

ESCOLA DE COMANDO E ESTADO-MAIOR DO EXÉRCITO
ESCOLA MARECHAL CASTELLO BRANCO

TC Com (OINA) SANTIAGO **AGUAYO MOYA**

**A POLÍTICA NACIONAL DE CIBERSEGURANÇA DO CHILE:
ANÁLISE A PARTIR DA ABORDAGEM DOS MÚLTIPLOS
FLUXOS PARA AS POLÍTICAS PÚBLICAS**



Rio de Janeiro

2021

TC Com (OINA) SANTIAGO **AGUAYO MOYA**

**A POLÍTICA NACIONAL DE CIBERSEGURANÇA DO CHILE:
ANÁLISE A PARTIR DA ABORDAGEM DOS MÚLTIPLOS
FLUXOS PARA AS POLÍTICAS PÚBLICAS**

Texto apresentado como Dissertação de Mestrado do Programa de Pós-Graduação em Ciências Militares do Instituto Meira Mattos da Escola de Comando e Estado-Maior do Exército, como requisito para a obtenção do título de Mestre em Ciências Militares.

Orientador: Prof^a. Dr^a Ana Luiza Bravo e Paiva

Rio de Janeiro

2021

M938p Moya, Santiago Aguayo.

A política nacional de Cibersegurança do Chile: Análise a partir da abordagem dos múltiplos fluxos para as políticas públicas. / Santiago Aguayo Moya. —2021.
118 f. : il. ; 30 cm

Orientação: Ana Luiza Bravo e Paiva.
Dissertação (Mestrado em Ciências Militares) — Escola de Comando e Estado -
Maior do Exército, Rio de Janeiro, 2021.
Bibliografia: f.88-94

**1. CIBERSEGURANÇA. 2. POLÍTICA PÚBLICA. 3. MODELO DE ANÁLISE
DOS MÚLTIPLOS FLUXOS. I. Título.**

CDD 003.5

TC Com (OINA) SANTIAGO AGUAYO MOYA

A POLÍTICA NACIONAL DE CIBERSEGURANÇA DO CHILE: ANÁLISE A PARTIR DA ABORDAGEM DOS MÚLTIPLOS FLUXOS PARA AS POLÍTICAS PÚBLICAS

Dissertação apresentada à Escola de Comando e Estado-Maior do Exército, como requisito parcial para a obtenção do título de Mestre em Ciências Militares.

Aprovada em 13 de dezembro de 2021

BANCA EXAMINADORA



ANA LUIZA BRAVO E PAIVA – Profª Drª – Presidente
Escola de Comando e Estado-Maior do Exército - ECEME



KARINA FURTADO RODRIGUES – Profª Drª – Membro
Escola de Comando e Estado-Maior do Exército - ECEME



CINTIENE SANDES MONFREDO MENDES – Profª Drª – Membro
Escola Superior de Guerra - ESG



Ciente

SANTIAGO ROBERTO AGUAYO MOYA – Ten Cel – Postulante
Escola de Comando e Estado-Maior do Exército

Aos meus amados pais, Santiago e Bernardina. A meus irmãos Oscar e Andrea. A todos por seu permanente amor e apoio no caminhar da vida.

À minha amada família, Giannina e meu filho Santi, pilares fundamentais da minha felicidade e luzes que me guiam como pessoa.

Ao meu apreciado camarada Subtenente Claudio Acevedo Muñoz (in memoriam).

AGRADECIMENTOS

À minha esposa Giannina e meu filho Santiago pelo apoio incondicional dado, pela paciência e compreensão em todos os momentos que levaram assumir mais uma vez, outro desafio.

Ao Exército do Chile por me dar a possibilidade de aumentar meu patrimônio cultural e profissional durante minha permanência no Brasil.

Ao Exército Brasileiro, e especificamente à ECEME e ao Instituto Meira Mattos pela possibilidade de poder participar do processo de mestrado e contribuir com a elaboração de um trabalho de dissertação, ampliando assim meu conhecimento profissional.

À minha orientadora, Prof. Dra. Ana Luiza Bravo e Paiva, os meus agradecimentos pela sábia e permanente orientação, representando um facilitador de muita importância na preparação e conclusão do trabalho.

“Sei bem o que posso esperar de vocês, que com admirável perseverança, moralidade e disciplina, suportaram os rigores da educação militar; sei bem que não preciso recomendar coragem e sacrifício, porque sei que o lema do nosso país “vencer ou morrer” está gravado nos vossos corações” (General Erasmo Escala Arriagada, assalto e conquista de Pisagua, 1879).

RESUMO

Esta dissertação apresenta uma análise a partir da abordagem dos múltiplos fluxos para a recente Política Nacional de Cibersegurança do Chile publicada em 2017. A política nacional estabelece as diretrizes políticas do Estado para acompanhar a evolução tecnológica com o objetivo de alcançar um ciberespaço livre, democrático, aberto, seguro e resiliente. Nessa perspectiva do estudo foi apresentada a evolução da institucionalidade digital do Chile de 1999 até 2017, para posteriormente, com uso do modelo de análise dos múltiplos fluxos de Kingdon, identificaram-se os intervenientes e ações específicas geradas no processo de definição da agenda pública para a política entre os anos de 2014 a 2017, usando a análise das correntes: dos problemas, das soluções, e da política, com o propósito de identificar as peculiaridades do processo de tomada de decisões para a definição da agenda governamental do Chile. Com os resultados obtidos, observou-se que a Política de Cibersegurança é parte de uma institucionalidade digital do país de mais de 20 anos, emergindo na agenda governamental do Chile pela junção de três fatores fundamentais: a existência de déficits de segurança digital em relação ao país. O desenvolvimento de uma solução baseada na proposta de um comité interministerial assessorados pela comunidade de especialistas, validada através de um processo de consulta pública e um ambiente de alta receptividade política. Como também, o produto de uma mudança na administração do Governo, aspetos que incidiram na abertura de uma janela política para a tomada de decisão para iniciar os trabalhos voltados na formulação da futura política nacional.

Palavras-chave: Cibersegurança – Política pública – Modelo de análise dos múltiplos fluxos.

ABSTRACT

This dissertation presents an analysis based on the approach multiple streams framework (MSK) of the recent Chilean National Cybersecurity Policy published in 2017. The national policy establishes the political guidelines of the State to accompany technological evolution with the purpose of promoting and ensuring a free, open, safe, and resilient cyberspace. In this perspective of the study, was presented the evolution of Chile's digital institutional from 1999 to 2017, and subsequently, using Kingdon's multiple streams analysis model, it was identified the actors and specific actions generated in the process of defining the agenda setting for the policy between the years 2014 to 2017, using the analysis of MS: problems, politics, and policies (solutions), with the purpose of identifying the peculiarities of the decision-making process for setting the governmental agenda in Chile. With the results obtained, it was observed that the Cybersecurity Policy is part of a digital institutionality in the country for more than 20 years, emerging on the Chilean government agenda through the combination of three fundamental factors: the existence of deficits in digital security at the country level. The development of a solution based on the proposal of an inter-ministerial committee assisted by the expert community, validated through a public consultation process and an environment of high political receptivity. As well as the product of a change in the administration of the Government, aspects that focused on the opening of a political window for decision-making to start the work aimed at formulating the future national policy.

Keywords: Cybersecurity – Public policy – Multiple streams analysis model.

LISTA DE FIGURAS

FIGURA 1 – Diagrama adaptado do modelo Kingdon.....	29
FIGURA 2 – Evolução da institucionalidade digital do Chile	30
FIGURA 3 – Resultado da pesquisa lexical da institucionalidade digital do Chile	39
FIGURA 4 – Relação de objetivos, medidas e indicadores da PNCS.....	42
FIGURA 5 – Instituições intervenientes na questão da Cibersegurança nacional e seus papéis.	43
FIGURA 6 – Crescimento dos indicadores de vitimização social concernente aos delitos cibernéticos no triênio 2015-2017	47
FIGURA 7 – Evolução dos problemas prioritários para a opinião pública do Chile no quaternio 2014-2017	48
FIGURA 8 – Resultados da busca de termos sobre os assuntos de ataques cibernéticos em 2017	52
FIGURA 9 – Evolução da percepção cidadã em relação com governo, congresso e partidos políticos	65
FIGURA 10 – Evolução da percepção cidadã em relação ao Governo de Bachelet	66
FIGURA 11 – Evolução da aprovação cidadã em relação as principais coligações políticas representadas no país	66
FIGURA 12 – Distribuição de lugares no Congresso Nacional do Chile, período 2014-2018.....	69
FIGURA 13 – Sequências de acontecimentos que originaram a PNCS	71
FIGURA 14 – Diagrama da formação da agenda para PNCS 2017	79

LISTA DE QUADROS

QUADRO 1 – Variáveis de pesquisa	7
QUADRO 2 – Registro de notícias escolhidas sobre ataque cibernético de ransomware desde maio a julho de 2017	51

LISTA DE TABELAS

TABELA 1 – Material de pesquisa por capítulo.....	11
TABELA 2 – Sumários dos incidentes acontecidos no ciberespaço global que foram identificados como ciberataques	46
TABELA 3 – Registro de dotação orçamental do Ministério de Economia para projetos associados à Agenda digital.....	49
TABELA 4 – Participantes do Comitê Interministerial sobre Cibersegurança.....	57
TABELA 5 – Participantes da audiência pública para a elaboração da PNCS.....	59
TABELA 6 – Modificações inseridas no rascunho da PNCS após consulta pública	62
TABELA 7 – Diagnóstico da situação digital do país em 2015	72
TABELA 8 – Trabalho parlamentar sobre a CS no período 2014-2017	75
TABELA 9 – Resultados das intervenções sobre a CS na comissão defesa do Senado no período 2014-2017.....	76

LISTA DE ABREVIATURAS E SIGLAS

AD	Agenda digital
ANEPE	Academia nacional de Estudos políticos e Estratégias
BID	Banco Interamericano de Desenvolvimento
CCDCOE	Centro de Excelência de Ciberdefesa Cooperativa da OTAN
CEAD	Centro de Estudos e Análise do Crime
CEP	Centro de Estúdios Públicos Chile
CEPAL	Comissão Econômica para a América Latina e o Caribe
CICS	Comitê Interministerial de Cibersegurança
CMSI	Cúpula Mundial sobre a Sociedade da Informação
COMSEC	Secretaria da Commonwealth
CS	Cibersegurança
CTO	Organização de Telecomunicações da Commonwealth
ENCS	Estratégia Nacional de Cibersegurança
ENISA	Agência Europeia de Segurança de Redes e Informação
JID	Junta Interamericana De Defesa
MS	Multiple streams framework
NIC	Network Information Center Chile
OCDE	Organização de Cooperação e Desenvolvimento Econômico
OEA	Organização dos Estados Americanos
ONU	Organização das Nações Unidas
PDI	Polícia de investigações do Chile
PNCD	Política Nacional de Ciberdefesa
PNCS	Política Nacional Cibersegurança
RCE	Rede de conectividade do Estado
TIC	Tecnologias de informação e comunicação
UE	União Europeia
UIT	União internacional de Telecomunicações
UNESCO	Organização das Nações Unidas para Educação, Ciência e Cultura.

SUMÁRIO

INTRODUÇÃO	1
1 APRESENTAÇÃO DA PESQUISA	4
1.1 PROBLEMA DA PESQUISA	4
1.2 OBJETIVOS	6
1.3 HIPÓTESES OU SUPOSIÇÃO	6
1.4 METODOLOGIA DA PESQUISA	7
2 REFERENCIAL TEÓRICO	12
2.1 A CIBERSEGURANÇA E A QUESTÃO POLÍTICA	12
2.2 AS POLÍTICAS PÚBLICAS COMO ESPAÇO DE AÇÃO DO ESTADO E O PROCESSO DE DEFINIÇÃO DA AGENDA	20
2.3 A ANÁLISE DAS POLÍTICAS PÚBLICAS A PARTIR DO MODELO DOS MÚLTIPLOS FLUXOS DE KINGDON	24
3 A EVOLUÇÃO DAS POLÍTICAS DIGITAIS DO CHILE DE 1997 a 2015. TENDÊNCIAS E DESAFIOS DOS PRECURSORES DA INSTITUCIONALIDADE DIGITAL	30
4 A ANÁLISE DA POLÍTICA NACIONAL DE CIBERSEGURANÇA DO CHILE 2017	40
4.1 APRESENTAÇÃO DA PNCS	40
4.2 FORMAÇÃO DE AGENDA DA PNCS	44
4.2.1 O fluxo dos problemas (problems streams)	44
4.2.1.1 Os indicadores que precisaram da atenção governamental	45
4.2.1.2 Eventos focalizadores (Focusing events)	50
4.2.1.3 Retroalimentação (feedback)	53
4.2.2 O fluxo das soluções ou alternativas (policy stream)	56
4.2.3 O fluxo político (political stream)	63
4.3 JANELAS DE OPORTUNIDADE (POLICY WINDOWS)	71
4.4 EMPREENDEDORES DE POLÍTICAS (POLICY ENTREPRENEURS)	74
5 CONCLUSÕES E RECOMENDAÇÕES	80
REFERÊNCIAS BIBLIOGRÁFICAS	88
APÊNDICE A – QUADRO DE COMPARAÇÃO DAS AGENDAS DIGITAIS DO CHILE 1999-2015	95

APÊNDICE B – DECRETO PRESIDÊNCIA N.001, INSTRUI A IMPLEMENTAÇÃO DA POLÍTICA NACIONAL DE CIBERSEGURANÇA	101
---	------------

INTRODUÇÃO

Em 2015, o Chile lançou um documento de trabalho nomeado “Bases para política nacional de Cibersegurança”, texto matriz que definiu um roteiro para elaborar uma política pública de Cibersegurança de âmbito nacional, a fim de avançar em direção ao desenvolvimento da segurança digital do país por meio do levantamento de um diagnóstico da situação tecnológica, da construção de eixos fundamentais, e medidas concretas para a formação de uma equipe de trabalho para enfrentar o problema (CHILE, 2015c).

Desse modo, o Chile possui uma Política Nacional de Cibersegurança (PNCS) desde 2017 que contém as diretrizes políticas do Estado para acompanhar a evolução tecnológica a partir de uma perspectiva integral e sistêmica com foco na segurança do ciberespaço. Essa perspectiva aponta para que em 2022, cumpra-se com o objetivo de alcançar um ciberespaço livre, democrático, aberto, seguro e resiliente, que seja apropriado para salvaguardar a segurança das pessoas no ciberespaço, proteger a segurança do país, promover a colaboração e coordenação entre instituições e gerenciar os riscos do ciberespaço. (CHILE, 2017a)

A ideia de elaborar uma estratégia nasceu da necessidade de desenvolver um plano para modificar, com a maior urgência possível, o cenário de Cibersegurança do país, caracterizado pelos seguintes aspectos: ciberataques e atividades de espionagem nas diferentes redes, a interceptação massiva de redes de telecomunicações, desativação do serviço de Internet, surgimento de casos de espionagem contra governos e empresas, assim como, ataques contra infraestruturas críticas como serviços básicos, instituições financeiras, entidades governamentais, entre outros. (CHILE, 2017a)

Portanto, nas ponderações iniciais relativas a essa questão, o país ajuizou que “uma transformação desta magnitude não pode deixar de implicar em desafios importantes para o Estado, pois é imprescindível colocar este potencial tecnológico a serviço das pessoas e da convivência social” (CHILE, 2017a, p. 5, tradução nossa). No mesmo sentido, a PNCS evidencia uma acentuada preocupação do Estado chileno em aprofundar os relacionamentos baseados na cooperação e nas relações internacionais em torno da Cibersegurança no contexto global, através de

diferentes instâncias de comunicação, coordenação e colaboração, que fomentem a construção de confiança e a capacidade para fornecer uma resposta comum aos riscos e ameaças do ciberespaço.

Pelos motivos expostos, de acordo com a análise desenvolvida, a política de Cibersegurança não somente constitui-se numa política pública que cresce em estratégia multisetorial que abrange fatores de natureza doméstica e externa, como também políticos, sociais, econômicos e estratégicos setoriais, representando ainda, de forma concreta, o modo de ação do governo para alcançar seus objetivos em relação a um problema ou uma necessidade social que precisa de sua atenção.

Nesta perspectiva, é importante observar como as questões relevantes para a sociedade chilena, com a participação de diferentes atores e instituições, configuram um ambiente favorável para a formação da agenda política com o intuito de agir sobre a dinâmica das diversas interações que acontecem no ambiente virtual do ciberespaço.

Assim, gerar análises das políticas públicas que compreendam as origens e justificativas dos processos políticos em um contexto de recente evolução, constituem um desafio, pois, a partir deles surgirão a construção de possíveis explicações teóricas que fundamentem as escolhas políticas do Estado Chileno em contextos históricos diferentes, como as peculiaridades de seu funcionamento institucional e dos fatores que intervierem na composição de sua agenda política, trazendo consigo contribuições plausíveis para futuras análises nesse âmbito.

Consequentemente, a pesquisa apresentada, a partir do método de análise de fluxos múltiplos baseado no estudo de caso, avaliou diferentes fontes documentais, incluindo todas as políticas digitais concebidas e encaminhadas como resposta estatal no ciberespaço do ano de 1999 até 2017, os diferentes programas de governo dos presidentes de Chile (2010-2017), leis, decretos e regulamentações para uso do ciberespaço, mensagens presidenciais ao Congresso nacional (2014-2018), sondagens de opinião, entre outros, a fim de determinar os fatores que contribuíram para o processo de configuração da agenda governamental que permitiu a divulgação da política pública de Cibersegurança nacional em 2017.

Com a aplicação do modelo dos múltiplos fluxos de Kingdon (2003), que abrange o processo de tomada de decisão nas políticas públicas através da

representação da confluência de três correntes dinâmicas: a corrente dos problemas (problem stream); das soluções (policy stream) e da política (political stream) que permitem a abertura de janelas de oportunidades políticas. Conclui-se que a partir de 2010, o produto do exponencial aumento da massificação no uso das redes digitais em todos os âmbitos do Chile, começaram a incrementar, paulatinamente, potenciais riscos para segurança do país e da sociedade civil.

Observou-se, de acordo com os resultados obtidos, que esse problema necessitava da atenção governamental, pois era prioritário atenuar as brechas de segurança para manter os avanços do país no que diz respeito ao desenvolvimento digital, com o objetivo de recuperar os retrocessos na competitividade e posicionamento do país na América Latina em 2014.

Dessa forma, a nova administração do país assumida no ano de 2014, sob um contexto político favorável a seus postulados e fortalecendo sua posição por meio de uma manobra para conseguir amplos consensos com todos os setores da sociedade, concebeu prioridade ao cumprimento de suas ideias políticas, inseridas no programa de governo, o qual considerava o desenvolvimento de uma estratégia de segurança digital que passou a fazer parte da agenda governamental e logo, da decisória, transformando-se na PNCS.

A solução foi o resultado de uma proposta apresentada por parte de um comitê interministerial assistido pela comunidade de especialistas e acadêmicos, e validada através de um processo de consulta pública (CHILE, 2015c), permitindo o surgimento da PNCS durante a janela de oportunidade política, acrescida entre os anos de 2015 a 2017. Assim, a convergência das potenciais deficiências de segurança no âmbito digital que danificariam o alcance dos objetivos das diferentes políticas governamentais, somado a mudança no governo e início do segundo mandato presidencial de Bachelet, acondicionaram uma agenda governamental balizada em direção à segurança no ciberespaço como um novo campo de ação do Estado.

Finalmente, para fins de organizar o processo de cumprir com os objetivos previstos, esta dissertação estrutura-se no formato monográfico baseado em quatro capítulos, elaborados de acordo a metodologia apresentada e coerentes na estruturação com a finalidade proposta. Inicialmente, procura-se estabelecer uma abordagem teórica para a definição dos principais conceitos e funções que enquadram

a nossa pesquisa, em termos de limitar a relação da Cibersegurança e a função do Estado, as políticas públicas como espaço de ação do estado e o modelo dos Múltiplos fluxos que delimita a pesquisa.

Na sequência, analisa-se a institucionalidade digital para identificar suas mudanças e sua relação com os novos espaços para a ação do estado. Dessa forma, avalia-se o processo de fortalecimento da institucionalidade pública frente aos desafios estatais no ciberespaço e suas possíveis lacunas. Neste sentido, determina-se as concorrências e integrações entre as distintas políticas setoriais promovidas pelos diferentes Ministérios, a fim de estabelecer os mecanismos causais que alinham as decisões governamentais no âmbito do ciberespaço desde 1999.

Logo, procede-se a aplicação do método descrito no estudo de caso a partir da decomposição de cada uma das variáveis para realizar uma síntese das evidências obtidas com o fenômeno. Seu foco, além de definir as variáveis que são parte do modelo, será determinar sua evolução histórica e a reconstrução do ambiente onde se propiciou vislumbrar as contribuições dos diferentes órgãos durante a construção das soluções para a futura PNCS, com a finalidade de pesquisar sobre as causas para a sua incorporação na agenda governamental. Na parte final, apresenta-se as conclusões e recomendações a partir dos objetivos levantados.

1 APRESENTAÇÃO DA PESQUISA

1.1 PROBLEMA DE PESQUISA

A Política nacional de Cibersegurança do Chile cumpre um papel inédito no âmbito da segurança para o ciberespaço do país (BARRIOS, 2018). Por essa razão, apresenta-se como um campo ainda em desenvolvimento para a ação do Estado, na medida em que a política já enumerada e suas políticas subsidiárias, ainda se encontram em uma etapa de implementação (CHILE, 2017a).

Em vista disso, o caso de estudo proposto contribui a conhecer e ponderar o funcionamento institucional de um país a partir da dimensão política, de seu relacionamento direto com a conformação de agendas decisórias e com a formulação das políticas governamentais. Do mesmo modo, é interessante verificar empiricamente o desenho das políticas públicas que situaram as interações

funcionais entre os órgãos institucionais para a incorporação das inspirações e ideais que foram adotadas pelo Estado Chileno durante a década de 2010. Tais combinações permitiram assentar as bases da Cibersegurança como uma política pública e, portanto, a construção de políticas secundárias para diferentes setores da sociedade que refletirão sobre o futuro do país (CHILE, 2017a).

Desse ponto, de acordo a investigação bibliográfica realizada, evidencia-se uma falta de pesquisas que estabeleçam diferentes análises e estudos sobre a definição da agenda governamental para as políticas mais modernas do país, incluindo, a Cibersegurança (CS), não somente no que diz respeito aos processos de tomada de decisão das diferentes ações governamentais, bem como, aqueles que estão ligados à configuração das alternativas existentes, a participação de diferentes atores, a convergência de interesses e as condições presentes no contexto do cenário político nacional, razões que condicionam a agenda decisória do governo.

Além disso, este âmbito setorial da CS, a partir da perspectiva de uma análise da ação pública, é um campo escassamente desenvolvido em relação à quantidade de pesquisas por instituições acadêmicas, assim como a carência de desenhos de pesquisas que incorporem uma visão multifatorial de análise em relação as variáveis que compõe o fenômeno. Além disso, a referida política constitui o quadro normativo essencial para o avanço de outras políticas subordinadas no ambiente do ciberespaço e assim, sua formulação e implementação têm implicações diretas sobre as mesmas, assim como a construção de futuras políticas relativas à segurança, como a política de Ciberdefesa (CHILE, 2017a).

Por conseguinte, a referida análise do processo de definição da agenda governamental para a política do ciberespaço e seus efeitos, de acordo com a nossa pesquisa preliminar, não tem explicações satisfatórias, portanto, surgem possíveis interpretações para justificar sua decisão, dentro das quais é viável assumir que seria o resultado de um processo de definição da atenção governamental sob estímulos externos, devido ao maior grau de desenvolvimento tecnológico com efeitos sobre a sociedade, o resultado da convergência entre diferentes atores e interesses devido a uma crescente ameaça à segurança do país

dentro do sistema político ou como parte de uma crescente interdependência com outras políticas públicas como a política exterior e de segurança pública.

Surge, então, uma problemática inicial, sobre a identificação dos fatores que participaram do processo de definição da agenda governamental para o caso da PNCS, com a finalidade de justificar sua inclusão como uma política nacional no contexto político do período de 2014 a 2017. Conseqüentemente, determinou-se como questão fundamental para investigar:

Por que se incluiu na agenda governamental do Chile a criação de uma política pública de Cibersegurança nacional?

1.2 OBJETIVOS

Segundo Vergara (1998, p. 25) “o objetivo é um resultado a alcançar” e seu valor prático está, de acordo com Hernandez-Sampieri et al. (2014), em “estabelecer que se pretende com a pesquisa” para atingir ao objetivo final, se alcançado, dá resposta ao problema. (HERNÁNDEZ-SAMPIERI et al, 2014, p. 37). Neste sentido, determinou-se como objetivo da pesquisa: analisar os elementos intervenientes na definição da agenda e na formulação da Política nacional de Cibersegurança de Chile.

Posteriormente, de acordo com a sequencialidade e coerência com a delimitação da pesquisa foram esboçados os objetivos específicos: (1) Identificar o processo de evolução da institucionalidade digital do Chile; (2) Vislumbrar os fatores incidentes na conformação da agenda governamental para a PNCS a partir da abordagem do modelo de múltiplos fluxos de Kingdon; (3) Identificar os elementos que permitiram a abertura das janelas de oportunidade política para a futura PNCS.

1.3 HIPÓTESES OU SUPOSIÇÃO

De acordo com Hernandez-Sampieri (2014), as hipóteses originam-se da teoria existente e constituem os lineamentos para uma investigação. Sua função principal indica o que estamos tentando testar e são definidos como explicações provisórias do fenômeno investigado. (HERNÁNDEZ-SAMPIERI et al., 2014, p.

104). Em vista disso, e conjuntamente com os reflexos feitos, a partir das análises iniciais do fenômeno que orienta o processo analítico, devemos estabelecer a seguinte hipótese: “O maior nível de desenvolvimento tecnológico, produziu brechas na segurança digital do país provocando altos riscos de impactos sobre as pessoas, sociedade civil e segurança nacional, demandando a atenção governamental para a priorização de uma agenda decisória focada em incrementar a segurança no ciberespaço, o que originou a estruturação da política pública”.

Conseqüentemente, tem se definido as variáveis iniciais para a pesquisa, de acordo com o quadro metodológico proposto por Gil (2002) para o conceito de variável, refere-se a “tudo aquilo que pode assumir diferentes valores ou diferentes aspectos, segundo os casos particulares ou as circunstâncias” (GIL, 2002, p. 32). De tal modo, as variáveis serão:

QUADRO 1 – Variáveis de Pesquisa.

Variáveis	Tipo de variáveis
Segurança digital	Independente
Atenção governamental	Dependente

Fonte: Elaborado pelo autor.

1.4 METODOLOGIA DA PESQUISA

De acordo com os objetivos definidos pela pesquisa e sua coerência metodológica, e seguindo os argumentos de Yin (1994) se adotou o desenvolvimento de uma “pesquisa empírica com um projeto de pesquisa focado no processo de coletar, analisar e interpretar observações do fenômeno” (NACHMIAS e NACHMIAS, 1992, apud YIN, 1994, p. 41), norteado pela análise do modelo do Múltiplos fluxos de Kingdon para o processo de tomada de decisão para a criação de uma política de Cibersegurança durante o quadriênio 2014-2017; do mesmo modo que, a determinação dos aspectos que permitiram balizar avanços no desenvolvimento das políticas estatais para o ciberespaço e a sua construção da institucionalidade digital de acordo com o recorte temporal de 1999 a 2017.

A pesquisa apresentada desenvolveu um processo analítico que tentou obter evidências para a construção de inferências causais que proporcionassem uma solução que explicasse o fenômeno da definição da agenda governamental no

Chile para a questão do ciberespaço, baseado na contextualização dos diferentes métodos focados no analítico e explicativo para a produção de conhecimento científico, segundo recomenda Cunha e Araújo¹. Complementando, Hernandez-Sampieri (2014) argumenta que quando se manifesta esse processo lógico e indutivo orientado a explorar e descrever para gerar perspectivas teóricas, pode-se observar o desenvolvimento de uma pesquisa qualitativa em termos de seu “enfoque o aproximación cualitativa” (HERNÁNDEZ-SAMPIERI et al, 2014, p. 8).

Desse modo, devido as peculiaridades do estudo em discussão, focado na reconstrução de um processo decisório de uma política pública específica dentro de um contexto preciso, como o ambiente político nacional do Chile, utilizou-se uma abordagem de tipo “qualitativa” por estar mais alinhado com o propósito da pesquisa e que se fundamenta nas argumentações de Cunha e Araújo (2018):

Sobre a pesquisa qualitativa colabora no estudo da dinâmica interna do fenômeno e no contexto em que ocorrem, de modo a buscar uma compreensão mais acurada por meio do exame em profundidade de um caso específico. (RAGIN, 1994; GERRING, 2007; BYRNE, 2013 apud CUNHA e ARAÚJO, 2018, p. 14)

Conseqüentemente, o trabalho é encaminhado de acordo com o tipo de pergunta de pesquisa oferecida, que está estabelecida na compreensão e justificação de um fenômeno. Portanto, enquadra-se como uma “pesquisa explicativa” de acordo com a perspectiva de Gil (2002), cuja explicação sobre esse tipo de investigação tem como “preocupação central identificar os fatores que determinam ou que contribuem para a ocorrência dos fenômenos. Esse é o tipo de pesquisa que mais aprofunda o conhecimento da realidade, porque explica a razão, o porquê das coisas” (GIL, 2002, p. 42).

Na sequência, o estudo do contexto político do Chile e seu clima nacional (national mood) em nossa pesquisa constituiu um aspecto essencial para definir a ocorrência do fenômeno dentro de um ambiente, justificando-se seu estudo devido à dependência causa – efeito para o caso em análise. Deste modo, “apesar de um conjunto de condições iniciais comuns, um mesmo mecanismo gera diferentes

¹ “Ser analítico aponta para a decomposição de um todo em suas partes, cuja análise possibilita produzir uma síntese; ser explicativo atenta para a produção de explicações, inclusive aquelas sobre o que causa determinados fenômenos” (CUNHA e ARAÚJO, 2018, p. 10).

resultados, em razão da dependência do contexto, ainda que o mecanismo opere da mesma maneira” (FALETTI; LYNCH, 2009; KAY; BAKER, 2015 apud CUNHA e ARAÚJO, 2018, p. 46).

Desse modo, para cumprir com os objetivos deste trabalho e aprofundar o conhecimento da realidade institucional e sobretudo, a determinação dos fatores intervenientes na definição de agenda política do Chile no período em estudo, utilizou-se o quadro de análise do modelo dos múltiplos Fluxos de Kingdon², que direcionou a pesquisa para uma estratégia de Estudo de caso³, cujo objetivo principal consistiu em analisar os fatores intervenientes no desenho de uma política pública. Sendo assim, o modelo permitiu analisar a tomada de decisão da autoridade política baseado na observação de três fluxos de forças: o fluxo dos problemas, que incluiu as questões reconhecidas pelos diferentes atores dentro do ambiente político nacional e que influenciaram na definição da agenda do governo de Michelle Bachelet (2014-2018); o fluxo das soluções, propostas ou alternativas, que incluíram os possíveis condicionamentos políticos para a resolução da problemática identificada; e os fluxos políticos, esboçados pelos componentes que incidiram no clima político de nível nacional, como as forças políticas organizadas e as mudanças no governo derivadas pelos efeitos das políticas elaboradas.

Desta forma, a determinação da amostra abrangeu o segundo governo de Bachelet (2014-2018) em que se possibilitou, empiricamente, a definição de uma agenda governamental para a política pública. “A amostra pode ser uma única unidade de análise, como no estudo de um só caso” (MERTENS, 2010 apud HERNÁNDEZ-SAMPIERI et al., 2014, p. 386, tradução nossa). Sob outra perspectiva, a abordagem territorial está delimitada ao espaço geográfico do Chile, porém, durante as diferentes explanações foram analisados antecedentes de diferentes índoles que fizeram referência ao cenário regional, entendendo-se sua abrangência ao continente sul-americano, onde concentra-se a nossa análise e

² O modelo dos múltiplos fluxos de John W. Kingdon foi descrito em seu primeiro livro "Agendas, Alternatives and Public Policies" publicado em 1984. Essa abordagem possibilita compreender o ciclo político das políticas públicas para além de uma compreensão linear, abordando o dinamismo e a complexidade dos processos de tomada de decisão (OLAVARRÍA, 2013).

