Geral do Estado da Espanha, a Direção Geral de Governança Pública exerce as suas funções com o objetivo de:

> orientar e dirigir a atividade administrativa numa tripla perspectiva: coordenação da organização para garantir uma ação ordenada para evitar duplicações e conseguir uma utilização adequada dos recursos, avaliação da gestão administrativa para melhorar o

> funcionamento dos serviços e orientação da organização e dos serviços para o cidadão (Espanha, 2022).

Apesar de o significado geral de governança na Espanha ter sido apresentado pela Direção Geral de Governança Pública, não é esse órgão que trata diretamente da Governança Cibernética, como poderá ser verificado no decorrer deste capítulo.

5.2 A ESPANHA NA ERA DA INFORMAÇÃO

A Espanha vem implementando o desenvolvimento de uma infraestrutura para acesso à Internet e todas as atividades que garantam esse acesso como estratégia de governo. Inicialmente, foi estabelecida a Agenda Digital para a Espanha (Espanha, 2013), a qual foi um *framework* que definiu estratégias em matéria de Tecnologia da Informação e Comunicação (TIC) e administração electrónica no país e sua inserção na Agenda da Europa; buscou aumentar a produtividade e a competitividade; e viabilizou para que a sociedade espanhola fizesse o uso eficiente e intensivo dos meios de TIC.

A seguir e por conta dos danos causados pela crise do Covid-19, foi instituído outro plano, o de Recuperação, Transformação e Resiliência. Esse plano tem como um de seus vetores o Plano de Desenvolvimento Digital Espanha, o qual tem como objetivo garantir a conectividade digital adequada para toda a população espanhola, promovendo desaparecimento do fosso digital entre as zonas rurais e urbanas (Espanha, 2020). Esse plano está vigente e alinhado com a Agenda 2030 para o Desenvolvimento Sustentável da Espanha.

Outra implementação realizada foi o Geverno Digital Espanhol, iniciativa instituida pela Lei 19/2013, a qual tratou de transparência, acesso à informação pública e boa governança. Uma das entregas desse diploma legal foi o Portal da Transparência do Governo Espanhol, bem como a prestação de mais de 90% dos serviços públicos de forma digital. Nesse diapasão, tanto o comércio digital também se desenvolvou com grande parte da população espanhola realizando compras através de meios de TIC (Cendoya, 2016). Tudo isso elevou a quantidade de incidentes cibernéticos, colocando a Espanha em terceiro lugar no ranking mundial em 2015.

5.3 A ESTRATÉGIA NACIONAL DE SEGURANÇA CIBERNÉTICA NA ESPANHA

A Espanha é considerada um país que alcançou excelentes resultados no que tangem à efetividade das capacidades cibernéticas, com respostas significativas às demandas de segurança aos meios de TIC e modestos meios empregados (Garcia et al, 2022).

Esse esforço para alcançar uma segurança adequada ao país foi iniciado com a Estratégia Nacional de Segurança, publicada em 2011 e com atualizações em 2017 e 2021. Assim, a Espanha passou a listar um conjunto de ameaças e ataques cibernéticos, além de mapear os principais riscos. Como consequência da primeira iniciativa, foi criado o Departamento de Segurança Nacional subordinado ao Gabinete do Primeiro-Ministro do país.

Outrossim, as Estratégias de Segurança Nacional desenvolvidas pela Espanha reforçaram a relevância do Setor cibernético para o país. Essa importância foi explicitada no último documento sobre Estratégia (2021) por conta da aceleração do processo de digitalização, colocando a interação digital como o cerne das atividades públicas e privadas. Isso foi uma consequência marcante da pandemia do Covid-19 (Espanha, 2021).

Nesse contexto, todos os documentos de Estratégia de Segurança Nacional espanhola demonstraram importância ao Setor cibernético, o que pode ser verificado com inserções diretas do termo “cyber” em diversos pontos do respectivo documento. Ademais, a última atualização do documento dedicou uma seção para detalhar as vulnerabilidades cibernéticas no entendimento daquele país.

Para maiores detalhamentos, de acordo com Espanha (2021), as ameaças no ciberespaço enquadram-se em duas categorias gerais: os ataques cibernéticos (ações disruptivas com impacto nos sistemas e nos elementos tecnológicos; e a utilização do ciberespaço para a realização de atividades ilícitas, como a cibercriminalidade, a ciberespionagem, o financiamento do terrorismo ou a promoção da radicalização. Dessa forma, a Estratégia Nacional de Segurança Cibernética na Espanha continua com a devida relevância em seu arcabouço maior.

Nesse diapasão, foi criada a Estratégia Nacional de Segurança Cibernética em 2013 e atualizada em 2019. Essa iniciativa foi adotada pelo Conselho de Segurança Nacional e apoiada pelo Conselho Nacional de Segurança Cibernética em 2014, o qual gerou direcionamentos para garantir a segurança no espaço cibernético e coordenar as organizações com jurisdição na matéria a nível nacional, bem como desenvolveu o Plano Nacional de Segurança Cibernética e seus planos decorrentes.

Assim, a abordagem seguida foi a de cooperação entre os órgãos públicos, o setor privado e a população, proporcionando maior permeabilidade entra as diversas partes da sociedade espanhola (Cendoya, 2016).

Ainda sobre a Estratégia de 2019 e alinhado com a Estratégia de Segurança Nacional de 2017, foi expandido o objetivo de Segurança Cibernética. Assim, como objetivo “macro” a Espanha garantirá uma utilização segura e confiável do ciberespaço, protegendo os direitos e liberdades dos cidadãos e promovendo o progresso socioeconómico (Espanha, 2019). Além disso, foram definidos 5 (cinco) objetivos específicos, conforme descritos a seguir (Espanha, 2019):

- Segurança e resiliência das redes e sistemas de informação e comunicação para o setor público e serviços essenciais;
- Uso seguro e confiável do ciberespaço para evitar usos ilícitos ou maliciosos;
- Proteger o ecossistema empresarial e social e os cidadãos;
- Cultura e compromisso com a segurança cibernética e fortalecimento de competências humanas e tecnológicas; e
- Segurança do ciberespaço internacional.

Esses objetivos foram aperfeiçoados, também, por conta de uma tendência global, o aumento substancial da digitalização, a qual demonstra impulsionar mudanças com implicações para a segurança. Dessa forma, a Espanha busca uma estratégica mais adequada na qual a segurança cibernética é utilizada para abrir novos caminhos que conduzem a um modelo de segurança presente e futuro (Espanha, 2019).

5.4 A ESTRUTURA ORGANIZACIONAL PARA SEGURANÇA E DEFESA CIBERNÉTICAS NA ESPANHA

A estrutura organizacional de segurança da Espanha foi definida pela Estratégia Nacional de Defesa (END), de 2013, e ratificada pela sua atualização em 2021. Nesses documentos, foi definido o Sistema de Segurança Nacional (SSN), o qual se divide, basicamente, 4 (quatro) níveis bem definidos dentro da estrutura de governo: Político e Estratégico; Operacional; Tático; e Técnico. A seguir, serão apresentados cada um dos níveis, sua composição e, sumariamente, suas principais funções, inclusive destacando-se o que tange ao ambiente cibernético no país.

5.4.1 O NÍVEL POLÍTICO E ESTRATÉGICO

No nível Político e Estratégico, o Primeiro-Ministro é o responsável pelo gerenciamento, liderança e promoção da política de segurança nacional. Além disso, a principal organização desse nível é o Conselho de Segurança Nacional (CSN), a qual é composta pelo próprio Primeiro-Ministro, por Ministros e Secretários de Estado relevantes e por outros membros do governo (Cendoya, 2016).

O CSN é o órgão mais relevante do SSN e responsável pela supervisão e coordenação das ações de gestão de crises. Essas ações têm como objetivo: detectar e avaliar riscos e ameaças específicas à segurança nacional; facilitar a tomada de decisões; e garantir uma resposta óptima e coordenada utilizando os recursos estatais necessários (Espanha, 2021). O CSN é apoiado por diversas estruturas, as chamadas Comitês Especializados. Os comitês mais diretamente associados à Cibernética são o Comitê de Situação e o Conselho Nacional de Segurança Cibernética (CNSC).

Por conseguinte, o Comitê de Situação será apoiado pelas comissões especializadas (por exemplo, o CNSC). Esse apoio relaciona-se com os seguintes aspectos: na avaliação de riscos e ameaças; na análise de possíveis cenários de crise, em especial aos que possam conduzir a um problema de segurança nacional; e na avaliação de resultados (Espanha, 2021).

Ademais, o CNSC é um órgão colegiado que apoia o CSN no assessoramento do Primeiro-Ministro em questões de segurança cibernética,

tanto nacional quanto internacionalmente, por meio de análises, estudos e iniciativas. Outrossim, esse Conselho é responsável pela coordenação, pela colaboração e pela cooperação das administrações públicas relevantes em matéria de segurança cibernética e tem a incumbência de fortalecer as relações entre os setores público, privado e sociedade civil (Cendoya, 2016).

5.4.2 O NÍVEL OPERACIONAL

Acerca do nível Operacional, tem-se a Secretária de Estado da Segurança (SES) responsável pela promoção das condições para o exercício dos direitos fundamentais, nos termos estabelecidos na Constituição espanhola e nas leis que os desenvolvem, especialmente em relação à liberdade e segurança pessoal, à inviolabilidade do domicílio e das comunicações e à liberdade de residência e movimento, bem como a direção e coordenação das políticas de cibersegurança no âmbito das competências do Ministério e outras diversas funções relacionadas a segurança da Espanha (Espanha, 2024a).

Além dessa Secretaria, há a Secretaria de Estado de Digitalização e Inteligência Artificial (SEDIA), que pertence ao Ministério da Transformação Digital e Serviço Público, a qual tem a missão de promover a digitalização da sociedade e da economia, de forma que respeite os direitos individuais e coletivos, bem como os valores do ordenamento jurídico espanhol (Espanha, 2024b), o que, por conseguinte, fortalece a segurança cibernética e a privacidade, bem como a confiança os serviços da Sociedade da Informação.

Ainda no nível Operacional, existem o Estado-Maior de Defesa (EMAD) e o Centro Nacional de Inteligência (CNI). A primeira é a organização criada para o desenvolvimento da atuação conjunta e combinada em operações, tanto no território nacional como no estrangeiro (Espanha, 2024c). Já a segunda fornece informações, análises, estudos ou propostas que permitam prevenir e evitar qualquer perigo, ameaça ou agressão contra a Espanha (Espanha, 2024d).

5.4.3 O NÍVEL TÁTICO

No que tange ao nível Tático, existem dois órgãos que se destacam: o Instituto Nacional de Segurança Cibernética (*Instituto Nacional de*

Ciberseguridad – INCIBE), subordinado ao SEDIA, e o Comando Conjunto para o Ciberespaço (*Mando Conjunto del Ciberespacio* - MCCE), conhecido até 2020 como Comando Conjunto de Defesa Cibernética (*Mando Conjunto de Ciberdefensa* – MCCD) e subordinado ao EMAD.

Nesse contexto, o INCIBE trabalha para fortalecer a confiança digital, aumentar a segurança cibernética e a resiliência e contribuir para o mercado digital de uma forma que promova a utilização segura do ciberespaço na Espanha (Espanha, 2024e). Além disso, O Instituto coordena esforços com agências nacionais e internacionais responsáveis pela segurança cibernética. E, em caso de ameaça grave, ele encaminhará a situação para a SEDIA (Cendoya, 2016).

Já o MCCE é o órgão responsável pelo planejamento, direção, coordenação, controle e execução das ações relativas à garantia da liberdade de atuação das Forças Armadas no domínio do ciberespaço. Assim, atuará de modo a garantir o adequado funcionamento dos elementos físicos, lógicos e virtuais críticos à Defesa espanhola (Espanha, 2024f).

Além desses dois órgãos diretamente associados ao tema cibernético, há outras duas instituições no nível tático que pela sua relevância merecem ser citados: o Centro Criptológico Nacional (CCN) e o Centro Nacional de Proteção de Infraestruturas Críticas (CNPIC).

A primeira é o órgão responsável por coordenar as ações de inteligência cibernética para suporte das diferentes instituições (públicas e privadas) na Espanha que utilizam meios ou procedimentos criptográficos, garantindo a segurança das TIC. Além disso, o CCN possui atividades para prevenir o roubo de informações sensíveis e a espionagem industrial, protegendo o patrimônio tecnológico espanhol (Espanha, 2024g).

Já o CNPIC trata do tema segurança, mas com direcionamentos diferentes das outras instituições, com viés de cuidar das infraestruturas físicas estratégicas. Dessa forma, esse substancial sistema tático de segurança e defesa cibernéticos na Espanha se completam.

5.4.4 O NÍVEL TÉCNICO

O nível Técnico é aquele que trata as questões mais relacionadas ao desenvolvimento e divulgação de regras, instruções, orientações e recomendações de caráter tecnológico, mas que devem estar alinhados aos níveis superiores (níveis Táticos, Operacionais, Políticos e Estratégicos). Nesse nível, as instituições tomam decisões baseadas em padrões e regras bem definidas, como por exemplo, aceitação da qualidade de um produto com base em especificações claramente descritas (Rocha, 2018).