³ Segundo YIN (1994), é uma “maneira de se investigar um tópico empírico seguindo-se um conjunto de procedimentos pré-especificados” (YIN, 1994, p.35).

identifica-se algumas influências sobre a posição do país, em especial, dos atores internacionais e outros como empreendedores de políticas (policy entrepreneurs).

Em relação a coleta de dados, realizou-se através de uma pesquisa do tipo “documental” um recorte flexível a partir de 1999, quando surgiu o primeiro relatório elaborado pela Comissão Presidencial nomeado como "Novas tecnologias de informação e comunicação" (CHILE, 1999); e com ênfase no quadriênio 2014-2017 quando se produz o processo de definição da agenda para o ciberespaço (CHILE, 2017a). Segundo Gil (2002), “a pesquisa documental vale-se de materiais que não recebem ainda um tratamento analítico, ou que ainda podem ser reelaborados de acordo com os objetos da pesquisa”. (GIL, 2002, p. 45). Assim, apesar de estabelecer explicações em um período definido, os dados foram obtidos de outros segmentos de tempos, não declarados explicitamente neste início, devido às dificuldades metodológicas para se incluir uma definição temporal concisa de todos os dados a serem cumpridos com o propósito da pesquisa.

A nossa opção metodológica pela análise documental justificou-se como estratégia para obter uma posição mais clara e objetiva para identificar as posições de governo, autoridades, instituições e diferentes atores sobre os assuntos estudados neste trabalho. No entanto, não se fizeram entrevistas por questões de caráter administrativo para executar os requerimentos às autoridades de nível político, devido às situações provenientes do Estado de Exceção Constitucional de Emergência no Chile.

Em seguida, como método complementar, empregou-se a triangulação de fontes, segundo o apresentado por Yin (1994), cujo resultado se orienta para melhorar o recolhimento de evidências por meio de fontes mais diversificadas, abrangentes e acessíveis de diferentes origens como: documentos oficiais, registros de arquivos, declarações, discursos, sondagens de opinião, e relatórios técnicos disponíveis nos web sites de Governo do Chile, Congresso Nacional, Ministérios da Defesa, e Interior e Segurança Pública.

TABELA 1 – Material de pesquisa por capítulo.

Tipo de dado	Capítulo	Origem / tipo de dado
Documental	03	<ul style="list-style-type: none"> – Agenda Digital, Chile: Hacia la sociedad de la información, 1999. – Agenda Digital 2004-2006: “Te acerca al futuro” <ul style="list-style-type: none"> – “Estratégia digital 2007-2012” – Agenda Digital 2013-2020 “Imagina Chile,” – Agenda Digital 2020, “Chile digital para tod@s”
	04	<ul style="list-style-type: none"> – Fundo documental da administração 2014 - 2018 – Bases para uma Política Nacional de Cibersegurança 2015. <ul style="list-style-type: none"> – Estratégia Nacional de Cibersegurança 2017. – Programa de Governo 2014-2018 “Chile de todos”. – Programa de Governo 2018-2022 “Construamos melhores tempos para Chile”. <ul style="list-style-type: none"> – Leis de Orçamento do setor público 2014-2017 – Mensagem presidencial 2014-2018 (Secretaria geral da presidência) <ul style="list-style-type: none"> – Decreto 533/2015: Cria Comitê Interministerial Cibersegurança – Regulamentos para o funcionamento do Comitê Interministerial de Cibersegurança <ul style="list-style-type: none"> – Decretos de Cibersegurança

Fonte: Elaborado pelo autor.

De acordo com Yin (1994), utilizou-se para análise dos dados uma estratégia geral baseada em “proposições teóricas”⁴, devido ao uso do modelo dos múltiplos fluxos como uma referência teórica que balizou o estudo de caso em termos de seu desenho, prioridades, estratégias e questões da pesquisa. Por isso, como técnica de análise específica, escolheu-se o tipo de “adequação ao padrão” que, segundo o autor, é uma das estratégias mais desejáveis para utilizar, já que essa “lógica compara um padrão fundamentalmente empírico com outro de base prognóstica ou com várias outras previsões alternativas” (TROCHIM, 1989 apud YIN, 1994, p. 136). Logo, empregou-se como métodos complementares: primeiro, a construção da explanação para analisar os dados coletados, do mesmo modo, levantar uma interpretação satisfatória sobre os fatores intervenientes e determinantes no processo de tomada de decisões governamentais (Yin, 1994); segundo, a análise de conteúdo aplicado para a linguística (discursos de autoridades) e ao análise documental para os textos

⁴ De acordo com o autor, as proposições dariam forma ao plano da coleta de dados e, por conseguinte, estabeleceriam a prioridade às estratégias analíticas relevantes (YIN, 1994).

oficiais (BARDIN, 1977); e terceiro, a codificação de textos com apoio do software MAXQDA.

Contudo, devido às limitações metodológicas derivadas na utilização do método de caso, assim como, para remediar a falta de entrevistas que fortaleçam o esquema de rigorosidade metodológica, procurou-se incrementar a busca de declarações públicas, sondagem de opinião, discursos pragmáticos e alocações na mídia e na imprensa de diferentes autoridades governamentais ou outros atores intervenientes como empreendedores de políticas (policy entrepreneurs) e participantes dentro do processo político ponderado.

2 REFERENCIAL TEÓRICO

A definição de um quadro teórico - referencial da pesquisa em função da natureza do problema de investigação, propõe um plano mínimo para a compreensão do fenômeno analisado para enquadrar as relações que surgem entre as variáveis associadas à pesquisa. Neste sentido, de acordo com HERNÁNDEZ SAMPIERI et al. (2010) serão apresentadas as conceitualizações iniciais para a construção de uma perspectiva teórica que nos forneça de uma visão sobre o lugar onde se situa a abordagem proposta dentro do campo de conhecimento em que será desenvolvida, bem como a importância dos conceitos na construção de teorias (BOWDISH, 2013) que consolidem a identificação dos conceitos básicos como unidades de pensamento (SARTORI, 2009).

2.1 A CIBERSEGURANÇA E A QUESTÃO POLÍTICA

Segundo Caro (2010) e outros, o conceito do ciberespaço vem do termo “ciber”, que evoluiu a partir da obra de Norbert Wiener, que definiu o termo cibernética em seu livro «Controle e comunicação no animal e na máquina». A ideia de que os humanos podem interagir com as máquinas e que o sistema resultante fornece um ambiente alternativo para a interação entre elas, cria a base para o conceito de ciberespaço. (CARO, 2010). Segundo Todd (2009) acrescenta a essa perspectiva ao argumentar que “a informação é o elemento central para a existência do Ciberespaço” (TODD, 2009, p. 64, tradução nossa).

Nesse sentido, o acelerado desenvolvimento das tecnologias que empregam o ciberespaço, segundo Gonzalez (2010) tem facilitado abundantemente a promoção de todos os tipos de atividades, incluindo interações comerciais, sociais e governamentais, constituindo uma dimensão importante para os Estados, organizações e indivíduos e, conseqüentemente, a segurança do ciberespaço tem crescido significativamente diante das ameaças.

Por outro lado, Acosta (2009) argumenta:

Como a sociedade atual depende amplamente da tecnologia da informação (TI), isso leva ao surgimento de novas ameaças desconhecidas no passado. Devido à natureza global das redes, os incidentes de segurança de TICs que as afetam podem causar interrupções permanentes ou falhas na infraestrutura de informação do país. (ACOSTA, 2009, p.33, tradução nossa).

Então, neste campo de desenvolvimento tecnológico e de surgimento de novas ameaças, o ciberespaço foi declarado pelo “The Economist” (THE ECONOMIST REVIEW, 2010); Cornish (2011) citado por Castrillón-Riascos (2015); a Junta Interamericana de Defesa (JID) (2020); Arreola (2020) como o “quinto domínio”⁵ depois da terra, do mar, do ar e do espaço. Pois, durante a primeira década do século XXI, apareceram novos paradigmas de ataque pelo ciberespaço, que se baseavam em diferentes modos de agressões e variadas motivações, tanto individuais como coletivas, igualmente como tipos de alvos que tentaram afetar instituições, governos e várias corporações empresariais.

Neste contexto, em 2013, dentro dos aspectos mais relevantes, havia empiricamente um número crescente de ameaças cibernéticas, que se concentraram na infraestrutura de informação civil. Em âmbito regional, os países que registaram o maior número de ataques cibernéticos na América Latina foram: Brasil, Argentina, Colômbia, México e Chile (PRANDINI, 2013). Além disso, o acesso ou roubo de informações de um computador infectado, chamado de botnets, predominou na região. Até mesmo um tipo específico deste código malicioso chamado dorkbot gerou mais de 80 mil ações contra o sistema virtual, concentrando-se no Chile (44%), Peru

⁵ Para que um determinado ambiente seja considerado um domínio de operações, ele deve atender a seis critérios: 1. Requer recursos exclusivos para operar nessa área; 2. Não é totalmente englobado por qualquer outra área (terrestre, marítima, aérea, espacial). 3. É caracterizada por uma presença compartilhada de capacidades aliadas e adversárias. 4. É capaz de exercer controle sobre um oponente por meio de influência e domínio. 5. Oferece oportunidades de sinergia com outras áreas. 6. Oferece oportunidades assimétricas em todas as áreas (JID, 2020).

(15%) e Argentina (11%) (BID, 2016). Desde 2017, pode-se notar um crescente número de ciberataques aos órgãos governamentais. Em 2019, os governos foram o terceiro maior alvo de ciberataques no mundo (FIREEYE, 2020).

Como resultado desse incremento exponencial das ameaças cibernéticas, o relatório de Defesa digital do Microsoft em 2020 forneceu uma análise mais profunda de algumas das atividades observadas nos estados-nação, com ênfase na frequência dos setores-alvo e as motivações dos atacantes. Neste sentido, dentro dos setores de alvos de ataques de hackers pode-se observar que 32% correspondem a organizações não - governamentais; 13% organizações governamentais; 7% empresas de desenvolvimento tecnológico; 7% Instituições educacionais; 31% serviços profissionais e 10% em organizações internacionais. (MICROSOFT CORPORATION, 2020)

Desta forma, segundo Feliu (2013), uma ameaça tem sido descrita como: “a percepção da capacidade de um potencial adversário possui para infligir dano ou detrimento, especialmente se não se atua como ele deseja” (FELIU, 2013, p.40, tradução nossa). Por sua vez, Gonzalez (2010) argumenta que o conceito de ameaças cibernéticas será constituído por ataques perpetrados ou patrocinados por Estados (ataques a infraestruturas críticas), ataques cometidos por grupos terroristas ou por qualquer outra manifestação de extremismo, seja político, ideológico ou religioso.

Neste cenário, surgem também, os ataques de crime organizado denominados “Cibercrimes⁶” e, enfim, os “ataques discretos”, que pela sua natureza muito heterogênea, atingem as pessoas de forma transversal, por meio da usurpação de informação pessoal até fraudes de diferentes ordens (GONZALEZ, 2010, p. 93, tradução nossa). Esse escopo está inserido nas Tendências Estratégicas Globais do Ministério da Defesa da Grã-Bretanha para o ano de 2050, onde se aprecia uma visão estratégica de maior abrangência, ao se estabelecer: “There could also be an increasing threat of cyber-attack from criminals and terrorists as information, communications and critical national infrastructure become more integrated” (UNITED KINGDOM, 2018).

⁶ Os cibercrimes são atos ilícitos em que o ciberespaço é o meio para o crime ou sua principal ferramenta para a prática de ações contra indivíduos, organizações, empresas ou governos. (CHILE, 2015c).

Por conseguinte, segundo Castrillón-Riascos (2015), o advento dessa revolução tecnológica, com o aumento das conexões no ciberespaço e, o surgimento dessas ameaças teve uma consequência comum a todos os Estados. De uma forma ou de outra, em grau maior ou menor, todos estão envolvidos em uma “Ciberguerra”, seja por ações de outros Estados-Nação ou de criminosos comuns; as pessoas e governos encontram cada vez mais riscos à sua segurança digital (CASTRILLÓN-RIASCOS, 2015). Desse modo, Clarke, R. e R. Knake (2011) integra na sua argumentação que o “Cyberspace is now a warzone where many of the decisive battles of the 21st century will be fought” (CLARKE e KNAKE, 2011, p. 192), por conseguinte, sugere uma visualização de ações coativas dos mais diversos tipos com uma participação dos Estados por assegurar seus objetivos neste ambiente. Assim, Choucri (2012) ratifica que as diferentes interações no ciberespaço para os Estados têm criado condições sem claras prescrições sobre as ações relacionadas com a soberania dos Estados, estabilidade e segurança.

Segundo Reardon e Chocri (2012), é razoável esperar que o desenvolvimento do ciberespaço, devido à sua crescente relevância para um número cada vez maior de atividades sociais e políticas, comece a exercer influência no curso da política global. Da mesma maneira, as significativas mudanças no ciberespaço apresentam um “efeito transformador na política internacional, particularmente com respeito ao empoderamento de grupos anteriormente marginalizados; e a relação dependente entre política internacional e mudança tecnológica” (MANJIKIAN, 2010 apud REARDON e CHOUCRI, 2012, p. 26, tradução nossa).

Nesta conjuntura, Choucri (2012) argumenta que surgem novos desafios para a Segurança Nacional, de fontes de vulnerabilidade sem precedentes, novas dimensões de segurança nacional combinadas com incerteza, medo e ameaças de fontes desconhecidas. Ainda assim, a criação de ciberespaço propõe possibilidades para o desenvolvimento de políticas para as novos interesses e desafios. Neste âmbito, segundo Caro (2010), emerge uma relação entre o ciberespaço e a segurança nacional, já que a “Cibersegurança é um objetivo estratégico para a segurança nacional” (CARO, 2010, p. 76, tradução nossa). Da mesma forma, Reardon e Chocri (2012), ressaltam que: “Ataques estratégicos em grande escala através do ciberespaço contra a ‘infraestrutura crítica’ representam

uma grave ameaça à segurança nacional” (CLARKE, 2009; LYNN, 2010; WESLEY K. AND LEVIN, 2010 apud REARDON e CHOUCRI, 2012, p. 22, tradução nossa).

Sendo assim, segundo Newmeyer (2015), o paradigma exibido faz parte de uma das três correntes comumente apresentadas que analisam o fenômeno da Cibersegurança, tendo sua origem em teorias de segurança nacional, existindo outras, ainda, que provém das teorias econômicas ou teorias de saúde pública. Essa perspectiva da segurança “determina a estrutura conceitual da estratégia, o foco das relações do setor público-privado e os meios usados para monitorar a implementação” (MULLIGAN e SCHNEIDER, 2012 apud NEWMAYER, 2015, p. 10, tradução nossa).

Sendo assim, “a Cibersegurança é agora uma questão de segurança nacional que pode impactar nas vidas dos cidadãos todos os dias” (KLIMBERG, 2012 apud NEWMAYER, 2015, p. 10, tradução nossa). Segundo Barmpaliou (2020), a Cibersegurança se constitui em “Un asunto transversal en la política nacional”, (BID, 2020, p. 28) devido a presença dos sistemas digitais em todas as áreas de atividade humana, evidenciando níveis sem precedentes de inovação tecnológica e interdependência.

De acordo com Newmeyer (2015), vários países industrializados, como Estados Unidos, Reino Unido, Austrália, Nova Zelândia e outros da União Europeia (UE) têm desenvolvido e publicado estratégias nacionais de Cibersegurança nos últimos anos para responder as ameaças cibernéticas através de diferentes focos, motivações e questões concretizadas em políticas de governo.

Newmeyer (2015) argumenta ainda que o objetivo de uma estratégia nacional de Cibersegurança é alinhar todos os esforços do governo para alcançar ou melhorar a Cibersegurança (NEWMAYER, 2015, p. 11, tradução nossa). Assim, as estratégias eficazes definem os “parâmetros para a cooperação do setor público-privado e coordenação dos esforços de Cibersegurança, bem como o fornecimento de uma indicação clara das intenções do país para outros países e partes interessadas” (LUIIJF et al., 2013 apud NEWMAYER, 2015, p.12). Porém, “A alocação de responsabilidades de Cibersegurança varia entre os governos” (NEWMAYER, 2015, p. 13, tradução nossa). Conseqüentemente, Newmeyer (2015) expressa que o elemento essencial é a elaboração e implementação das estratégias nacionais com “altos níveis de eficácia de Cibersegurança para

aumentar as chances de sucesso nos objetivos que contenha” (NEWMAYER, 2015, p. 18).

Por sua vez, Reardon e Chocri (2012), caracterizam a Cibersegurança a partir de sua evolução: “Um termo que foi originalmente reservado para a integridade técnica de redes, tornou-se uma questão de segurança nacional e alta política” (REARDON e CHOUCRI, 2012, p. 24 apud HANSEN e NISSENBAUM, 2009, tradução nossa). Contudo, Newmeyer (2015), além de reforçar esse paradigma, justifica a ênfase na segurança nacional inserida na estratégia e doutrina da Cibersegurança, devido à necessidade de “proteger a infraestrutura crítica e à importância dos sistemas públicos e privados nas operações do governo” (AGRESTI, 2010, apud NEWMAYER, 2015, p. 10, tradução nossa).

Fundamentado nisso, nascem diferentes abordagens que misturam a segurança nacional com a proteção de infraestrutura crítica nacional sob uma estratégia de governança integrada em Cibersegurança (KRAMER, 2011; AGRESTI, 2010; VACCA, 2011 apud NEWMAYER, 2015), que poderia ser entendida devido a uma “falta de definições cibernéticas comuns e harmonizadas entre as nações” (LUIIJF, 2013, p. 5, tradução nossa).

Levando isso em conta, como parte de um esforço para orientar as nações para o desenvolvimento de um entendimento da Cibersegurança, a União internacional de telecomunicações (UIT) dependente da Organização das Nações Unidas (ONU) em 2010 apresenta a Cibersegurança como uma série de ferramentas para proteger os ativos e usuários de organizações no ambiente cibernético desde os Estados até às pessoas.

A Cibersegurança é o conjunto de ferramentas, políticas, conceitos de segurança, salvaguardas de segurança, diretrizes, métodos de gestão de risco, ações, treinamento, melhores práticas, seguros e tecnologias que podem ser usadas para proteger ativos da organização e usuários no ambiente cibernético. Ativos e usuários da organização são dispositivos de computação conectados, usuários, serviços / aplicativos, sistemas de comunicação, comunicações multimídia e todos das informações transmitidas e / ou armazenadas no ambiente cibernético. (UIT, 2010, tradução nossa).

Por sua vez, a Agência de Cibersegurança e Infraestrutura dos EUA define a Cibersegurança como: “a arte de proteger redes, dispositivos e dados contra acesso não autorizado ou uso criminoso e a prática de garantir a confidencialidade,

integridade e disponibilidade de informações” (SECURITY, s.d., tradução nossa). Igualmente, segundo a JID (2020), “A Cibersegurança se concentra na proteção e recuperação dos próprios sistemas de Tecnologias de informação e comunicação (TICs)” (JID, 2020, p. 41, tradução nossa).

No que lhe concerne, o Chile definiu seu conceito de Cibersegurança na PNCS:

A Cibersegurança é uma condição caracterizada por um mínimo de riscos para o ciberespaço, entendida como o conjunto de infraestruturas físicas, lógicas e interações humanas que acontecem nesse lugar. Neste sentido, e seguindo os padrões internacionais, os principais atributos para proteger são a: confidencialidade, integridade e disponibilidade das informações, o que por sua vez geram um ciberespaço robusto e resiliente (CHILE, 2017a, p.16, tradução nossa).

Assim, indistintamente do tipo de abordagem analisada, surge como um aspecto complementar, a incorporação da concepção da Cibersegurança de acordo com os preceitos gerais dos Estados, como um fator que promove a cooperação e a integração do conhecimento como uma forma de mitigar ameaças (JID, 2020) e através de “arranjos cooperativos em segurança contribuir para os objetivos de segurança e estratégicos dos Estados” (MUTHANNA, 2006 apud PEREIRA REZENDE, 2015, p. 527).

Com tal característica, a JID (2020) expõe que a Cibersegurança internacional se baseia fundamentalmente na cooperação entre os órgãos responsáveis por cada um dos pilares da Cibersegurança nacional, com seus homólogos em outros países e organizações internacionais através de diferentes convenções (JID, 2020, p. 87). Deste modo, os governos podem responder eficientemente aos problemas gerados pela “interdependência complexa” e, nesse sentido, produzir bens públicos globais ou regionais (MILANI, 2020, p. 82) que podem ter escopo nos assuntos que dizem respeito à Cibersegurança.

Devido a isso, segundo Herczynski (2020), a publicação do Reporte de Cibersegurança do BID (2020), expõe que a natureza global da ameaça e os desafios que representa para os Estados, no contexto da “Diplomacia cibernética”, fomentará a construção e desenvolvimento de alianças fortes e parcerias com outros países para a prevenção e dissuasão de ataques cibernéticos, que são cada vez mais importantes para a estabilidade e segurança internacional. Frente ao

incremento das ameaças e seus potenciais efeitos no ciberespaço de entorno global, regional e local surge como um bem público a segurança coletiva em termos de proteger as interações e direitos no ciberespaço onde convivem os Estados e os indivíduos.

Deste modo, segundo o autor, nasce como um assunto indispensável para os Estados a obrigação de cooperar para conseguir uma estabilidade cibernética global baseada no desenvolvimento de capacidades regionais e nacionais de todos os países para prevenir e reagir diante dos incidentes cibernéticos. Neste sentido, segundo Choucri (2012), a escolha política de cooperar justifica-se:

In general, countries collaborate either (1) in the pursuit of common interests or (2) in the management of common aversions. In the first instance, states seek to collaborate as a way to pursue jointly some objective they might not be able to attain individually. In the second, collaboration is driven by the recognition that states face shared adverse conditions that require coordinated action for the most effective management. (CHOUCRI, 2012, p.156)

Newmeyer (2015) reforça a importância de contar com quadros legais para detectar e prevenir ilegalidades que acontecem no ciberespaço, aspecto que contribui para a cooperação internacional e a diminuição de crimes associados neste ambiente. No entanto, no âmbito de nossa região, o reporte de Cibersegurança 2020 do BID colocou em evidência que na Região da América Latina e do Caribe ainda não está suficientemente preparada para confrontar os ataques que são produzidos no ciberespaço. Apenas sete países dos trinta e dos analisados no reporte possuem um plano de proteção de sua infraestrutura crítica e só vinte tem implementado algum tipo de equipe de resposta a incidentes, então a situação limita a capacidade para identificar ataques e respondê-los oportunamente.

Em razão disso, dentro desta publicação já nomeada, a Chefe de Políticas e iniciativas públicas do Fórum Econômico Mundial Nayia Barmpaliou faz um destaque da importância das organizações regionais na promoção da estabilidade regional, na segurança e nos esforços para construir confiança no ciberespaço, através de medidas de criação de segurança, ratificando-se a importância da contribuição interestatal com foco na cooperação internacional no âmbito do ciberespaço (BID, 2020).

Neste novo cenário, segundo Paz y Paz (2016), a Organização dos Estados Americanos (OEA), em seu caráter de foro político hemisférico, por meio da Secretaria de Segurança Multidimensional, promove e coordena a cooperação entre os Estados membros da organização para avaliar, prevenir, enfrentar e responder efetivamente sobre as novas ameaças à Cibersegurança. De tal modo, durante 2017 os governos de Chile e Paraguai adotaram os respectivos Planos de Cibersegurança. Ambos se uniram a países como Colômbia, Trinidad e Tobago, Panamá e Jamaica que de acordo com a OEA tem fornecido apoio técnico do “Programa de Cibersegurança do Comité Interamericano Contra o terrorismo da OEA” (OEA, 2017).

Finalmente, segundo a BID (2020) a Cibersegurança não pode ser analisada por meio de uma perspectiva isolada, como um assunto técnico ou uma área de política independente, pois, a Cibersegurança se localiza na intersecção de múltiplas disciplinas e áreas políticas: acesso digital e conectividade, resiliência, justiça criminal, diplomacia, segurança e defesa internacional, economia e comércio digital, como novas tecnologias e, portanto, deve ser abordada através de uma perspectiva ampla.

2.2 AS POLÍTICAS PÚBLICAS COMO ESPAÇO DE AÇÃO DO ESTADO E O PROCESSO DE DEFINIÇÃO DA AGENDA

O desenvolvimento e análise das diferentes políticas públicas é um elemento chave em uma sociedade civil. De acordo com Sabatier (2007), existem variadas definições sobre o escopo da política pública por efeito das diferentes abordagens sobre o assunto e a forma como se concebe nos diferentes processos de definição da agenda e na implementação de políticas públicas. Em conformidade com Lotta (2019), os estudos sobre a implementação de políticas públicas são, geralmente, analisados como um ciclo que decorre nas diferentes fases: agenda, formulação, implementação e avaliação, e cujo valor radica no entendimento dos processos decisórios que os compõem.

Em vista disso, a primeira fase da agenda, segundo Souza (2003); Capella (2006); Lotta (2019); estabelece as questões que são prioritárias, portanto, são temas que recebem a atenção governamental de maneira preferencial sobre outros assuntos

públicos. Na sequência, durante a segunda fase de formulação, segundo Lotta (2019), as políticas serão planejadas e decididas de acordo com uma metodologia que relaciona modelos e objetivos. Durante a terceira fase de implementação, as ideias se transformam em ações concretas. Segundo o autor, é o “momento que depende fortemente da ação de burocratas e dos instrumentos de ação estatal” (LOTTA, 2019, p.13). Na última fase da avaliação, serão mensuradas as diferentes políticas públicas: respeito na eficiência, eficácia, efetividade, etc.

Assim sendo, existem diferentes abordagens para fazer análises sob as quais baseia-se uma investigação. Neste sentido, tem destaque a abordagem de Meny e Thoenig (1992), considerada como uma bibliografia clássica, pois fornece uma primeira abordagem para a análise de políticas e seus fundamentos conceituais, em ordem de embasar o estudo das políticas públicas sob as ações das autoridades públicas no contexto da função do Estado. Para mais, selecionou-se duas bibliografias que se encontram alinhadas ao objetivo da pesquisa, que segundo Durán (2017), estão “vocacionadas à identificação de problemas e definição da agenda como Kingdon, 1984, e Cobb e Elder 1972” (DURÁN, 2017, p.5), e também de outras fontes secundárias.

Segundo Meny e Thoenig (1992), o conceito de políticas públicas evoluciona no campo das ciências políticas e administrativas dos Estados Unidos para a solução de problemas dentro de “uma dinâmica democrática e vinculada às etapas do processo decisório” (LAHERA, 2002 apud DOÑA, 2005, p. 34, tradução nossa).

Conforme Doña (2005), o estudo das políticas públicas não seria outra coisa que o estudo da ação das autoridades nas atividades da sociedade, ou seja, “um estudo do que os governantes produzem em relação aos resultados que eles esperam e pelos meios que possuem” (MENY e THOENING, CLAUDE, 1992 apud DOÑA, 2005, p. 32, tradução nossa)

Assim, de acordo com esta pesquisa, as políticas públicas serão entendidas sob a perspectiva de Lahera (2004): “são cursos de ação e fluxos de informação relacionados a um objetivo público definido democraticamente; aquelas que são desenvolvidas pelo setor público e, frequentemente, com a participação da comunidade e do setor privado” (LAHERA, 2004, p. 8, tradução nossa).

Desta forma, “as políticas são desenhos para ação pública” (LAFUENTE & ROJAS, 2010, p. 4, tradução nossa) bem como, “aquelas que correspondem a

soluções específicas de como gerir assuntos públicos” (LAHERA, 2004, p. 7, tradução nossa), cujo âmbito estimula às autoridades e aos atores da sociedade a participarem ativamente sobre sua abrangência e modernização através da gestão pública, o que tem produzido “mudanças nos modos de gerir o Estado” (OLAVARRÍA, NAVARRETE, & FIGUEROA, 2011, p. 110, tradução nossa).

Nessa perspectiva, Meny e Thoening (1992) distinguem quais são os problemas que originam a intervenção pública: um diz respeito à fase de definição de um problema, a formulação das demandas; o outro refere-se às estratégias de resposta implantadas de acordo com as demandas. Por outro lado, Elder, Cobb, & J. (1993) estabelecem que a definição de um problema se dá em um contexto de limites de plausibilidade por restrições ideológicas, restrições de recursos e sua definição inicial de um problema. Na maioria dos casos, não permanece estável, nem invariável, devido a sua transcendência no contexto político. Ademais, “Um problema será levado a sério em consideração apenas se os custos previstos de sua solução forem realistas e aceitáveis, no contexto dos recursos públicos previsíveis e atualmente acessíveis (ELDER, COBB, & J., 1993, p.94, tradução nossa).

Assim, Meny e Thoening (1992) expressam certas condições necessárias e suficientes para que um assunto ou problema esteja incluído na agenda do governo, dentro dos principais, deve ser da responsabilidade das autoridades públicas em geral, ou de uma determinada autoridade pública; que seja percebido como um assunto de percepções problemáticas, que o definam como merecedor de “atenção pública”; e que o problema possa constituir-se acessível em termos de ação pública. Além disso, Elder et al (1993) adiciona que “da mesma forma que os problemas insolúveis são descartados, o surgimento de novas soluções torna possível criar novos problemas” (ELDER, COBB, & J., 1993, p.95, tradução nossa).

Conseqüentemente, segundo Meny e Thoening (1992), o que leva as autoridades públicas a agirem é a “agenda”, que pode ser definida como “o conjunto de problemas que apelam a um debate público, incluindo a intervenção (ativa) de autoridades públicas legítimas... são institucionais, sistêmicos ou conjunturais” (PADIOLEAU, 1982, apud MENY e THOENING, 1992, p. 114, tradução nossa). Também para o Kingdon (2003), a agenda é:

The agenda, as I conceive of it, is the list of subjects or problems to which governmental officials, and people outside of government closely associated

with those officials, are paying some serious attention at any given time.
(KINGDON, 2013, p. 3)

Segundo Doña (2005), a definição de uma agenda é importante devido ao “grau de consenso ou conflito que gera, porque este seria o elemento que indicaria a oportunidade da autoridade intervir e como deve fazê-lo” (DOÑA, 2005, p. 34). Logo, Elder, Cobb, & J. (1993) argumenta que “o processo de preparação da agenda é o momento em que o governo decide se decidirá ou não sobre determinado assunto, no qual delibera e decide intervir ou decide não intervir, adiar a sua intervenção” (ELDER, COBB, & J., 1993, p.27-28, tradução nossa).

Desse modo, Capella (2018), em relação a definição da agenda, enfatiza os aportes feitos por John Kingdon (2003), quando avançou na diferenciação entre o conceito de agenda governamental e a noção de agenda decisória. Segundo o autor, baseado no trabalho de Kingdon (2003), a agenda governamental diz respeito aos assuntos que concentram a atenção de governo num determinado momento. Já a agenda decisória se fundamenta nas questões inseridas dentro da agenda governamental que estão prontas para a tomada de decisão pelos formuladores das políticas.

Sobre isso, Meny e Thoening (1992) argumentam no contexto das decisões, que uma autoridade pública tem uma multiplicidade de respostas para uma demanda incluída na agenda, que varia desde aceitar a demanda com ações diretas até a inação. Logo, o autor expressa que “Agir é tomar decisões” (MENY e THOENING, 1992, p. 129, tradução nossa). Segundo Doña (2005):

A autoridade atua quando toma uma decisão e, portanto, ocupa um lugar importante no processo de formulação de políticas públicas. A decisão resolve um problema, selecionando alternativas, marcando uma descontinuidade no tempo, antes e depois da adoção da decisão (DOÑA, 2005, p. 34, tradução nossa).