Na Tabela 04 serão apresentadas as principais instituições e um resumo de suas missões e áreas de atuação básicas, a seguir:

TABELA 04 – Principais instituições do nível Técnico que compõem a Estrutura Organizacional para Segurança e Defesa Cibernéticas na Espanha.

Nome	Subordinação	Missão e área de atuação
INCIBE-CERT (antigo CERTSI)	INCIBE	INCIBE-CERT é o centro de referência de resposta a incidentes de segurança para cidadãos e entidades de direito privado em Espanha, operado pelo Instituto Nacional de Cibersegurança (INCIBE). Ele se articula com as outras equipes nacionais e internacionais para melhorar a eficácia no combate aos crimes que envolvem redes e sistemas de informação, reduzindo os seus efeitos na segurança pública (Espanha, 2024h).
CSIRT.es	-	CSIRT.es é uma organização independente e sem fins lucrativos que tem como objetivo proteger o ciberespaço espanhol, trocando informações sobre incidentes de segurança cibernética para agir de forma rápida e coordenada perante qualquer situação que possa afetar simultaneamente diferentes entidades

		na Espanha (Espanha, 2024i).
ESPDEF-CERT	MCCE	Este centro opera a nível técnico para facilitar o trabalho de defesa, exploração e resposta, utilizando laboratórios forenses e outras instalações de pesquisa, desenvolvimento e inovação. A sua atuação ocorre nos casos em que afetam a Defesa Nacional (Cendoya, 2016).
CCN-CERT	CCN	Busca garantir a plena implementação do Esquema Nacional de Segurança por meio da implementação das capacidades de inteligência, detecção, análise e resposta do CCN-CERT e dos seus sistemas de detecção precoce e de alerta. Além disso, o Centro tem a missão de contribuir para a melhoria da segurança cibernética espanhola, com a incumbência de ser o centro nacional de alerta e resposta a incidentes de forma rápida e eficiente nos casos de ataques cibernéticos e da necessidade de coordenação a nível público estatal com diferentes capacidades de resposta a incidentes ou centros de operações de segurança cibernética (Espanha, 2024j).

Fonte: O autor (2024).

5.5 OS PILARES DA GOVERNANÇA CIBERNÉTICA NA ESPANHA

O conceito de governança cibernética já foi apresentado em seu sentido mais geral no início desta pesquisa. Além disso, foi trazido no início deste

capítulo uma definição de governança na visão da Espanha. Por conseguinte, para que a governança cibernética na Espanha esteja bem alicerçada, ela precisa desenvolver alguns pressupostos.

Nesse sentido, o país precisa organizar-se para que os atores tenham autoridade legal e lhes sejam incumbidas de missões claramente definidas, bem como sejam dotados de recursos adequadamente. Assim, a governança institucional é a base para uma eficaz e coordenada, especialmente em questões complexas com múltiplas partes, como é o caso do ciberespaço (Garcia *et al.*, 2022).

Com base nos estudos de Garcia *et al.* (2022), foi definido um conjunto de critérios para avaliar a governança cibernética de um país. Cada um dos critérios será descrito na Tabela 05, a seguir, e serão a base de comparação para esta pesquisa.

TABELA 05 – Critérios para avaliar a governança cibernética de um país.

Critério	**Explicação sobre o Critério**
Liderança institucional claramente definida sobre inteligência cibernética	A distribuição do fluxo de informações sobre questões cibernéticas no governo acelera o desenvolvimento da capacidade nacional. Isto acontece de maneira mais rápida e eficiente quando houver acesso institucional a especialistas em inteligência cibernética.
Comando e Doutrina Cibernética Militar estabelecidos	O país estabelecer um comando militar cibernético e possuir sua respectiva doutrina desenvolvida.
Responsabilidade legal para segurança cibernética	Dado que o ciberespaço permeia praticamente todos os aspectos da sociedade, a sua segurança se torna de interesse universal. Assim, para organizar esforços num âmbito tão amplo, é essencial tê-los coordenados sob um mandato legal negociado com as partes interessadas da sociedade em geral.
Funções e responsabilida-	Papéis e responsabilidades bem definidos e

des bem definidas para todas as instituições governamentais com competências cibernéticas	intercoordenados são importantes para uma ação governamental efetiva e eficiente.

Fonte: Garcia et al (2022).

Acerca da inteligência cibernética, o CCN possui a liderança institucional claramente definida por meio do Decreto Real 421, de 12 de março de 2004, o qual concede a autoridade para atuar nessa área, além de possibilitar atuação de maneira efetiva sobre esse tema (Espanha, 2023b).

Já sobre Comando e Doutrina Cibernética Militar estabelecidos, a Espanha criou o MCCE em 2013 e possui uma doutrina acerca do tema estabelecida e em processo de consolidação (Garcia et al, 2022).

Em relação à responsabilidade legal para segurança cibernética, a responsabilidade pela segurança cibernética na Espanha é formalmente compartilhada e bem estabelecida entre três entidades principais: o CCN, o MCCE e o INCIBE. Isso demonstra que o país possui situação consolidada sobre esse quesito (Garcia *et al.*, 2022; Espanha, 2024d; Espanha, 2024f; Espanha, 2024g).

Sobre possuir funções e responsabilidades bem definidas para todas as instituições governamentais com competências cibernéticas, há um Conselho presidido pelo Diretor da CNI com a participação de representantes de diversos Ministérios. O seu objetivo é promover a coordenação, cooperação e colaboração entre todas as entidades públicas com competências cibernéticas e, também, responsável por emitir e atualizar a Estratégia de Cibersegurança, bem como supervisionar a sua implementação. Nesse quesito, a Espanha encontra-se em alto nível de maturidade (Garcia *et al.*, 2022).

5.6 AS CONCLUSÕES SOBRE A GOVERNANÇA CIBERNÉTICA NA ESPANHA

A governança cibernética estruturada de forma efetiva é um dos fatores que possibilita o país estar mais preparado para as ameaças no espaço cibernético, garantindo uma maior segurança e defesa em diversas áreas.

A Espanha buscou desenvolver esse tipo governança cibernética com o objetivo de incrementar suas capacidades e permitir que seus cidadãos possam navegar pelos meios digitais com menos restrições.

Assim, a atuação da inteligência cibernética, o estabelecimento de ambiente multi-institucional para tratar do tema segurança/defesa cibernética e a promoção da interação dos setores governamentais, setores privados, universidades proporcionaram o sucesso em cibernética na Espanha.

Por fim, a Espanha é um exemplo a ser seguido pela capacidade cibernética estabelecida e pela forma adequada que o país tratou e continua tratando o tema.

6 A GOVERNANÇA CIBERNÉTICA NO BRASIL

Este capítulo tem por finalidade descrever como funciona a Governança Cibernética no Brasil e como foram, bem como estão sendo implementados os arcabouços basilares para a sua consecução.

6.1 UMA VISÃO DA GOVERNANÇA NO BRASIL

A governança, conceito estabelecido na década de 1980, vem sofrendo alteração desde então. Naquele período, a definição surgiu de organizações internacionais, como por exemplo o Fundo Monetário Internacional (FMI), com a designação de responsabilidades dos governos para viabilização do livre mercado, segurança dos investimentos e garantia da propriedade privada (Rezende, 2020). No entanto, antes de tratarmos de Governança Cibernética no Brasil, apresentaremos conceitos gerais sobre o tema mais geral na visão basileira e a seguir será abordado o tema mais específico.

Nesse diapasão, o conceito de governança pode ser relativamente diferente de país para país. Assim, buscou-se a definição de governança em

fontes do Brasil com o objetivo de contextualizar melhor sobre o seu significado naquele país.

Já na visão empresarial brasileira, a governança foi caracterizada no Código Brasileiro de Governança Corporativa. Nesse documento é estabelecido que os pilares da boa governança são possíveis por meio de 4 pilares (IGCB, 2016). São eles:

- Transparência: disponibilizar o desempenho econômico-financeiro, os fatores (inclusive intangíveis) da ação gerencial e aqueles que conduzem à preservação e à otimização do valor da companhia para todas as partes interessadas.

- Equidade: realizar um tratamento justo e isonômico de todos os sócios e demais partes interessadas (*stakeholders*).

- Prestação de Contas (*accountability*): prestar contas sobre sua atuação de modo transparente, conciso e tempestivo, responsabilizando-se por suas ações e omissões.

- Responsabilidade Corporativa: zelar pela viabilidade econômico-financeira das companhias, diminuir as externalidades negativas de seus negócios e operações e ampliar as positivas.

Outrossim, a Controladoria-Geral da União (CGU), órgão do governo federal brasileiro responsável pela defesa do patrimônio público e pelo incremento da transparência na gestão, define governança como:

> um sistema composto por mecanismos e princípios que as instituições possuem para auxiliar a tomada de decisões e para administrar as relações com a sociedade, alinhado às boas práticas de gestão e às normas éticas, com foco em objetivos coletivos (CGU, 2024).

Apesar de o significado geral de governança no Brasil ter sido apresentado pela CGU, não é esse órgão que trata diretamente da Governança Cibernética no país, como poderá ser verificado no decorrer desse capítulo.

6.2 O BRASIL NA ERA DA INFORMAÇÃO

O Brasil vem experimentando um considerável aumento no uso de tecnologias computacionais na última década, como pode ser verificado nas pesquisas realizadas pelo *Cetic.br* (Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação), órgão instituído com o objetivo de cooperar com países da América Latina e Lusófonos na África para a construção de sociedades do conhecimento inclusivas.

Esse Centro realiza pesquisas sistemáticas e periódicas no Brasil. Nesses levantamentos, há a indicação que o país possui em 2023 84% dos domicílios com acesso à Internet e 50% dos usuários brasileiros realizando compras *on-line*, ante a 51% e 39% em 2015, respectivamente (CETIC, 2023).

Esse aumento também ocorreu nos órgãos públicos. Um exemplo foi a proporção de órgãos públicos federais e estaduais que ofereceram serviços *on-line* à população. A métrica utilizada para esse caso foi o serviço público mais procurado pelos cidadãos nos últimos 12 meses. As pesquisas indicaram que o percentual passou de 30% para 41% nos órgãos que prestam serviço inteiramente (CETIC, 2024).

Esse aumento na disponibilização de serviços em meios digitais passou a ser política pública no Brasil. Assim, o governo federal institucionalizou a gestão pública digital a partir de 2016 com as seguintes iniciativas: a Estratégia de Governança Digital (EGD) e a Política de Governança Digital – PGD, que alcança os órgãos e as entidades da Administração Pública Federal direta, autárquica e fundacional.

A EGD e PGD alcançam a sociedade e tem a capacidade de proporcionar melhorias baseada no uso da informação e dos recursos de TIC na prestação de serviços públicos; encorajar a cidadania participativa, em especial na formulação, na participação, no monitoramento e na avaliação dos serviços públicos disponibilizados em meio digital; além de buscar assegurar a disponibilação de informações pela sociedade.

Nesse sentido, o Governo Digital assenta-se no uso de tecnologias digitais, como parte integrada das abordagens para a modernização governamental, com o objetivo de proporcionar melhorias para a sociedade. É baseado em um conjunto de sistemas de governamental digital o qual orquestra atores de governo, de empresas, de organizações da sociedade civil e de indivíduos que apoiam a produção e o acesso a dados, serviços e conteúdos mediante interações com o governo (OCDE, 2014).

Pelo aumento considerável do acesso aos sistemas digitais no Brasil na esteira de políticas públicas efetivas e, também, pelo incremento das interconexões globais (possibilitando a ocorrência de crimes cibernéticos além fronteiras), o país alcançou em 2023 a liderança em no *ranking* latino-americano de ataques cibernéticos com mais de 23 bilhões de incidentes registrados (Rosti, 2024). Por tudo isso, o Brasil tem dado especial atenção aos temas Segurança e Defesa Cibernáticas nas últimas décadas.

6.3 A ESTRATÉGIA NACIONAL DE SEGURANÇA CIBERNÉTICA NO BRASIL

O Brasil tem realizados esforços significativos para adquirir e desenvolver capacidades cibernéticas, bem como proteger-se de ações maliciosas no ciberespaço (Goldoni, Rodrigues e Medeiros, 2024).

As primeiras iniciativas decorreram da instituição da Política de Defesa Nacional (PDN) instituída em 1996. Nesse documento, o país fixou os objetivos de defesa nacional, orientou o preparo e o emprego da capacitação nacional, em todos os níveis e esferas de poder, tanto em âmbito civil quanto em militar (Brasil, 1996). Há apenas três passagens na PND que fazem referência a tecnologia, sem citar os termos cibernética ou segurança da informa.

A seguir, no ano de 2005, a PDN sofreu uma atualização na qual aborda pela primeira vez, de forma explícita, o termo “cibernético” na forma a seguir descrita:

> 6.19 Para minimizar os danos de possível **ataque cibernético**, é essencial a busca permanente do aperfeiçoamento dos dispositivos de

> segurança e a adoção de procedimentos que reduzam a vulnerabilidade dos sistemas e permitam seu pronto restabelecimento.
>
> XII - aperfeiçoar os dispositivos e procedimentos de segurança que reduzam a vulnerabilidade dos sistemas relacionados à Defesa Nacional contra **ataques cibernéticos** e, se for o caso, permitam seu pronto restabelecimento.