Meny e Thoening (1992) complementam que o processo de tomada de decisões nas políticas públicas é composto de duas fases principais: a fase de formulação e de legitimação. A primeira corresponde ao trabalho pelo qual uma questão pública está inscrita na agenda do governo ou se transforma em alternativas para a ação (soluções). A fase de legitimação se desenvolve quando o responsável formal, o indivíduo ou grupo, ao qual institucionalmente corresponde ao direito e o

dever de resolver. Neste sentido, refere-se a um ato de poder discricionário por parte das autoridades investidas de capacidade de decisão, que segundo o autor: “tem seu valor agregado, o que é política e simbolicamente decisivo: pelo seu voto, pela sua assinatura, você legitima a opção e a torna oficial, autorizada e irreversível” (MENY e THOENING, 1992, p. 138, tradução nossa).

Do mesmo modo, Meny e Thoening (1992) expõem que o tomador de decisão é o precursor para a elaboração das políticas públicas, pois é ele quem assina e resolve em última instância, mas na prática depende das soluções concretas que nascem de outros especialistas. Segundo Aguilar (1993):

Quem define é quem decide "é uma máxima que ele ressalte o fato de que os grupos sociais e / ou governamentais que tiverem a capacidade de oferecer a abordagem e definição da parte aceitável da questão são aqueles que efetivamente influenciam a decisão" (ELDER, et al, 1993, p.52, tradução nossa).

Finalmente, Meny e Thoening (1992) enunciam a existência de grupos de terceiros que fornecem essas soluções, elaboram as opções e garantem a sua legitimidade operacional. Em síntese, as medidas adotadas não seriam respostas obrigatórias às demandas da sociedade e de seus representantes políticos, mas do produto de atividades feitas por intermediários.

2.3 A ANÁLISE DAS POLÍTICAS PÚBLICAS A PARTIR DO MODELO DOS MÚLTIPLOS FLUXOS DE KINGDON

De acordo com o objetivo da pesquisa, é importante aprofundar as abordagens teóricas sobre como conceber as políticas públicas dentro de um sistema político. Segundo Dye (2009), os modelos que servem para estudar as políticas públicas são modelos conceituais que estão focados em outros tópicos: “esclarecer as ideias sobre políticas e políticas públicas, identificar aspectos importantes de questões políticas e problemas sociais, direcionar nossos esforços para compreender melhor as políticas públicas...” (DYE, 2009, p. 100).

Da mesma forma, o autor afirma que antes de iniciar o estudo de uma política pública é importante compreender que modelo deve orientar a pesquisa, a partir de uma análise operacional, ou seja: “Referir-se a fenômenos do mundo real, que possam ser observados, medidos e verificados. Um conceito ou uma série de

conceitos interrelacionados (modelo) devem sugerir relações no mundo real, que possam ser testadas e verificadas” (DYE, 2009, p. 127)

Neste sentido, considerando as peculiaridades do fenômeno em estudo e os alcances de nossa pesquisa centrada na determinação da formação da política de Cibersegurança, preferiu-se empregar o padrão de análise delineado em “Agendas, Alternatives and Public Policies” por John Kingdon (1984). O autor apresentou a abordagem dos múltiplos fluxos⁷ (multiple streams) para explicar como certos problemas conseguem se posicionar na agenda dos governos e se tornarem políticas públicas através dos processos de definição da agenda e de determinação de políticas alternativas⁸. Essas noções favorecem a nossa pesquisa, na medida em que as características do modelo permitem reduzir e simplificar a realidade analisada para inferir adequadamente, respeitando os comportamentos observados, o funcionamento institucional e a tomada de decisões dentro da dinâmica do sistema político nacional do Chile.

Segundo Capella (2018), as mudanças na agenda de acordo com o modelo dos múltiplos fluxos resultam do processo de convergência de três fluxos: problemas (problems stream), soluções ou alternativas (policy stream) e política (political stream) numa temporalidade específica, definida pela existência de janelas de oportunidade (policy windows) com a participação de empreendedores de políticas (policy entrepreneurs), durante dois momentos concretos: formação da agenda e definição de alternativas, processos que permitem o surgimento de uma política como resposta a um problema.

Zahariadis (2007) sugere que esse fluxo de problemas definido por Kingdon (1984) consiste em várias condições que os formuladores de políticas e os cidadãos desejam abordar. Capella (2018) adiciona que esse fluxo se encontra embasado dentro do processo para determinar as questões que são problemas. Do mesmo

⁷ Refere-se ao modelo dos múltiplos fluxos, como um padrão que é aplicável a uma ampla variedade de políticas e foi citado cerca de oitenta vezes por ano no Social Science Citation Index (SABATIER, 2007).

⁸ Segundo Capella (2018) esse modelo de formação de agenda proposto por Kingdon tem suas raízes no “modelo da lata do lixo” (*garbage can model*), proposto por Cohen, March e Olsen (1972). Esse modelo foi desenvolvido para a análise de organizações que se configuram como “anarquias organizadas”, operando em condições de grande incerteza e ambiguidade como governos nacionais. (Capella, 2018, p. 39).

modo, segundo Ramírez (2007); Capella (2018), as questões se transformam em problemas ao chamar a atenção dos participantes do processo decisório.

Zahariadis (2007) diz que os formuladores de políticas descobrem essas condições por meio de indicadores, eventos focalizadores (Focusing events) e retroalimentação (feedback). O autor define ainda que são indicadores os custos de um programa, taxas de mortalidade infantil ou mortes em rodovias, entre outros. Capella (2018) adiciona como exemplos, as variações na folha de pagamento de servidores e evolução do déficit público. Assim, segundo autores, os indicadores podem ser utilizados para caracterizar uma questão como um problema, capazes de estabelecer condições que precisam de atenção e atuação governamental.

Em relação com eventos focalizadores (Focusing events), segundo Kingdon (2003); Ramírez (2007); Capella (2018), as situações de crises e emergência ou eventos de grande magnitude, concentram a atenção pública e levam uma resposta imediata. Logo, o terceiro elemento é retroalimentação (feedback), que segundo Zahariadis (2007) considera o fluxo de informação que recebem os governos através dos diferentes programas em desenvolvimento, a fim de implementar com sucesso, uma solução em uma área onde possa ser transferida para outra, facilitando a adoção da mesma solução.

Por último, Capella (2018) reforça que os problemas são “construções sociais que envolvem uma interpretação” (CAPELLA, 2018, p. 40), de tal modo, a forma como é definido um problema em relação a sua articulação e a concentração do grau de atenção dos formuladores determinam o sucesso de uma questão no processo de agenda-setting.

A seguir, no processo das soluções ou alternativas (policy stream), Zahariadis (2007) baseado no texto de Kingdon (1984), é fundamentado que o fluxo de políticas inclui uma “sopa de ideias” que competem para ganhar aceitação nas redes de políticas. Essas são geradas por especialistas que formam comunidades políticas, redes que incluem burocratas, membros do Congresso, acadêmicos e pesquisadores que compartilham preocupação comum em uma única área específica. Kingdon (2013) define que a geração de propostas de políticas é um processo de produção de ideias que se assemelha à “seleção natural”, ou seja, apenas algumas ideias persistem e conseguem sobreviver, pois são dotadas de características que lhes permitem permanecer vivas, quando entram em contato com outras, são revisadas e

se misturam até se tornarem soluções viáveis. Segundo o autor, aquelas propostas que sobrevivem às diferentes avaliações devem atender a vários critérios, incluindo sua viabilidade técnica, sua adequação aos valores dominantes, o clima político nacional atual, sua viabilidade orçamentária e o apoio político ou oposição que possam experimentar. Em suma, o sistema de seleção restringe o conjunto de propostas concebíveis e seleciona desse grande conjunto uma pequena lista de propostas que serão parte do processo decisório.

Por fim, no processo dos três fluxos, encontra-se o fluxo da política (political stream), segundo Kingdon (2013) descreve que essa corrente política é composta de fatores como oscilações de humor nacional ou clima político, mudança de governo (turnover) ou legislativo, e as pressões de grupos de interesse. Portanto, os itens da agenda potencial que são congruentes com o clima nacional têm maior probabilidade de ganhar destaque na agenda, pois gozam de apoio de grupos de interesse ou não têm oposição organizada, na medida em que se encaixam nas orientações das coalizões legislativas prevaletentes ou da administração atual, diferente dos itens que não atendem a essas condições. Em particular, para Kingdon (2013) os elementos que têm efeitos influentes sobre as agendas políticas, serão as mudanças no clima nacional e as mudanças dentro do governo (turnover). Contudo, as mudanças na percepção do sentimento nacional, e da rotatividade de funcionários eleitos nas agendas, apresentam maiores probabilidades de afetar as alternativas já elaboradas, devido ao equilíbrio das forças organizadas.

Ademais, Capella (2018) acentua a importância desses três fluxos – problemas, soluções e política, quando em determinadas circunstâncias convergem gerando uma oportunidade de mudança na agenda, processo denominado como “janelas de oportunidade política” (policy windows) (KINGDON, 2003, apud CAPELLA, 2018, p. 43). Para Kingdon (2014) essas janelas são: “an opportunity to push pet proposals or one’s conceptions of problem” (KINGDON, 2013, p. 194). Desse modo, Ramirez (2007) analisa os fundamentos apresentados por Kingdon, asseverando que as janelas de oportunidade política se abrem indistintamente, no fluxo dos problemas ou no fluxo da política. Portanto, há janelas de problemas e janelas de política. Infere, baseado no autor, que as janelas têm uma temporalidade definida e estão disponíveis por um tempo deduzido. Logo, quando essas encontram-se abertas, carregam o sistema de problemas e propostas, e, portanto, obrigam a mobilizar recursos para

manter a pressão. Contudo, Capella (2018) destaca que a abertura das janelas pode se dar de forma periódica e previsível, devido as mudanças antecipadas nos governos, no congresso, e, nas fases do ciclo orçamentário, produto de sua periodicidade. Portanto, a oportunidade de mudança na agenda “pode se dar tanto de forma programada quanto de maneira não-previsível” (CAPELLA, 2018, p. 44).

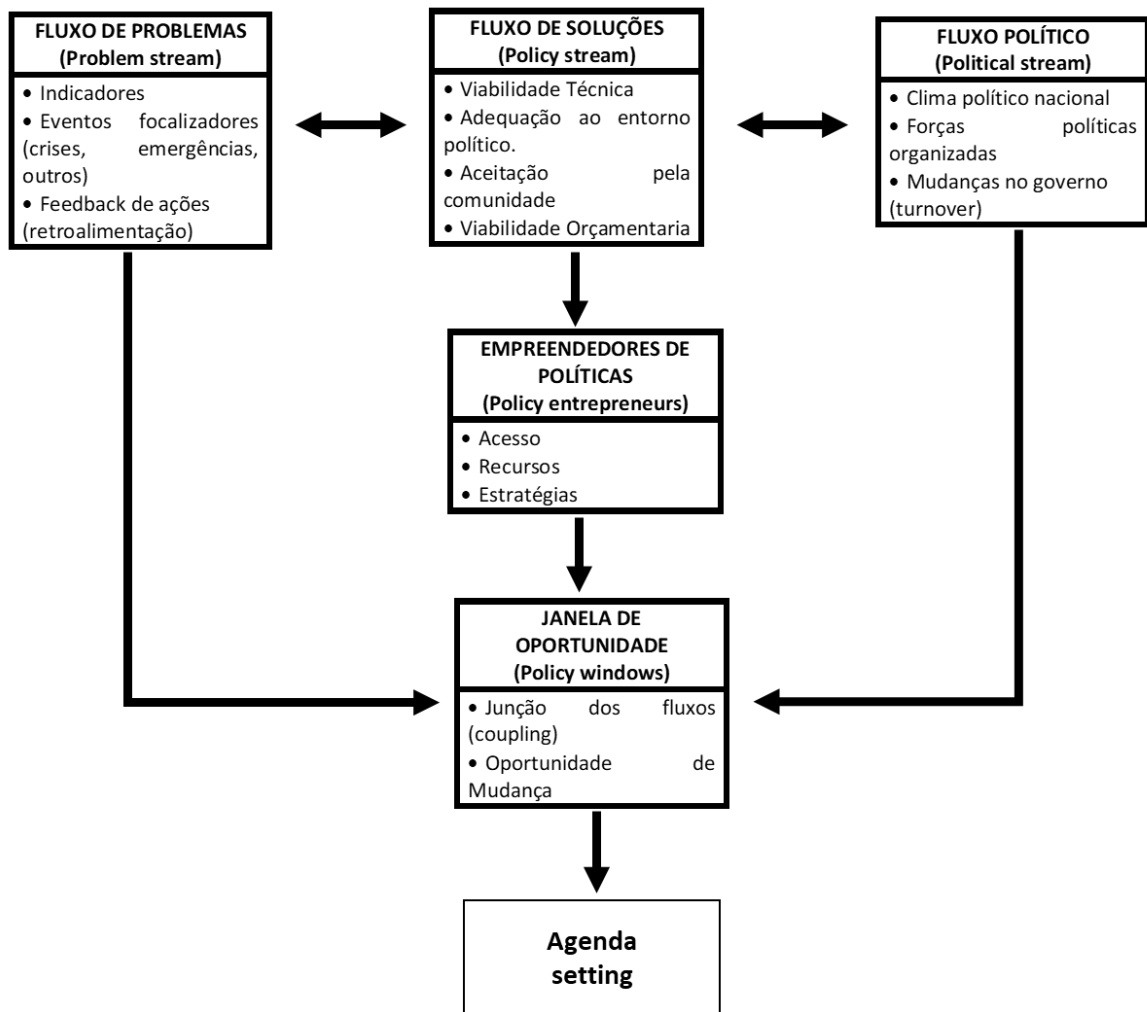
Segundo Capella (2018), ocorre nos momentos em que as janelas estão abertas, uma junção (coupling) dos fluxos dos problemas, soluções e políticas. Nesse contexto, Kingdon (2013), em relação ao processo de junção dos fluxos, argumenta a importância que adquirem os empreendedores de políticas (policy entrepreneurs⁹) para a existência dessa junção. Os empreendedores de políticas mantêm sua proposta, esperando por uma, de duas coisas: um problema que pode flutuar ao qual possa anexar a sua solução ou um desenvolvimento na corrente política, como uma mudança de administração, que fornece um clima receptivo para sua proposta. Segundo a própria autora ressalta, o papel como aqueles responsáveis pela ligação entre os fluxos de problemas, soluções e políticas de acordo com um momento político ou um evento, que sem sua presença não aconteceria devido à falta de proposta e a incapacidade para aproveitar a oportunidade. Além disso, Zahariadis (2007) ratifica que os “empreendedores de políticas mais bem-sucedidos são aqueles que têm maior acesso aos formuladores de políticas” (ZAHARIADIS, 2007, p. 74, tradução nossa).

Finalmente, em relação aos participantes do processo de formação de políticas, segundo Ramirez (2007); Capella (2018); baseados no trabalho de Kingdon, identificam uma diversidade de atores, os que estão classificados como atores visíveis e não visíveis. Os primeiros distinguem os participantes dentro do governo, como o Presidente e seu gabinete, a Administração estatal, Congresso etc., são aqueles que estão dentro do governo, têm autoridade legal-formal para tomar decisões e estão sujeitos a regras de prestação de contas (accountability), tal qual são considerados como “centrais nas mudanças da agenda”, devido a atenção do público e da imprensa (CAPELLA, 2018, p. 46). Os segundos são participantes de fora do governo, como: grupos de interesse, mídia de massa, partes, consultores etc., Conforme Capella (2018), eles “têm influência predominante sobre a geração das alternativas e soluções”, tal como, na agenda de decisão (CAPELLA, 2018, p. 46); embora

⁹ They could be in or out of government, in elected or appointed positions, in interest groups or research organizations (KINGDON, 2014).

reconhecendo que a “linha divisória é difícil de traçar e os canais de comunicação entre os de dentro e os de fora são mantidos abertos, enquanto as ideias fluem de um lado para o outro” (RAMIREZ, 2007, p. 253-254, tradução nossa).

FIGURA 1 – Diagrama adaptado do modelo Kingdon.

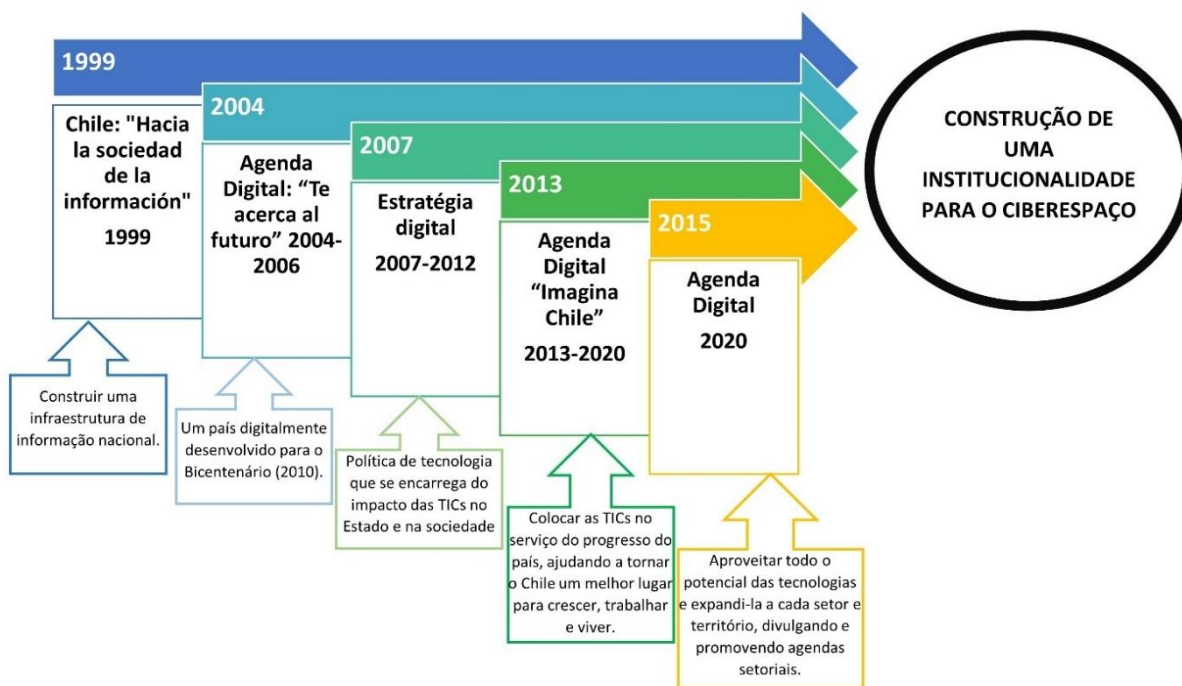


Fonte: adaptado de Zahariadis, (2003, p. 71); Capella, (2018, p. 45).

3 A EVOLUÇÃO DAS POLÍTICAS DIGITAIS DO CHILE DE 1997 ATÉ 2015. TENDÊNCIAS E DESAFIOS DOS PRECURSORES DA INSTITUCIONALIDADE DIGITAL

Na esfera nacional, nas últimas décadas, o Chile contou até 2014 com quatro instrumentos de planejamento na área de “Sociedade da Informação” e posteriormente, nas “Sociedades do conhecimento”¹⁰ que balizaram as diversas políticas governamentais nesta área (CHILE, 2013a). Em 2015 foi publicada uma última versão de uma agenda digital que considerou o desenvolvimento de uma PNCS sob a responsabilidade do Ministério do Interior e Segurança Pública, através de um comité interministerial (CHILE, 2015a)

FIGURA 2 – Evolução da institucionalidade digital do Chile



Fonte: Elaborado pelo autor a partir das diferentes políticas digitais feitas pelo Governo do Chile no período de 1999 a 2015.

¹⁰ Em 2005, a UNESCO participou da Cúpula Mundial sobre a Sociedade da Informação (CMSI), que sugere uma migração do conceito de sociedade da informação para o de sociedade do conhecimento. Em seu Relatório Mundial, intitulado “Em direção às sociedades do conhecimento” identifica, quatro dimensões principais das sociedades do conhecimento: liberdade de expressão e liberdade de informação; acesso universal à informação e ao conhecimento; educação de qualidade para a todos e respeito pela diversidade linguística e cultural (MANSELL e TREMBLAY, 2015)

A primeira delas foi durante a administração de Eduardo Frei Ruiz-Tagle¹¹, nomeada como: “Chile: Hacia la sociedad de la información”¹², que tentou estabelecer os desafios e oportunidades gerados pela difusão no país das novas tecnologias de informação e comunicação, e a maneira que essa revolução tecnológica tinha impactos genéricos em todos os aspectos da vida econômica, social e cultural de nossa nação (CHILE, 1999).

Neste sentido, o escrito apresenta as bases de uma estratégia de longo prazo, que apontava para 2010 com o objetivo de que “todo o país tenha acesso às redes de informação digital, seja em casa, na escola, na comuna, no trabalho ou nas instituições e espaços públicos” (CHILE, 1999, p. 9, tradução nossa). Da mesma forma, propõe um plano de ação de curto prazo visando assegurar, no biênio 1999-2000, o arranque da construção de um novo tipo de infraestrutura de informação, que permitiria ao país avançar ainda mais rumo à sociedade da informação e do conhecimento durante a primeira década do século XXI (CHILE, 1999), por intermédio de uma política do Estado com 61 ações (11 prioritárias) que “compromete sucessivos governos, independentemente de suas orientações políticas” (CHILE, 1999, p.19, tradução nossa).

A realidade nacional descrita na agenda digital (AD), estabelece que há um contraste importante entre o desenvolvimento acelerado da infraestrutura de telecomunicações e “o lento avanço da infraestrutura de informação que, até 1998, não cobria mais de 5% das empresas e 2% dos domicílios”. (CHILE, 1999, p. 28). Além disso, identifica-se quatro dificuldades para o desenvolvimento da infraestrutura da informação no país: uma distribuição territorial e social altamente desigual; lenta integração das empresas nas redes de informação digital para conduzir negócios, apesar da rápida informatização destas; apresentação, por parte do setor público, de um processo de informatização, inorgânico e desordenado, que atrasa a construção de uma autoestrada digital governamental de informação integrada à Internet, de fácil acesso para pessoas e empresas, falta, ainda, de conteúdo nacional de alta qualidade nas redes de informação digital (CHILE, 1999).

¹¹ Governou durante os anos 1994-2000.

¹² A política está baseada no relatório que foi preparado pela Comissão Presidencial “Novo Tecnologias da Informação e Comunicação”, instituído pelo Decreto Supremo de 1º de julho de 1998. Seus trabalhos foram encerrados em 26 de janeiro de 1999, com a entrega deste relatório ao Presidente da República, Sr. Eduardo Frei Ruiz-Tagle. (CHILE, 1999, p.3)

Consequentemente, a agenda propõe uma visão estratégica de futuro baseada em três objetivos: garantir que o acesso às redes de informação digital e aos serviços que oferecem seja universal e a custos razoáveis, desenvolver novas capacidades competitivas com base nas oportunidades oferecidas pela rápida evolução das tecnologias de informação e comunicação digital, utilizar o potencial das tecnologias digitais e da autoestrada da informação para promover a modernização do Estado em benefício dos cidadãos e das empresas (CHILE, 1999). Nesta lógica, observe-se que a estratégia será uma expressão compartilhada em torno de um projeto de futuro, em que adquirem um “papel de protagonista a sociedade civil, as empresas e o Estado, que deve assumir um papel proativo” (CHILE, 1999, p. 31, tradução nossa). Desse modo, o Estado deve acelerar sua própria informatização para induzir efeitos multiplicadores no resto da economia e na sociedade, bem como, na promoção de políticas públicas concretas, além do quadro jurídico e regulatório adequado, orientadas à formação de recursos humanos e a cooperação público-privada para fomentar o desenvolvimento tecnológico. Em síntese, “impulsar una modernización con creciente integración social; la aspiración de construir una sociedad abierta y culturalmente avanzada; el anhelo de vivir en una sociedad participativa que brinde oportunidades para todos” (CHILE, 1999, p. 17, tradução nossa)

Por sua vez, no Governo de Ricardo Lagos¹³, com a participação de profissionais de instituições governamentais, representantes do setor empresarial, o setor acadêmico e outros poderes do Estado, foi apresentada a Agenda Digital do Chile 2004-2006: “Te acerca al futuro”¹⁴, cujo objetivo era “contribuir para o desenvolvimento do Chile por meio do uso de TICs para aumentar a competitividade, igualdade de oportunidades, liberdades individuais, qualidade de vida e a eficiência e transparência do setor público” (CHILE, 2004, p. 5), conforme um amplo acordo público-privado sobre uma extensa estratégia nacional, olhando para a celebração do Bicentenário nacional em 2010.

¹³ Governou durante os anos 2000-2006.

¹⁴ A Agenda Digital (AD) é o resultado de um trabalho iniciado em abril de 2003 com a constituição do Grupo de Ação Digital (GAD), presidido pelo Coordenador de Governo de TICs, composta por instituições governamentais, entidades representativas do setor empresarial, do setor acadêmico e demais poderes do Estado. (CHILE, 2004, p.5).

Neste cenário, a AD enfrenta um período em que os usuários da Internet quintuplicaram (1998-2003), os estabelecimentos de ensino conectados à Internet dobraram e o número de pequenas empresas com acesso triplicou. No final de 2003, cerca de 3,7 milhões de mulheres e homens chilenos acessavam a Internet de suas casas, empregos, estabelecimentos de ensino e infocentros, com um incremento potencial até fins do 2005, o que poderia ultrapassar cinco milhões, surgindo novas oportunidades para o desenvolvimento econômico e social (CHILE, 2004).

Em vista disso, a AD apresenta um Plano de Ação para o período de 2004 a 2006, que inclui 34 iniciativas agrupadas em seis áreas de atuação: acesso, educação e capacitação; governo eletrônico, empresas, Indústria de TIC e quadro jurídico-regulatório. Também, incorpora na sua conceptualização os princípios da “Primeira Cúpula Mundial da Sociedade da Informação, de Genebra, 2003” (CHILE, 2004).

Dessa forma, para cumprir as metas estabelecidas para 2010, atingiu os níveis mínimos dos membros da Organização para a Cooperação e Desenvolvimento Econômico (OCDE)¹⁵ definindo seis objetivos gerais: uma infraestrutura de informação sólida e segura em banda larga para a internet, uma força de trabalho alfabetizada digitalmente e uma força de trabalho qualificada com padrões de excelência mundial em TIC; um Estado online a serviço do cidadão, comércio eletrônico altamente desenvolvido, fomento de uma massa crítica de empresas de TIC capazes de competir internacionalmente; construção de um moderno quadro jurídico-regulatório que facilitou o desenvolvimento da sociedade da informação (CHILE, 2004).

Em suma, a AD tenta avançar na convergência entre dinâmica de mercado, política do Governo, a aspiração social e o consenso político. Desta forma, “a presença ou ausência de estratégias e políticas públicas com alto grau de consenso, pode acelerar ou retardar a expansão e o uso das redes digitais, afetando direta e indiretamente o crescimento das nações” (CHILE, 2004, p. 9, tradução nossa).

¹⁵ Chile assinou seu acordo de adesão a OCDE em 2010, sendo o primeiro país de sul-americana. Fonte: <https://www.oecd.org/newsroom/chileprimerpaissudamericanomiembrodelaoecd.htm>

Mais tarde, durante o primeiro governo de Michelle Bachelet¹⁶, foi criada a “Estratégia digital 2007-2012”¹⁷ que considerava a formação de uma nova institucionalidade nomeada como Comitê de Ministros para o Desenvolvimento Digital, que teve como objetivo desenhar e executar uma política pública de ampla abrangência para um uso “mais profundo e intensivo das TICs por parte dos cidadãos, das empresas e do próprio Estado” (CHILE, 2007, p. 7, tradução nossa). Desse modo, “o desenvolvimento digital do Chile só terá sucesso se for o resultado da contribuição de todos: o setor público, o setor privado e a sociedade civil” (CHILE, 2007, p. 7, tradução nossa).

Por esse motivo, identifica-se como uma das principais tarefas deste período, a instalação de uma institucionalidade que permita levar adiante a política pública de desenvolvimento digital através de um arcabouço institucional que conceda sustentabilidade e continuidade à estratégia digital já feita (CHILE, 2007). Conseqüentemente, a AD define um objetivo principal:

“Contribuir para o desenvolvimento econômico e social do país por meio das potencialidades do uso das TICs para melhoria da qualidade da educação, aumento transparência, aumento da produtividade e competitividade e melhor governança, por meio de maior participação e comprometimento do cidadão” (CHILE, 2007, p. 16, tradução nossa).

Neste contexto, a partir dos objetivos para alcançar essa estratégia digital, estrutura-se quatro linhas de ação, sendo abordadas pela formação de grupos de trabalho público - privado que exigiram a participação ativa de atores especialistas de centros de estudo, indústria, estado e a sociedade civil, que é essencial para garantir o sucesso sobre um plano geral com metas específicas organizadas em um Plano Estratégico Nacional para TICs. As quatro linhas de ação: política tecnológica para o desenvolvimento digital, projetos e programas de desenvolvimento digital, estratégia de desenvolvimento da indústria TIC, desenho institucional (CHILE, 2007, p.23, tradução nossa).

¹⁶ Governou em seu primeiro mandato no Chile durante os anos 2006-2010.

¹⁷ A Estratégia de Desenvolvimento Digital do Chile 2007 – 2012 reflete sobre o trabalho realizado por o Comitê de Ministros para o Desenvolvimento Digital, criado em fevereiro de 2007. Como parte de seu processo de desenho, se apresentou este documento, que representa o trabalho interdisciplinar de um grupo de pessoas do mundo empresarial, das universidades, da sociedade civil e do Estado, coordenado pela Secretaria Executiva do Comitê de Ministros (CHILE, 2007).

A Política tecnológica para o desenvolvimento digital aborda os problemas sociais e econômicos que surgem com o avanço na introdução e uso das TIC, sendo assim, as novas políticas públicas devem adotar os novos paradigmas da inclusão digital, incluindo temas como segurança digital, uso de normas, adaptação do marco legal e uso de software livre (CHILE, 2007). Do mesmo modo que, “a criação de um quadro institucional especializado na questão da tecnologia, concentra a definição de políticas, gera consenso nacional, administra recursos e instâncias. Em suma, é uma institucionalidade que transcende o contexto político particular” (CHILE, 2007, p.33, tradução nossa).

Deste modo, o Chile se prepara para acionar sobre um cenário, que segundo mostra o relatório feito pelo Fórum Econômico Mundial, para o período 2006-2007, em Tecnologias de Informação e Comunicação, considerando 122 países ao redor do mundo, o Chile obteve o 31º lugar, sendo o país da América Latina com a avaliação mais alta (Gobierno de Chile, 2007, p.54, tradução nossa). Outra referência nesse assunto é o ranking elaborado pela “Intelligence Unit of The Economist”, que mede a preparação e as capacidades das pessoas, empresas e do Estado de um país no aproveitamento de TIC de forma eficaz, baseado em cerca de cem variáveis e seis categorias: conectividade e infraestrutura tecnológica; ambiente de negócios; ambiente social e cultural; enquadramento jurídico; políticas públicas e uso de TIC por consumidores e empresas, posicionando em 2007, num total de 69 países (desenvolvidos e em desenvolvimento), o 30º lugar para o Chile na classificação, sendo o país melhor avaliado na América Latina (GOBIERNO DE CHILE, 2007, p.56, tradução nossa).