Assim, com o tema “cibernética” tendo sido inserido nos assuntos da Defesa e juntamente com a importância que o assunto adquiriu no mundo, a PND direcionou a instituição da primeira versão da Estratégia Nacional de Defesa (END) em 2008. Nesse diploma legal, o setor cibernético alcançou importância estratégica, ao lado de outros dois setores, o espacial e o nuclear.

A END sofreu outras duas atualizações aprovadas nos anos de 2012 e 2016, ainda com uma nova revisão em apreciação no Congresso Nacional do Brasil desde 2020. Em 2012 a Política recebeu nova denominação, a Política Nacional de Defesa (PND). Em todas essas atualizações, o Setor Cibernético obteve destaque, reforçando esse setor como estratégico e indicando que ele deve ser usado no mais amplo espectro de emprego civil e militar (Brasil, 2016b).

Por conseguinte, foi instituída a Estratégia Nacional de Segurança Cibernética (E-Ciber) por meio de decreto. Esse regulamento trouxe desígnios acerca o tema e estabeleceu ações estratégicas relativas à Segurança cibernética nacional e internacional. No entanto, apesar de essa estratégia não ter sido formalmente revogada, ela traz em seu corpo que “terá validade no quadriênio 2020-2023” (Brasil, 2020c). A nova Estratégia Nacional de Segurança Cibernética encontra-se em fase de elaboração pelo Comitê Nacional de Cibersegurança (CNCiber) (Cruz, 2024).

Nesse contexto, o Decreto nº 11.856, de 26 de Dezembro de 2023 foi responsável pela formalização da Política Nacional de Cibersegurança, a qual trouxe princípios e objetivos com a finalidade de orientar a atividade de segurança cibernética no país. Além disso, esse diploma legal foi o responsável por instituir o CNCiber, o qual possui as seguintes competências:

> I - propor atualizações para a PNCiber, a Estratégia Nacional de Cibersegurança e o Plano Nacional de Cibersegurança;

> II - avaliar e propor medidas para incremento da segurança cibernética no País;
>
> III - formular propostas para o aperfeiçoamento da prevenção, da detecção, da análise e da resposta a incidentes cibernéticos;
>
> IV - propor medidas para o desenvolvimento da educação em segurança cibernética;
>
> V - promover a interlocução com os entes federativos e a sociedade em matéria de segurança cibernética;
>
> VI - propor estratégias de colaboração para o desenvolvimento da cooperação técnica internacional em segurança cibernética; e
>
> VII - manifestar-se, por solicitação do Presidente da Câmara de Relações Exteriores e Defesa Nacional do Conselho de Governo, sobre assuntos relacionados à segurança cibernética (Brasil, 2023).

Assim, com essa abordagem de utilizar o mesmo Decreto para instituir a política para o setor cibernético e criar o comitê com as atribuições precípuas de alto nível sobre o tema, o poder executivo brasileiro buscou dar a devida importância e iniciar a organização acerca do tema para que seja possível estruturar a governança cibernética de maneira adequada. Pois, até o momento da promulgação do Decreto, “o Brasil desenvolveu uma miríade de legislações relativas ao seu ciberespaço desconexas e com implementações nebulosas” (Goldoni, Rodrigues e Medeiros, 2024).

6.4 A ESTRUTURA ORGANIZACIONAL PARA SEGURANÇA E DEFESA CIBERNÉTICAS NO BRASIL

A estrutura organizacional de segurança do Brasil foi definida pelas diversas atualizações da PND, desde 1996, e seguida pela END até sua última atualização em 2016. Nesses documentos, não foi definida uma estrutura fixa para a Segurança Cibernética como feita em alguns outros países, como por exemplo na Espanha, que definiu o SSN.

Os níveis Político e Estratégico, Operacional, Tático e Técnico se confundem nas diversas legislação. A estrutura definida é sobreposta e sustentada por diferentes e esparsas políticas e estratégias, o que cria um sistema complexo de interação e governança no espaço cibernético do Brasil (Goldoni, Rodrigues e Medeiros, 2024).

Acerca do Nível Operacional e alinhado com a Política Nacional de Segurança da Informação (PNSI), aprovada pelo Decreto nº 9.637/2018, destaca o GSI como instituição que coordena diversas outras, adotando uma abordagem *top-down* (Goldoni, Rodrigues e Medeiros, 2024).

Nesse sentido, o Decreto Nº 10.748, de 16 de Julho de 2021 instituiu a Rede Federal de Gestão de Incidentes Cibernéticos (ReGIC), coordenada pelo GSI. Essa Rede tem por finalidade:

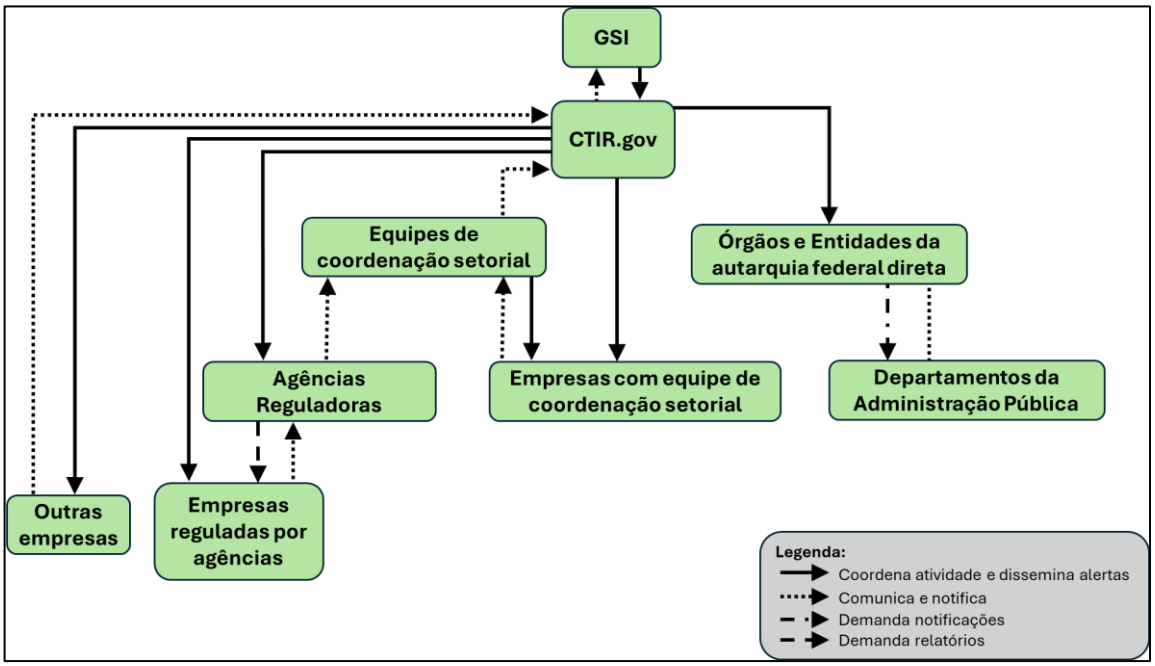
> aprimorar e manter a coordenação entre órgãos e entidades da administração pública federal direta, autárquica e fundacional para prevenção, tratamento e resposta a incidentes cibernéticos, de modo a elevar o nível de resiliência em segurança cibernética de seus ativos de informação (Brasil, 2021).

Segundo Goldoni, Rodrigues e Medeiros (2024), o termo governança encontra-se ausente na documentação da ReGIC, porém o Decreto detalha como responder a incidentes cibernéticos, com a descrição de procedimentos de resposta a esses incidentes, bem como os órgãos responsáveis. Assim, a ReGIC busca alcançar os seguintes objetivos:

> I - divulgar medidas de prevenção, tratamento e resposta a incidentes cibernéticos;
>
> II - compartilhar alertas sobre ameaças e vulnerabilidades cibernéticas;
>
> III - divulgar informações sobre ataques cibernéticos;
>
> IV - promover a cooperação entre os participantes da Rede; e
>
> V - promover a celeridade na resposta a incidentes cibernéticos (Brasil, 2021).

A maneira que o ReGIC foi construída preconiza que o GSI coordene os esforços no sentido de realizar a resposta aos incidentes cibernéticos dos membros da Rede, enquanto as equipes participantes de forma obrigatória ou voluntária relatem as vulnerabilidades e/ou incidentes em infraestruturas críticas nacionais (Goldoni, Rodrigues e Medeiros, 2024). Tudo isso é realizado conforme a Figura 3 – Estrutura de Governança da ReGIC, a seguir.

Figura 3 - Estrutura de Governança da ReGIC



Fonte: Adaptado da ReGIC (Decreto nº 10.748, 2021) (Goldoni, Rodrigues e Medeiros, 2024)

Dessa forma, de acordo com o decreto que instituiu a ReGIC, devem ser estabelecidos planos setoriais para a gestão de incidentes de rede. Estes planos foram implementados em um subconjunto das agências reguladoras, o que compromete a alcançabilidade da implementação (Goldoni, Rodrigues e Medeiros, 2024).

6.5 OS PILARES DA GOVERNANÇA CIBERNÉTICA NO BRASIL

De maneira similar ao item 5.5 deste trabalho de pesquisa, mas que aborda o tema com o viés da Espanha, esta Seção aborda a parte relativa aos pilares da governança cibernética na visão do Brasil. Por conseguinte, para que a governança cibernética no país esteja bem alicerçada, ela precisa desenvolver alguns pressupostos.

Nesse sentido, o Brasil precisa organizar-se para que os atores governamentais tenham a autoridade legal devida e lhes sejam incumbidas de missões claramente definidas, bem como sejam dotados de recursos financeiros e humanos de maneira adequada. Assim, a governança institucional é a base para uma eficaz e coordenada, especialmente em questões complexas com múltiplas partes, como é o caso do ciberespaço (Garcia et al, 2022).

Com base nos estudos de Garcia *et al.* (2022), foi definido um conjunto de critérios para avaliar a governança cibernética de um país. Cada um dos critérios já foi descrito na Tabela 05 (Critérios para avaliar a governança cibernética de um país), pertencente à Seção 5.5 (OS PILARES DA GOVERNANÇA CIBERNÉTICA NA ESPANHA), e serão, também, a base de comparação para esta pesquisa.

Acerca da inteligência cibernética, o Centro de Pesquisa e Desenvolvimento para a Segurança das Comunicações – CEPESC (parte da estrutura da ABIN responsável pelo desenvolvimento de programas e ferramentas que garantam a transmissão segura de informações) é unidade criptográfica do Brasil que detêm a responsabilidade sobre a inteligência cibernética nacional. Contudo, fluxo de informações sobre questões cibernéticas carece de uma abordagem sistemática e enérgica (Garcia *et al.*, 2022).

Já sobre Comando e Doutrina Cibernética Militar estabelecidos, o Brasil possui uma capacidade estabelecida e adequada aos objetivos estratégicos do país. Assim, o país criou em 2014 o Comando de Defesa Cibernética (ComDCiber), no âmbito do Ministério da Defesa e com a função de ser o Comando Cibernético das Forças Armadas, incorporando o Centro de Forças Conjuntas de Defesa Cibernética criado anteriormente em 2012. Além disso, instituiu-se, também em 2014, a doutrina militar de Defesa Cibernética de forma direta e objetiva, com definições precisas de responsabilidades e regras de envolvimento (Garcia *et al.*, 2022).

Em relação à responsabilidade legal para segurança cibernética, ela está dispersa entre muitos atores com poder legal insuficiente. O GSI possui o Departamento de Segurança da Informação responsabilidade sobre instituições governamentais. Porém, esse Departamento não possui instrumentos para determinar ações ou auditá-las. E no setor privado não possui qualquer comandamento. O GSI também administra um centro de resposta a incidentes cibernéticos para instituições governamentais. Porém, ele está severamente limitado no que tange à recursos humanos (Garcia *et al.*, 2022).

Ademais, a ABIN, a Polícias Federal e o ComDCiber compartilham a tarefa de proteger o ciberespaço brasileiro sob diferentes aspectos e condições, mas sem uma coordenação interinstitucional estabelecida. Logo, no que diz respeito, o Brasil encontra-se em fase embrionária, com discussões genéricas e eventuais ações isoladas ou descoordenadas, com discussão básica e consenso entre as partes interessadas a serem alcançados (Garcia et al, 2022).

Sobre possuir funções e responsabilidades bem definidas para todas as instituições governamentais com competências cibernéticas, a doutrina cibernética na área militar brasileira está bem definida. No entanto, a segurança pública e a inteligência estatal ainda carecem de definição das suas regras de engajamento e cooperação em termos mais concretos (GARCIA et al, 2022). Um passo adiante da melhoria dessa situação foi a instituição CNCiber por meio da PNCiber (Cruz, 2024). Essa criação definiu competências que estavam esparsas e proporcionará uma melhor governança cibernética no Brasil.

6.6 AS CONCLUSÕES SOBRE A GOVERNANÇA CIBERNÉTICA NO BRASIL

A governança cibernética demanda uma estrutura organizada pois assim ela proporciona ao país formas de atuação mais eficiente no espaço cibernético, estando mais preparado para as ameaças existentes nesse setor, bem como garantindo uma maior segurança e defesa em diversas áreas.

Nesse sentido, o Brasil, apesar de ter tentado desenvolver de maneira plena sua governança cibernética, tem tido dificuldade no que tange à miríade de legislações. Além disso, o país não tem conseguido instituir responsabilidades organizacionais às instituições e organismos de maneira clara e hierarquizada fim-a-fim.

Assim, a atuação da inteligência cibernética, o estabelecimento de ambiente multi-institucional para tratar do tema segurança/defesa cibernética e a promoção da interação dos setores governamentais, setores privados, universidades têm sido comprometidos no ambiente cibernético brasileiro.

Por fim, o Brasil precisa aperfeiçoar sua capacidade cibernética e um dos

caminhos seria organizar sua governança nesse setor.

7 A GOVERNANÇA CIBERNÉTICA NOS ESTADOS UNIDOS DA AMÉRICA (EUA)

Este capítulo visa descrever como funciona a Governança Cibernética nos EUA e como foram, bem como estão sendo implementados os arcabouços basilares para a sua consecução.

7.1 UMA VISÃO DA GOVERNANÇA NOS EUA

O mercado de capitais norte americano é o mais pujante, possuindo maior volume negociado, maior capitalização e maior número de companhias listadas, cerca de um quinto das maiores corporações do mundo (Deutsch, 2013).

Na década de 1980, já por conta dessas características anteriormente citadas, pelo país possuir um mercado altamente pulverizado e por existirem leis que dificultavam a atuação direta dos acionistas em suas respectivas companhias (Deutsch, 2013), surgiu a necessidade de se constituir um modelo de governança corporativa próprio “pelo qual os financiadores das empresas podem se assegurar de receberem um retorno sobre seus investimentos” (Scherer, 2003).

Nesse sentido, a Governança Corporativa foi “criada para disciplinar a possibilidade de prevenção e/ou mitigação dos conflitos entre investidores e administradores” (Pedroso Neto, 2021). Além disso, o conceito de governança pode ser relativamente diferente de país para país. Assim, buscou-se a definição de governança em fontes dos EUA com o objetivo de contextualizar melhor sobre o seu significado naquele país.

Nesse diapasão, as fontes de leis e regulamentações de governança corporativa nos Estados Unidos da América são variadas e inter-relacionadas (EGCI, 2024). Existem quatro fontes principais:

> leis corporativas estaduais (predominantemente Delaware, na qual mais da metade de todas as corporações de capital aberto dos EUA são incorporadas); o *Securities Act* federal de 1933 e o *Securities Exchange Act* de 1934, e os regulamentos da *Securities and Exchange Commission* (*SEC*) sob esses Atos; regulamento de listagem de bolsa de valores (predominantemente a *New York Stock Exchange* (NYSE) e a NASDAQ); e estatutos federais em relação a áreas específicas de

> prática corporativa (por exemplo, regulamentos promulgados pelo Federal Reserve e outras agências federais e estaduais com relação a bancos e outras instituições financeiras, e por outros órgãos reguladores semelhantes em relação a comunicações, transporte e outros campos regulamentados) (EGCI, 2024).

Outrossim, por conta dessa variedade de fontes de regulamentos federais e estaduais, as corporações nos EUA estão sujeitas a um conjunto extenso de obrigações regulatórias em cada nível de governo, o que cria um ambiente de evolução e mudanças frequente (EGCI, 2024).

7.2 OS EUA NA ERA DA INFORMAÇÃO

Os EUA são uma potência na área científica e tecnológica. De acordo com o Global Innovation Index 2023, o país é o terceiro do *ranking* mundial em Índice Global de Inovação da Organização Mundial da Propriedade Intelectual (OMPI), a agência das Nações Unidas que atende os inovadores e criadores do mundo (OMPI, 2024).

Além disso, a economia dos EUA é fortemente alicerçadas na parte tecnológica. De acordo com Ahmed Sherif, pesquisador da equipe de tecnologia e telecomunicações da Statista (*https://www.statista.com/*) e especialista em tendências globais do mercado de TI, o setor de tecnologia dos Estados Unidos contribuiu com quase dois trilhões de dólares americanos para o produto interno bruto (PIB) geral do país, compondo aproximadamente 9,3% do PIB total em 2022 (Sherif, 2024).

Outrossim, o impacto da indústria *tech* nos EUA atua em quase todos os estados do país. Além disso, 23 estados do setor já se encontram entre os top 5 dos maiores contribuintes para a economia local, o que influenciou diretamente na criação de empregos entre os anos de 2010 até 2018, com cerca de 1,4 milhão de postos de trabalho criados (Cyberstates, 2019).

Outro dado importante é a quantidade e o crescimento de usuários com acesso à Internet no país. Em 2024, aproximadamente 97,1% dos indivíduos nos Estados Unidos acessaram a Internet, um aumento de quase 75% em relação a 2012. Assim, os Estados Unidos são um dos maiores mercados *online* do mundo e, em 2022, havia quase 299 milhões de usuários de Internet no país (Petrosyan, 2024).

Por conta da abrangência do acesso à Internet e, também, pela

necessidade de disponibilizar serviços de melhor qualidade, os EUA fundaram em 2014 o *US Digital Service* (USDS). O USDS é uma unidade de sediada no Gabinete Executivo do Presidente dos Estados Unidos a qual fornece serviços de consultoria para agências federais em tecnologia da informação. Ela busca melhorar e simplificar o serviço digital e melhorar os sites federais (White House, 2014).

Dentro desse diapasão, o acesso aos sistemas *on-line*, a grande influência da Internet na economia, a considerável quantidade de serviços públicos prestados à população norte americana, bem como o incremento das interconexões globais (possibilitando a ocorrência de crimes cibernéticos além fronteiras) contribiui para que os EUA obtivessem bilhões de incidentes cibernéticos. Entre Novembro de 2023 e Junho de 2024, o país obteve cerca de 6,84 bilhões de registros conhecidos violados em 2.741 incidentes divulgados publicamente (IT Governance USA, 2024a).

Pelas características apresentadas nesta Seção e pelos EUA estarem estado na vanguarda do desenvolvimento de políticas e estratégias de segurança cibernética em todo o mundo (Pernik, Wojtkowiak e Verschoor-Kirss, 2015), o país permanece dando especial atenção aos temas Segurança e Defesa Cibernéticas.

7.3 A ESTRATÉGIA NACIONAL DE SEGURANÇA CIBERNÉTICA NOS EUA

Ao contrário da União Europeia e de seus diversos Estados-membro, os EUA não possuem uma lei federal única que regule a segurança cibernética e a privacidade. Os diversos estados daquela nação possuem suas próprias leis de segurança cibernética e notificação de violação de dados (IT Governance USA, 2024b). Assim, existe uma miríade de legislações esparsas, cada uma com suas características, dificultado o entendimento de todo o arcabolço legal sobre o tema.

Porém, os EUA tem sido referência na instituição de estratégia nacional no que tange à área cibernética. Já em 2003, o governo daquele país emitiu a primeira estratégia nacional de segurança cibernética, antes mesmo de países europeus.

Nesse contexto, a Estratégia Nacional para Proteger o Ciberespaço de 2003 estabeleceu três objectivos estratégicos para a segurança do ciberespaço

norte americano: “prevenir ataques cibernéticos contra infraestruturas críticas nacionais; reduzir a vulnerabilidade nacional aos ataques cibernéticos; e minimizar os danos e o tempo de recuperação de ataques cibernéticos que ocorrem” (Pernik, Wojtkowiak e Verschoor-Kirss, 2015).

A supracitada estratégia abordou cinco prioridades nacionais para atingir esses 3 objetivos estratégicos para a segurança do ciberespaço:

> - proteger sistemas e redes de computadores federais;
> - desenvolver um sistema de resposta;
> - estabelecer um programa de redução de ameaças e vulnerabilidades;
> - iniciar um programa de sensibilização e formação para a segurança cibernética; e
> - desenvolver um sistema de cooperação internacional (Pernik, Wojtkowiak e Verschoor-Kirss, 2015).

Somente após quinze anos, em 2018, foi estabelecida uma nova estratégia, delineando as etapas que o governo federal estava tomando para promover um ciberespaço aberto, seguro, interoperável e confiável (USA, 2018a). Essa Estratégia Cibernética Nacional descreve os seguintes objetivos:

> - defender a pátria protegendo redes, sistemas, funções e dados;
> - promover a prosperidade americana, fomentando uma economia digital segura e próspera e promovendo uma forte inovação interna;
> - preservar a paz e a segurança, fortalecendo a capacidade dos Estados Unidos — em concertação com aliados e parceiros — para dissuadir e, se necessário, punir aqueles que utilizam ferramentas cibernéticas para fins maliciosos; e
> - expandir amplamente a influência americana para ampliar os princípios-chave de uma Internet aberta, interoperável, confiável e segura (USA, 2018b).

Outrossim, essa estratégia estabelecida em 2018 buscou desenvolver a capacidade cibernética de nossos parceiros internacionais, por meio de uma variedade de compromissos bilaterais e multilaterais, bem como por meio de programação de assistência estrangeira. Esses parceiros foram auxiliados a estabelecer e executar estratégias nacionais de segurança cibernética, abordando crimes cibernéticos, instituindo padrões de segurança cibernética e protegendo infraestrutura crítica de ameaças cibernéticas (USA, 2018a).

Por conseguinte, em 2023, os EUA lançaram a Estratégia Nacional de Segurança Cibernética (USA, 2023a). Dentre os diversos objetivos, tem-se os o de fornecer uma Internet segura, confiável e protegida para uso comercial e pessoal. Ademais, essa estratégia descreve outros objetivos, como por exemplo: incluir a segurança econômica e a prosperidade, respeitar os direitos humanos

e liberdades fundamentais, buscar proporcionar maior confiança na democracia e nas instituições democráticas, bem como e uma sociedade equitativa e diversa (USA, 2023b).

Nessa Estratégia de 2023, há cinco pilares, conforme descritos a seguir:

> - Defender a infraestrutura crítica;
> - Interrompa e desmantele os agentes de ameaças;
> - Moldar as forças do mercado para impulsionar a segurança e a resiliência;
> - Invista em um futuro resiliente; e
> - Forjar parcerias internacionais para perseguir objetivos compartilhados (USA, 2023b).

Em comparação com a estratégia anterior, a versão de 2023 destaca duas mudanças fundamentais sobre como são alocados os papéis, as responsabilidades e os recursos (USA, 2023b). Elas incluem:

> 1. Reequilibrar a responsabilidade de defender o espaço cibernético: Partindo da premissa que nem todos têm os mesmos recursos e capacidades, o plano coordenará para que os atores mais capazes e melhor posicionados atuarão para tornar a Internet mais segura. A estratégia reforça a responsabilidade dos proprietários, dos operadores e dos provedores de tecnologia em proteger o espaço cibernético.
> 2. Realinhar os incentivos para favorecer investimentos de longo prazo: além de uma responsabilidade compartilhada de defesa, essa estratégia também descreve incentivos para uma força de trabalho cibernética mais forte, mais segurança no *design* e pesquisa colaborativa (USA, 2023b).

Já no âmbito do Departamento de Defesa (DOD) dos EUA (homólogo ao Ministério da Defesa no Brasil), a Estratégia Cibernética do DOD de 2023, também baseada na estratégia de 2018, é o documento base de como o Departamento está operacionalizando as prioridades da Estratégia de Segurança Nacional de 2022, Estratégia de Defesa Nacional de 2022 e Estratégia de Segurança Cibernética Nacional de 2023 (USA, 2023c).

Nesse sentido, a principal mudança foi o enfoque em uma abordagem já publicada na Estratégia de 2018, mas que nessa última vem sendo reforçada: “Defend Forward” (Defender para a frente). *Defend Forward* é uma estratégia de segurança cibernética em que as organizações adotam uma abordagem ofensiva para proteger sua infraestrutura e dados críticos. Em vez de reagir a incidentes, o objetivo é interromper ou interromper proativamente atividades

cibernéticas maliciosas nos estágios iniciais (USA, 2023d).

Com o objetivo de operacionalizar o *Defend Forward*, são necessários os seguintes princípios:

> - Detectar e interromper as atividades maliciosas nos estágios iniciais;
> - Desenvolver uma compreensão profunda das últimas táticas, técnicas e procedimentos (TTPs) cibernéticos;
> - Reunir informações sobre potenciais adversários trabalhando fora da sua rede; e
> - Concentrar-se no engajamento persistente para informar aliados e parceiros sobre ameaças cibernéticas (USA, 2023d).

Assim, os EUA desenvolveram um conjunto de legislações capazes de proteger seus cidadãos no Espaço Cibernético, com uma Estratégia de Segurança e Defesa Cibernética bem definidas. Isso ocorre mesmo com legislações esparsas e variadas em cada um dos estados do país, pois existe uma Estratégia de âmbito nacional que direciona a forma adequada de atuação nacionalmente.