Sob este quadro, é apresentada em 2013, a Agenda Digital “Imagina Chile, 2013-2020”¹⁸ durante a administração de Sebastián Piñera¹⁹, que constitui-se numa estratégia para a inclusão digital e desenvolvimento de serviços e aplicações, incorporando os avanços realizados e com a certeza de que a aplicação da tecnologia é uma ferramenta cada vez mais relevante para o desenvolvimento do país,

¹⁸ A AD “Imagina Chile, 2013-2020” foi desenhada pelo um grupo de especialistas nacionais e internacionais orientados para o desenvolvimento de uma estratégia virada para o cidadão e seu uso que o cidadão faz das tecnologias ao usar serviços e aplicativos para melhorar sua qualidade de vida. (CHILE, 2013a, p.5)

¹⁹ Governou em seu primeiro mandato no Chile durante os anos 2010-2014. É atualmente o Presidente da República até março de 2022.

melhorando a qualidade da vida de seus cidadãos, que considerou os aportes introduzidos pela OCDE e os resultados da participação do Chile nos trabalhos prévios da assinatura da Declaração de Seul para o Futuro da Economia da Internet (CHILE, 2013a).

Neste sentido, a AD tem o propósito de manter os avanços do país em termos de competitividade e desenvolvimento digital, que foi concretizado por uma política pública pioneira em telecomunicações que deve ser projetado para além 2020, da mesma forma que, tem seu foco no uso produtivo de tecnologias e da internet como fator relevante na economia digital, em que os benefícios de desenvolvimento digital se traduzem numa melhor qualidade de vida para os cidadãos (CHILE, 2013a).

Dessa forma, a AD buscou colocar as TICs “no serviço do progresso do país, ajudando a tornar o Chile um melhor lugar para crescer, trabalhar e viver” (CHILE, 2013a, p. 13, tradução nossa). Conseqüentemente, a AD determina como sua meta: “Transformar a economia chilena em uma economia do conhecimento, sustentável e inclusiva, projetando que as TICs representem, em 2020, 10% do PIB do país, por meio do uso generalizado de tecnologias como facilitadores da mudança (CHILE, 2013a, p. 18, tradução nossa).

Igualmente, a estratégia possui cinco eixos que são os pilares para o desenvolvimento digital: conectividade e inclusão digital; entorno para o desenvolvimento digital; educação e capacitação; inovação e empreendimento; serviços e aplicativos digitais (CHILE, 2013a). Além disso, considera 14 linhas de ação que detalham os focos de trabalho e 30 iniciativas ligadas a essas linhas (CHILE, 2013a). Segundo o governo, no desenvolvimento da AD participaram mais de “200 pessoas, incluindo os setores privado, acadêmico, empresarial, especialistas, líderes de opinião e associações” (CHILE, 2013, p. 31, tradução nossa).

Durante o segundo governo de Michele Bachelet²⁰ foi publicada a Agenda Digital 2020, “Chile digital para tod@s”²¹. Essa agenda fornece um roteiro político vinculado aos setores produtivos para tornar visíveis e consolidar as iniciativas de alto impacto que já estão em andamento no Chile. Também, dissemina e dá coerência ao

²⁰Governou em seu segundo mandato no Chile durante os anos 2014-2018.

²¹ A AD 2020 é um roteiro que estabelece as próximas etapas de planejamento e ação para definir uma política de desenvolvimento inclusiva e sustentável por meio de TIC, através de um novo órgão multissetorial e operacional que atua na execução das diretrizes prestadas nesse documento. (CHILE, 2015a, p. 5)

trabalho dos diferentes ministérios e instituições públicas que têm impacto no desenvolvimento digital do Chile. Ademais, estabelece a base para enfrentar os desafios que as tecnologias impõem em relação a busca de coesão, promoção e equidade para todas as pessoas de acordo com um padrão internacional (CHILE, 2015a).

Este novo cenário se encontra caracterizado pelo impacto das TICs, que permitiu no início de 2015, 67% que as famílias chilenas tivessem acesso à rede e 70% se declarassem usuárias da Internet. No entanto, existem fortes diferenças de acordo com as áreas geográficas e a situação socioeconômica das famílias. Enquanto nas cidades, a taxa de inserção destas tecnologias é de 70%, nos setores rurais atinge apenas 42%. Na quinta parte de renda esse número chega a 86%, nas famílias do primeiro quintil atinge apenas 54% (CHILE, 2015a).

Nesta continuidade, a AD está focada em aproveitar as oportunidades geradas pelas tecnologias para melhorar a qualidade de vida das pessoas e sua inserção na economia digital por meio de abordagens integradas, parcerias público-privadas, que combinam diferentes incentivos para a promoção de infraestrutura, usos sofisticados de tecnologias, empreendedorismo e inovação, aumento da participação cidadã e proteção dos direitos das pessoas nos ambientes digitais (CHILE, 2015a).

Possui seis objetivos específicos: respeito total pelos direitos das pessoas que se relacionam com a internet e TICs, obtenção de uma conectividade universal que permita o acesso para todas as pessoas às redes de alta velocidade e qualidade; apoio ao uso e desenvolvimento de TICs para melhorar a qualidade de vida de todas as pessoas, contribuição para o desenvolvimento e massificação da economia digital, posicionamento das tecnologias a serviço da qualidade da educação. Ainda, promoção e sustento do desenvolvimento de políticas públicas de desenvolvimento digital por meio de uma instância multissetorial que aborda o escopo e o impacto da tecnologia nas diferentes áreas da sociedade (CHILE, 2015a, p. 7-9, tradução nossa).

Adiciona-se, também, cinco eixos: direitos para o desenvolvimento digital, conectividade digital, governo digital, economia digital, competências digitais e são apresentadas treze linhas de ação subsidiárias. Desse modo, tem-se por finalidade executar os esforços necessários para que os benefícios da sociedade da informação alcancem todas as pessoas que habitam no país e cumprir os objetivos que “nós

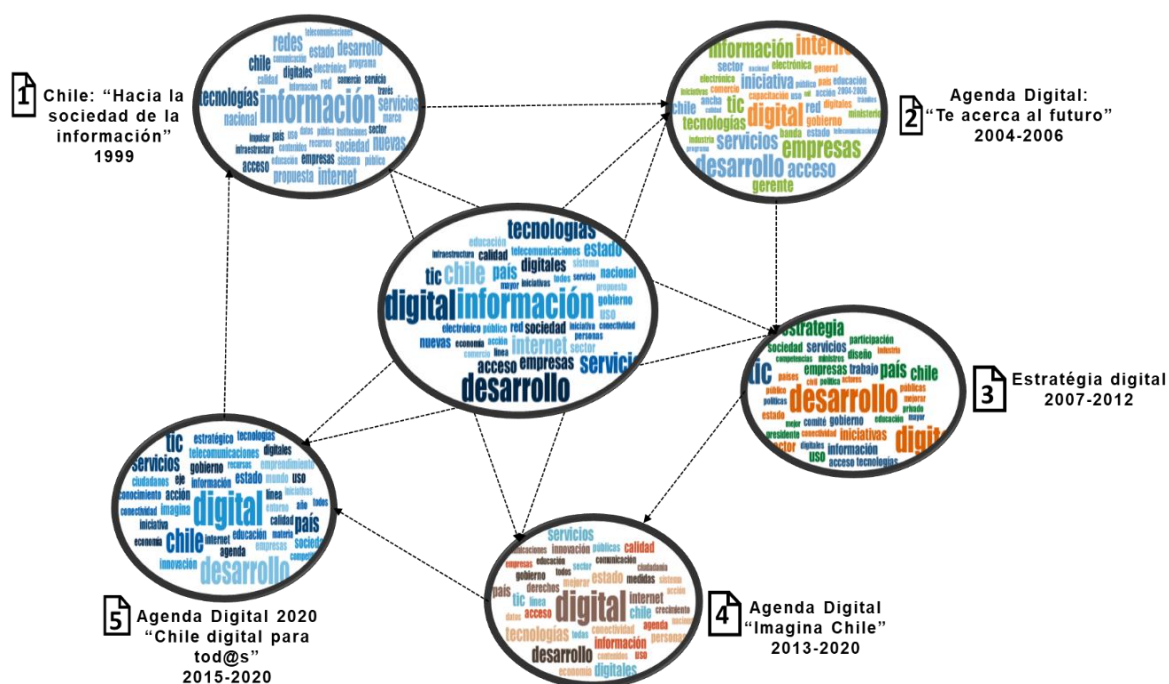
propusemos como um país inserido na comunidade internacional” (CHILE, 2015a, p. 6, tradução nossa).

Sendo assim, a AD considerou pela primeira vez na transformação digital do país, incluir a questão de Cibersegurança por meio de ações específicas. Por meio da medida núm. 25, estipulou: “o desenvolvimento de uma estratégia de cibersegurança” no concernente a sua Linha de Ação n.6, “Apoiar as políticas setoriais do Estado por meio do uso de tecnologias” (CHILE, 2015a, p.36, tradução nossa).

Em suma, cada etapa das agendas verificadas contribuiu em diferentes medidas para a transformação digital do país, aportando para a construção de uma institucionalidade digital que balizou o percurso traçado pelo Estado, em ordem de inserir o país na sociedade da informação e logo, na sociedade do conhecimento. A fim de começar, paulatinamente, um processo de transformação político, tecnológico, econômico e social que permitiu gerar os espaços dentro do funcionamento do Estado para se adaptar, promover e divulgar a relevância da TIC para o futuro desenvolvimento em termos mais amplos da sociedade. Por isso, concentra-se na promoção de maior conectividade e integração digital, deixando uma tarefa pendente no que diz respeito a possuir uma “estratégia orientada para o cidadão e o uso que o cidadão faz das tecnologias, ao usar serviços e aplicativos para melhorar sua qualidade de vida” (Gobierno de Chile, 2013a, p. 11, tradução nossa).

Não obstante, através da pesquisa lexical feita aos documentos históricos que foram parte da evolução da institucionalidade digital do Chile, consegue-se ratificar que o conceito de “segurança” não foi um aspecto que esteve presente nas diferentes temáticas exibidas nos textos.

FIGURA 3 – Resultado da pesquisa lexical da institucionalidade digital do Chile.



Fonte: Elaborado pelo autor a partir das diferentes políticas digitais feitas pelo Governo do Chile no período 1999-2015.

Consequentemente, neste itinerário evolutivo, com a finalidade de diminuir o fosso detectado a partir da publicação da AD 2013-2020 se tentou avançar paulatinamente através de diferentes propostas intersetoriais com maiores abrangências sociais na direção do progresso, além do próprio Estado, incorporando o imperativo de atender aos desafios de segurança que surgem desse maior desenvolvimento digital da sociedade (CHILE, 2013a).

Na sequência, a AD 2020 incorporou na sua visão um maior escopo e se focar nas pessoas com maiores dificuldades para se incorporar na nova era digital, para "seguir em frente com um suporte eficaz para quem busca empreender, com determinadas ações relevantes para impulsionar as vocações produtivas dos diferentes cantos do nosso país" (CHILE, 2015a, p. 15, tradução nossa) e como aspecto relevante, evidenciou um ambiente incerto, com riscos de segurança que podem evoluir ao ponto de afetar as pessoas e as instituições que deviam ser atendidas pelo Estado.

Sendo assim, as ADs surgiram como políticas públicas dentro de um contexto histórico-social que permitiu delimitar o desenvolvimento digital do país, focado

inicialmente no crescimento econômico do país, para depois avançar na promoção de aspectos essenciais de um “governo digital” que prosseguisse no resguardo das liberdades e direitos das pessoas no ciberespaço.

Finalmente, no Apêndice A se apresenta um quadro de comparação das Agendas digitais do Chile no período analisado, ponderando os fatores de objetivos, documentos estrangeiros incorporados, atores envolvidos, eixos e iniciativas.

4 A ANÁLISE DA POLÍTICA NACIONAL DE CIBERSEGURANÇA DO CHILE 2017

4.1 APRESENTAÇÃO DA PNCS

Em 2013, dentro das aspirações políticas consagradas no Programa de Governo da Sra. Michele Bachelet²² para seu futuro Governo no Chile (2014-2018) se considerava relevante o desenvolvimento de uma AD que permitisse enfrentar a partir de uma perspectiva institucional os desafios digitais para o país e o desenvolvimento de uma estratégia de segurança digital para “proteger usuários privados e públicos contra possíveis ações de violação de fontes de dados, juntamente com a proteção da privacidade dos nossos cidadãos” (CHILE, 2013b, p. 57, tradução nossa).

A exposição da Presidente da República na introdução da PNCS ratifica que a política pública tem sua origem na conexão das expressões políticas do programa de governo e das orientações particulares da AD 2020 (CHILE, 2017a). Dessa forma, se concretiza uma pretensão governamental com objetivo de modernizar seu funcionamento nas questões de segurança no ciberespaço, pois “qualquer erro ou ataque bem-sucedido pode violar o bem-estar e os direitos de chilenos e chilenas, afetar interesses privados e comuns e afetar serviços essenciais para o funcionamento do país” (CHILE, 2017a, p. 5, tradução nossa).

Face a esta realidade, a PNCS no contexto nacional, segundo Sancho (2015), é “uma política pública fundamental para garantir o bom funcionamento do

²² O Programa de Governo, Michelle Bachelet 2014-2018, “Chile de todos”, descreve as reformas substantivas propostas: educacional, tributária e da Constituição, indicando os pilares e princípios que regerão cada uma delas. Além disso, incorpora um programa econômico, e seus áreas de relevância, como: proteção e oportunidades; descentralização, território e desenvolvimento, e refere-se aos direitos dos cidadãos. (UNESCO, 2018)

ciberespaço e das informações que são geradas, armazenadas e transferidas” (SANCHO, 2016, p. 74, tradução nossa). Em vista disso, a política dá resposta aos requerimentos básicos demandados pela sociedade chilena: “Proteger a segurança das pessoas no ciberespaço; proteger a segurança do país; promover a colaboração e coordenação entre instituições; gerenciar os riscos do ciberespaço” (CHILE, 2017a, p. 12, tradução nossa). Assim, a presidente Bachelet na Cerimônia de publicação da política, expressou:

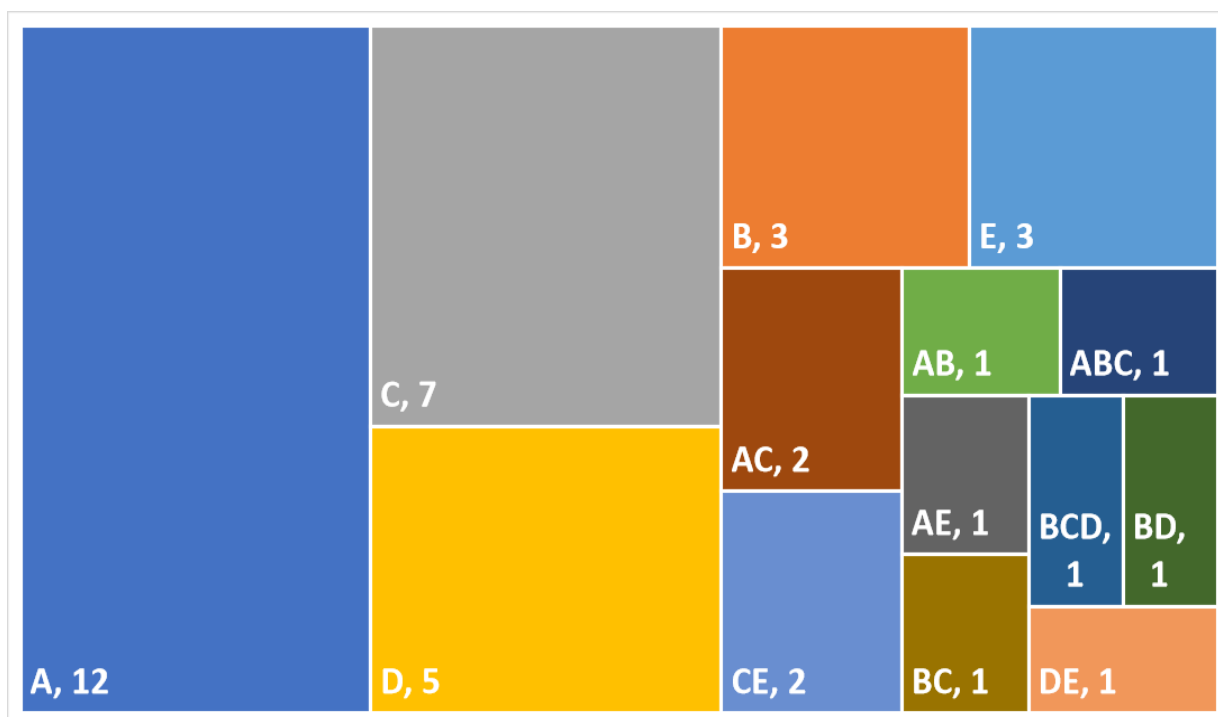
É por isso que o Chile, por meio desta política, traça um caminho, eu diria, responsável, democrático e justo para o desenvolvimento não só das interações no ciberespaço, mas também para garantir os direitos das pessoas e o desenvolvimento integral em um mundo cada vez mais aberto e digital. (CHILE, 2017c, p. 5, tradução nossa)

De natureza igual, a política descreve um roteiro baseado, primeiramente, em objetivos de alto nível e longo desenvolvimento através de uma estrutura que define uma política do Estado desenhada com um horizonte em 2022; como de médio prazo por meio de uma AD que delinea as medidas para executar durante o biênio 2017 e 2018 (CHILE, 2017a).

Dentro dos objetivos para 2022 que orientam os esforços do país, assim como, a priorização e racionalização das medidas subsidiárias descritas no registro, encontram-se:

A. Ter uma infraestrutura de informação capaz de suportar e se recuperar em caso de ataques e incidentes de cibersegurança; B. Garantir os direitos das pessoas no ciberespaço, C. Desenvolver uma cultura de cibersegurança em torno da educação, boas práticas e responsabilidade na gestão de tecnologias digitais; D. Estabelecer relações de cooperação em cibersegurança com outros atores que participará ativamente de fóruns e discussões internacionais; E. Promover o desenvolvimento de uma indústria de cibersegurança que atenda aos seus objetivos estratégicos. (CHILE, 2017a, p. 18-23, tradução nossa).

FIGURA 4 – Relação de Objetivos, medidas e Indicadores da PNCS^{23, 24}.



Fonte: Elaborado pelo autor a partir da PNCS, 2017.

Sendo assim, para cumprir esses objetivos, com foco no cumprimento do objetivo “A”, a PNCS estabelece uma “Institucionalidade para a Cibersegurança^{25, 26}”, que constitui um modelo de governança e de cibersegurança²⁷, a partir de padrões de países que já contam com esse tipo de estruturas, focadas na execução de tarefas

²³ De acordo com a PNCS existe uma mistura de medidas que abrangem dois ou mais objetivos. Tomando o objetivo AB por exemplo, exibe uma medida que está relacionada com os objetivos A e B. (CHILE, 2017a).

²⁴ Observe-se que o objetivo “A”: Ter uma infraestrutura de informação capaz de suportar e se recuperar em caso de ataques e incidentes de Cibersegurança”, concentra de maior forma, as atividades derivadas da política.

²⁵ Corresponde a uma das seis linhas de trabalho definidas no documento precursor da PNCS, nomeado “Bases para uma PNCS”. (ALVAREZ, 2015 apud SANCHO, 2016)

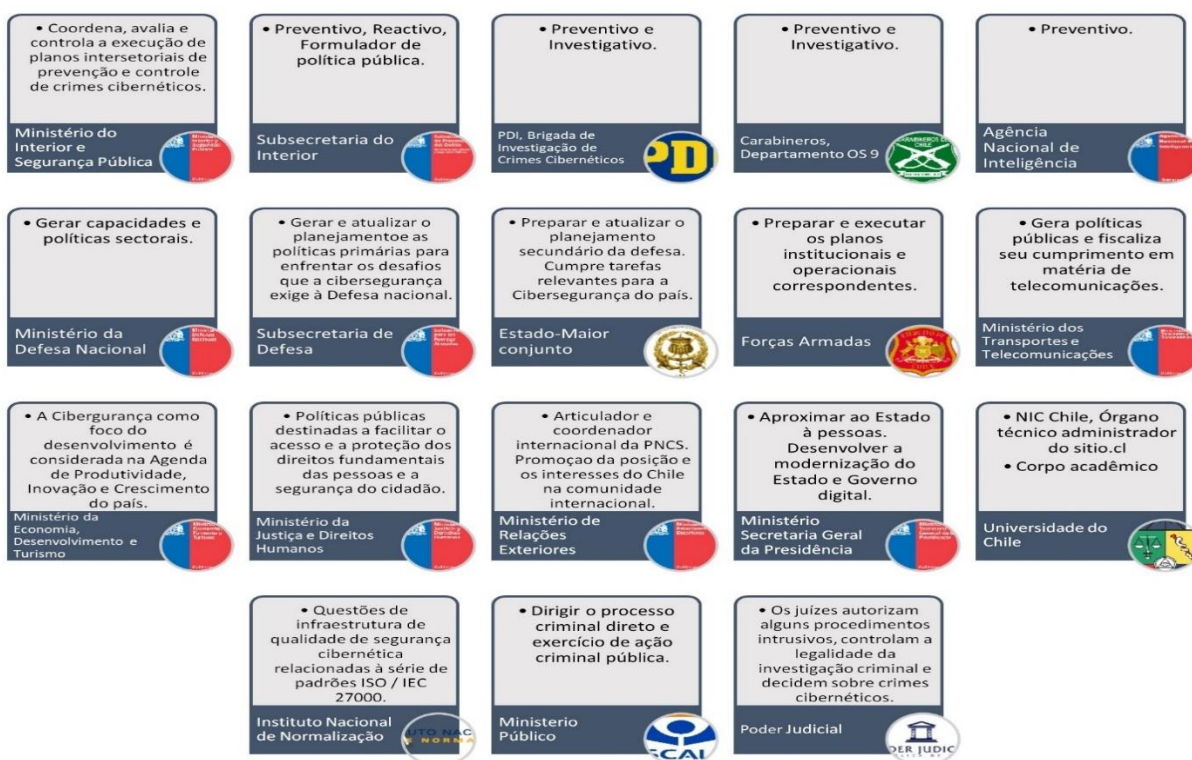
²⁶ Este documento estabelece que o atual quadro institucional de cibersegurança do Chile está distribuído entre várias organizações e entidades, portanto, requer de uma coordenação estratégica para aprimorar seu funcionamento. (CHILE, 2017a, p. 18-23).

²⁷ As primeiras recomendações para uma Governança no ciberespaço surgem pela UIT em 2011. Esse aspecto foi reforçado pela ITU e outros em 2018, quando se propôs estabelecer dentro da Estratégia nacional de Cibersegurança de um país, a existência de uma estrutura de governança clara que defina as funções e responsabilidades das principais partes, incluindo a identificação da entidade responsável pela gestão e avaliação estratégica, tal como uma entidade responsável pela sua gestão e execução em geral, seja uma autoridade central ou um conselho nacional de Cibersegurança. (Unión Internacional de Telecomunicaciones, el Banco Mundial, la Secretaría de la Commonwealth (Comsec), la Organización de Telecomunicaciones de la Commonwealth (CTO), el Centro de Excelencia de Ciberdefensa Cooperativa de la OTAN (CCDCOE OTAN), 2018, pp. 35-40)

essenciais e que facilitam a coordenação dos diferentes componentes do quadro institucional.

Desta forma, a PNCS propõe um modelo de governança de acordo com uma estrutura organizacional moderna que considera as necessidades do ciberespaço e do desenvolvimento digital do país, focada, principalmente na criação de um conselho assessor para a integração multissetorial²⁸ e uma série de funções primordiais encaminhadas para a gestão das relações interinstitucionais, gestão de incidentes, funcionamento como ponto de contato nacional e internacional nesta área, função comunicacional, função técnica normativa e assessoria sobre a regulamentação geral, função de acompanhamento e avaliação das medidas (CHILE, 2017a).

FIGURA 5 – Instituições intervenientes na questão da Cibersegurança nacional e seus papéis.



Fonte: Elaborado pelo autor a partir da PNCS, 2017, p. 33-36.

²⁸ Enquanto o projeto de lei sobre cibersegurança está sendo discutido e na fase de aprovação no Congresso Nacional, algumas funções identificadas como essenciais, serão cumpridas no nível político através do mandato ampliado do Comitê Interministerial sobre Cibersegurança, no que se refere à função de comunicação, coordenação e monitoramento de medidas apresentadas no PNCS. (CHILE, 2017a)

4.2 FORMAÇÃO DE AGENDA DA PNCS

4.2.1. O fluxo dos problemas (problems streams)

O processo da construção da PNCS aconteceu a partir de um cenário de desenvolvimento e uso massivo de tecnologias de informação e comunicação. Segundo AD 2013-2015, mostra que a convergência tecnológica, virtualização, e dispositivos de nova geração que utilizam múltiplas plataformas de comunicação permitiram corrigir o fosso digital existente no país, ao reduzir as distâncias geográficas e expandir seus ganhos às pessoas inseridas nas sociedades do conhecimento, por meio de novas oportunidades de trabalho e educação, tal qual, uma melhoria das condições do país para atingir seu desenvolvimento pleno através do uso produtivo das tecnologias e da Internet como fator relevante na economia digital, na inovação e no investimento público-privado nas TIC. (CHILE, 2013a). Segundo o relatório da UIT nomeado “Medición de la Sociedad de la Información 2014”, observa-se a situação mundial e a do país:

Até o final de 2014, quase 3 bilhões de pessoas usarão a Internet, comparativamente com 2.700 no final de 2013”, representando um crescimento de 300 milhões de usuários no último ano em todo o mundo. Enquanto isso, o mesmo órgão estimou em 2014 que 66,5% dos chilenos usaram a Internet. (CHILE, 2015a, p. 4)

Da mesma forma, na apresentação da PNCS se confirma esse cenário de permanente evolução, através dos impactos gerados para o país no triênio 2014-2016:

Os acessos à Internet cresceram 45,3% nos últimos dois anos, passando de 52,2 acessos por 100 habitantes no início de 2014, para 73,8 acessos por 100 habitantes em março de 2016. A economia digital Nacional, por sua vez, cresceu cerca de 11% em no último biênio, passando de 34.127 milhões de dólares em 2014 para 39.485 milhões de dólares em 2015. (CHILE, 2017a, p.5, tradução nossa).

Em vista disso, o papel do Estado no âmbito digital segundo AD 2013-2020 “não tem apenas um aspecto legal ou normativo, mas deve ser complementado com um quadro institucional. As TICs são transversais a diferentes setores da economia e da sociedade” (CHILE, 2013a, p. 31, tradução nossa). Nessa perspectiva, o documento “Bases para uma PNCS” (CHILE, 2015c) expõe que na comunidade

internacional surgem dessemelhantes esforços para desenvolver estratégias de Cibersegurança para agir no ambiente digital. Em 2003, de acordo com dados da Agência Europeia de Segurança de Redes e Informação (ENISA), mais de 35 países tinham uma Estratégia Nacional de Cibersegurança (ENCS) e países como Holanda e Estônia já possuíam mais de uma versão. Como efeito, os países têm tido avanços significativos nas áreas técnicas e instrumentos normativos, a partir de uma “perspectiva de segurança internacional e interna de cada país”. (CHILE, 2015c, p.5, tradução nossa). Contudo, até o 2015, o Chile não tinha uma PNCS. Assim, no registro já referido era exposto:

No Chile, até o momento não existe uma política pública que se encarregue deste fenômeno, sendo necessário assumir o desafio de propor ações que permitam enfrentar as vulnerabilidades, riscos e ameaças geradas pela interação no ciberespaço, tanto para o país como para a comunidade internacional. (CHILE, 2015c, p.5, tradução nossa).

4.2.1.1 Os indicadores que precisaram de atenção governamental

Segundo infere-se das apreciações iniciais descritas na PNCS, o uso massivo das TICs junto com a ajuda no desenvolvimento do país, ocasiona riscos e ameaças que podem afetar certos espaços ligados aos “direitos das pessoas, a segurança pública, a infraestrutura crítica, o governo digital, os interesses essenciais e a segurança externa do Chile” (CHILE, 2017a, p.11, tradução nossa).

Neste contexto, no documento “Bases para uma PNCS” (CHILE, 2015c) se estabelece que devido à natureza global do ciberespaço, as fontes de ameaças decorrem tanto do exterior quanto do nível interno, abrangendo às atividades criminosas realizadas a partir do país ou através de outros países, como atividades de espionagem e vigilância realizadas com diversos fins, que podem afetar a confidencialidade, integridade e disponibilidade dos ativos de informação no ciberespaço (CHILE, 2015c).

A respeito das fontes de ameaças externas, o mesmo escrito alude que nessa época, os ciberataques²⁹ consistiam em atividades de espionagem e ataques de

²⁹ Os ataques cibernéticos são ações hostis realizadas no ciberespaço com o objetivo de invadir, explorar, negar, degradar ou destruir a infraestrutura tecnológica, componente lógico ou suas interações e podem ter diferentes níveis dependendo na duração, frequência e danos gerados. (CHILE, 2015c).

negação de serviço distribuído (DDoS)³⁰ na Internet, como a interceptação em massa das redes de telecomunicações, a desativação do serviço de Internet, a espionagem contra governos e empresas, bem como ataques contra infraestruturas críticas, como bancos e serviços governamentais. Na América Latina, em 2013, o Chile estava dentro dos países com maior número de ataques cibernéticos (CHILE, 2015c). Nesse sentido, a evidência recolhe os principais incidentes acontecidos no ciberespaço global.

TABELA 2 – Sumários dos incidentes acontecidos no ciberespaço global que foram identificados como ciberataques.

Ano	País / ator	Tipo de incidente
2010	Irã	Vírus informático inutiliza centrífugas nucleares.
2007	Estônia	Ataque sobre infraestrutura crítica nacional.
2011	Estados Unidos	Espionagem industrial contra empresas de defesa (Lockheed)
2013	Edward Snowden	Revelações sobre espionagem massiva das agências de inteligência dos EUA.
2014	Estados Unidos	Espionagem contra indústria de entretenimento (Sony)

Fonte: O autor adaptado do documento “Bases para uma PNCS” (CHILE, 2015c)

Em nível local, estudando o escrito já referido, observou-se indicadores que no triênio 2010-2013 trazem a questão de segurança no ciberespaço e exhibe um acréscimo no número de atividades detectadas e possíveis riscos para o país. Conseqüentemente, “No Chile, a Rede de conectividade do Estado (RCE) sofreu inúmeros ataques cibernéticos”. (CHILE, 2015c, p.6, tradução nossa).

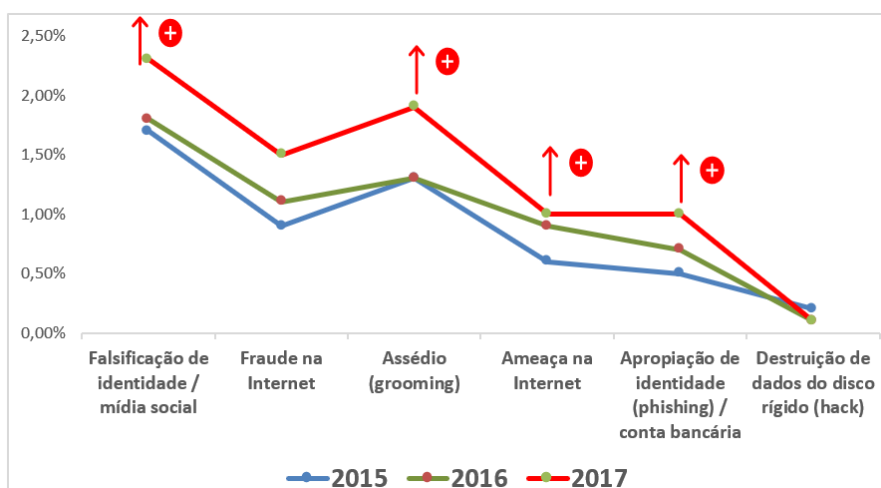
Nesse contexto, segundo a publicação analisada, houve “registros de incidentes para ataques DDoS ou hackers em sites do governo, observando um crescimento importante destes entre 2010 e 2013”. Durante o ano de 2014, segundo a Divisão de Tecnologia da Informação do Ministério do Interior, a rede governamental mostrou 64.590.567 registros de potenciais padrões maliciosos detectados. (CHILE, 2015c, p.6-7, tradução nossa).