7.4 A ESTRUTURA ORGANIZACIONAL PARA SEGURANÇA E DEFESA CIBERNÉTICAS NOS EUA

A estrutura organizacional de segurança dos EUA é vasta e diversificada, o número exato de agências, escritórios, conselhos e comissões é desconhecido (Pernik, Wojtkowiak e Verschoor-Kirss, 2015). Embora as responsabilidades pela liderança da política cibernética sejam amplamente distribuídas, o principal papel de coordenação da política é assumido pelo Conselho de Segurança Nacional (Pernik, Wojtkowiak E Verschoor-Kirss, 2015).

Outrossim, a Lei de Segurança Interna de 2002 (Homeland Security Act *of* 2002) criou o Departamento de Segurança Interna (*Department of Homeland Security* - DHS) e encarregou-o, entre outras coisas, de coordenar os esforços nacionais relativos à proteção de infraestruturas críticas nos setores de TIC (Pernik, Wojtkowiak e Verschoor-Kirss, 2015).

Ainda, a Lei de Compartilhamento de Informações de Segurança Cibernética de 2015 (*Cybersecurity Information Sharing Act of* 2015) dá responsabilidade ao DHS, Diretor de Inteligência Nacional (*Director of National Intelligence* - DNI), Departamento de Defesa (*Department of Defense* - DoD) e Departamento de Justiça (*Department of Justice* - DOJ) para "desenvolver procedimentos para compartilhar informações sobre ameaças à segurança

cibernética com entidades privadas, agências não federais, governos estaduais, tribais e locais, o público e entidades sob ameaças" (USA, 2024a).

Nesse escopo, o DHS desempenha um papel-chave de liderança no fortalecimento da segurança cibernética nos EUA, investigando atividades cibernéticas maliciosas e promovendo a segurança cibernética (USA, 2024b). Para tanto, foi criada a Agência de Segurança Cibernética e de Infraestrutura (*Cybersecurity and Infrastructure Security Agency* - CISA) pela Lei Nº 115–278 de 16 de novembro de 2018 (*Cybersecurity and Infrastructure Security Agency Act of 2018, Public Law 115–278 — Nov. 16, 2018*) subordinada ao DHS e líder operacional de segurança cibernética federal e o coordenador nacional de segurança e resiliência de infraestruturas críticas (USA, 2024c).

Detalhando mais sobre a CISA, ela está no centro da troca de informações de segurança cibernética e colaboração operacional defensiva entre o governo federal e governos estaduais, locais, tribais e territoriais (SLTT), o setor privado e parceiros internacionais (USA, 2024d). Além disso, a agência tem duas funções operacionais principais:

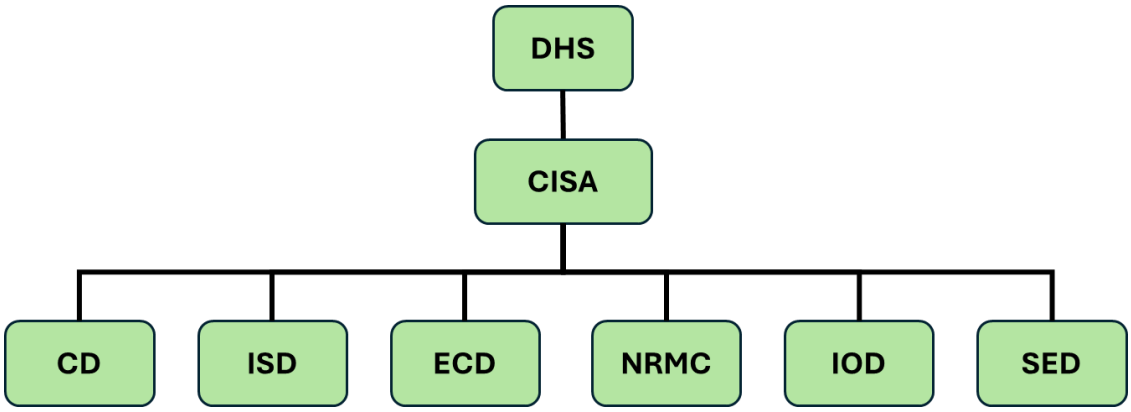
> • líder operacional para a segurança cibernética federal, encarregada de proteger e defender as redes do poder executivo civil federal em estreita parceria com o *Office of Management and Budget*, o *Office of the National Cyber Director* e os *Chief Information Officers* e *Chief Information Security Officers* da agência federal; e
>
> • coordenadora nacional para segurança e resiliência de infraestrutura crítica, trabalhando com parceiros em todo o governo e na indústria para proteger e defender a infraestrutura crítica do país (USA, 2024d).

A CISA como principal responsável pela segurança cibernética e proteção da infraestrutura em todos os níveis de governo, ela se divide em Divisões e Gabinetes. As Divisões da CISA se concentram na nossa missão operacional e os Gabinetes concentram-se em apoiar as Divisões e a agência em geral com pessoal, orçamento, logística e outro apoio operacional vital (USA, 2024e).

As Divisões operacionais da CISA são: 1. Divisão de Segurança Cibernética (*Cybersecurity Division* - CD); 2. Divisão de Segurança de Infraestrutura (*Infrastructure Security Division* - ISD); 3. Divisão de Comunicações de Emergência (*Emergency Communications Division* - ECD); 4. Centro Nacional de Gestão de Riscos (*National Risk Management Center* - NRMC); 5. Divisão de Operações Integradas (*Integrated Operations Division* - IOD); e 6. Divisão de Engajamento das Partes Interessadas (*Stakeholder*

Engagement Division - SED) (USA, 2024e). Na Figura 4, encontra-se a Estrutura Organizacional Resumida de Coordenação de Segurança Cibernética nos EUA.

Figura 4 - Estrutura Organizacional Resumida de Coordenação de Segurança Cibernética nos EUA



Fonte: o autor.

A seguir, será detalhada a missão e a visão geral de cada uma das divisões operacionais da CISA na Tabela 6.

Divisão	Missão	Visão Geral
CD	A missão da CD é defender e proteger o ciberespaço liderando esforços nacionais dos EUA para impulsionar e permitir uma defesa cibernética nacional eficaz, resiliência de funções críticas nacionais e um ecossistema de tecnologia robusto (USA, 2024f).	O CD é responsável por: fortalecer as defesas cibernéticas do país contra ameaças e vulnerabilidades imediatas; construir a capacidade de longo prazo da nação para resistir e operar durante incidentes cibernéticos; e busca realizar um ecossistema ciberespaço defensável garantindo que as mudanças no ecossistema transfiram a vantagem para os defensores da rede (USA, 2024f).
ISD	A ISD tem por missão liderar o esforço nacional para proteger as infraestruturas críticas do	O ISD coordena e colabora entre o governo e o setor privado. A Divisão realiza avaliações de vulnerabilidade

	país dos perigos, gerenciando riscos e aumentando a resiliência por meio da colaboração com a comunidade que trata de infraestrutura crítica (USA, 2024g).	com o objetivo de ajudar proprietários e operadores de infraestruturas críticas e parceiros estaduais, locais, tribais e territoriais a entender e abordar riscos à infraestrutura crítica. Além disso, realiza treinamentos para apoiar parceiros no governo e na indústria a gerenciar os riscos aos seus ativos, aos seus sistemas e às suas redes (USA, 2024g).
ECD	A ECD lidera os esforços de comunicação de segurança pública, segurança nacional e preparação para emergências com a finalidade de manter os EUA seguros, protegidos e resilientes (USA, 2024h).	A Divisão apoia e promove as comunicações usadas por equipes de emergência e autoridades governamentais e lidera os esforços de comunicações de segurança pública operáveis e interoperáveis e de segurança nacional e preparação para emergências (NS/EP) da Nação (USA, 2024h).
NRMC	O Centro que fornece análises de risco para garantir uma infraestrutura crítica segura e resiliente (USA, 2024i).	O NRMC fornece suporte analítico e estratégico vital para mitigar o risco à infraestrutura cibernética e física da qual os norte-americanos dependem. Dessa forma, o Centro identifica os riscos mais significativos em todos os 16 setores de infraestrutura crítica e promove atividades de redução de riscos para melhorar a segurança e a resiliência da infraestrutura crítica agora e no futuro (USA, 2024i).
IOD	A IOD prepara, planeja e	A Divisão lidera as operações da

	gerencia as operações da CISA e a entrega de recursos e serviços da CISA para dar suporte à defesa e à segurança da infraestrutura do nosso país (USA, 2024j).	CISA para mitigar riscos e aumentar a resiliência da infraestrutura crítica dos EUA (USA, 2024j).
SED	A SED lidera as parcerias e engajamentos voluntários nacionais e internacionais da CISA, ao mesmo tempo em que atua como o centro da agência para informações compartilhadas das partes interessadas que unificam a abordagem da CISA para a colaboração operacional e o compartilhamento de informações em todo o país (USA, 2024k).	Proteger a infraestrutura cibernética e física dos EUA é uma responsabilidade compartilhada que coloca o engajamento e a colaboração persistentes das partes interessadas. Assim, coma a ativação de uma rede de relacionamento com parceiros confiáveis e mecanismos de comunicação bem estabelecidos são realizadas atividades para responder, recuperar e mitigar ameaças e incidentes (USA, 2024k).

Fonte: (USA, 2024f); (USA, 2024g); (USA, 2024h); (USA, 2024i); (USA, 2024j); e (USA, 2024k).

Além da CISA, responsável pela Segurança Cibernética dos EUA e subordinada ao DHS, existe, também, o Comando Cibernético dos Estados Unidos (*United States Cyber Command* - USCYBERCOM), um dos onze comandos unificados de combate do Departamento de Defesa dos Estados Unidos (DoD).

Nesse sentido, o USCYBERCOM tem três focos: defender a Rede de Informações do DoD (*Department of Defense Information Network* - DODIN), apoiar na execução de suas missões ao redor do mundo e fortalecer a capacidade dos EUA em resistir e responder a ataques cibernéticos (USA, 2024l).

Esse Comando tem como missão unificar a direção das operações no espaço cibernético, fortalecer as capacidades do espaço cibernético do DoD e reforçar a expertise cibernética do DoD. Além disso, o Comando busca melhorar

as capacidades do DoD em operar redes de informação e comunicação resilientes e confiáveis; combater ameaças ao espaço cibernético e garantir acesso a esse espaço (USA, 2024l).

Outrossim, a missão do USCYBERCOM evoluiu para atender e combater ameaças aos sistemas do DoD e à infraestrutura crítica da nação, ao uso da internet por terroristas e às tentativas dos adversários de influenciar e interromper a coesão social e os processos democráticos dos EUA (USA, 2024m).

Essas ações, conduzidas pelo USCYBERCOM, ajudaram a preparação da segurança cibernética dos EUA, contribuíram para a capacidade de combate da Força Conjunta e estabeleceram ou reforçaram fortes relações de partilha de informações com uma série de nações (USA, 2023a).

Dessa forma, as responsabilidades das atividades atinentes à Segurança Cibernética e à Defesa Cibernética estão bem caracterizadas e definidas nos EUA, indicando que o país trata o tema com a adequada atenção.

7.5 OS PILARES DA GOVERNANÇA CIBERNÉTICA NOS EUA

De maneira similar ao item 5.5 deste trabalho de pesquisa, mas que aborda o tema com o viés da Espanha, esta Seção aborda a parte relativa aos pilares da governança cibernética na visão dos EUA. Por conseguinte, para que a governança cibernética no país esteja bem alicerçada, ela precisa desenvolver alguns pressupostos.

A governança cibernética nos EUA é considerada responsabilidade do poder executivo. Dirigidas pela Casa Branca por meio de ordens executivas e executadas pelo DHS, agências setoriais e pelo DoD, as atividades cibernéticas são altamente centralizadas – um processo *top-down* em que o poder executivo define os termos do debate, proíbe ou autoriza normas, além de estabelece mecanismos de colaboração público-privada (Mussington E Maclellan, 2018).

Com base nos estudos de Garcia et al (2022), foi definido um conjunto de critérios para avaliar a governança cibernética de um país. Cada um dos critérios já foi descrito na Tabela 05 (Critérios para avaliar a governança cibernética de um país), pertencente à Seção 5.5 (OS PILARES DA GOVERNANÇA

CIBERNÉTICA NA ESPANHA), e serão, também, a base de comparação para esta pesquisa.

Acerca da inteligência cibernética, o CISA possui a liderança institucional claramente definida por meio da Lei Nº 115–278 de 16 de novembro de 2018 (*Cybersecurity and Infrastructure Security Agency Act of 2018, Public Law 115–278 — Nov. 16, 2018*), o qual concede a autoridade para atuar nessa área, além de possibilitar atuação de maneira efetiva sobre esse tema (USA, 2018c).

Já sobre Comando e Doutrina Cibernética Militar estabelecidos, os EUA possuem o USCYBERCOM operante e com plenas capacidades para atender aos objetivos estratégicos do país. Esse Comando está subordinado ao Comando Estratégico dos Estados Unidos e possui doutrina plenamente estabelecida.