³⁰ Os ataques de negação de serviço distribuído (DDoS) muitas vezes são chamados ataques de rede. Esse tipo de ataque aproveita os limites de capacidade específicos que se aplicam a todos os recursos de rede, como a infraestrutura que viabiliza o site de uma empresa.

O Ministério Público do Chile, dentro da publicação apresentada, aportou dados relativos aos crimes cibernéticos identificados no período 2009 - 2013, pautados como “crimes informáticos” o total foi de 3.063 processos. Por sua vez, a Polícia de Investigações (PDI) disponibilizou a informação que durante o mesmo intervalo foram realizados 1.980 inquéritos, os quais foram qualificados como ações que mostram maior complexidade na sua execução. (CHILE, 2015c, p.7-8).

Com tal característica, segundo os dados obtidos do Centro de Estudos e Análise do Crime (CEAD em espanhol) da Subsecretaria de Prevenção de delito³¹ por meio da Pesquisa urbana nacional de Segurança Cidadã (ENUSC em espanhol)³² aprecia-se um incremento porcentual dos indicadores da vitimização social concernente aos delitos cibernéticos durante o período elencado que dão um quadro de referência prévio à discussão da definição da agenda de Cibersegurança. O estudo identifica uma significativa variação estatística entre 2016 e 2017, bem como, evidencia-se um crescimento sustentável na temporalidade avaliada. (CHILE, 2017b).

FIGURA 6 - Crescimento dos indicadores de vitimização social concernente aos delitos cibernéticos no triênio 2015-2017



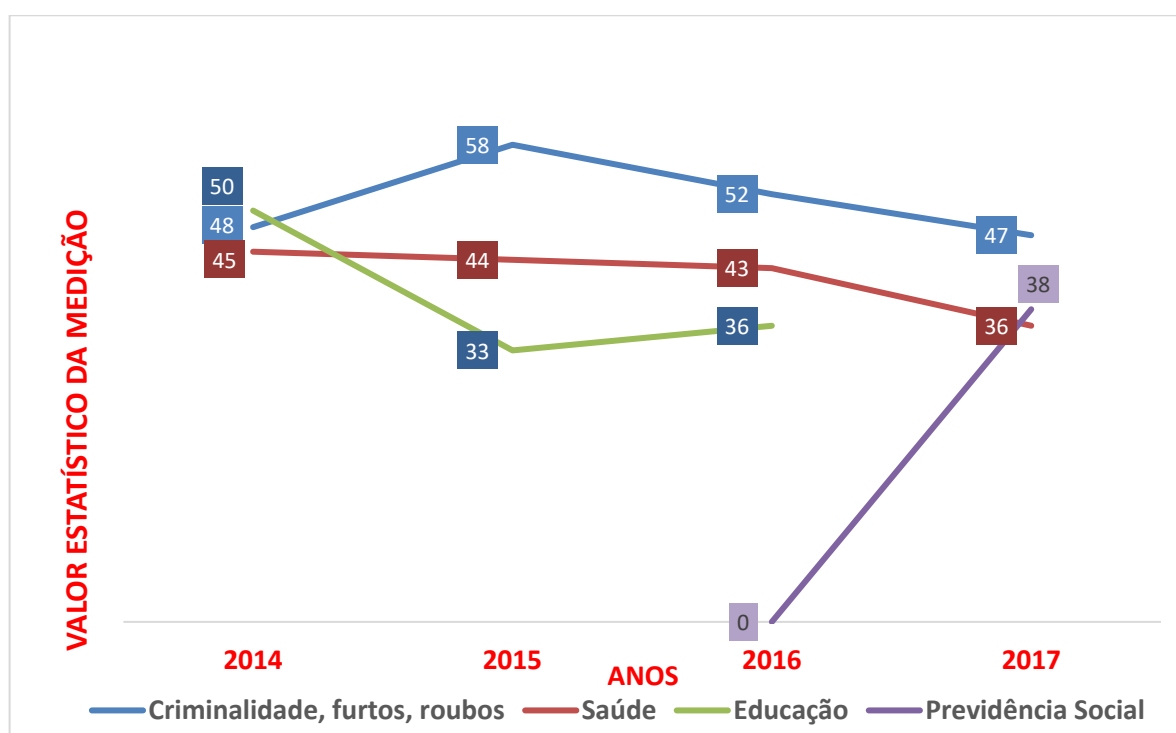
Fonte: O autor baseado nos dados fornecidos pela Pesquisa urbana nacional de Segurança Cidadã 2017 (CHILE, 2017b).

³¹ O Centro de Estudos e Análise do Crime (CEAD) é um sistema abrangente de monitoramento, análise de informações, elaboração e avaliação de programas e geração de conhecimento, que atua no âmbito da Divisão de Programas e Estudos da Subsecretaria de Prevenção do Crime. Fonte: <http://cead.spd.gov.cl/quienes-somos/>.

³² Respeito da ENUSC, através da assessoria de um conselho de expertos, aprimorou-se a metodologia para o levantamento de dados, incorporando-se, pela primeira vez, os delitos cibernéticos em 2015. (CHILE, 2017b).

Complementando as informações apresentadas, ao ponderar os Estudos nacionais de opinião pública feitos pelo Centro de estudos Públicos³³ (CEP), durante os anos 2014-2017, pode-se dizer que as situações sociais que demandam uma maior atenção governamental estavam associadas principalmente com a criminalidade, furtos, roubos; saúde; e educação³⁴. Por meio desta sondagem de opinião foram identificados os três principais problemas nos quais o governo deveria concentrar a sua gestão para resolvê-los. O quadro abaixo apresenta a síntese da evolução dos problemas prioritários para a opinião pública do Chile no quadriênio 2014-2017.

FIGURA 7 - Evolução dos problemas prioritários para a opinião pública do Chile no quadriênio 2014-2017



Fonte: O autor baseado nos Estudos nacionais de Opinião Pública N.72, 75, 78 e 81 (CENTRO DE ESTUDIOS PÚBLICOS (CEP), 2017)

³³ O Centro de Estudos Públicos (CEP) é uma fundação acadêmica privada sem fins lucrativos. Tem como objetivo o estudo e a produção de conhecimento sobre temas de interesse público, da mesma forma que a divulgação dos valores, princípios e instituições fundamentais para uma sociedade livre e democrática. Fonte: <https://www.cepchile.cl/cep/que-es-el-cep>.

³⁴ No ano 2017, os resultados da pesquisa de opinião variaram, gerando o incremento da percepção cidadã a respeito de priorizar a Previdência social como um aspecto que precisava de maior atenção do Governo. Estudos nacionais de Opinião Pública N.81 (CENTRO DE ESTUDIOS PÚBLICOS (CEP), 2021)

Por outro lado, desde a dimensão econômica, surgem aspectos que colaboram à análise das condições que se transformaram em problemas, quando segundo Capella (2018), elas chamam a atenção dos participantes do processo decisório. Neste cenário, é interessante identificar, se no orçamento nacional existiu uma evolução nas dotações ornamentais correspondentes como resposta a novas demandas políticas e sociais. Nas prioridades orçamentais definidas pelo Governo do Chile através dos documentos nomeados “Projetos Lei de orçamento nacional”³⁵ durante no quaternio 2014-2017, incrementaram-se os recursos destinados aos planos de Segurança pública, no entanto, os documentos estudados não expressam definições políticas específicas sobre a Cibersegurança, delitos digitais, ou projetos associados a essa questão. Apesar disso, nas Leis de Orçamento do setor público do mesmo intervalo, existem fundos atribuídos ao Ministério de Economia, Desenvolvimento e Turismo para o desenvolvimento de “Agenda digital”, identificado com mesma denominação (CHILE, 2017c). Não obstante, segundo a AD 2020 existiram outras agendas setoriais que promoveram o desenvolvimento tecnológico-digital do país sem considerar questões de segurança, tais como, o projeto de conectividade liderada pela Subsecretaria de Telecomunicações, produtividade, inovação e crescimento pelo Ministério de Economia, governo eletrônico e transparência guiada pela Secretária-geral da Presidência da República, além das iniciativas singulares realizadas pelos ministérios da Saúde, Educação, Trabalho e Fazenda (CHILE, 2015a).

Tabela 3 – Registro de dotação orçamental do Ministério de Economia para projetos associados à Agenda digital.

Ano	Denominação / rótulo	Dotação orçamental (valor em milhares de pesos chilenos)
2014	Programa Digitaliza Chile	\$325.398
2015	Agenda Digital	\$561.968 ▲
2016	Agenda Digital	\$436.302 ▼
2017	Agenda Digital	\$229.148 ▼

Fonte: O autor baseado nos dados da Leis de Orçamento do setor público 2014-2017. (CHILE, 2014c).

³⁵ Gobierno de Chile, Dirección de presupuestos. Fonte: <https://www.dipres.gob.cl/598/w3-propertyvalue-2129.html>

Em síntese, através dos indicadores apresentados, tais como, o incremento de ações delitivas originadas no ciberespaço a nível global e interno (nacional); acréscimo no número de atividades de ciberataques detectados e maiores riscos para o país e o incremento porcentual dos indicadores da vitimização social concernente aos delitos cibernéticos, pode-se examinar como as condições da interação política – social no ciberespaço vão configurando um cenário evolutivo com “impacto real” na sociedade, além de uma situação social percebida pela população. Neste sentido, de acordo com Kingdon (2003), as variações estatísticas mostradas são percebidas e definem um problema quando os “Policy makers consider a change in an indicator to be a change in the state of a system”. (Kingdon, 2003, p.92). Consequentemente, a mudança no sistema político nacional foi observada quando se reconheceu que as ações delitivas originadas no ciberespaço constituíam uma questão que requeria a atenção do governo devido as mudanças explícitas apresentadas, por tanto, cumpre a premissa de Kingdon (1995) que argumentou: “os problemas contêm um elemento perceptivo e interpretativo” (KINGDON 1995 apud ZAHARIADIS 2007, p. 71). Segundo o documento “Bases para uma PNCS”:

Os cibercrimes constituem uma ameaça à segurança, privacidade e confidencialidade na Internet, e afeta todos os seus usuários, impedindo-os de exercer suas funções, violando segredos de estado e comerciais e ameaçando os direitos fundamentais das pessoas, especialmente aqueles relacionados à proteção de sua vida privada e inviolabilidade de suas comunicações. (CHILE, 2015c, p.8, tradução nossa).

4.2.1.2 Eventos focalizadores (Focusing events)

De acordo com Kingdon (2003), alguns problemas não são visíveis somente pelos dados aportados pelos indicadores, pois precisam de “um pequeno impulso para chamar a atenção das pessoas dentro e ao redor do governo”. (KINGDON, 2003, p.94, tradução nossa). Neste sentido, segundo Zahariadis (2007), as “condições e eventos focalizadores direcionam a atenção para dimensões avaliativas específicas de problemas particulares, a atenção é fixada pela mídia ou empreendedores de políticas”. (BIRKLAND, 1997 apud ZAHARIADIS, 2007, p. 1997). Desta forma, além dos indicadores apresentados no apartado anterior; segundo Viollier (2017), referindo-se à questão da PNCS, argumenta-se que os “Ataques cibernéticos em grande escala,

cada vez mais sofisticados e frequentes, transformaram a Cibersegurança em um tema de interesse para a opinião pública”. (VIOLLIER, 2017, p. 5). Logo, ele expõe que existiu um incremento dessa tendência no Chile a partir do 2017, quando aconteceu uma série de ataques de tipo “ransomware³⁶”, detectando-se no Chile 270 casos de equipamentos infectados (VIOLLIER, 2017), sendo o mais sério até essa data o nomeado como “wannacry³⁷”. Neste contexto, a mídia nacional fez um destaque dos acontecimentos da notícia devido às repercussões e impactos produzidos a nível internacional, como a nível nacional.

Como é possível observar no quadro abaixo, os distintos de tipos de meios de imprensa, selecionados de um jeito aleatório, utilizando as palavras chaves: wannacry, ransomware, vírus, segurança, divulgaram a informação segundo sua audiência e colocou em evidência de acordo com a análise executada, os seguintes conteúdos: muita exposição do país frente à ameaça, um impacto nos sistemas informáticos de diferentes empresas e uma negativa posição de destaque do país a respeito do ataque cibernético na região.

QUADRO 2 – Registro de manchetes de notícias escolhido sobre ataque cibernético de ransomware desde maio a julho do 2017.

Meio de imprensa / data	Manchete de notícias	Pesquisa lexical	Referência
Bío-Bío Chile; 12 de maio de 2017	Ataque de computador afeta a área telefônica em todo o mundo, incluindo Movistar no Chile.	Companhia – arquivos – ataque - Chile	https://www.biobiochile.cl/noticias/internacional/europa/2017/05/12/ataque-informatico-afecta-a-telefonica-a-nivel-mundial-incluido-movistar-en-chile.shtml
Emol; 12 de maio de 2017	Especialista registra 36 mil detecções de vírus em todo o mundo: Chile está entre os afetados.	Chile – computadores – malware - detecções	https://www.emol.com/noticias/Tecnologia/2017/05/12/858113/Experto-registra-36-mil-detecciones-de-virus-a-nivel-mundial-Chile-esta-entre-los-afectados.html
La Tercera digital; 15 de maio de 2017	Qual foi o impacto do ataque cibernético no Chile e na América Latina?	Vírus – Chile – arquivos - origem	https://www.latercera.com/noticia/ha-impacto-del-ciberataque-chile-latinoamerica/

³⁶ De acordo com o sítio web do Kaspersky, “Ransomware” é um software de extorsão que pode bloquear o seu computador e depois exigir um resgate para desbloqueá-lo. Fonte: <https://www.kaspersky.com.br/resource-center/threats/ransomware>.

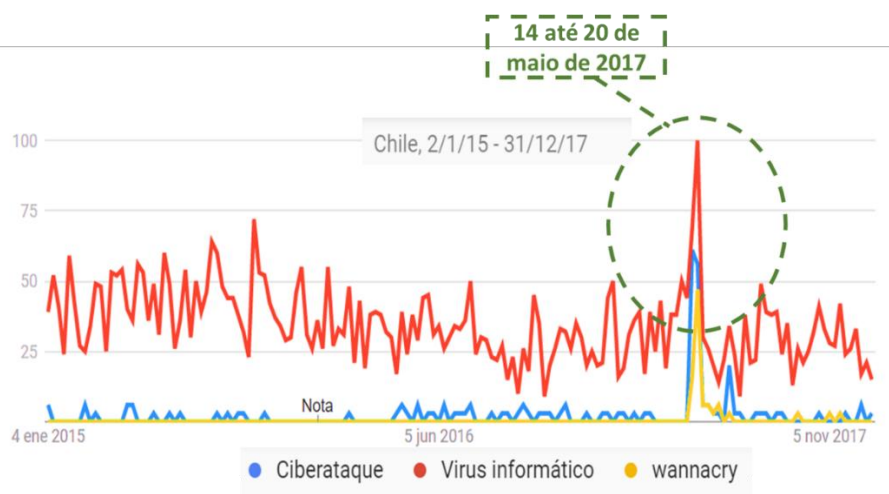
³⁷ Um dos maiores e mais sérios ataques de ransomware ocorreu em maio de 2017 e se chamou WannaCry. Durante o ataque, cerca de 200.000 vítimas de cerca de 150 países foram coagidas a pagar um resgate em bitcoins. Fonte: <https://www.kaspersky.com.br/resource-center/threats/ransomware>.

Meio de imprensa / data	Manchete de notícias	Pesquisa lexical	Referência
BBC Mundo; 16 de maio 2017	Quais são os países latino-americanos mais afetados pelo WannaCry, o principal vírus do ciberataque global.	Wannacry – américa – mundo – vírus	https://www.bbc.com/mundo/noticias-america-latina-39931455
CNN espanhol; 15 de maio 2017	Este é o país da América Latina mais afetado pelo ciberataque WannaCry.	México, américa, país, sexta-feria.	https://cnnespanol.cnn.com/2017/05/15/este-es-el-pais-de-latinoamerica-mas-afectado-por-el-ciberataque-wannacry/
T13; 6 de julho 2017	Chile fue el tercer país latinoamericano más afectado por virus WannaCry.	Chile- wannacry – seguridad – informática.	https://www.t13.cl/noticia/tendencias/tecnologia/chile-fue-tercer-pais-latinoamericano-mas-afectado-virus-wannacry .
Economia y Negocios; 6 de julho 2017	O ataque do vírus WannaCry atingiu o Chile com mais força do que você pensa	Chile- wannacry – vírus – segurança.	http://www.economiaynegocios.cl/noticias/noticias.asp?id=376288

Fonte: O autor baseado nos dados da imprensa coletados na referência apresentada.

Da mesma forma, segundo Google Trends, em maio 2017, mostrou-se que dentro dos termos mais procurados na web no Chile foram “wannacry” e “ciberataques”, com valores de máxima notoriedade entre os dias 14 a 20 de maio. Embora, a palavra “vírus informático” foi a mais procurada dentro do contexto no estudo, na mesma data e ao longo do mesmo ano de 2017 (GOOGLE, 2021).

FIGURA 8 – Resultados da busca de termos sobre os assuntos de ataques cibernético em 2017.



Fonte: O autor a partir de uma adaptação dos dados fornecidos pelo Google Trend Chile (GOOGLE, 2021)

Portanto, através dos acontecimentos acrescidos como ataques informáticos surgidos a partir do 2010 no contexto global, e específicos em 2013 a nível nacional, com um ponto alto em 2017, quando se produziram os ataques de tipo ransomware nomeado como “wannacry”, corroboraram-se a existência de eventos de impacto midiático que influenciaram na captação da atenção da audiência, produzindo nos habitantes uma sensação de instabilidade baseada em uma posição vulnerável diante das ameaças emergidas e uma relação de proximidade com a questão cibernética que constatou uma preocupação social sobre esses eventos e seus efeitos.

4.2.1.3 Retroalimentação (feedback)

Segundo Zahariadis (2007), considera-se que o “feedback de programas anteriores é importante porque ajuda a identificar aquilo que funciona daquilo que não está”. (ZAHARIADIS, 2007, p. 72). Em complemento, segundo Capella (2018), o centro de atenções dos formuladores de políticas pôde colocar a atenção nos resultados destes programas. Desta perspectiva, ao analisar a AD 2020 que impulsionou o desenvolvimento da PNCS junto a outros documentos como já foi apresentado, evidenciou-se que pertenceu ao eixo “Governo digital”, um dos cinco eixos da AD 2020 (CHILE, 2015a, p.11). Neste sentido, o eixo “Governo digital” considerou quatro linhas de ação e 18 medidas específicas, dentro das quais, o desenvolvimento de uma estratégia de cibersegurança estava inserida na Linha de ação num. 6, “Apoiar as políticas setoriais do Estado por meio do uso de tecnologias”. Justificando seu agir devido as demandas de uma sociedade mais interligada que requer uma mudança de um “governo eletrônico” ao “governo digital” amparado na “promoção do uso estratégico e coordenado de ferramentas como TIC e a inovação no Estado, pois é fundamental melhorar a experiência do cidadão ao interagir com os serviços públicos em todas as suas dimensões”. (CHILE, 2015a, p.30, tradução nossa).

Neste processo de mudanças, a AD já referenciada mencionou que o Chile será um dos líderes no desenvolvimento de políticas nesta matéria na América latina, pois entrou nessa categoria no ranking de Governo Eletrônico publicado pelas Nações

Unidas em 2014 devido a um crescimento menor em relação com Uruguai³⁸. Assim sendo, a fim de reverter a situação descrita não só em termos de melhorar seu posicionamento regional, mas também, acelerar o processo de transformação digital, o Estado assumiu a “necessidade de dar maior prioridade às políticas públicas de desenvolvimento digital”. (CHILE, 2015a, p.31, tradução nossa). A Presidente Bachelet, no discurso de lançamento da PNCS, reforçou esse aspecto da liderança regional³⁹, no contexto da cooperação em Cibersegurança e na adoção de padrões internacionais semelhantes a EU; OCDE; OEA; ONU: “Chile aspira a uma posição de liderança na região e abrirá espaços para avançar em um ciberespaço livre, aberto e seguro”. (CHILE, 2017c, p. 4, tradução nossa).

Além disso, não somente a falta de um adequado desenvolvimento de uma política eficiente de governo digital, e a rapidez na implementação no uso das tecnologias digitais contribuíram para determinar a atenção dos formuladores das políticas públicas durante a transformação digital do país, embora esta surgirá segundo Kingdon (2003) desde outra perspectiva, quando eles anteciparem a “existência de consequências negativas que originarão um problema”. (KINGDON, 2003, p. 103, tradução nossa)

Nessa lógica, segundo os documentos que acompanham essa avaliação, “Bases para uma PNCS” (CHILE, 2015c) e AD 2020 (CHILE, 2015a), estabeleceram que a transformação digital, além de produzir ganhos no relacionamento das pessoas com o Estado, também pode gerar vulnerabilidades de segurança no ciberespaço, apresentando-se como uma implicação contraproducente. Assim, o governo da época identificou no primeiro documento sua percepção geral sobre a questão: “Devido à facilidade de acesso à Internet e aos equipamentos de informática, o ciberespaço é uma fonte cada vez mais considerável de riscos e ameaças, situação da qual o Chile não está isento”. (CHILE, 2015c, p.9, tradução nossa).

³⁸ Chile cedeu sua condição de liderança no Índice de Desenvolvimento do Governo Eletrônico (E-Government Development Index em inglês) na América do sul em 2014, ficando no lugar num. 33 a nível global e segundo a nível local, crescendo só 6 lugares dentro do índice. Uruguai atingiu o primeiro lugar na região passando desde a posição num. 50 em 2012 até o lugar num. 26 em 2014. (United Nations E-Government Survey, 2014) Fonte: https://publicadministration.un.org/egovkb/portals/egovkb/documents/un/2014-survey/e-gov_complete_survey-2014.pdf

³⁹ Segundo AD 2020, o que procura o país mediante a liderança digital na região, é manter uma condição de “vantagem competitiva que favoreça positivamente o crescimento econômico do país”. (CHILE, 2015a).

Em termos idênticos, a AD 2020 em particular, mencionou os desafios na segurança no ciberespaço: “A era digital abre possibilidades infinitas, mas também traz novos riscos para a segurança de pessoas e instituições, colocando novos desafios em relação à confiabilidade e privacidade em redes” (CHILE, 2015a, p.30, tradução nossa). Assim, evidencia-se que os responsáveis das políticas digitais, começaram a visualizar de maneira antecipada que a transformação digital, teria efeitos sobre as questões de segurança, o que fornece uma explicação porque nesse mesmo relatório se descrevesse a conveniência de ter uma política de segurança digital. Segundo o relatório escolhido: “é imprescindível e urgente definir uma política do país nesta matéria”. (CHILE, 2015a, p.36, tradução nossa).

Em suma, de acordo com os documentos analisados, pode-se perceber que existiu uma modificação da atenção do governo de acordo com as retroalimentações originadas depois da publicação do relatório do Índice de Desenvolvimento do Governo Eletrônico da ONU⁴⁰ em 2014, que mostrou retrocessos na efetividade, posicionamento do país na região e, na velocidade de avanço das políticas públicas focadas no desenvolvimento digital do Governo. De natureza igual, foram identificadas no percurso das melhorias implementadas nos processos de transformação digital do Estado, uma série de potenciais deficiências de segurança no âmbito digital que comprometeriam atingir os objetivos das diferentes políticas e, o papel do Estado em termos de gerar as condições de segurança para o normal funcionamento do país. Assim, os resultados de ambas as questões exigiram do governo, dar maior prioridade e harmonizar as políticas públicas para um bom desenvolvimento digital, incluindo como um aspecto transversal, a segurança digital, e isso, segundo a AD 2020 é:

O sucesso de um governo digital é dado pelo uso que os cidadãos e os cidadãos dão para as plataformas e serviços disponíveis. Para alcançar rápida mudança cultural na forma como a cidadania e o estado interagir, será melhorada a oferta de serviços públicos com maior impacto social, como segurança, saúde e desenvolvimento social. (CHILE, 2015a, p.36, grifo nosso, tradução nossa)

⁴⁰ Sometimes, the feedback comes to officials in the form of rather systematic monitoring and evaluation studies. (KINGDON, 2003).

4.2.2. O fluxo das soluções ou alternativas (policy stream)

Nesta elaboração de alternativas, como tem sido explicado na abordagem, existem diferentes grupos de participantes que provém de diferentes áreas. Segundo Capella (2018): “As alternativas e soluções são desenvolvidas dentro das comunidades de políticas, compostas por pesquisadores, assessores parlamentares, acadêmicos, funcionários públicos, analistas pertencentes a grupos de interesses, entre outros”. (CAPELLA, 2018, p.41). Assim, segundo Zahariadis (2003), essas ideias são geradas pelos especialistas que competem para que sua ideia seja parte dessa política pública, conseqüentemente, “algumas ideias sobrevivem ao período inicial basicamente sem alterações, não obstante, outros são combinados em novas propostas, e ainda outros simplesmente desaparecem” (ZAHARIADIS, 2003, p. 72, tradução nossa).

Dessa forma, ao analisar o documento “Bases para uma PNCS” (CHILE, 2015c) é válido ressaltar que o projeto da PNCS se realizou por meio de um Comitê de Trabalho Interministerial⁴¹, (CTI) presidida pelo Ministério de Interior y Seguridad pública⁴² e uma secretaria executiva dependente do Ministério da Defesa Nacional (MDN), através de um método de trabalho organizado por seis eixos temáticos de acordo com uma série de orientações específicas⁴³. O fortalecimento da sua organização e a formalização do trabalho da entidade ficaram estabelecida após um mês, pelo Decreto num.533 que criou o “Comitê Interministerial de Cibersegurança (CICS)” em 27 de abril de 2015. O mesmo decreto determinou sua principal missão:

Proponer una política nacional de ciberseguridad, sugerir alternativas de seguimiento a su avance e implementación, y asesorar en la coordinación de acciones, planes y programas en materia de ciberseguridad de los distintos actores públicos y privados en la materia. (CHILE, 2015b)

⁴¹ No mesmo documento foi nomeada também como Comitê Interministerial sobre Cibersegurança.

⁴² Corresponde ao Ministério do Interior e Segurança Pública a coordenação, implementação e avaliação das políticas, planos e programas de segurança pública, para o qual pode solicitar a colaboração das outras organizações que compõem a Administração do Estado, atendendo o âmbito de ação. (CHILE, 2015b)

⁴³ Os eixos foram: Infraestrutura de informação; Prevenção e sanção; Conscientização, treinamento e divulgação; Cooperação e relações internacionais; Institucionalidade da Cibersegurança. (CHILE, 2015c, p.11, tradução nossa)

Da mesma forma, a norma recentemente citada definiu os membros participantes do comitê. Assim, pode-se observar na tabela abaixo a participação de atores permanentes e outros temporais que serão acionados de acordo com as necessidades do comitê.

TABELA 4 – Participantes do CICS

Membros permanentes	Membros Consultivos segundo convite
<ul style="list-style-type: none"> - Um representante da Subsecretaria do Interior. - Um representante da Subsecretaria de Defesa. - Um representante da Subsecretaria de Relações Exteriores. - Um representante da Subsecretaria de Justiça. - Um representante da Subsecretaria Geral da Presidência. - Um representante da Subsecretaria de Telecomunicações - Um representante da Subsecretaria de Economia e Empresas menores. - Um representante da Subsecretaria de Finanças - Um representante da Subsecretaria de Mineração - Um representante da Subsecretaria de Energia - Um representante da Direcção Nacional do Agência Nacional de Inteligência. 	<ul style="list-style-type: none"> - Funcionários da administração pública do Estado ou outras autoridades públicas. - Representantes de entidades internacionais, públicas ou privadas. - Acadêmicos - Agrupamentos da sociedade civil ou setor privado

Fonte: elaborado pelo autor

De acordo com o texto, a comissão é de caráter multissetorial; segundo Viollier (2017), implementou-se esse tipo de modelo devido a infraestrutura das redes digitais, que depende de privados e é gerenciada por diferentes organizações técnicas. Além disso, as análises feitas e descritas no APÊNDICE “A” sobre as Agendas digitais do Chile 2009-2015, oferecem uma explicação sobre a adaptação a esse tipo de modelo ter sido implementada de maneira permanente e sistêmica no Chile desde a primeira AD publicada em 1999.

Em continuidade, pode-se dizer que é um produto que explicita que o desenvolvimento tecnológico é um fator transversal nos âmbitos de transformação da sociedade e, também, como produto das assessorias recebidas por organismos internacionais, que promovem a participação de grupos de trabalhos multissetoriais compostos por diferentes atores do campo público, privado e acadêmico, sendo coerente com a necessidade do país, focalizada na “colaboração, coordenação e sinergia de todas as organizações envolvidas na segurança do ciberespaço, em suas

múltiplas dimensões, de uma perspectiva sistêmica e progressiva”. (CHILE, 2015c, p.1, tradução nossa)

Por outro lado, o Decreto num.533, indicou uma comissão de índole técnico, que assessorou à CICS nas matérias técnicas de Cibersegurança, como a elaboração de protocolos e a coordenação técnica na sua implementação e ações frente os cenários de riscos no ciberespaço. Sua organização considerou um trabalho multidisciplinar com um representante da Subsecretaria Geral da Presidência; da Agência Nacional de Inteligência; da Subsecretaria de fazenda, da Subsecretaria de Defesa e da Subsecretaria do Interior.

Conseqüentemente, a respeito dos ganhos da integração multissetorial, o Secretário Executivo do CICS e Subsecretario da Defesa em 2015 afirmou:

La Política, que se espere esté finalizada en marzo de 2016, buscará promover la identificación y gestión de riesgos en el ciberespacio para que el sector público, privado, la sociedad civil y el mundo académico puedan prevenir, minimizar y sobreponerse a éstos, con especial énfasis en aquellas infraestructuras críticas para el funcionamiento del país. (ROBLEDO, 2015)

Então, segundo Kingdon (2013), essas ideias que vêm e vão, que flutuam no ambiente, que batem entre si, que se misturam, precisam de um clima e tempo apropriado para ganhar força e ter probabilidades de supervivência para se transformarem em decisões políticas. Neste argumento, existiram determinados critérios que permitiram sua supervivência. Dentro da proposição de trabalho proposta para a elaboração de alternativas para a futura PNCS, a análise demonstra que atendeu o critério da “factibilidade técnica” de acordo com uma série de condições e restrições no momento em que começou o trabalho da CICS⁴⁴, as que se orientaram e asseguraram sua viabilidade funcional e operacional⁴⁵, assumindo que era imprescindível desenvolver como questões fundamentais dentro das opções para a futura PNCS: Proteger a segurança das pessoas no ciberespaço; proteger a

⁴⁴ Cada eixo agrupava várias medidas que cumpriam normas internacionais no âmbito das políticas de Cibersegurança e que eram necessárias de acordo com a realidade nacional. Tinham um prazo limite e uma metodologia de trabalho predefinida. (CHILE, 2015c)

⁴⁵ Dentro de suas orientações iniciais estabeleceu: “Uma vez terminadas as sessões, será necessário definir um mecanismo de consulta com outros atores, a fim de socializar e legitimar o trabalho realizado”. Gobierno de Chile, Subsecretaría del Interior del Ministerio del Interior y Seguridad Pública y la Subsecretaría de Defensa Nacional del Ministerio de Defensa Nacional, 2015, p.12, tradução nossa)

segurança do país; Promover a colaboração e coordenação entre instituições; e Gerenciar riscos do ciberespaço. (CHILE, 2015c, p.10, tradução nossa)

Com o objetivo de satisfazer esse critério, segundo Viollier (2017), o CICS conduziu uma série de audiências públicas, que convidaram diferentes atores para comentar o documento “Bases para uma PNCS” (CHILE, 2015c), assim como, responder as diferentes preocupações do comitê sobre a proposição de tópicos não presentes no escrito. Neste sentido, segundo o autor, identificam-se organizações provenientes da sociedade civil, setor privado, instituições públicas, academia, comunidade técnica e pessoas físicas. (VIOLLIER, 2017, p. 11, tradução nossa).