Em relação à responsabilidade legal para segurança cibernética, apesar de a CISA ser o principal vetor responsável pela segurança cibernética, existe, também, responsabilidades compartilhadas entre outros órgãos do governo federal, governos estaduais, governos locais, tribais e territoriais (SLTT), o setor privado e parceiros internacionais (USA, 2024d). Porém, a coordenação geral está legalmente instituída para a CISA, garantindo efetividade à essa responsabilização.

Sobre possuir funções e responsabilidades bem definidas para todas as instituições governamentais com competências cibernéticas, a doutrina cibernética na área militar norte-americana está bem definida. Há o Conselho de Segurança Nacional (*National Security Council* - NSC), o principal fórum do Presidente para considerar questões de segurança nacional e política externa com os seus conselheiros seniores e funcionários do gabinete. O NSC também trata das questões de Segurança Cibernética em mais alto nível (WHITE HOUSE, 2024). Além desse fórum, há o HSM, o DoD e os diversos órgãos com funções bem caracterizadas, garantindo a responsabilidade bem definida em todos os escalões dos governos e da sociedade.

7.6 AS CONCLUSÕES SOBRE A GOVERNANÇA CIBERNÉTICA NOS EUA

A governança cibernética estruturada de forma efetiva é um dos fatores que possibilita o país estar mais preparado para as ameaças no espaço cibernético, garantindo uma maior segurança e defesa em diversas áreas.

Os EUA são referência no quesito governança, sendo o primeiro país a explorar o tema. Além disso, no setor Cibernético também desenvolve adequadamente esse tipo governança de maneira plena com o objetivo de garantir que suas corporações, aliados e cidadãos possam agir tanto no ambiente digital quanto no físico com menos restrições.

Assim, a atuação da inteligência cibernética, o estabelecimento de um ambiente institucional em todas as esferas de governo (federal, estaduais, locais, tribais e territoriais - SLTT) para tratar do tema segurança/defesa cibernética e a promoção da interação dos setores governamentais, setores privados, setores públicos, universidades, instituições de pesquisa proporcionaram a efetividade em cibernética nos EUA.

Por fim, os EUA são um exemplo de sucesso a ser seguido pela pujança cibernética estabelecida e pela primazia com que o país vem tratando o tema.

8 UMA COMPARAÇÃO ENTRE OS MODELOS DE GOVERNANÇA APRESENTADOS E INTERAÇÃO COM OUTROS ATORES

Este capítulo tem por finalidade realizar uma breve comparação entre os modelos de Governança Cibernética apresentados neste trabalho de pesquisa. Além disso, esta parte da pesquisa abordará possíveis aspectos relevantes de modo a incrementar a efetividade do modelo nacional.

Ademais, com base nas informações levantadas nos capítulos anteriores, será exposto como as capacidades cibernéticas ofensivas e defensivas interagem com outros atores.

8.1 UMA COMPARAÇÃO DOS MODELOS DE GOVERNANÇA CIBERNÉTICA

A Espanha, o Brasil e os EUA apresentam características diferenciadas em relação aos seus respectivos setores cibernéticos. Cada país buscou desenvolver um modelo de governança cibernética que, teoricamente, pudessem atender suas necessidades e desenvolver capacidades para atender

a segurança e a defesa cibernéticas.

Dessa forma, a Espanha desenvolveu um arcabouço legal que hierarquiza a de forma mais efetiva e a nível nacional as diversas entidades responsáveis pelo setor cibernético do país. Já os EUA, apesar de definir uma hierarquia a nível federal, conceberam uma interação em nível com a participação dos órgãos em todas as esferas de governo (federal, estaduais, locais, tribais e territoriais - SLTT). No que diz respeito ao Brasil, há somente definição de responsabilidades de maneira esparsa às organizações de âmbito nacional, sem qualquer menção às outras esferas do governo.

Acerca da Liderança Institucional, a Espanha foi o país estudado que demonstrou possuir essa característica de maneira mais latente. Há um órgão em âmbito nacional, o CCN, responsável por realizar a inteligência cibernética, facilitando a governança. Já os EUA, possuem, também, um órgão central, o CISA e isso é um facilitador. No entanto, as características do ordenamento jurídico do país, que proporciona responsabilidade nas diversas esferas de governo, tem potencial de atrapalhar a atuação nacional. Sobre o Brasil, o CEPESC detém a responsabilidade sobre a inteligência cibernética. Porém, não existe sistemática de troca de informações definida e as legislações atuais são confusas e sobrepostas.

No que tange ao Comando e Doutrina Cibernética Militar estabelecidos, todos os 3 países tratados nesta pesquisa possuem essa característica bem desenvolvidas. A Espanha e o Brasil se encontram em situação similar e apesar de estarem estabelecidos em relação a esta parte, estão em situação inferior aos EUA. Este país possui maior capacidade de Comando Cibernético pois possui o USCYBERCOM operante e com plenas capacidades. Além disso, sua doutrina está em pleno uso pois suas Forças Armadas estão em preparo constante e emprego em ambiente real em diversas partes do globo.

Em relação à responsabilidade legal para segurança cibernética, a Espanha definiu de maneira inequívoca entre órgãos em âmbito nacional, o que facilita a atuação. Já os EUA possuem um órgão em âmbito nacional, o CISA, mas há responsabilidades entre outras esferas de governo, setor privado e aliados internacionais, dificultado a coordenação geral. Já o Brasil é o país que se encontra em situação menos favorável pois sua legislação sobre responsabilização legal encontra-se dispersa em diversos diplomas legais

contraditórios com muitos atores com poder legal insuficiente e sem capacidade de ação seja por falta de instrumentos regulatórios seja por falta de comandamento ou coordenação interinstitucional estabelecida.

Sobre possuir funções e responsabilidades bem definidas para todas as instituições governamentais com competências cibernéticas, a Espanha possui um Conselho, presidido pelo Diretor da CNI, o qual além de coordenar as ações cibernéticas em âmbito nacional é responsável pela estratégia de cibersegurança espanhola, garantindo elevado de maturidade nesse quesito. Já o Brasil, há carência de regras de engajamento e cooperação e a doutrina militar, apesar de ter sido estabelecida, carece de maior maturidade.

Outrossim, a situação encontra-se consideravelmente diferente que dos EUA pois o país possui funções e responsabilidades muito bem definidas com o Conselho de Segurança Nacional (*National Security Council* - NSC) tratando das questões de Segurança Cibernética em mais alto nível e o HSM, bem como o DoD e os diversos órgãos com funções muito bem caracterizadas, garantindo a responsabilidade bem definida em todos os escalões dos governos e da sociedade.

Os modelos de governança cibernética nos três países pesquisados apresentam considerável diferença. A que mais ressalta é que tanto a Espanha quanto os EUA desenvolveram um arcabouço legal acerca desse tema de modo linear, com uma lei ou um conjunto de leis que não se sobrepõem ou contradizem a concepção geral da segurança e/ou defesa cibernética. De modo diferente, O Brasil possui uma miríade de legislações contraditórias e dispersas, dificultando a atuação do país no setor cibernético de maneira efetiva.

8.2 ASPECTOS RELEVANTES DE MODO A INCREMENTAR A EFETIVIDADE DO MODELO NACIONAL

A governança cibernética no Brasil carece de melhorias com o objetivo de ser mais efetiva e garantir a capacidade do país em face das questões de segurança e defesa nesse domínio operacional.

O primeiro passo no sentido de organizar a legislação foi realizada no sentido de publicar a Política Nacional de Cibersegurança (Decreto nº 11.856, de 26 de Dezembro de 2023), que mesmo sem ser uma lei no sentido estrito, preenche uma lacuna na atualização da política do setor. Além dessa renovação

da política, esse Decreto determina que a Estratégia Nacional de Cibersegurança seja atualizada, o que vem ocorrendo em grupos de tabalho durante o corrente ano (EBC, 2024; CPQD, 2024).

Outrossim, o Brasil requer um aperfeiçoamento no tratamento de incidentes de rede. Os Centros de Resposta a Incidentes, por exemplo o CERT.br e o CTIR.gov não possuem capacidade prevista (nem responsabilidade legal) para enviar equipes durante crises de incidentes de segurança. Para esse tipo de apoio, a ABIN é convocada caso a caso e de maneira pontual nos incidentes priorizados, caracterizando um necessidade de apimoramento (GARCIA *et al.*, 2023).

Além disso, uma abordagem que tem funcionado bem tanto na Espanha quanto nos EUA é a definição de responsabilidades cibernéticas de maneira clara e em um diploma legal de alto nível nacional. Caso essa estatégia fosse realizada no Brasil, o país incrementaria a efetividade de sua governança cibernética.

Outro ponto a ser destacado é a que diz respeito à Liderança Institucional no que tange à inteligência cibernética. O Brasil carece tanto de sistemática bem definida quanto legislação na qual indica a responsabilidade inequívoca. Logo, o país melhoraria suas capacidades cibernéticas caso definisse explicitamente a Liderança Institucional cibernética.

Ademais, a Doutrina Cibernética, inclusive o Manual de Campanha - Guerra Cibernética (EB70-MC-10.232) do Exército Brasileiro tem espaço para atualização por ser um documento de 2017 e o setor cibernético ter a característica do dinamismo e do surgimento de novas necessidades. Assim, esse aperfeiçoamento requer a atenção que o tema demanda.

Dentro desse diapasão, o Brasil possui pouca maturidade em regras de engajamento em situações de incidentes cibernéticos e descentralização nas cooperação com organismos internacionais (MPF, 2024), o que dificulta a difusão de uma consciência nacional sobre os questões cibernéticas, inclusive crimes nessa área. Dessa forma, regras de engajamento claras e cooperação internacional centralizada incrementaria a givernança cibernética no país.

Sobre a sinergia com a sociedade civil, tanto a Espanha quanto os EUA são referência. O primeiro possui a Rede Nacional de Excelência em Investigação em Cibersegurança (*National Network of Excellence in*

Cybersecurity Research - RENIC) com a missão de apoiar e coordenar a investigação no domínio da cibersegurança envolvendo INCIBE e as principais instituições acadêmicas do país (Garcia *et al.*, 2022).

Já os EUA trabalham em estreita cooperação com o setor privado, responsabilizando os maus atores e os cibercriminosos que atentam contra a segurança e privacidade por meios cibernéticos (USA, 2023a). Porém, o Brasil possui poucas iniciativas nessa área (Garcia *et al.*, 2022). Logo, o país poderia estabelecer maiores interações com a sociedade civil com o objetivo de incrementar essa sinergia.

Acerca das cooperações internacionais, a Espanha coopera muito com Portugal e outros países europeus, além de possuir extensos programas de formação com países iberoamericanos (Garcia *et al.*, 2022). E os EUA têm estreitos laços com seus aliados e parceiros ao redor do mundo com objetivo de melhorar suas capacidades de defesa coletiva e de resposta às ameaças cibernéticas, em especial de Estados autoritários ou aqueles que vão contra os seus interesses nacionais (USA, 2023a).

Nesse ponto, o Brasil, mesmo estando aberto à cooperação, possui capacidade limitada, pois são realizadas pela ABIN quando relacionadas à segurança do Estado Brasileiro ou pela Justiça/Ministério da Justiça e Segurança Pública em caso judicializados, dificultando uma sistematização em âmbito nacional. Assim, procedimentos padronizados em âmbito federal tem potencial de aperfeiçoar as cooperações internacionais.

Por fim, um possível aperfeiçoamento da Doutrina nacional de atuação cibernética seria avaliar a possibilidade de uso da estratégia “*Defend Forward*” (Defender para a frente), adotada pelos EUA (USA, 2023a). Essa forma de atuação permitiria uma ação mais decisiva por utilizar uma abordagem ofensiva, interrompendo proativamente atividades cibernéticas maliciosas nos estágios iniciais, na proteção de suas infraestruturas e dados críticos, em vez de somente reagir a incidentes.

9 CONSIDERAÇÕES FINAIS

O presente trabalho teve o objetivo de analisar os modelos de Governança Cibernética nos EUA e na Espanha, países do arco do conhecimento, e verificar se são adequados às necessidades estratégicas brasileiras, bem como se as

capacidades cibernéticas ofensivas e defensivas interagem com outros atores, por exemplo setores da sociedade civil.

Nesse sentido, foi realizada análise de conteúdo e o levantamento comparativo, a partir da metodologia de pesquisa bibliográfica e documental, com objetivo de exploradas as similaridades e diferenças dos modelos de governança cibernética em cada um dos países estudados.

Inicialmente, foram apresentados os principais conceitos acerca dos temas Governança Corporativa e Governança Cibernética, além de realizar exame e interconexões sobre o as partes mais atinentes às empresas e corporações (atores que também são relevantes no ambiente cibernético), além das relativas às normativas legais.

A seguir foi analisado o funcionamento da Governança Cibernética na Espanha, a estratégia de segurança cibernética, sua estrutura organizacional, além de ser analisado cada um dos critérios para avaliar a governança cibernética de um país.