TABELA 5 – Participantes da audiência pública para a elaboração da PNCS

Participantes	Categorização
<ul style="list-style-type: none"> – Fundación País Digital – Derechos Digitales 	Sociedade civil
<ul style="list-style-type: none"> – Cámara de Comercio de Santiago – Asociación Chilena de Empresas de Tecnología de Información – Asociación Gremial de Desarrolladores de Software 	Setor privado
<ul style="list-style-type: none"> – Carabineros de Chile – Defensoría Penal Pública – Fiscalía de Chile – Poder Judicial – Policía de Investigaciones – Servicio de Impuestos Internos 	Instituições públicas
<ul style="list-style-type: none"> – Centro de Estudios en Derecho Informático – Consejo de Rectores – Duoc UC (Universidad) 	Academia
<ul style="list-style-type: none"> – CLCert (Grupo Chileno de Respuesta a Incidentes de Seguridad Computacional) – NIC Chile (Entidad encargada de la administración de nombres de dominio) 	Comunidade técnica

Fonte: adaptado de VIOLLIER, 2017.

Como resultado, é evidente a metodologia desenvolvida pelo comitê e suas interações, procedimentais, técnicas e funcionais, descrito por Kingdon (2013) em relação a tentar, desde um primeiro momento, durante o levantamento de soluções, eliminar gradualmente as inconsistências, aprofundar em detalhes e tecnicismos focados na viabilidade de implementação, como nos mecanismos reais pelos quais a ideia seja realizada, assim, "It's important to do your homework, to be prepared, to do in-depth research, and don't sell people on something that won't work". (KINGDON, 2013, p.131), concentrando-se em 75% das atividades a ser executadas durante o

ano de 2015 de acordo com cronograma de trabalho do documento “Bases para uma PNCS” (CHILE, 2015c).

Do mesmo modo, o processo de consulta a externos do comitê, determina a presença de um segundo critério apontado por Kingdon (2003) como “Value Acceptability”. Segundo Capella (2018), corresponde à solução feita através de valores compartilhados e aceitos pela comunidade de especialistas⁴⁶. Então, observe-se que essa visão de gerar acordos iniciais, criar uma visão compartilhada e aperfeiçoar o trabalho do comitê desde um primeiro momento, não somente foi ratificada no impresso de “Bases para uma PNCS” (CHILE, 2015c), senão também, foi alentado em 2015 pelo Secretário Executivo do CICS durante a etapa de elaboração de alternativas para PNCS: “Este Comité interministerial ya está abocado a la tarea de elaborar una política nacional de ciberseguridad, que fije una visión común y una hoja de ruta que nos permita enfrentar este tema de una manera integral y armónica”. (ROBLEDO, 2015, grifo nosso).

Dessa maneira, aprecia-se uma vinculação dos participantes (institucionais e comunidade de especialistas) através de uma configuração institucional que facilitou o diálogo transversal, gerou maior integração e concordâncias e admitiu um acesso restrito nesta parte da elaboração das propostas⁴⁷, a fim de alcançar os objetivos previstos para a elaboração da política pública dentro dos limites de janela de funcionamento dos 13 meses que foram estabelecidos.

Em função dos resultados, é possível perceber o ressaltado por Capella (2018) quando, a partir das propostas feitas por Kingdon, expressa como um elemento para essa condição de supervivência das ideias, o levantamento de soluções com custos antecipados e toleráveis. Dessa forma, os documentos analisados mostram que foi um tema considerado no levantamento de opções, porém, foi restrito ao orçamento institucional de cada organismo público participante, sem maior relevância na discussão:

⁴⁶ Existem diferentes de incentivos, dentro dos quais: “people sometimes advocate proposals because they want to promote their values or affect the shape of public policy”. (KINGDON, 2003)

⁴⁷ Institutional configurations, or, to put it differently, the level of integration, differ across countries, affecting the mode and tempo of ideas, that is, how ideas germinate in the policy stream and how fast they rise to prominence. Integration refers to linkages among participants and is distinguished by variations in four dimensions: size, mode, capacity, and access. (ZAHARIADIS, 2007)

En el marco de lo conversado en la primera sesión, las instituciones participantes podrán hacer una estimación del presupuesto que deben considerar en materia de ciberseguridad para el año 2016 y consignarlo en la programación que deberán entregar a sus respectivas autoridades. (CHILE, 2015c, p.12)

Entretanto, um dos tópicos relevantes na contenda das ideias que se mantem no tempo, segundo Kingdon (2014), corresponde aqueles que são aceitos pelo público em geral, indistintamente se são um maior ou menor número de pessoas. Neste sentido, segundo Viollier (2017), foi desenvolvido o processo de consulta pública⁴⁸ para validar as impressões e recomendações compiladas na etapa das audiências públicas em relação a proposta que ocasionou o trabalho, como as desenvolvidas pela própria CICS que foram descritas no rascunho da futura PNCS.

Este rascunho foi submetido para consulta pública, de acordo com a Lei 20.500 sobre Associações e Participação Cidadã na Gestão Pública, entre 29 de fevereiro e 18 de março de 2016. A entrada de comentários foi feita por meio de um formulário online, no qual os participantes eles tiveram que se identificar e a instituição eles representaram. O formulário continha dois questões abertas, uma de natureza geral sobre o documento e outro solicitando apontar erros de fato ou apreciação. Logo, foi dado um espaço para comentar sobre cada um dos cinco eixos estratégicos, o quadro institucional e o medidas de política pública 2017-2018. Após a conclusão do processo de consulta pública, os comentários dos participantes foram feitos público no site do CICS⁴⁹. (VIOLLIER, 2017, p. 10, grifo nosso, tradução nossa)

Desse modo, no lançamento da PNCS, a presidenta Bachelet fez um destaque das contribuições ocorridas durante o procedimento de ponderação da política: “se sometió al proceso de consulta pública que establece la ley N°20.500 sobre participación de la sociedad civil, donde se recibieron numerosas contribuciones que sin duda ayudaron a mejorar la propuesta”. (CHILE, 2017a, p. 5).

Segundo a análise Viollier (2017), participaram cerca de 43 entidades provenientes de variados setores da sociedade chilena, corroborando-se uma participação maioritária do setor privado e empresas relacionadas com as TICs, concentrando a atenção nos eixos de Infraestrutura e institucionalidade. Conforme

⁴⁸ A consulta pública foi estabelecida na Lei 20.500 sobre Associações e Participação Cidadã na Gestão Pública. Dessa forma, o Estado reconhece que as pessoas têm o direito de participar de suas políticas, planos, programas e ações através de diferentes modalidades de participação. A consulta deve ser realizada de forma informada, pluralista e representativa. As opiniões recolhidas serão avaliadas e ponderadas pelo respectivo órgão, da forma que a norma de aplicação geral indica.

⁴⁹ O web site de CICS já não está disponível e em funcionamento.

Robledo, durante o processo de consulta pública, foram recebidas mais de cinquenta observações, comentários e críticas. (CHILE, 2017a). A tabela abaixo mostra as principais modificações inseridas depois da consulta pública.

TABELA 6 – Modificações inseridas no rascunho da PNCS após da consulta pública.

Objetivo	Eixos inseridos no documento Bases para PNCS 2015 (março 2015)	Modificações sugeridas pela consulta pública (fevereiro 2016)	Objetivos da PNCS 2017 (abril 2017)
Objetivo A	Infraestrutura de informação	<ul style="list-style-type: none"> – Adicionar uma definição do conceito de CS. – Mencionar que a expansão da capacidade de vigilância estatal ou privada não faz parte da estrutura de CS. – Controlar e monitorar a segurança dos sensores e dispositivos operados do ciberespaço. – Promover a criação de CSIRTs setoriais por diferentes órgãos. 	Ter uma infraestrutura de informação capaz de suportar e se recuperar em caso de ataques e incidentes de cibersegurança
Objetivo B	Prevenção e sanção	<ul style="list-style-type: none"> – Mudança do título: "O Estado deve assegurar os direitos das pessoas no ciberespaço, por meio da prevenção e punição efetiva de crimes, garantindo pleno respeito aos direitos humanos" ao referido na coluna da direita. – Promover a criptografia ponto a ponto. – Incrementar a proteção dos direitos de grupos vulneráveis e abordagem de gênero. 	Garantir os direitos das pessoas no ciberespaço
Objetivo C	Conscientização, treinamento e divulgação	Não apresenta diferenças significativas	Desenvolver uma cultura de cibersegurança em torno da educação, boas práticas e responsabilidade na gestão de tecnologias digitais
Objetivo D	Cooperação e relações internacionais	A Adesão à Convenção de Crime Cibernético, deve ser feito através de reservas e cautelas coerentes com o PNCS	Estabelecer relações de cooperação em cibersegurança com outros atores e participará ativamente de fóruns e discussões internacionais
Objetivo E	Institucionalidade da Cibersegurança	Não apresenta diferenças significativas	Promover o desenvolvimento de uma indústria de cibersegurança que atenda aos seus objetivos estratégicos

Fonte: adaptado de VIOLLIER, 2017; de Bases para PNCS, 2015; da PNCS, 2017.

Enfim, as alternativas e soluções para a futura PNCS foram desenvolvidas dentro das comunidades de políticas formadas pelos representantes de setores do poder Executivo (ministérios e subsecretarias), acadêmicos, funcionários públicos, analistas pertencentes a grupos de interesses e outros provenientes da sociedade civil com a finalidade de conceber opções de maneira sinérgica, abrangente e sistêmica. Da mesma maneira, a construção de diferentes instâncias de audiências públicas com especialistas, as quais têm sua origem desde as primeiras políticas públicas digitais geradas em 1999, como as consultas públicas realizadas em 2016 que permitiram referendar o trabalho desenvolvido pelo CICS para dar garantia à validade a sua elaboração, viabilidade na sua implementação e assegurar a aceitação das ideias consignadas nas propostas pela própria sociedade, bem como no cumprimento dos prazos previsto na sua elaboração.

4.2.3. O fluxo político (political stream)

De acordo com Zahariadis (2007), quando nos referimos ao humor nacional, refere-se à noção de que um número grande de indivíduos de um determinado país tende a pensar de forma semelhante a respeito de algumas questões, mas que podem existir mudanças durante o tempo. Nessa perspectiva, essas mudanças são monitoradas por meio de pesquisas da opinião pública, ações de funcionários do governo para promover certos itens da agenda ou, inversamente, para obscurecer as perspectivas dos outros. Assim, Capella (2018) enfatiza a importância de identificar as características do humor nacional porque cria ou inibe um ambiente para a promoção de algumas ideias.

Neste cenário, o desenvolvimento da PNCS aconteceu durante o segundo Governo de Michele Bachelet (2014-2018) que alcançou a máxima magistratura do país representando a coligação política da “Nueva mayoría”, depois de obter no segundo turno das eleições do 2013 um 62,17% dos votos⁵⁰. Ao início de seu mandato, em maio 2014, apresentou suas prioridades políticas e a forma de promover suas ideias de governo durante sua mensagem presidencial ao Congresso Nacional:

⁵⁰ Serviço Eleitoral do Chile, Fonte: <https://oficial.servel.cl/elecciones-presidenciales-resultados-globales/>.

Y aquí me refiero específicamente a temas tan relevantes como la salud, la vivienda, las relaciones laborales, calidad de vida, cultura, transporte, deporte, lo que unido a un potente programa económico⁵¹ y energético que genere crecimiento y empleo, serán las grandes prioridades de mi gobierno.

Esta propuesta de cambio interpela a todas las fuerzas políticas y sociales del país. Así como antes fuimos capaces juntos de poner a Chile en la senda del crecimiento económico con democracia, hoy necesitamos hacer un nuevo esfuerzo para que el desarrollo y el crecimiento sean más armónicos e integrales.

Y quiero ser muy clara en este punto: durante mi gobierno haremos las transformaciones que prometimos y las haremos con gobernabilidad, paz social, de manera democrática y transparente. Gobernaremos dialogando con todos los sectores, las veces que sea necesario, pero con el objetivo claro de que como país debemos avanzar en una sociedad con menores desigualdades y que le dé bienestar a todos y todas. (CHILE, 2014a, p. 4, grifo nosso)

Por sua vez, a conjuntura política do país durante a definição da agenda teve uma evolução significativa em termos dos níveis de confiança nas instituições, os apoios à gestão do governo e as principais coligações políticas. Segundo os dados aportados pelo CEP desde julho 2014 até o período abril-maio 2017⁵², a situação política do país expressava, no período analisado, uma perda significativa da confiança cidadã em relação com Governo, Congresso e partidos políticos; bem como, um incremento nos índices de desaprovação do Governo de Bachelet⁵³. Assim como, uma mudança da aprovação cidadã em relação as principais coligações políticas, e o predomínio de uma percepção social de “regular” respeito ao funcionamento da democracia no Chile⁵⁴.

Assim, na perspectiva da percepção cidadã, aprecia-se uma significativa redução de confiança dentro dos principais órgãos que impulsionam as ideias para a criação das políticas públicas. Ao mesmo tempo, a própria Presidente ratificou essa situação durante sua mensagem presidencial em maio do 2017 ao Congresso Nacional quando proferiu: “La política chilena vive un momento difícil. Se ha debilitado

⁵¹ Inicialmente, as AD foram parte das temáticas inseridas nas agendas de desenvolvimento econômico dos diferentes governos.

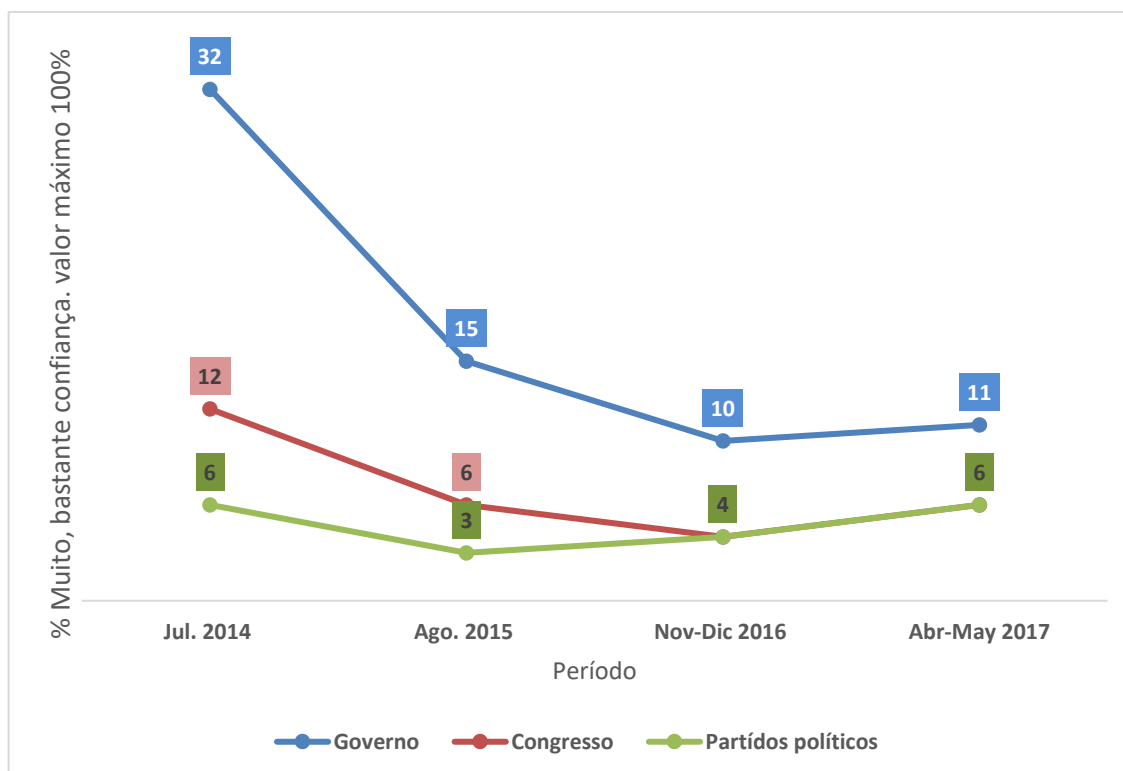
⁵² Em abril do 2017, foi publicada a versão final da PNCS.

⁵³ O 19 de novembro do 2017 foram realizadas as eleições presidenciais para o período 2018-2022.

⁵⁴ Segundo os dados do Estudo nacional de Opinião Pública N.79 existe uma média de um 54,2% dos entrevistados escolheram essa preferência. (CENTRO DE ESTUDIOS PÚBLICOS (CEP), 2021)

la confianza entre los ciudadanos, sus representantes y las instituciones, sean ellas del Estado o privadas". (CHILE, 2017d, p. 32, grifo nosso).

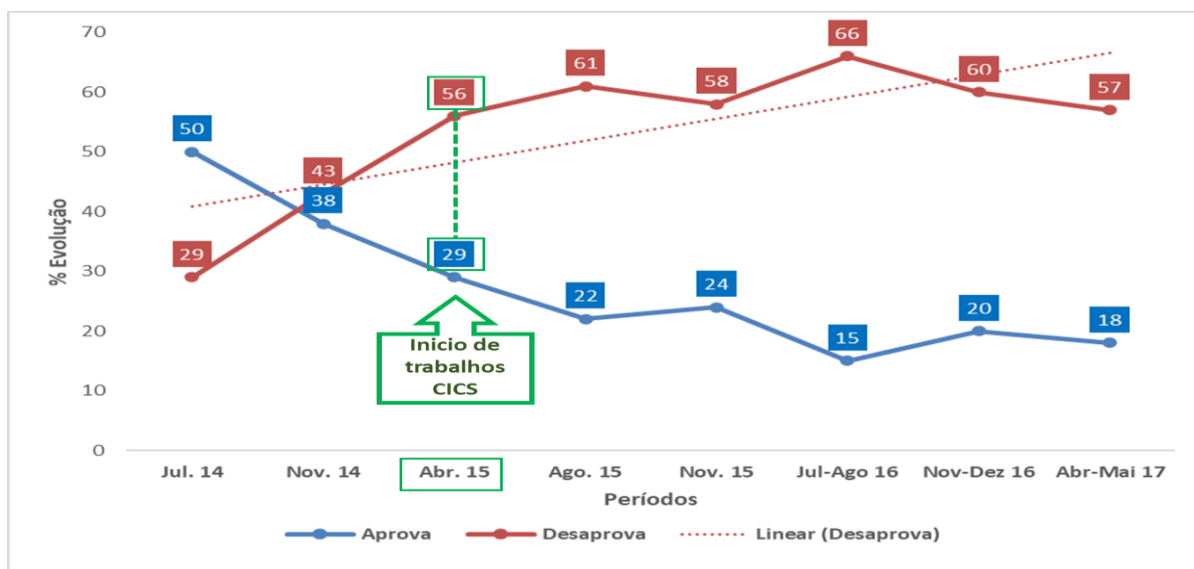
FIGURA 9 - Evolução da percepção de confiança cidadã em relação com Governo, Congresso e partidos políticos.



Fonte: O autor baseado nos Estudos nacionais de Opinião Pública N.79 (CENTRO DE ESTUDIOS PÚBLICOS (CEP), 2017)

Na figura abaixo, observa-se uma forte tendência de diminuição do apoio ao Governo, referente ao momento de início dos trabalhos do CICS em 2015. Em maio deste ano, a Presidente percebeu essa realidade social: "Los chilenos y chilenas son exigentes, porque han trabajado duro y quieren un país a la altura de sus esfuerzos y méritos. No quieren un Estado, una economía y una política ajenos a sus aspiraciones". (CHILE, 2015d, p. 3, grifo nosso).

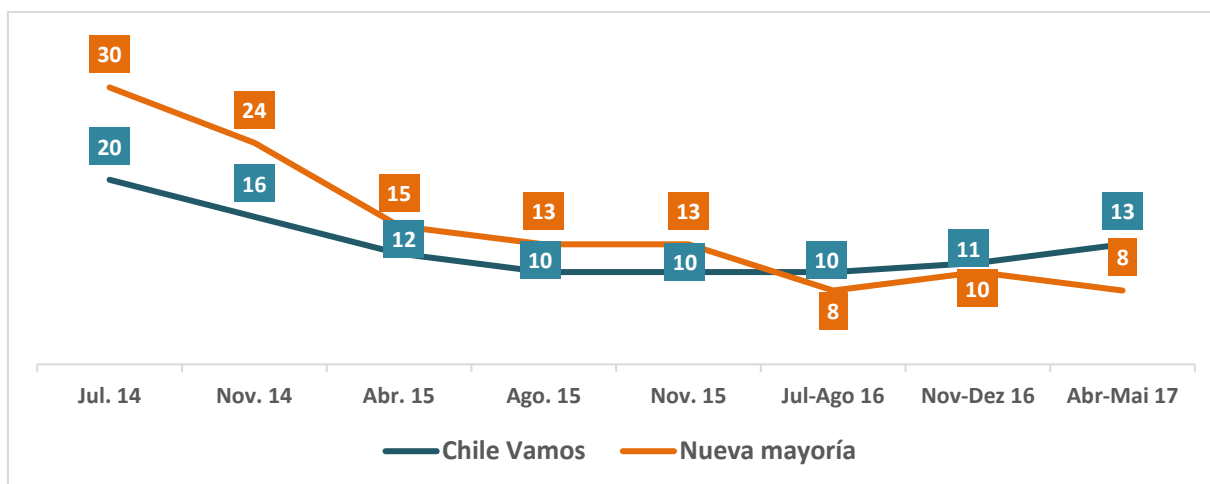
FIGURA 10 - Evolução da percepção cidadã em relação com Governo de Bachelet.



Fonte: O autor baseado nos Estudos nacionais de Opinião Pública N.79 (CENTRO DE ESTUDIOS PÚBLICOS (CEP), 2017)

Na mesma tendência, de acordo com os dados do CEP, as principais forças políticas do país representadas como coligações políticas de maior representatividade no Congresso Nacional, vivenciaram diferentes níveis de aceitação por parte da população. Na figura abaixo, pode ser observada a evolução da percepção cidadã sobre o desempenho político destas.

FIGURA 11 - Evolução da aprovação cidadã em relação com as principais coligações políticas representadas no país.



Fonte: O autor baseado nos Estudos nacionais de Opinião Pública N.79 (CENTRO DE ESTUDIOS PÚBLICOS (CEP), 2017)

Embora, a aparição dessas percepções que condicionaram o clima ou humor nacional com questões diferentes e ideias desfavoráveis as estimativas do governo, o estudo demonstra que foram recebidas e aceitas durante o mandato. Assim, evidencia-se uma atitude do governo de agir em maior profundidade frente à situação política que estava caminhando em uma direção contrária a suas estimações. Dessa forma, como resposta a essas demandas, priorizou o cumprimento de suas ideias políticas inseridas no seu programa de governo⁵⁵ que balizaram seu projeto para a sua chegada ao poder. Nesse cenário, a Presidente expressou:

La institucionalidad de Chile tiene las capacidades para ponerse al nivel de las demandas de sus ciudadanos y a tono con las exigencias del siglo XXI. Sin duda, podemos más. Por eso nos comprometimos con los ciudadanos a emprender esos cambios. Y ese compromiso está plasmado en nuestro programa.

En este primer año hemos avanzado actuando con determinación. Hemos hecho reformas históricas, de las que hoy daré cuenta. Promulgamos leyes largamente esperadas, ejecutamos nuestros programas y presupuestos, tomamos medidas para estimular la economía, hemos mantenido y ampliado los servicios públicos del Estado, enfrentado emergencias, dialogado con la sociedad y trabajado con el sector privado; fortalecido nuestros lazos con el mundo y promovido la paz. (CHILE, 2015d, p. 4, grifo nosso).

Consequentemente, corrobora-se que existiu um panorama de demandas sociais no país em 2015 sobre o qual o governo necessitava de um determinado consenso político para criar um ambiente favorável para o desenvolvimento de suas propostas governamentais que sustentassem o seu ideário, dentro das quais se encontrava a PNCS. Segundo Kingdon (2004), a construção desse consenso na arena política, ocorre por meio de um processo de negociação. A partir desse ponto de vista, justifica-se a convocação da Presidente para estabelecer um espaço de diálogo político amplo para construção de um melhor país no contexto político-social, que se configurou a partir da tomada de posse em março de 2014:

Este es el sello que le he impuesto a mi gobierno en esta nueva fase que iniciamos y he demandado de mis colaboradores una acción más eficaz, acorde a las exigencias ciudadanas y a las necesidades del país.

Y hoy los convoco a todos, hombres y mujeres, trabajadores, estudiantes, profesores, parlamentarios y científicos, artistas y emprendedores, partidarios de la coalición de gobierno y de la oposición, a reconstruir nuestras

⁵⁵ O Programa de Governo, Michelle Bachelet 2014-2018, “Chile de todos” foi publicado em outubro de 2013 (CHILE, 2013b).

confianzas, a trabajar unidos y en diálogo franco y transparente para aprovechar esta oportunidad histórica. (CHILE, 2015d, p. 5, grifo nosso).

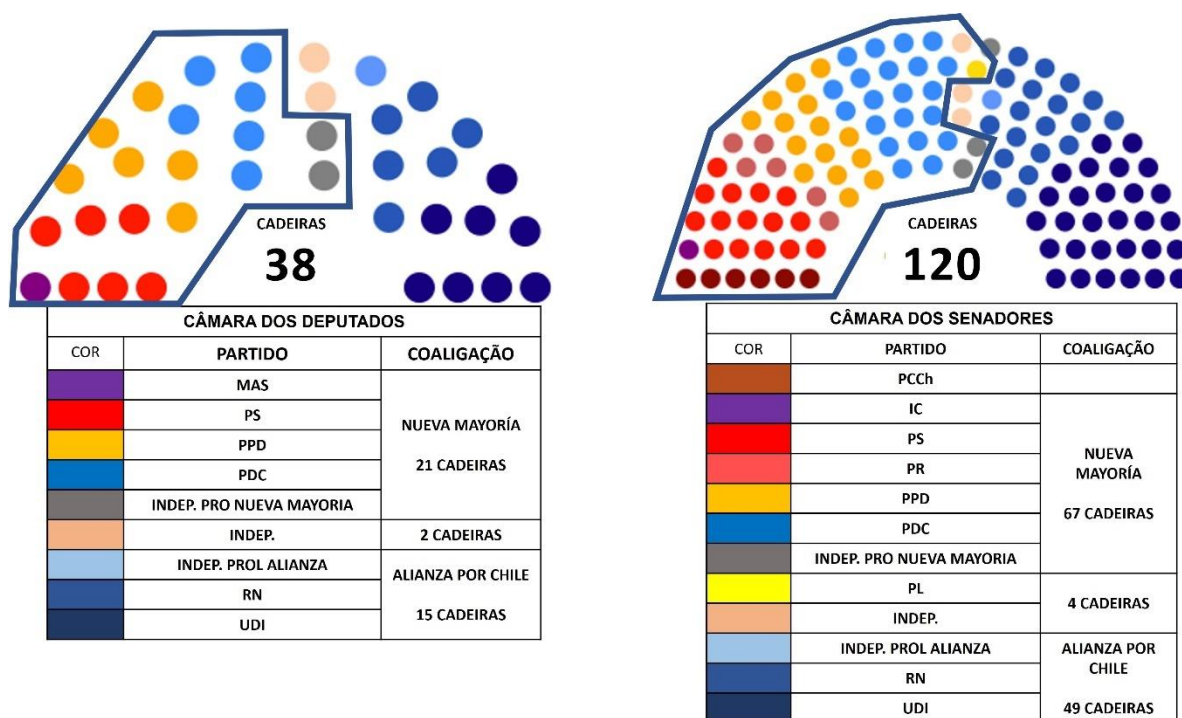
Como um aspecto chave, o governo tinha o patrocínio da coligação política “Nueva mayoría”⁵⁶ que era a maior força política do país, sendo parte ativa desse governo, razão que fosse catalogado pela própria Presidente como o “Gobierno da Nueva mayoría”.

Segundo Bachelet, para cumprir com o propósito dessa coligação com boa governança e segurança das transformações políticas com governabilidade, era necessário “incorporar e privilegiar os interesses de todos sobre os benefícios e interesses de alguns” (CHILE, 2013b, p. 7, tradução nossa). Desta forma, o Governo tinha muito consenso dentro de seu próprio pacto político para levar suas aspirações políticas, ao cumprir as premissas expressadas por Kingdon (2014) em relação a avaliação do nível de consenso dentro de uma força política organizada: a existência de um acordo generalizado entre essas forças, as frequências ou intensidade de suas comunicações e, o nível dos recursos disponíveis dos vários grupos que o conformam.

A figura abaixo, mostra a distribuição de lugares no parlamento durante o segundo mandato de Bachelet com destaque no maior predomínio da Coligação governante nas respectivas Câmaras do Congresso Nacional. Mesmo assim, tinha em torno de 55% dos lugares dos Deputados e 56% dos Senadores. Além disso, segundo Serviço Eleitoral do Chile (2021), a composição apresentada teve sua origem nas eleições parlamentares feitas em 2013 e começou seus labores em 11 março de 2014, no mesmo dia que começava o segundo mandato de Bachelet (CHILE, 2014b).

⁵⁶ A “Nueva Mayoría” foi uma coalizão político-eleitoral fundada em 30 de abril de 2013, por partidos e movimentos de centro e esquerda. Foi composta pelo Partido Demócrata Cristão, o Partido Socialista do Chile, o Partido para a Democracia, o Partido Social-Democrata Radical, o Partido Comunista do Chile, o Partido Cidadão de Esquerda do Chile e o Movimento Social Amplo. Nas eleições presidenciais daquele ano, ela apoiou Michelle Bachelet Jeria, Presidente da República no período 2014-2018, como parte de seu governo. Fonte: Biblioteca nacional do Congresso, https://www.bcn.cl/historiapolitica/partidos_politicos/wiki/Nueva_Mayor%C3%ADa.

FIGURA 12 – Distribuição de lugares no Congresso Nacional do Chile, período 2014-2018.



Fonte: adaptação baseada nos dados históricos do Serviço Eleitoral do Chile⁵⁷.

Não obstante, devido as particularidades do sistema político chileno, a futura PNCS não foi discutida formalmente no Congresso nacional, na medida em que apenas é uma diretriz com visão de Estado, tornando-se, segundo Barrios (2018) no primeiro instrumento de política do governo tendendo a desenvolver uma estratégia nacional nesta matéria, sem que exista uma lei sobre Cibersegurança no Chile até hoje⁵⁸. Entretanto, de acordo com análise efetuada durante o período entre o 10 de março 2014 até 20 de abril 2017 na câmara de deputados⁵⁹, existiram outras tentativas de formação de leis específicas no âmbito do ciberespaço, dessa forma, foram apresentadas duas moções parlamentares para modificar a lei nº 19.223 sobre delitos digitais.

Consequentemente, segundo Kingdon (2014), um dos maiores propulsores de modificação da agenda governamental está constituído pelas mudanças de governo

⁵⁷ Fonte: <https://www.servel.cl/infografias-de-resultados-electorales-2/>

⁵⁸ De acordo com o Ministerio del Interior y Seguridad Pública ainda constitui o grande desafio da Cibersegurança no Chile. Fonte: <https://www.camara.cl/pdf.aspx?prmID=176320&prmTIPO=DOCUMENTOCOMISION>

⁵⁹ N° Boletín: 10145-07 do 18Jun.2015.

(Turn over) e as transformações do clima nacional. Neste caso, a existência de um novo mandato presidencial em 2014 permitiu gerar as condições políticas para o desenvolvimento de uma política pública para o ciberespaço através de diferentes etapas, cumprindo com os objetivos de seu programa de governo onde estava inserido o desenvolvimento de uma Estratégia de CS.

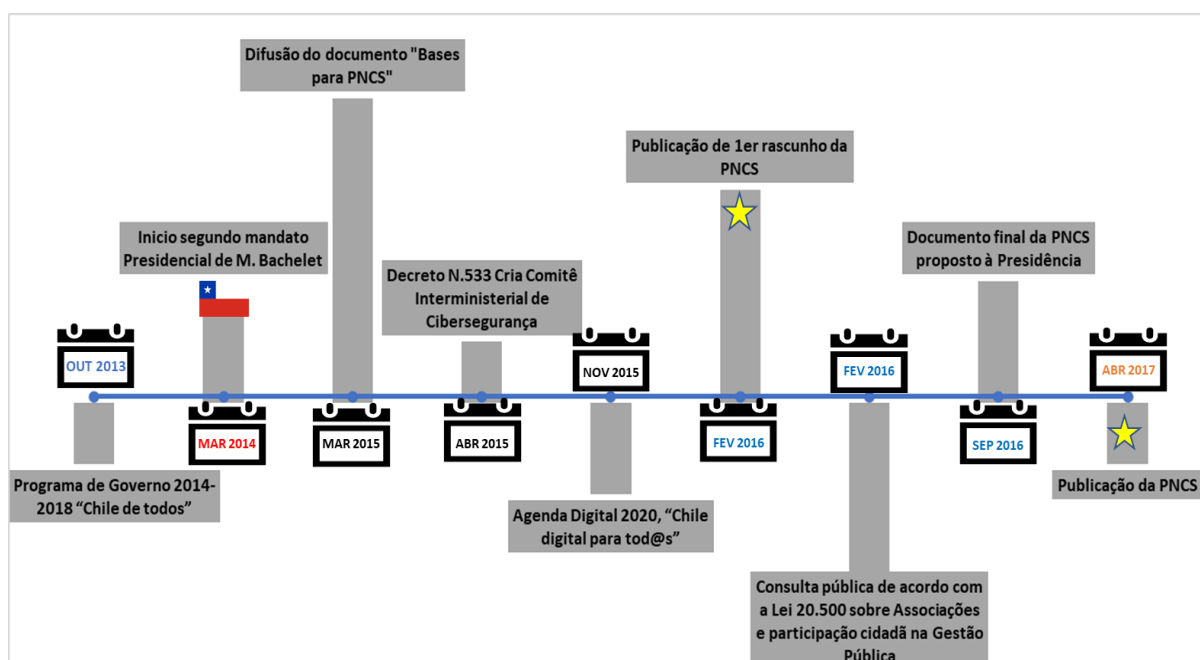
Em suma, a respeito do clima nacional, os discursos presidenciais analisados permitem inferir que o Governo de Bachelet percebeu a existência de um ambiente com amplas questões sociais, gerando uma decisão política orientada para a satisfação destas, por meio da consolidação de seus projetos e aspirações políticas inseridas no seu programa de governo, que lhes permitiram ser escolhidas, mediante a uma busca permanente de consensos políticos com forças pertencentes a seu espaço, bem como, forças políticas contrárias e a cidadania em geral. Entre outros fins, está a necessidade de agilizar a tramitação e conseguir validação popular. Não se levantaram antecedentes a respeito da geração de discussões políticas sobre a necessidade de contar com uma futura PNCS devido a obediência de uma faculdade presidencial⁶⁰ a respeito do ditame de suas instruções específicas para o desenvolvimento da política, tramitação legal e aceitação por parte da população a entaves da consulta pública⁶¹, executada durante e posteriormente ao trabalho da comissão.

Através dos dados prévios levantados durante a análise dos diferentes fluxos executados, apresenta-se um Timeline sobre os eventos que marcaram o percurso para a publicação da PNCS.

⁶⁰ Segundo artigo segundo 32, número 6 da Constituição Política da República do Chile.

⁶¹ Lei 20.500 sobre Associações e Participação Cidadã na Gestão Pública.

FIGURA 13 – Sequências de acontecimentos que originaram a PNCS.



Fonte: Elaborado pelo autor.

4.3 JANELAS DE OPORTUNIDADE (POLICY WINDOWS)

Pode-se estimar que ao longo do período analisado (2014-2017), há dois momentos que abriram janelas de oportunidade política. Segundo Capella (2018) esses momentos surgem de circunstâncias em que há uma convergência dos fluxos dos problemas e dos políticos, permitindo o ingresso de diferentes questões na agenda (abertura da janela), na medida em que a permanência de um problema consegue captar a atenção do governo ou gera mudanças no ambiente político, portanto, gera-se uma oportunidade para essa mudança acesse à agenda.

O primeiro momento que marcou a abertura da janela foi a mudança do Governo do país, com a chegada ao poder da Presidente Bachelet em 2014 e o começo da sua administração. Segundo Zahariadis (2007) "Coupling takes place during open windows when certain policy makers happen to be in power". (ZAHARIADIS, 2007, p. 74). Nesta dinâmica, o novo governo ao início de seu período tinha um apoio majoritário do eleitorado e a representação da superior coalizão política do país. Em março de 2015, data de difusão do documento matriz para a futura PNCS, o governo tinha um 29% de aprovação popular (observe a Figura 10), além disso, contava com

suficiente informação multifatorial devido aos variados antecedentes fornecidos pelos ministérios e dados das pesquisas registradas durante os anos 2014 e 2015⁶² para tomar uma decisão sobre impulsionar na sua agenda governamental, logo, acrescenta-la de decisão, a elaboração da PNCS. De acordo com tabela abaixo, pode-se apreciar o diagnóstico da situação digital do país nesse período, o que justificaria uma intervenção estatal, portanto, a abertura de uma janela política.

TABELA 7 – Diagnóstico da situação digital do país em 2015.

-Importância das tecnologias de rede.
-Altas taxas de uso de internet.
-Tecnologias emergentes (IoT, Big Data, automação etc.)
-Aumento das ameaças e sofisticação dos ataques.
-Falhas de segurança e invasões que afetam as infraestruturas, capacidades e direitos.
-Carência de uma cultura de Cibersegurança.
-Ausência de uma política abrangente de Cibersegurança.

Fonte: Adaptado dos dados da Secretaria executiva do CICS.

Dessa forma, sob a premissa do cumprimento de seu próprio ideário político e o reconhecimento de um cenário social propício a esse projeto político. Sendo assim, a janela de oportunidade estava suscetível aos fluxos dos problemas. O governo, portanto, atuou decididamente para inserção desta questão já reconhecida⁶³ na agenda de prioridades políticas, destinando uma série recursos por meio de um planejamento publicado no documento “Bases para PNCS” (CHILE, 2015c), que dá conta de um problema monitorado constantemente pelas instituições estatais, associadas à segurança pública com maior ênfase a partir do triênio 2010-2013.

Foi tomada assim, a decisão de gerar uma estratégia nacional a partir do trabalho de um comitê intersetorial para fornecer às pessoas um nível de segurança que lhes permitisse o desenvolvimento normal de suas atividades pessoais, sociais e comunitárias no ciberespaço, assim como, evitar uma afetação a segurança pública, e até mesmo ao comprometimento da segurança externa do país, entre outros.

⁶² Alguns dos dados foram apresentados na parte dos indicadores e resultados das pesquisas CEP.

⁶³ Foi parte de seu programa de governo em 2013 (CHILE, 2013b).

Além da existência de uma mudança na administração do país, segundo Kingdon (2014), existem outras junções de fluxos de problemas e políticos que condicionam a abertura da janela de oportunidades. Desse modo, o autor descreve que a presença de um novo problema pode chamar a atenção de funcionários do governo. Neste sentido, a questão da segurança no ciberespaço, sob a responsabilidade estatal no Chile se posiciona como um problema de predominância recente na dinâmica social e política.

Ao examinar o desenvolvimento das ADs, as expressões relativas à segurança para o cidadão no mundo digital começaram a ser identificadas somente a partir da AD “Imagina Chile” 2013-2020, entendendo que as AD anteriores focaram sua atenção ao desenvolvimento digital nos âmbitos econômicos, sociais, educacionais e de infraestrutura digital⁶⁴.

Além disso, as deficiências de segurança digital e eventuais carências de resposta estatal no âmbito digital aludidas no fluxo dos problemas, tais como, o aumento das estatísticas de ações delitivas originadas no ciberespaço ou acréscimo no número de atividades de ciberataques, acontecidos contra a RCE, aparecem como uma dificuldade em maior ou menor medida, que pressionou ao governo. Assim, é coerente uma diretriz principal do futuro trabalho da PNCS, a fim de reverter a situação descrita de “melhorar os estândares de segurança digital do país” (CHILE, 2017a, p.9, tradução nossa).

Em síntese, os fluxos identificados provem por um lado, da corrente política, delineada como a mudança do governo, por outro, da corrente dos problemas, ao se identificar a existência de uma questão que requeria a atenção do governo em decorrência das brechas de segurança detectadas. De tal modo segundo Kingdon (2014), pode-se destacar que os fluxos separados chegam juntos em momentos críticos, como foram os déficits de seguranças descritos a partir do 2013. Dessa forma, existiu um problema relativo a segurança digital, que foi reconhecido pela comunidade política, a partir de então, iniciou-se o processo de acordar uma solução dentro da comunidade de políticos e especialistas que esteve receptiva frente a essa situação,

⁶⁴ Observe APÊNDICE A

consolidando essa aspiração após a mudança na administração do governo de forma periódica e previsível.

Consequentemente, a junção desses fluxos permitiu a abertura da janela política para a elaboração da política pública de CS em um tempo definido, cumprindo-se o afirmado pelo Kingdon (2014) que argumentou que quando se fundem os três componentes essenciais: problema, solução e receptividade política em um único elemento, aumentam drasticamente as probabilidades que esse problema ascenda até a agenda de decisão, como aconteceu no nosso caso.

4.4 EMPREENDEDORES DE POLÍTICAS (POLICY ENTREPRENEURS)

De acordo com Kingdon (2014) os empreendedores de políticas são indivíduos que empurram suas ideias de muitas maneiras dentro do contexto político, estando dispostos a investir recursos de vários tipos para um retorno positivo no futuro, de acordo com os seus propósitos. Neste sentido, de acordo com decreto num.533 que criou o CICS e determinou que sua estrutura estivesse presidida pelo Ministério de Interior y Segurança pública⁶⁵ acompanhada pela secretaria executiva sob a responsabilidade do Ministério da Defesa Nacional (CHILE, 2015b). Dessa forma, assumiram a presidência do comitê, o subsecretario do Interior, Sr. Mahmud Aleuy P., e como Secretário Executivo, o Subsecretario de Defesa, Sr. Marcos Robledo H. Assim, cumpriram as tarefas descritas por Kingdon (2014) a respeito de acoplar na janela de política aberta, prováveis soluções para diferentes problemas, superação as restrições e óbices, através da reformulação de propostas e do aproveitamento de eventos politicamente propícios.

O caso de Aleuy, encontra-se ligado a questão da CS e de outras demandas relativas à segurança pública desde antes de assumir-se formalmente como subsecretario do Interior, ao participar da preparação das novas funções, de uma tentativa de projeto prévio a investidura no governo para a criação de um novo Centro de comando e Cibersegurança. (REVISTA DE DEFENSA Y SEGURIDAD EN ESPAÑA Y LATINOAMÉRICA, 2014). Já em 2014, como Ministro do interior sub-

⁶⁵ Corresponde ao Ministério do Interior e Segurança Pública a coordenação, implementação e avaliação das políticas, planos e programas de segurança pública, para o qual pode solicitar a colaboração das outras organizações que compõem a Administração do Estado, atendendo o âmbito de ação. (CHILE, 2015b)

rogante cumprindo as responsabilidades de sua pasta, assistiu à comissão de Defesa do Senado para assumir a elaboração do futuro relatório sobre o estado de vulnerabilidade física e jurídica do país, bem como, dar conta do estado de avance da CS no país⁶⁶:

"La cartera tiene un conjunto de facultades legales para abordar este tema. Estamos trabajando hace un tiempo en esto y en la etapa actual estamos estableciendo con nitidez un concepto que podríamos llamar "moderno" de la ciberseguridad, además de un conjunto de medidas adicionales, tanto en el campo nacional como en el internacional, como son por ejemplo la identificación de la infraestructura crítica del país, los equipos de respuesta que habría que armar para eso y un conjunto de otras materias". (CHILE, 2014d)

Dessa forma, é ressaltado que as funções que assumiu o ministério mencionado e suas autoridades estão relacionadas ao papel estabelecido pelo decreto num.533 e ao âmbito de suas competências legais referentes à coordenação, implementação e avaliação das políticas de segurança pública. Por outro lado, em relação a figura do Subsecretario Robledo, sua função concerne à cooperação demandada pelo ministério do interior, às próprias da secretaria executiva e aquelas específicas da Defesa nacional (CHILE, 2015b). Ainda assim, as duas autoridades serão as faces públicas e principais protagonistas da futura PNCS, sendo responsáveis por apresentar o documento final da PNCS.

Da perspectiva de análise do Congresso nacional, em particular, no trabalho parlamentar de ambas as câmaras, de acordo com os dados históricos fornecidos pela Biblioteca do Congresso nacional do Chile⁶⁷ a respeito das participações sob o título de "Cibersegurança", se obtiveram os seguintes resultados para o período 2014-2017:

TABELA 8 – Trabalho parlamentar sobre a CS no período 2014-2017

Sessão / data	Câmara / intervenientes	Tema
Sessão Ordinária núm. 55 14 de outubro de 2014	Senado / senadores Sr. De Urresti, Sras. Allende e Muñoz. Sr Chahuán e Rossi.	Realizar gestões para a adesão do Chile à convenção de crime cibernético ou de Budapeste.

⁶⁶Fonte: <https://www.senado.cl/noticias/ciberseguridad-ministerio-del-interior-elaborara-informe-sobre-el>.

⁶⁷Fonte: <https://www.bcn.cl/laborparlamentari> (CHILE. Congreso Nacional de Chile, Senado, 2014)[a/wsgi/consulta/resultados.py?texto=CIBERSEGURIDAD#arriba](https://www.bcn.cl/laborparlamentari)

Sessão / data	Câmara / intervenientes	Tema
Sessão Ordinária núm. 63 16 de novembro de 2016	Senado / senadores Sr. Chahuán, Sr. Larraín Sr. Pizarro, Sr. Prokurica	Minuta de acordo, em segundo processo constitucional, aprovando o "Acordo sobre o crime cibernético"
Sessão especial núm. 64 23 de novembro de 2017	Senado / senadores Sr. Prokurica ⁶⁸	Discussão de pressuostos para o setor público de 2018 sobre aspectos da cibersegurança.

Fonte: O autor.

Neste seguimento, identifica-se que as participações dos parlamentares no que diz respeito a CS estiveram radicadas na Câmara do Senado, por meio do trabalho da comissão de defesa. Sobre esse aspecto, se apresentam os resultados da busca no sítio web da Câmara de Senado⁶⁹ para o período de 2014 a 2017 com seleção das sessões que trataram dos tópicos relacionados com a CS e seus participantes. Neste sentido, destaca-se que os temas tratados estiveram orientados para o aprofundamento do conhecimento da CS e dos desafios que haviam para o setor de Defesa nacional. Tais temas foram discutidos por meio da apresentação de diferentes palestras, seminários e conferências com a participação de especialistas, a fim de acrescentar a receptividade política em relação a ideias, experiências e soluções para a questão da segurança no ciberespaço, que começava a demandar a atenção de diferentes setores da sociedade na época.

TABELA 9 – Resultados das intervenções sobre a CS na comissão defesa do Senado no período 2014-2017.

Sessão / data	Câmara / intervenientes	Assunto	Palestrantes / convocados
02/09/2014	Senadores: – Prokurica – Araya Guerrero. – Bianchi Chelech – Guillier Álvarez – Pérez Varela.	Sobre os novos cenários cibernéticos na área de Segurança e Defesa.	– Señor Jaime Ravinet D. – Señor Sergio Briceño H. – Señor Luis Eduardo C.

⁶⁸ Nesta sessão o senador argumentou: "Quero me referir a uma questão que venho apontando há muito tempo, no sentido de chamar a atenção para a vulnerabilidade do país em termos de Cibersegurança. Apresentei um projeto de lei que cria um sistema nacional de Cibersegurança, que, claro, não teve a recepção desejada por parte do Governo" (CHILE, 2017e, tradução nossa).

⁶⁹https://www.senado.cl/appsenado/index.php?mo=comisiones&ac=ficha&id=190&tipo_comision=10

Sessão / data	Câmara / intervenientes	Assunto	Palestrantes / convocados
09/09/2014	Senadores: – Prokurica – Araya Guerrero. – Bianchi Chelech – Guillier Álvarez – Pérez Varela	A Cibersegurança na área de Defesa.	– Subsecretario Forças Armadas, – Subdirector del Estado Maior Conjunto – Director de la Dirección de Inteligencia del Estado Mayor Conjunto
05/01/2016	Senadores – Guillier Álvarez – Araya Guerrero – Navarro Brain – Pérez Varela – Prokurica	Exposição de Cibersegurança.	– Señor Juan Ignacio N.
17/05/2016	Senadores – Prokurica – Araya Guerrero. – Bianchi Chelech. – Guillier Álvarez – Pérez Varela	Seminário: Os desafios nacionais no Ciberespaço e Ciberdefesa, organizado pela comissão e a Biblioteca do Congresso Nacional.	– Ministro de Energía – Subsecretario Marcos Robledo – Director de Inteligencia e Planeamiento conjunto – Jefe de Brigada Cibercrimen – Analista Informático, Sr. Luis Carrasco. – ANEPE, Dra. Carolina Sancho
06/06/2016	Senadores – Prokurica – Araya Guerrero – Guillier Álvarez – Pérez Varela.	Exposição dos Comandantes do Exército, Marinha e Força aérea sob políticas institucionais em matéria de Ciberdefesa.	– Diretor de Inteligência Exército – Diretor de Inteligência Marinha – Diretor de Inteligência Força Aérea
16/05/2017	Senadores – Rossi Ciocca – Araya Guerrero – Bianchi Chelech – Prokurica	Exposição dos representantes do Executivo sobre PNCS recentemente publicada.	– Subsecretario Mahmud Aleuy – Subsecretario Marcos Robledo

Fonte: o autor

Consequentemente, pode-se determinar em função da frequência de aparições públicas, modelo de intervenções, trabalho parlamentar e seu desempenho como Presidente da comissão, que o Senador Baldo Prokurica se apresentava como o principal representante do Congresso em relação à questão da CS no período citado. Porém, não se levantaram outros antecedentes a respeito de seu relacionamento direto com os representantes da CICS ou a existência de contribuições explícitas na estruturação da solução para a PNCS em documentos oficiais, processo que foi desenvolvido através da procura dos antecedentes da CICS, imprensa e dados em relatórios oficiais.

Em resumo, durante a abertura da janela de oportunidade política, se identifica como os principais “atores visíveis” (empreendedores de políticas) dentro do processo da PNCS, os subsecretários designados que cumpriram as funções na presidência e

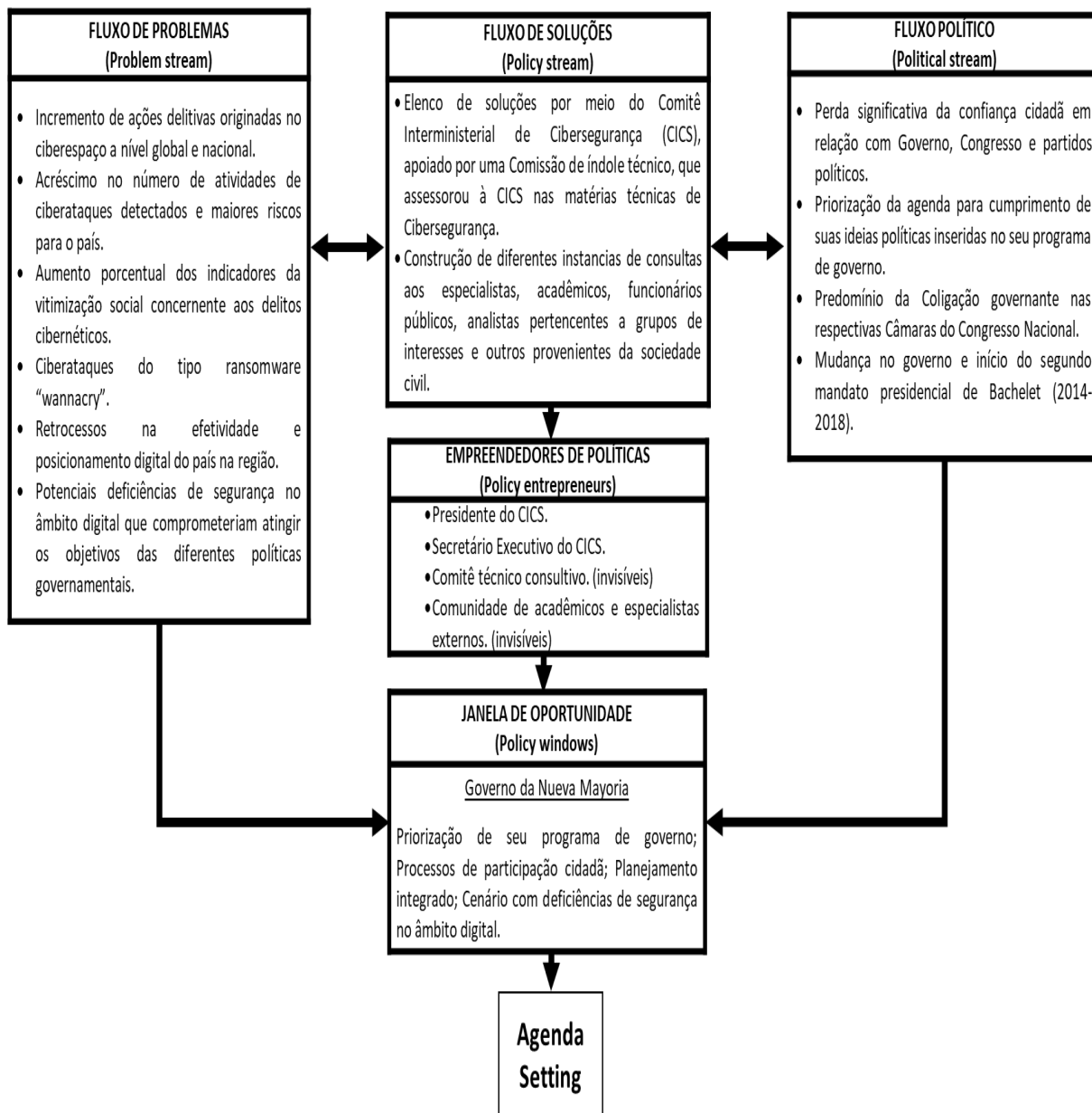
secretaria executiva do comitê. Sendo assim, devido aos papéis desempenhados dentro do CICS e as faculdades legais e administrativas que possuíam, facilitou-se a convergência das diferentes correntes de problemas e soluções, em um contexto político específico para levar adiante a transformação de suas iniciativas, por meio de recombinações de elementos e da procura permanente de consensos políticos.

Assim, influenciou-se sobre as ideias políticas que marcaram a discussão sobre a futura PNCS, conduzindo as diferentes propostas a uma condição de seriedade, suavizando o entorno público em geral, o público mais especializado e a própria comunidade política a respeito da viabilidade do problema-solução apresentada no trabalho da PNCS. Mesmo existindo outros atores “não-visíveis” que foram parte do CICS, como os pertencentes às comunidades de especialistas que participaram do comitê técnico consultivo, que assessorou à CICS nas matérias específicas de cibersegurança e como os acadêmicos requeridos durante o processo.

Ainda assim, é importante destacar que, neste caso, as informações disponibilizadas por meio da análise documental, permitiram vislumbrar somente a existência da figura dos empreendedores de políticas, sem permitir corroborar empiricamente o papel e a visão do problema pela limitação metodológica que abalizou a nossa pesquisa.

Por último, trazendo aqui o esquema proposto da adaptação do modelo de Kingdon para vislumbrar o processo de formação da agenda governamental para uma política pública, apresenta-se na sequência, o diagrama proposto da formação da agenda para PNCS 2017.

FIGURA 14 – Diagrama da formação da agenda para PNCS 2017.



Fonte: o autor.

5 CONCLUSÕES E RECOMENDAÇÕES

Mediante a análise apresentada da PNCS do Chile, identificaram-se intervenientes e ações específicas, geradas no processo de definição da agenda governamental durante o quadriênio de 2014 a 2017, para a criação da primeira política pública focada na formação de uma segurança digital para o país.

Dessa forma, a PNCS representou um marco importante no progresso da institucionalidade digital do Chile, pois mudou a atenção do governo a partir das políticas focalizadas no desenvolvimento digital como fator de transformação do funcionamento do Estado, de inclusão social e de crescimento econômico para o país. A questão da segurança digital também significou um aspecto de necessário atendimento, visto que não era possível avançar na agenda setorial de transformação tecnológica sem diminuir as contínuas brechas de segurança que se manifestaram ao longo do tempo.

Assim, comprovou-se o estabelecido na hipótese da pesquisa através das diferentes evidências encontradas, que permitiram estabelecer as relações entre os eventos identificados e explicar suas ocorrências para determinar a conformação da agenda no que diz respeito ao problema de segurança no ciberespaço.

Neste sentido, as descobertas que ratificam o desenvolvimento da questão da segurança digital, surgiram no contexto de uma institucionalidade tecnológica de permanente transformação desde 1999. Foi a partir da publicação da AD 2013-2020, quando o progressivo incremento de cenários de maiores riscos e ameaças geraram uma percepção de vulnerabilidade frente ao uso acelerado e a presença massiva das tecnologias e redes digitais nos âmbitos produtivos, de funcionamento do Estado e, inclusive, das próprias pessoas.

Nesse período, se identificou um aumento substancial nas ações de fortalecimento da institucionalidade digital com o apoio de atores de diversas procedências dentro da sociedade civil, acadêmica e de especialistas externos: ONU, OCDE e UIT, que acompanharam os planos e linhas de ação para permitir o cumprimento dos objetivos levantados e a disposição de objetivos a longo prazo, abordando, pela primeira vez, a necessidade de intervir na segurança do ciberespaço como um aspecto relevante para o usuários.

O papel da AD 2020, inserida em um contexto caracterizado pelo incremento exponencial da conectividade das redes e a presença massiva de serviços digitais em nível global, regional e local, foi atribuir relevância concreta na questão de segurança, definindo uma perspectiva institucional para abordar os desafios da segurança digital do país, através da criação de uma estratégia de segurança digital para a proteção dos usuários privados e públicos contra possíveis ações de violação a fontes de dados e da privacidade.

Consequentemente, a existência de uma institucionalidade digital desde a década de 1990 no país, e aprimorada em 2013 e 2015, permitiu contar com o conhecimento, experiência e uma estrutura elementar em diferentes Ministérios e órgãos de assessoria especializados, cujas capacidades foram acrescentadas ao longo desses anos, ajudando a assentar as bases para incorporação de outras questões associadas ao desenvolvimento digital, aguardando a decisão do Governo para a definição política sobre a questão da segurança neste âmbito.

Assim, o modelo de fluxos aplicado no estudo de caso, determinou como o problema da segurança no ciberespaço conseguiu se posicionar na agenda do governo durante a administração de Bachelet, tornando-se uma política pública a partir dos processos de definição da agenda e da determinação de alternativas políticas. Ratifica-se que a abordagem tornou possível verificar que os problemas nem sempre são gerados na sociedade, pelo contrário, são questões de conhecimento do governo, que necessita de impulsos para posicioná-las na sua agenda.

O processo explica-se pela decorrência do método de convergência dos três fluxos. O primeiro, evidenciou que a partir de 2010, houve um acréscimo de ações delitivas originadas no ciberespaço em escala global, as quais tiveram incidência sobre a estrutura da defesa nacional, indústrias privadas, e agências de inteligência de diferentes países. No nível nacional essas ações afetaram à Rede de conectividade do Estado (RCE) e produziram um incremento percentual dos indicadores da vitimização social relativos aos delitos cibernéticos, além disso, a criminalidade apresentou uma situação social que demandava uma maior atenção governamental nos anos de 2014 a 2017. Percebeu-se uma mudança na atenção do governo, ao reconhecer essa realidade de forma explícita em 2015, sendo caracterizada como uma ameaça à segurança das pessoas e usuários da internet. Em seguida, o índice de Desenvolvimento do Governo Eletrônico da ONU em 2014 reconheceu a perda de

efetividade, posicionamento do país na região e, diminuição da celeridade das políticas públicas para transformação digital do Estado.

Portanto, a combinação dos resultados das atividades delitivas no ciberespaço e a falta de condições estruturais para fomentar a transformação digital de forma acelerada, de acordo com as tendências internacionais, exigiram do governo o aprimoramento das decisões políticas, com vista a impulsionar ações para o fortalecimento do desenvolvimento digital, incluindo a segurança digital como um aspecto emergente.

O segundo, a análise dos fluxos das soluções, permitiu identificar os princípios da viabilidade e “value acceptability” asseverados por Kingdon. Inferindo-se nos resultados dos estudos feitos às séries de ações executadas pelo Comitê Interministerial de Cibersegurança (CICS), órgão responsável pela proposta da futura PNCS e de suas propostas. Desse modo, são descobertos os antecedentes que consolidam essa visão, os quais derivam a partir de sua própria conformação, que definiu um grupo de trabalho multissetorial de diferentes atores do campo público, privado e acadêmico, incluindo na sua dinâmica de trabalho a participação de assessores externos durante o desenvolvimento das propostas. E que, somado as consultas e audiências públicas convocadas durante as etapas de elaboração e de revisão, deram visibilidade ao processo, outorgando o sustento político-técnico das ideias em discussão, validando o trabalho perante a sociedade.

Conseqüentemente, os produtos (soluções) proporcionaram um soluto transversalmente reconhecido e de acordo com a realidade nacional. Nesse sentido, foi coerente com seu propósito original, representativo dos conteúdos estabelecidos como prioritários e capacitado para que fosse implementado como política pública ao longo de um curto período.

O terceiro aspecto, o estudo do fluxo das políticas, evidenciou que a discussão da questão de segurança através de uma estratégia, foi parte de uma aspiração política estipulada no programa de governo para a futura administração de Bachelet. A ideia de priorizá-la e impulsioná-la aconteceu em um ambiente político particularmente demandante em relação as ações do Executivo, que estava baseado nas análises dos discursos da Presidente no congresso nacional e dos dados fornecidos pelas consultas de opinião.

Assim, os resultados obtidos caracterizam um entorno onde se advertiu uma perda de confiança das instituições por parte dos cidadãos e a diminuição do apoio popular ao governo. Neste cenário, a administração do país tentou suscitar uma política de acordos com outros setores do congresso para impulsionar sua agenda política, a fim de satisfazer suas questões e fortalecer sua posição, que incluía, em particular, uma estratégia de CS.

Nesse momento, como o apoio de uma coalizão favorável aos seus propósitos representava a maior força política do país, influenciando as instancias para levar adiante a construção de uma política nacional de Cibersegurança, através de uma prerrogativa própria do governo. Em março de 2015, surgiu então, o documento matriz nomeado “Bases para uma PNCS”, que criou um roteiro para concretizar as aspirações políticas relativas à questão da cibersegurança em ações concretas que ficaram estabelecidas no documento final da PNCS. Assim, a aplicação da teoria dos múltiplos fluxos verificada no estudo de caso, reafirmou a alegação de Kingdon a respeito dos resultados da conjugação dos três fluxos apresentados. Esses, incidiram na abertura de uma janela para uma oportunidade política.