De forma similar, foram realizadas as análises dos modelos de Governança Cibernética nos EUA e no Brasil. Em cada um desses países foram apresentadas informações de como a Governança Corporativa se desenvolveu e como a Governança Cibernética está em relação à sua maturidade. Foram, também, expostas as suas estratégias de segurança e suas estruturas organizacionais cibernéticas. Em ambos os casos foram analisados os pilares da Governança Cibernética nesses países.

Por fim, foram comparados os modelos de Governança Cibernética da Espanha e do EUA com o modelo do Brasil, tratando de possíveis aspectos relevantes com o objetivo de incrementar a efetividade do modelo nacional. Ademais, foram expostos como as capacidades cibernéticas ofensivas e defensivas interagem com outros atores.

Como trabalhos futuros, indica-se realizar a comparação com outros países, em especial aqueles que se encontram em conflitos bélicos na atualidade. Assim, seria possível analisar como a Governança Cibernética influência nos combates e nas atuações no Teatro de Operações.

REFERÊNCIAS

BAARS, Hans; HINTZBERGEN Kees; HINTZBERGEN Jule; SMULDERS, André. Fundamentos de Segurança da Informação: com Base na ISO 27001 e na ISO 27002 Capa comum – Edição padrão, 24 janeiro 2018. Edição Português. Rio de Janeiro: Brasport, 2018. 235 p.

BODIN, Jean. Os Seis Livros da República - Livro Primeiro 1ª ed. Ícone Editora Ltda. – 2011.

BRASIL. Presidência da República. Política de Defesa Nacional (PDN). 1996. Disponível em: http://www.biblioteca.presidencia.gov.br/publicacoes-oficiais/catalogo/fhc/politica-de-defesa-nacional-1996.pdf. Acessado em 03 de Agosto de 2024.

BRASIL. Presidência da República. Política de Defesa Nacional (PDN). 2005. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2004-2006/2005/decreto/d5484.htm. Acessado em 03 de Agosto de 2024.

BRASIL. Exército. ECEME. Elaboração de Projetos de Pesquisa na ECEME - ME 21-259. Rio de Janeiro, 2012.

BRASIL. Constituição (1988). Constituição da República Federativa do Brasil. promulgada em 5 de outubro de 1988. Brasília-DF: Pres. República Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acessado em 22 Abril de 2024.

BRASIL. Presidência da República. Política Nacional de Defesa (PND). 2016a. Disponível em: https://www.gov.br/defesa/pt-br/assuntos/copy_of_estado-e-defesa/pnd_end_2016.pdf. Acessado em 03 de Agosto de 2024.

BRASIL. Presidência da República. Estratégia Nacional de Defesa (END). 2016b. Disponível em: https://www.gov.br/defesa/pt-br/assuntos/copy_of_estado-e-defesa/pnd_end_2016.pdf. Acessado em 03 de Agosto de 2024.

BRASIL. Exército. Estado-Maior. EB70-MC-10.232 Manual de Campanha - Guerra Cibernética. 1ª ed. Brasília, DF. 2017.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. Glossário de Segurança da Informação. Brasília, DF: GSI, Decreto Nº 93, de 18 de outubro de 2021.

BRASIL. Exército Brasileiro. Estado-Maior. EB20-MF-03.106 Estratégia. 5ª ed. Brasília, DF. 2020a.

BRASIL. Tribunal de Contas da União. Referencial básico de governança aplicável a organizações públicas e outros entes jurisdicionados ao TCU / Tribunal de Contas da União. Edição 3 - Brasília: TCU, Secretaria de Controle Externo da Administração do Estado – SecexAdministração, 2020b. 242p.

BRASIL. Presidência da República. Estratégia Nacional de Segurança Cibernética - E-Ciber. Brasília-DF, 2020c. Disponível em: https://www.in.gov.br/en/web/dou/-/decreto-n-10.222-de-5-de-fevereiro-de-2020-241828419. Acesso em 26 de Abril de 2024.

BRASIL. Ministério da Defesa. Estratégia Nacional de Defesa. Política Nacional de Defesa. Brasília, DF: MD, 2020d. Versão sob apreciação do Congresso Nacional (Lei Complementar 97/1999, art. 9º, § 3º). Disponível em: https://www.gov.br/defesa/pt-br/arquivos/estado_e_defesa/pnd_end_congresso_.pdf. Acesso em 22 de Abril de 2024.

BRASIL. Presidência da República. Rede Federal de Gestão de Incidentes Cibernéticos - ReGIC. Brasília-DF, 2021. Disponível em: https://www.in.gov.br/en/web/dou/-/decreto-n-10.748-de-16-de-julho-de-2021-332610022. Acesso em 04 de Agosto de 2024.

BRASIL. Presidência da República. Política Nacional de Cibersegurança - PNCiber. Brasília-DF, 2023. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/D11856.htm. Acesso em 03 de Agosto de 2024

BUTA, B. O.; TEIXEIRA, M. A. C. Governança pública em três dimensões: conceitual, mensural e democrática. Organizações & Sociedade, v. 27, n. 94, p. 370-395, 2020.

CALDERARO, Andrea & CRAIG, Anthony J. S. (2020): Transnational governanceof cybersecurity: policy challenges and global inequalities in cyber capacity building, Third WorldQuarterly, DOI: 10.1080/01436597.2020.1729729.

CARLOTTO, Julio. Modelo de Governança e os Pilares da Gestão Integrada. 2019. Disponível em: https://pt.linkedin.com/pulse/modelo-de-governança-e-os-pilares-da-gestão-integrada-julio-carlotto. Acessado em 20 de Abril de 2024.

CENDOYA, Alexander. National Cyber Security Organisation Spain. 2016. Disponível em: https://ccdcoe.org/uploads/2018/10/CS_organisation_SPAIN_092016.pdf. Acessado em 29 de Junho de 2024.

CETIC, Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação. TIC Domicílios 2023. 2023. Disponível em: https://cetic.br/media/analises/tic_domicilios_2023_coletiva_imprensa.pdf Acessado em 08 de Julho de 2024.

CETIC, Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação. TIC Domicílios 2015 e 2023. 2024. Disponível em: https://cetic.br/pt/tics/governo/2015/orgaos/C4A/ e https://cetic.br/pt/tics/governo/2023/orgaos/C4A/ Acessado em 08 de Julho de 2024.

CPQD (Centro de Pesquisa e Desenvolvimento em Telecomunicações). CPQD integra grupo de trabalho do CNCiber responsável pela atualização da Estratégia Nacional de Cibersegurança. 2024. Disponível em:

https://www.cpqd.com.br/noticias/cpqd-integra-grupo-de-trabalho-do-cnciber-responsavel-pela-atualizacao-da-estrategia-nacional-de-ciberseguranca/. Acessado em 05 de Setembro de 2024.

CYBERSTATES. The definitive guide to the U.S. tech industry and tech workforce. Research report. 2019. Disponível em: https://nhtechalliance.org/wp-content/uploads/2019/10/CompTIA_Cyberstates_2019.pdf?x84255. Acessado em 24 de Agosto de 2024.

CGU. Controladoria-Geral da União. 2024. Disponível em: https://www.gov.br/cgu/pt-br/centrais-de-conteudo/campanhas/integridade-publica/governanca. Acessado em 06 de Julho de 2024.

CLARKE, Richard A.; KNAKE, Robert K. Guerra Cibernética: A próxima ameaça a segurança o que fazer a respeito. Rio de Janeiro: Brasport, 2015. 241 p.

CRUZ, Elaine Patricia. Empresa Brasil de Comunicação. GSI recebe nesta quinta-feira propostas para cibersegurança no país. Disponível em: https://agenciabrasil.ebc.com.br/geral/noticia/2024-07/propostas-para-ciberseguranca-no-pais-sao-encaminhadas-hoje-ao-gsi. Acessado em 03 de Agosto de 2024.

DEUTSCH, Alan. Histórico da Governança Corporativa nos Estados Unidos da América. 2013. Disponível em: https://www.jusbrasil.com.br/artigos/historico-da-governanca-corporativa-nos-estados-unidos-da-america/112320660. Acessado em 23 de Agosto de 2024.

EBC (Empresa Brasil de Comunicação). GSI recebe nesta quinta-feira propostas para cibersegurança no país. 2024. Disponível em: https://agenciabrasil.ebc.com.br/geral/noticia/2024-07/propostas-para-ciberseguranca-no-pais-sao-encaminhadas-hoje-ao-gsi. Acessado em 05 de Setembro de 2024.

ECGI (*The European Corporate Governance Institute*). *Corporate Governance in the United States*. 2024. Disponível em: https://www.ecgi.global/publications/codes/countries/corporate-governance-in-the-united-states. Acessado em 23 de Agosto de 2024.

ESPANHA. Gobierno de España. Ministério da Energia, Turismo e Agenda Digital e Ministério das Finanças e Função Pública. Digital Agenda for Spain. February 2013. Disponível em: https:// plantl.mineco.gob.es/digital-agenda/Documents/digital-agenda-for-spain.pdf. Acessado em 29 de Junho de 2024.

ESPANHA. Estrategia Nacional de Ciberseguridad, 2019. Disponível em: https://www.dsn.gob.es/es/documento/estrategia-nacional-ciberseguridad-2019. 2019. Acessado em 26 Abril de 2024.

ESPANHA. Gobierno de España. Ministério da Energia, Turismo e Agenda Digital. Plan para la Conectividad y las Infraestructuras Digitales de la sociedad,

la economía y los territórios. 2020. Disponível em: https://espanadigital.gob.es/sites/ espanadigital/files/2022-06/Plan%20para%20la%20Conectividad.pdf Acessado em 29 de Junho de 2024.

ESPANHA. Estrategia de Seguridad Nacional, 2021. Disponível em: https://www.dsn.gob.es/es/documento/estrategia-seguridad-nacional-2021 ou https://www.dsn.gob.es/es/file/7272/download?token=miLM79u6 (Língua Inglesa). Acessado em 30 de Junho de 2024.

ESPANHA. Gobierno de España, Ministerio para la Transformatión Digital y la Función Pública, Secretaría de Estado de Función Pública, “Gobernanza Pública”, 2022. Disponível em: https://funcionpublica.digital.gob.es/gobernanza-publica.html. Acessado em 28 de Junho de 2024.

ESPANHA. Good Governance Code On Cybersecurity. Administración General del Estado, 2023a Disponível em: https://foronacionalciberseguridad.es/index.php/documentacion/publico/124-good-governance-code-on-cybersecurity/file. Acessado em 22 Abril de 2024.

ESPANHA. Gobierno de España. Centro Criptológico Nacional. Ciberamenazas y tendencias. Edición 2023. CCN-CERT IA-35/23. Análisis de las ciberamenazas nacionales e internacionales, de su evolución y tendencias futuras. Administración General del Estado, 2023b. Disponível em: https://www.ccn-cert.cni.es/es/informes/informes-ccn-cert-publicos/7188-ccn-cert-ia-35-23-ciberamenazas-y-tendencias-edicion-2023/file.html. Acessado em 05 Junho de 2024.

ESPANHA. Gobierno de España, Ministerio del Interior, 2024a. Disponível em: https://www.interior.gob.es/opencms/es/el-ministerio/funciones-y-estructura/secretaria-de-estado-de-seguridad/. Acessado em 01 de Julho de 2024.

ESPANHA. Gobierno de España,Ministerio del Interiorpara la Transformación Digital y de la Función Pública, 2024b. Disponível em: https://avancedigital.mineco.gob.es/es-es/SecretariaDeEstado/Paginas/secretaria_estado.aspx. Acessado em 01 de Julho de 2024.

ESPANHA. Gobierno de España, Ministerio de Defensa, 2024c. Disponível em: https://emad.defensa.gob.es/emad/?__locale=es. Acessado em 01 de Julho de 2024.

ESPANHA. Gobierno de España, Ministerio de Defensa, 2024d. Disponível em: https://www.cni.es/en/about-the-cni/objectives-and-values. Acessado em 01 de Julho de 2024.

ESPANHA. Gobierno de España, Ministerio del Interior para la Transformación Digital y de la Función Pública, 2024e. Disponível em: https://www.incibe.es/incibe/informacion-corporativa/que-es-incibe. Acessado em 02 de Julho de 2024.

ESPANHA. Gobierno de España, Ministerio de Defensa, 2024f. Disponível em: https://emad.defensa.gob.es/unidades/mcce/. Acessado em 02 de Julho de 2024.

ESPANHA. Gobierno de España, Ministerio de Defensa, 2024g. Disponível em: https://www.ccn.cni.es/images/stories/normas/pdf/rd421-2004centrocriptologiconacional.pdf. Acessado em 05 de Julho de 2024.

ESPANHA. Gobierno de España, Ministerio del Interior para la Transformación Digital y de la Función Pública, 2024h. Disponível em: https://www.incibe.es/incibe-cert/sobre-incibe-cert/que-es-incibe-cert. Acessado em 02 de Julho de 2024.

ESPANHA. CSIRT.es, 2024i. Disponível em: https://www.csirt.es/index.php/es/. Acessado em 02 de Julho de 2024.

ESPANHA. Gobierno de España, Ministerio de Defensa, 2024j. Disponível em: https://www.ccn-cert.cni.es/es/sobre-nosotros/faq.html. Acessado em 02 de Julho de 2024.

FRANÇA, Raimundo, & DOS SANTOS, Simone Cabral Marinho. O sentido da política como vocação em Max Weber. REVISTA DE CIÊNCIA POLÍTICA, DIREITO E POLÍTICAS PÚBLICAS - POLITI(k)CON. UNEMAT. VOL.2 Nº 1, agosto/dezembro, 2021. ISSN: 2763-5945.

FUKUYAMA, Francis, What is Governance? (January 25, 2013). Center for Global Development Working Paper No. 314, Available at SSRN: https://ssrn.com/abstract=2226592 or http://dx.doi.org/10.2139/ssrn.2226592.

GARCIA, M., F. Mendonça and R. De Oliveira Albuquerque, "Assessments on National Cyber Capability: A Brazilian Perspective in a Comparison with Spain," *2022 17th Iberian Conference on Information Systems and Technologies (CISTI)*, Madrid, Spain, 2022, pp. 1-6, doi: 10.23919/CISTI54924.2022.9866889.

GARCIA, M. (2023). Key Factors for a Cybersecurity and Cyberintelligence Policy in Brazil. Professional Master's Thesis, Department of Electrical Engineering, University of Brasília, Brasília, DF, PPEE.MP.044, 74 p.

GOLDONI, L. R. F.; RODRIGUES, K. F.; MEDEIROS, B. P. Qual é o futuro da governança de cibersegurança no Brasil?. Cadernos Gestão Pública e Cidadania, São Paulo, v. 29, p. e90972 , 2024. DOI: 10.12660/cgpc.v29.90972. Disponível em: https://periodicos.fgv.br/cgpc/article/view/90972.

IGCB. Instituto Brasileiro de Governança Corporativa (IBGC). Código Brasileiro de Governança Corporativa: Companhias Abertas / Grupo de Trabalho Interagentes; coordenação Instituto Brasileiro de Governança Corporativa. São Paulo, SP: IBGC, 2016. 64 p. ISBN: 978-85-99645-45-1

IT Governance USA. Data Breaches and Cyber Attacks – USA Report 2024. 2024a. Disponível em: https://www.itgovernanceusa.com/blog/data-breaches-and-cyber-attacks-in-2024-in-the-usa. Acessado em 24 de Agosto de 2024.

IT Governance USA. Federal Cybersecurity and Data Privacy Laws Directory. 2024b. Disponível em: https://www.itgovernanceusa.com/federal-cybersecurity-and-privacy-laws. Acessado em 25 de Agosto de 2024.

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

LODI, J. B. Estratégia de negócios: planejamento a longo prazo. Revista de Administração de Empresas, Rio de Janeiro: FGV, v. 9, n. 1, p. 5- 32, mar. 1969.

MALATJI, Masike; MATLI, Walter. The Potential Benefits and Challenges of a BRICS+ Agency for Cybersecurity Intelligence Exchange. Journal of Information Security and Cybercrimes Research, v. 6, n. 2, p. 116-129, 2023.

MINTZBERG, Henry; QUINN, James Brian. O processo da estratégia. 3 ed. Porto Alegre: Bookman, 2001.

MPF (Ministério Público Federal). Cooperação para Criminalidade Cibernética e Provas Eletrônicas. 2024. Disponível em: https://www.mpf.mp.br/atuacao-tematica/sci/dados-da-atuacao/assessoria-juridica/cooperacao-ativa/cooperacao-para-criminalidade-cibernetica-e-provas-eletronicas. Acessado em 05 de Setembro de 2024.

MUSSINGTON, David, and MACLELLAN, Stephanie. “US Cyber Policy: Sources of and Impediments to Rapid Progress.” Governing Cyber Security in Canada, Australia and the United States, edited by Christian Leuprecht, Centre for International Governance Innovation, 2018, pp. 9–12. JSTOR, http://www.jstor.org/stable/resrep17311.7. Acessado em 29 de Agosto de 2024.

OCDE (2014), *Recommendation of the Council on Digital Government Strategies*, OCDE, 2014, Paris, Disponível em: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0406. Acessado em 29 de Agosto de 2024.

OMPI. Organização Mundial da Propriedade Intelectual (OMPI). Global Innovation Index 2023: Switzerland, Sweden and the U.S. lead the Global Innovation Ranking; Innovation Robust but Startup Funding Increasingly Uncertain. 2024. Disponível em: https://www.wipo.int/pressroom/en/articles/2023/article_0011.html Acessado em 24 de Agosto de 2024.

PAWLAK, Patryk. “Capacity Building in Cyberspace as an Instrument of Foreign Policy.” Global Policy 7, no. 1 (2016): 83–92. doi:10.1111/1758-5899.12298.

PEDROSO NETO, Marcos. Corporate Governance, Historical Rescue And Relationship With Compliance. ESG Studies Review, São Paulo (SP), v. 4, n. ssue, p. e01611, 2021. DOI: 10.37497/esg.v4issue.1611. Disponível em: https://esglawreview.org/convergencias/article/view/1611. Acesso em: 23 de Agosto de 2024.

PERNIK, Piret; WOJTKOWIAK, Jesse; VERSCHOOR-KIRSS, Alexander. National Cyber Security Organisation: United States. 2015. Disponível em:

https://ccdcoe.org/uploads/2018/10/CS_organisation_USA_122015.pdf. Acessado em 24 de Agosto de 2024.

PETROSYAN, Ani. United States internet penetration 2000-2024. 2024. Disponível em: https://www.statista.com/statistics/209117/us-internet-penetration/. Acesso em: 23 de Agosto de 2024.

RAE – La Real Academia Española. “Diccionario de la lengua española”, 2001. Disponível em https://www.rae.es/drae2001/gobernanza . Acessado em 28 de Junho de 2024.

REIS, Claudio A. "Todo o poder emana do povo": o exercício da soberania popular e a constituição de 1988. p. 255-273, Capítulo do livro Constituição de 1988: o Brasil 20 anos depois / Os Cidadãos na Carta Cidadã, Ano de Publicação: 2008. Editora: Senado Federal, Instituto Legislativo Brasileiro. ISBN: 978-8587499-03-5.

REZENDE, G.S.; NASCIMENTO, N.E. Governança Global: o desafio ecológico e sua aplicabilidade no Sistema Internacional. Revista Mosaico, v.11, n.1, p. 02-09, 2020. doi: https://doi.org/10.21727/rm.v11i1.1885

ROCHA, Ivan, Iida Itiro. Intuition and wisdom in decision making. Production [en linea]. 2018, 28( ), 1-8 [fecha de Consulta 2 de Julio de 2024]. ISSN: 0103-6513. Disponível em: https://www.redalyc.org/articulo.oa?id=396754754013. Acessado em 02 de Julho de 2024.

ROSE-ACKERMAN, Susan. (2016). What Does “Governance” Mean?: What Does “Governance” Mean?. Governance. 30. 10.1111/gove.12212.

ROSTI, Andrea. Ameaças Cibernéticas Crescentes: Brasil Lidera Ranking De 2023 Na América Latina. 2024. Disponível em: https://safewayconsultoria.com/ameacas-ciberneticas-crescentes-brasil-lidera-ranking-de-2023-na-america-latina/. Acessado em 13 de Julho de 2024.

SAVAŞ, S., KARATAŞ, S. Cyber governance studies in ensuring cybersecurity: an overview of cybersecurity Governance Int. Cybersecur. Law Rev., 3 (1) (2022), pp. 7-34, 10.1365/s43439-021-00045-4.

SCHERER, A. (2003). O modelo norte-americano de governança corporativa: gênese, instrumentos e consequências. Ensaios FEE, Porto Alegre, v. 24, n. 2, p. 429-452, 2003 https://revistas.planejamento.rs.gov.br/index.php/ensaios/article/viewFile/671/948. Acessado em 23 de Agosto de 2024.

SHERIF, Ahmed. Tech sector as a percentage of total gross domestic product (GDP) in the United States from 2017 to 2022. Disponível em: https://www.statista.com/statistics/1239480/united-states-leading-states-by-tech-contribution-to-gross-product/. Acessado em 24 de Agosto de 2024.

SILVA, G. J., & AMARAL, C. S. T. (2023). Governança do habitat de inovação – contratos de inovação. Revista de Gestão e Secretariado (Management and

Administrative Professional Review). 14(4), 4555-4575. DOI: https://doi.org/10.7769/gesec.v14i4.1920.

USA. Release of the 2018 National Cyber Strategy. Disponível em: https://2017-2021.state.gov/release-of-the-2018-national-cyber-strategy/. 2018a. Acessado em 25 de Agosto de 2024.

USA. Release of the 2018 National Cyber Strategy. Disponível em: https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf. 2018b. Acessado em 25 de Agosto de 2024.

USA. Cybersecurity And Infrastructure Security Agency Act of 2018 (Public Law 115–278—Nov. 16, 2018). 2018c. Disponível em: https://www.govinfo.gov/content/pkg/PLAW-115publ278/pdf/PLAW-115publ278.pdf. 2018c. Acessado em 30 de Agosto de 2024.

USA. National Cybersecurity Strategy. Disponível em: https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf. 2023a. Acessado em 26 de Abril de 2024.

USA. Summary of the 2023 National Cybersecurity Strategy: Part 1. Disponível em: https://www.cai.io/resources/thought-leadership/summary-of-2023-national-cybersecurity-strategy-part-1. 2023b. Acessado em 25 de Agosto de 2024.

USA. DOD Releases 2023 Cyber Strategy Summary. Disponível em: https://www.defense.gov/News/Releases/Release/Article/3523199/dod-releases-2023-cyber-strategy-summary/. 2023c. Acessado em 25 de Agosto de 2024.

USA. The Pentagon's 2023 cyber strategy: What you need to know. Disponível em: https://securityintelligence.com/articles/the-pentagons-2023-cyber-strategy-what-you-need-to-know/. 2023d. Acessado em 25 de Agosto de 2024.

USA. 5.3 Department of Homeland Security (DHS) - Key Organizations. Disponível em: https://www.cio.gov/handbook/key-organizations/dhs/. 2024a. Acessado em 25 de Agosto de 2024.

USA. Homeland Security - Cybersecurity. Disponível em: https://www.dhs.gov/topics/cybersecurity. 2024b. Acessado em 25 de Agosto de 2024.

USA. About CISA. Disponível em: https://www.cisa.gov/about. 2024c. Acessado em 25 de Agosto de 2024.

USA. DHS – Cybersecurity: Cybersecurity and Infrastructure Security Agency (CISA). Disponível em: https://www.dhs.gov/topics/cybersecurity 2024d. Acessado em 25 de Agosto de 2024.

USA. Cybersecurity and Infrastructure Security Agency - Divisions & Offices. Disponível em: https://www.cisa.gov/about/divisions-offices. 2024e. Acessado em 25 de Agosto de 2024.

USA. Cybersecurity and Infrastructure Security Agency - Cybersecurity Division. Disponível em: https://www.cisa.gov/about/divisions-offices/cybersecurity-division. 2024f. Acessado em 27 de Agosto de 2024.

USA. Cybersecurity and Infrastructure Security Agency - Infrastructure Security Division. Disponível em: https://www.cisa.gov/about/divisions-offices/infrastructure-security-division. 2024g. Acessado em 27 de Agosto de 2024.

USA. Cybersecurity and Infrastructure Security Agency - Emergency Communications Division. Disponível em: https://www.cisa.gov/about/divisions-offices/emergency-communications-division. 2024h. Acessado em 27 de Agosto de 2024.

USA. Cybersecurity and Infrastructure Security Agency - National Risk Management Center. Disponível em: https://www.cisa.gov/about/divisions-offices/national-risk-management-center. 2024i. Acessado em 27 de Agosto de 2024.

USA. Cybersecurity and Infrastructure Security Agency - Integrated Operations Division. Disponível em: https://www.cisa.gov/about/divisions-offices/integrated-operations-division. 2024j. Acessado em 27 de Agosto de 2024.

USA. Cybersecurity and Infrastructure Security Agency - Stakeholder Engagement Division. Disponível em: https://www.cisa.gov/about/divisions-offices/stakeholder-engagement-division. 2024k. Acessado em 27 de Agosto de 2024.

USA. U.S. Cyber Command - Our Mission and Vision. Disponível em: https://www.cybercom.mil/About/Mission-and-Vision/. 2024l. Acessado em 29 de Agosto de 2024.

USA. U.S. Cyber Command - Our History. Disponível em: https://www.cybercom.mil/About/History/. 2024m. Acessado em 29 de Agosto de 2024.

WHITE HOUSE. FACT SHEET: Improving and Simplifying Digital Services. 2014. Disponível em: https://obamawhitehouse.archives.gov/the-press-office/2014/08/11/fact-sheet-improving-and-simplifying-digital-services. Acessado em 24 de Agosto de 2024.

WHITE HOUSE. *National Security Council* (NSC). 2024. Disponível em: https://www.whitehouse.gov/nsc/. Acessado em 30 de Agosto de 2024.