Desse modo, durante o governo de Bachelet, especificamente no ano de 2015, foi necessário o atendimento aos problemas de segurança no ciberespaço, devido ao crescimento exponencial das ameaças e os potenciais riscos para o país em todos os âmbitos, assim como, impedir possíveis efeitos políticos sobre a popularidade do governo pela falta de ações concretas. Por meio de um planejamento integrado, que era parte de uma ideia política que apresentava um processo de amadurecimento desde a sua inclusão no programa do futuro governo de Bachelet, publicado em 2013, junto com os trabalhos executados em 2014, orientados a manter um monitoramento político e técnico-setorial dos órgãos responsáveis sobre a situação do ciberespaço, suscitaram um entorno ainda mais propício para a tomada da decisão política de 2015, que resolveu o início dos estudos pertinentes para a elaboração da futura política nacional. O CICS portanto, cumpre um papel fundamental na condução do processo e no alcance de seus objetivos, sobretudo, nas funções de empreendedores de políticas, que foram desenvolvidas pelo Presidente e o Secretário Executivo do CICS, respectivamente.

Em suma, o modelo permitiu vislumbrar como as condições de riscos e ameaças no ciberespaço identificadas pela administração do país em 2014 transformaram-se

em problemas de segurança de ampla abrangência, e receberam uma paulatina atenção pelos diferentes atores, gerando mudanças na conformação da agenda governamental durante a administração de Bachelet em 2015.

Desde então, o Governo encarregou ao CICS o processo de especificação de alternativas, junto com a definição de funções dos principais participantes que impulsionaram e deram viabilidade às diferentes propostas. Consequentemente, os resultados obtidos através da análise delineada, deram coerência e pertinência à análise de estudo de caso, e conseguiram proporcionar as evidências através da pesquisa documental, que justificam o cumprimento da hipótese desta pesquisa e os objetivos levantados para satisfação da mesma.

A respeito do modelo de análise de fluxo de Kingdon, conclui-se que apesar de ser um modelo adaptado para a análise da produção de políticas do governo federal dos EUA, desenvolvido em 1995, tem aplicabilidade para a realidade política avaliada, uma vez que é coerente com o propósito da nossa pesquisa, devido às considerações estabelecidas, segundo Zahariadis (2007), sobre a utilização do modelo, dado que é uma lente ou perspectiva teórica que contribui para determinar que as políticas são realizadas pelos governos nacionais sob condições de ambiguidade. Essa condição é: “Um estado de ter muitas maneiras de se pensar sobre mesmas circunstâncias ou fenômenos”. (FELDMAN, 1989 apud ZAHARIADIS, 2007, p.66, tradução nossa).

Dessa forma, o modelo serviu para entender o processo de definição da agenda e da formulação de políticas dentro do sistema político do Chile, respeitando as suas complexidades, aleatoriedades e permanente evolução, identificando seus comportamentos observáveis e peculiaridades que permitem diferenciá-lo de outro sistema político. O modelo, portanto, conseguiu explicar através da decomposição sequencial de uma série de fatores estabelecidos nas correntes apresentadas, o processo singular que ocasionou uma produção coletiva que deu origem aos resultados que justificaram a abertura das janelas políticas para inclusão na agenda governamental da questão de CS, e também, da compreensão do fenômeno estudado e do cumprimento dos objetivos levantados.

Aspecto importante a salientar do método é a sua utilidade para esclarecer o processo de formação da agenda e suas soluções por meio de critérios padronizados dentro de um processo estabelecido. Em função disso, o sistema explicou como a conjunção dos fluxos torna um produto, orientando a pesquisa a partir de uma análise

operacional predefinida sobre a política pública. Além disso, o método sugere possíveis explicações através de seu percurso para a justificação do processo com múltiplas variáveis, fortalecendo as justificativas sobre as meras descrições. Também é um aspecto destacável que o modelo foi adaptado a um caso de estudo que considerou a análise de uma política pública sem uma participação ativa do Congresso nacional.

Não obstante, o padrão usado expressa alguns limites nas dinâmicas analisadas. Constata-se que é difícil manter a separação entre as correntes, verificando-se a existência de sobreposições, assim como, a participação dos integrantes e suas possíveis atuações, presentes em uma ou mais correntes. Do mesmo modo, o modelo não consegue determinar como as interações presentes no ambiente político nacional (aquelas que ficam fora do esquema planteado e as próprias circunstâncias que influem para determinar os fluxos padronizados), e nos arranjos internacionais, exercem influências sobre o sistema político em seu conjunto

Da perspectiva metodológica, devido as peculiaridades de seu enfoque associado à ambiguidade dos sistemas políticos, apresenta baixa capacidade para prever fatos ou comportamentos. Enfatiza aspectos situacionais e temporais das mudanças políticas e não estabelece a maneira como o marco institucional delimita as decisões preliminares e ações dos participantes, outorgando um elevado papel de primeiro plano aos empreendedores que não estivessem de acordo com a realidade do nosso estudo do caso.

Enfim, a presença de um modelo de análise de predominância sistêmica como foi utilizado para a análise do estudo de caso desta dissertação, permitiu avançar para identificar o funcionamento dos processos políticos, suas instituições, e as atividades que se interrelacionaram para a adoção de decisões e ações no contexto político-social do Chile no quadriênio de 2014 a 2017, assumindo nesta perspectiva as limitações teóricas argumentadas, segundo Easton (1999), sobre as dificuldades e certas restrições teóricas que têm a ciência política e seus modelos: “não pode estudar todos os fenômenos; o mundo real precisa ser reduzido e simplificado de alguma forma”. (EASTON, 1999, p. 77).

De tal modo, segundo Dye (2009) os modelos de análise política têm como objetivos esclarecer as ideias sobre políticas e políticas públicas. Identificar aspectos

importantes de questões políticas e problemas sociais, que teoricamente, “direcionam nossos esforços para compreender melhor as políticas públicas e propor explicações para que essas prevejam as suas consequências” (DYE, 2009, p. 100, tradução nossa). Entende-se que o estudo realizado, permitirá estabelecer um ponto de início para futuras pesquisas de outras políticas públicas que são subsidiárias da PNCS. A partir da continuidade do modelo usado, ou complementado com outro, acrescentando-se antecedentes disponíveis para plausíveis estudos comparativos entre essas políticas ou outras afins, como as políticas dessa temática relacionadas ao nível regional.

Uma primeira recomendação é o atendimento a respeito do estudo das fases da implementação e avaliação da PNCS, incorporando outros tipos de análise a fim de complementar o nosso estudo e dar completa rastreabilidade à política nacional por meio de uma abordagem das fases do ciclo clássico que caracterizam o estudo de uma política pública. Outra recomendação é propiciar estudos comparados com outras políticas que tenham relação com prerrogativas do Governo nas áreas de Segurança e Defesa, para avaliar o desempenho do governo a respeito da definição da sua agenda, em um contexto político social distinto, com prioridades dessemelhantes e recursos limitados de diversos tipos. Como última recomendação, é admissível incorporar outras perspectivas de investigação para avaliar o grau de coordenação e interligação entre as diferentes políticas públicas que são subsidiárias da atual PNCS, tais como a PNCD e a Política internacional para o ciberespaço⁷⁰.

Finalmente, a PNCS representa a primeira política pública que atendeu a questão da CS no ciberespaço, balizando o roteiro para outras políticas subsidiárias, constituindo-se na pedra angular para a diminuição das brechas da segurança digital e na contribuição para o fortalecimento da institucionalidade digital do Chile. Aportando à construção de um estado mais moderno inserido em um entorno digital, capaz de atingir seu desenvolvimento econômico-social conforme os novos desafios que a transformação tecnológica pressupõe.

Neste sentido, a decisão política de inserir a questão de CS na agenda governamental, logo, na decisória, obedece à resposta estatal baseada na necessidade de atender as demandas da cidadania frente a uma questão em

⁷⁰ A política ainda está em elaboração pelo Ministério das Relações internacionais.

permanente evolução. Consequentemente, a pesquisa apresentada aportou à análise de uma política pública a partir de uma perspectiva teórica que ajudou a compreender as origens e justificativas dos processos políticos em um contexto de recente evolução, construindo uma admissível explicação sobre a conformação da agenda para fundamentar a escolha política do Estado Chileno e reconhecer as particularidades de seu sistema político.

REFERENCIAS BIBLIOGRÁFICAS

ACOSTA, P. A.. Cuadernos Catedra ISDEFE-UPM «Seguridad nacional y Ciberdefensa». Madrid: Fundación Rogelio Segovia para el desarrollo de las Telecomunicaciones. 2009.

ARREOLA, A. Ciberespacio: quinto dominio de la guerra. Disponible em: https://www.researchgate.net/publication/340819837_Ciberespacio_quinto_dominio_de_la_guerra. Acceso em: 12 de fevereiro de 2021. Abril de 2020.

BANCO INTERAMERICANO DE DESARROLLO (BID). **Ciberseguridad, riesgos, avances y el camino a seguir en América latina y el Caribe**. Acceso em 1 de janeiro de 2021. Disponible em: www.observatoriociberseguridad.com. 2020

_____. **Informe Ciberseguridad 2016: Ciberseguridad, ¿Estamos preparados en América Latina y el Caribe?**. Disponible em: <https://publications.iadb.org/bitstream/handle/11319/7449/Ciberseguridad-Estamos-preparados-en-America-Latina-y-el-Caribe.pdf?sequence=7>. Acceso em 12 de fevereiro de 2021. 2016.

BARDIN, Laurence. **Análise de conteúdo**. São Paulo: Edições 70, 1977.

BARRIOS, A. V. **Asesoría Técnica Parlamentaria: La Política Nacional de Ciberseguridad: 2017-2022**. Biblioteca del Congreso Nacional de Chile. 2018.

BOWDISH, R. Military Strategy: Theory and Concepts. Tesis (Doctorado en Filosofía). (D. d. Políticas, Ed.) Nebraska, Estados Unidos de Norteamérica: Universidad de Nebraska. 2013.

CAPELLA, A. C. **Formulação de Políticas Públicas**. Brasil: Enap Fundação Escola Nacional de Administração Pública. 2018.

CARO, B. M. «**Alcance y ámbito de la Seguridad Nacional en el Ciberespacio**». Em I. E. Estratégicos, Cuaderno de Estrategia Nº 149 Ciberseguridad. Retos y Amenazas a la Seguridad nacional en el Ciberespacio (pp. 48-82). Madrid: Imprenta del Ministerio de Defensa. 2010.

CASTRILLÓN-RIASCOS, J. A. **Nada volverá a ser igual: ciberguerra y ciberpoder**. Memorias, 13(23). doi:<http://dx.doi.org/10.16925/me.v13i23.1072>. 2015

CENTRO DE ESTUDIOS PÚBLICOS (CEP). **Encuestas CEP Chile. Estudos nacionais de Opinião Pública N.72, 75, 78 e 81**. Disponible em <https://www.cepchile.cl/encuestaCEP>. Acceso em 26 de julho de 2021. 2017.

CHILE. Ministerio de economía, Fomento y Turismo. **Chile: Hacia la sociedad de la Información**. Santiago: Comisión Presidencial "Nuevas Tecnologías de Información y Comunicación". Disponible em: <http://www.agendadigital.gob.cl/#/documentos/otras-agendas>. Acceso em: 10 de Maio de 2021, Santiago, 1999.

_____. Subsecretaría de Desarrollo Regional y Administrativo. **La Agenda Digital 2004-2006, Te acerca al futuro**. Secretaría Técnica del Grupo de Acción Digital. Disponible em: <http://www.agendadigital.gob.cl/#/documentos/otras-agendas>. Acceso em: 12 de Maio de 2021 Santiago, 2004.

_____. Ministerio de Economía, Fomento y Turismo. **Estrategía Digital 2007-2012**. Comité de ministros para el Desarrollo Digital. Disponible em: <http://www.agendadigital.gob.cl/#/documentos/otras-agendas>. Acceso em: 13 de Maio de 2021. Santiago, 2007.

_____. Gobierno de Chile. **Agenda digital Imagina Chile 2013-2020**. Secretaría Ejecutiva de Desarrollo Digital. Disponible em: <http://www.agendadigital.gob.cl/#/documentos/otras-agendas>. Acceso em: 1 de junho de 2021. Santiago, 2013a.

_____. Presidencia de la República. **Programa de Gobierno Michelle Bachelet 2014-2018**. Disponible em: http://www.subdere.gov.cl/sites/default/files/noticias/archivos/programamb_1_0.pdf. Acceso em: 10 de junho de 2021. Santiago, outubro, 2013b.

_____. Secretaría General de la Presidencia. **Mensaje Presidencial ante el Congreso pleno, 2014**. 21 de maio de 2014. Disponible em: https://www.bcn.cl/historiapolitica/corporaciones/cuentas_publicas/detalle?tipo=presidentes. Acceso em: 10 de junho de 2021. Santiago, 2014a.

_____. Congreso Nacional de Chile. Biblioteca del Congreso. **Historia política**. Disponible em: https://www.bcn.cl/historiapolitica/resenas_parlamentarias/wiki/Michelle_Bachelet_Jeria. Acceso em: 7 de julho de 2021. Valparaíso, 2014b.

_____. Ministerio de Hacienda. Dirección de Presupuestos. **Leyes de Presupuesto del Sector público (2014-2017)**. Disponible em: <https://www.dipres.gob.cl/598/w3-propertyvalue-15954.html>. Acceso em: 29 de Mayo de 2021, Santiago, 2014c.

_____. Congreso Nacional de Chile. Cámara de Senado. **Noticias**. 27 de setembro de 2014. Disponible em: <https://www.senado.cl/noticias/ciberseguridad-ministerio-del-interior-elaborara-informe-sobre-el>. Acceso em: 29 de Mayo de 2021, Santiago, 2014d.

_____. Gobierno de Chile. Agenda Digital 2020, **Chile Digital para Tod@s**. Gráfica LOM. Disponible em: <http://www.agendadigital.gob.cl/#/documentos/otras-agendas>. Acceso em: 18 de Maio de 2021. Santiago, 2015a.

_____. Ministerio del Interior y seguridad Pública, Biblioteca del Congreso Nacional de Chile. **Decreto 533, Crea Comité Interministerial sobre Ciberseguridad**, 27 de abril de 2015. Disponible em: <https://www.bcn.cl/leychile/navegar?idNorma=1079608>. Acceso em: 11 de setembro de 2021. Santiago, 2015b.

_____. Subsecretaría del Interior del Ministerio del Interior y Seguridad Pública y la Subsecretaría de Defensa Nacional del Ministerio de Defensa Nacional. **Bases para una Política Nacional de Ciberseguridad. Documento de trabajo.** Março de 2015. Disponível em: [https://www2.congreso.gob.pe/sicr/cendocbib/con5_uibd.nsf/0EE2B41802BD1CE80525831D005FBE91/\\$FILE/Bases Pol%C3%ADtica Nacional sobre Ciberseguridad .pdf](https://www2.congreso.gob.pe/sicr/cendocbib/con5_uibd.nsf/0EE2B41802BD1CE80525831D005FBE91/$FILE/Bases_Pol%C3%ADtica_Nacional_sobre_Ciberseguridad.pdf). Acceso em: 10 de março de 2021. Santiago, 2015c.

_____. Ministerio del Interior y Seguridad Pública. **Política Nacional de Ciberseguridad (PNCS).** Disponível em: <https://www.ciberseguridad.gob.cl/media/2017/05/PNCS-CHILE-FEA.pdf>. Acceso em: 05 de março de 2021. Santiago, 2017a.

_____. Ministerio del Interior y Seguridad Pública. **Encuesta Nacional Urbana de Seguridad Ciudadana (ENUSC).** Subsecretaría de Prevención del Delito. Disponível em: <http://cead.spd.gov.cl/estudios-y-encuestas/>. Acceso em: 28 de julho de 2021. Santiago, 2017b.

_____. Dirección de Prensa de la Presidencia. **Discurso de S.E. la Presidenta de la República, Michelle Bachelet Jeria en el lanzamiento de la PNCS.** 27 de abril de 2017. Disponível em: <http://archivospresidenciales.archivonacional.cl/index.php/presidenta-michelle-bachelet-encabeza-lanzamiento-de-la-politica-nacional-de-ciberseguridad>. Acceso em: 18 de maio de 2021. Santiago, 2017c.

_____. Secretaría General de la Presidencia. **Mensaje Presidencial ante el Congreso pleno, 2017.** 01 de junho de 2017. Disponível em: https://www.bcn.cl/historiapolitica/corporaciones/cuentas_publicas/detalle?tipo=presidentes. Acceso em: 19 de maio de 2021. Santiago, 2017d.

_____. Congreso Nacional. Intervenciones en sala. **Intervención del Senador Prokurika durante la discusión del Presupuesto de Sector Público para 2018.** 03 de outubro de 2017. Disponível em: https://www.senado.cl/appsenado/index.php?mo=sesionessala&ac=getDocumento&teseid=61766&idparl=693&tema=Proyecto&nrobol=1145205_P&legiid=&tagid=22. Acceso em: 19 de maio de 2021. Santiago, 2017e.

_____. Ministerio del Interior y Seguridad Pública. **Política de Ciberdefensa del Estado de Chile.** 9 de novembro de 2017. Disponível em: <https://www.diariooficial.interior.gob.cl/publicaciones/2018/03/09/42003/01/1363153.pdf>. Acceso em: 11 de abril de 2021. Santiago, 2018.

_____. Ministerio de Defensa Nacional de Chile. **Política de Defensa Nacional de Chile, 2020.** Disponível em: <https://www.defensa.cl/wp-content/uploads/POL%C3%8DTICA-DE-DEFENSA-NACIONAL-DE-CHILE-2020.pdf>. Acceso em: 11 de maio de 2021. Santiago, 2020.

CHOUCRI, N. **Cyberpolitics in international relations.** Cambridge, Massachusetts: Massachusetts Institute of Technology. 2012.

CLARK, R. A.. **Guerra en la Red: Los nuevos campos de Batalla**. Barcelona: Editorial Ariel. 2011.

CUNHA, E. S., & ARAÚJO, C. E. (2018). **Process tracing nas Ciências Sociais: fundamentos e aplicabilidade**. Brasília: Escola Nacional de Administração Pública (ENAP). 2011.

DOÑA, M. K. **Aplicación del concepto de política pública a la política de defensa de Chile, 1990-1999**. Universidad de Chile. Santiago: Instituto de asuntos públicos. 2005.

DURÁN, A. **Principales Enfoques del Análisis de Políticas Públicas que tienen una variable Explicativa Predominante**. *Serie Creación*, 25. 2017.

DYE, T. R. **Políticas Públicas e Desenvolvimento**. (F. G. Salm, Trad.) Brasília: Editora Universidade de Brasília. 2009.

DYE, T. R. **Understanding public policy**. Boston: Longman. 2011.
EASTON, E. **Esquema para el análisis político**. (A. C. Leal, Trad.) Buenos Aires, Argentina: Amorrortu editores. 1999.

ELDER, C. D., COBB, R. W., & J., N. B. **Problemas públicos y Agenda de Gobierno**. (L. F. VILLANUEVA, Ed.1993.

FELIU, L. «**Seguridad nacional y Ciberdefensa**» **Aproximación conceptual: Ciberseguridad y Ciberdefesa**. Disponible em: Escuela Superior de Ingenieros de Telecomunicaciones: <http://catedraisdefe.etsit.upm.es/wp-content/uploads/2013/01/Ponencia-Luis-Feliu.pdf>. 2013.

FIREEYE. **M-Trends 2020: Insights into Today's Cyber Attacks**. Disponible em: <https://content.fireeye.com/m-trends/wbmr-m-trends-2020-insights-into-todays-cyber-attacks>. 2020.

FUCCILLE, A., & REZENDE, L. ARTIGOS. **Complexo regional de segurança da América do Sul: uma nova perspectiva**. *Contexto Internacional*, 35, p.77-104. Jun de 2013.

GIL, A. C. **Como elaborar projetos de pesquisa**. Sao Paulo: Atlas. 2002.

GONZÁLEZ, C. J. «**Estrategias legales frente a las Ciberamenazas**». Em Instituto Español de Estudios Estratégicos, *Cuaderno de Estrategia Nº 149 Ciberseguridad. Retos y Amenazas a la Seguridad Nacional en el Ciberespacio*. Madrid: Imprenta del Ministerio de Defensa. 2010.

GOOGLE. **Google Trends**. Disponible em: https://trends.google.cl/trends/explore?date=2015-01-02%202017-12-31&geo=CL&q=%2Fm%2F0p78w_d,%2Fm%2F01qgr,wannacry. Acceso em: 6 de Agosto de 2021.

HERNÁNDEZ, R. F. «**Metodología de la Investigación**». México:: McGRAW-HILL/ Interamericana Editores. 2010.

JUNTA INTERAMERICANA DE DEFENSA (JID). **Guía de Ciberdefensa, Orientaciones para el Diseño, Planeamiento, Implantación y Desarrollo de una Ciberdefensa militar**. Disponible em: <https://www.iadfoundation.org/wp-content/uploads/2020/08/Ciberdefensa10.pdf>. Acceso em: 20 de dezembro de 2020. 2020.

KINGDON, J. W. **Agendas, Alternatives, and Public Policies**. Harlow: Pearson Education Limited. 2013.

LAHERA, P. E. **Política y políticas públicas**. Santiago: CEPAL, División de Desarrollo Social. 2004.

LOTTA, G. **Teoria e análises sobre implantação de políticas públicas no Brasil**. Brasília: Enap Fundação Escola Nacional de Administração Pública. 2019.

LUIIJF, E. B. **Nineteen national cyber security strategies**. (I. E. Ltd., Ed.) *International Journal of Critical Infrastructure Protection*, 9, 3-31. doi:10.1504/IJCIS.2013.051608. (January de 2013).

MANSELL, R., & Tremblay, G.. **La renovación de la visión de las sociedades del conocimiento para la paz y el desarrollo** (Vol. 1). (I. C.-U. Organización de las Naciones Unidas para la Educación, Ed., & t. a. Olcese, Trad.) São Paulo: Comitê Gestor da Internet no Brasil. 2015.

MENY, I., & THOENING, J.-C. **Las políticas públicas**. (F. Morata, Ed.) Barcelona: Editorial Ariel. 1992.

MICROSOFT CORPORATION. **Microsoft Digital Defense Report**. Disponible em: file:///C:/Users/funcional/Downloads/Microsoft_Digital_Defense_Report_2020_September.pdf. Acceso em: 21 de janeiro 2021. Setembro de 2020.

MILANI, C. R. **Solidariedade e Interesse. Motivações e estratégias na cooperação internacional para o desenvolvimento**. 1º ed. Curitiba: Appris de CS Mombelli. 2020.

NEWMeyer, K. **Elements of national cybersecurity strategy for developing nations**. (publications.excelsior.edu, Ed.) *National Cybersecurity Institute Journal*, 1, 9-19. 2015.

ORGANISATION FOR ECONOMIC, CO-OPERATION AND DEVELOPMENT, OECD. (2010). **Newsroom**. Disponible em <https://www.oecd.org/newsroom/chileprimerpaissudamericanomiembrodelaoocde.htm>. Acceso em 20 de setembro de 2021. 2010.

OLAVARRÍA, G. M., NAVARRETE, Y. B., & FIGUEROA, H. V. **¿Cómo se formulan las políticas públicas en Chile?** .Política y gobierno, XVIII, 109-154. 1er. semestre de 2011.

ORGANIZACIÓN DE LOS ESTADOS AMERICANOS (OEA). Centro de Noticias. Comunicados de Prensa, Fotonoticia, FNC-21545. Disponible em: https://www.oas.org/es/centro_noticias/fotonoticia.asp?sCodigo=FNC-21545. Acceso em 11 de Agosto de 2021. 28 de Abril de 2017.

PAZ, P. Y., & Claudia. **Discurso de la Secretaria de Seguridad Multidimensional de la OEA**. Decimoseptimo período ordinario de sesiones, Comité Interamericano contra el Terrorismo. Washington, D.C., Estados Unidos. Disponible em: scm.oas.org/doc_public/SPANISH/HIST_17/CICTE01120T03.doc. 2016.

PEREIRA REZENDE, L. **Sobe e Desce: Explicando a Cooperação em Defesa na América do Sul**. (U. d. Brasília, Ed.) Contexto Internacional, 1. 2015.

PRANDINI, P. y. «**Ciberdelito en América Latina y El Caribe. Una visión desde la sociedad civil**». Disponible em: LACNIC Registro de Direcciones de Internet para América Latina y Caribe.: https://www.proyectoamparo.net/files/ciberdelito_lac_lacnic_amparo_estudios2013_completo_vfinal.pdf. 2013.

RAMÍREZ, B. M. **El diseño de la agenda política y la construcción de alternativas de solución en la política de inmigración española**. Civilizar. Ciencias Sociales y Humanas, 7, 249-264. julio-diciembre de 2007.

REARDON, R., & CHOUCRI, N. **The Role of Cyberspace in International Relations: A View of the Literature**. San Diego, CA: Department of Political Science, MIT. 2012.

REVISTA DE DEFENSA Y SEGURIDAD EN ESPAÑA Y LATINOAMÉRICA. Chile creará un Centro Nacional de Mando y Ciberseguridad. Disponible em: <https://www.infodefensa.com/texto-diario/mostrar/3137867/chile-creara-centro-nacional-mando-ciberseguridad>. 26 de Feb de 2014.

ROBLEDO, H. M. Facultad de Derecho de Universidad de Chile. Disponible em: **Seminario Internacional Ciberseguridad y ciberdefensa en Chile 2015**. Disponible em: <http://www.derecho.uchile.cl/noticias/117175/-seminario-internacional-sobre-ciberseguridad->. 18 de 08 de 2015.

SANCHO, H. C. **Ciberespacio, bien público mundial en tiempos de globalización: Política pública de ciberseguridad, una necesidad imperiosa y la Ciberdefensa como desafío del siglo XXI**. Em E. S. Guerra, & J. C. Pinto (Ed.), Ciberdefensa e Cibersegurança: Novas Ameaças à Segurança Nacional (pp. 41-73). Rio de Janeiro, Brasil. 2016.

SANCHO, H. C. **Seguridad y defensa en el ciberespacio: tendencias contemporáneas y desafíos para el caso chileno**. Escenarios Actuales, 2, 49-72. Julio de 2020.

SARTORI, G. «**Guidelines for concept analysis, Concepts and method in social science**». Nueva York, Estados Unidos da America. 2009.

SECURITY, A. C. (s.d.). **Security Tip (ST04-001)**. Disponível em: <https://us-cert.cisa.gov/ncas/tips/ST04-001>. Acesso em 11 de Agosto de 2021. 04 de novembro de 2019.

THE ECONOMIST REVIEW. **Cyberwar, The threat from the internet**. The Economist Review, 396, núm. 8389. Disponível em: <https://www.economist.com/weeklyedition/2010-07-03>. July de 2010.

TODD, H. M. "**Armad attack in cyberspace: Deterring asymmetric warfare with an asymmetric definition**". The Air Force Law Review, ProQuest Military Collection., 64. 2009.

UNESCO. **Sistema de información de tendencias educativas en América Latina**. Buenos Aires, Argentina. mayo de 2018.

UNIÓN INTERNACIONAL DE TELECOMUNICACIONES (UIT). **Recomendación UIT-T X.1205**. Disponível em: <https://www.itu.int/es/about/Pages/default.aspx>. Acesso em 11 de Agosto de 2020. Noviembre de 2010.

UNIÓN INTERNACIONAL DE TELECOMUNICACIONES (UIT) et al. **Guía para la elaboración de una estrategia nacional de ciberseguridad - Participación estratégica en la ciberseguridad**. Disponível em: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-CYB_GUIDE.01-2018-PDF-S.pdf. Acesso em 11 de julho de 2020. Ginebra. 2018.

UNITED KINGDOM, Ministry of Defence (MOD). «**Strategic Trends Programme Global Strategic Trends - Out to 2050**». Disponível em: <https://www.gov.uk/government/publications/global-strategic-trends>. 2018.

UNITED STATES OF AMERICA. (s.d.). **Department of Homeland Security, Cybersecurity Overview**. Disponível em: Official website of the Department of Homeland Security: <https://www.dhs.gov/cybersecurity-overview>. Acesso em 11 de maio de 2021.

UNITED STATES OF AMERICA, Department of Defense. **Joint Publication 1-02 Dictionary of Military and Associated Terms**. Disponível em: https://irp.fas.org/doddir/dod/jp1_02.pdf. Acesso em 10 de abril de 2021. 2010.

VERGARA, S. **Projetos e relatórios de pesquisa em administração**. (2da. ed.). São Paulo: Atlas. 1998.

VIOLLIER, P. **La participación en la elaboración de la Política nacional de Ciberseguridad: Hacia un nuevo marco normativo**. Santiago: Derechos Digitales, Global Partners Digital. 2017.

YIN, R. K. **Estudo de caso: Planejamento e Métodos** (2a. Edição ed.). (D. Grassi, Trad.) São Paulo, SP: Artmed Editora S.A. 1994.

ZAHARIADIS, N. **The Multiple Streams Framework**. Em P. A. Sabatier, & W. Press (Ed.), *Theories of the Policy Process*. University of California, Davis. 2007.

APÊNDICE A – Quadro de comparação das Agendas digitais do Chile 1999-2015

FATORES	AGENDAS DIGITAIS				
	Chile: “Hacia la sociedad de la información” 1999	Agenda Digital: “Te acerca al futuro” 2004-2006	Estratégia digital 2007-2012	Agenda Digital “Imagina Chile” 2013-2020	Agenda Digital 2020 “Chile digital para tod@s” 2015-2020
OBJETIVO	<ul style="list-style-type: none"> – Outorgar um acesso universal às redes de informação digital e aos serviços que os fornecem, por meio do desenvolvimento de novas capacidades competitivas com base nas oportunidades oferecidas pela rápida evolução das TICs. – Usar o potencial das tecnologias digitais e da rodovia da informação para promover a modernização do Estado em benefício dos cidadãos e das empresas. 	<p>Contribuir para o desenvolvimento do Chile por meio do uso das TIC para aumentar a competitividade, igualdade de oportunidades, liberdades individuais, a qualidade de vida e a eficiência e transparência do setor público, enriquecendo ao mesmo tempo, a identidade cultural da Nação e seus povos nativos.</p>	<p>Contribuir para o desenvolvimento econômico e social de país através do potencial oferecido pelo uso das TICs para melhorar a qualidade da educação, aumentar a transparência, aumentar a produtividade e fazer competitividade e fazer melhor governança, por meio de maior participação e compromisso do cidadão.</p>	<p>Aproveite as novas tecnologias para fazer o Chile, um país mais próspero, mais desenvolvido, mais humano e mais justo, em que cada compatriota pode desenvolver-se plenamente seus talentos e busque a felicidade.</p>	<p>Aspirar que o uso massivo de tecnologias se torne um meio de ajudar para reduzir as desigualdades; para abrir mais e melhores oportunidades de desenvolvimento e, assim, contribuir para o respeito aos direitos de todos os homens e mulheres chilenos.</p>
DOCUMENTO DE REFERÊNCIA	<p>Declaração de Florianópolis (2000). Encontro Regional de</p>	<p>Primeira Cúpula Mundial da Sociedade da Informação, realizada em Genebra entre 10 e 12 de dezembro de 2003.</p>	<p>– Agenda de Tunis para a Sociedade da Informação, Cúpula da Sociedade da</p>	<p>– Plano de Ação sobre a Sociedade da Informação e a Conhecimento da América Latina e do</p>	<p>– Plano de Ação sobre a Sociedade da Informação e a Conhecimento da América Latina e do</p>

FATORES	AGENDAS DIGITAIS				
	Chile: “Hacia la sociedad de la información” 1999	Agenda Digital: “Te acerca al futuro” 2004-2006	Estratégia digital 2007-2012	Agenda Digital “Imagina Chile” 2013-2020	Agenda Digital 2020 “Chile digital para tod@s” 2015-2020
ESTRANGEIROS INTERVENIENTES	Tecnologia da Informação para o Desenvolvimento, CEPAL, Florianópolis, Brasil, junho de 2000.		<p>Informação Mundial, 2005.</p> <p>– Plano de Ação sobre a Sociedade da Informação e a Conhecimento da América Latina e do Caribe, eLAC2015 (2011-2015),</p> <p>– Lima, novembro de 2010.</p>	<p>Caribe, eLAC2015 (2011-2015), Lima, novembro de 2010.</p> <p>– Recomendações de órgãos como a União Telecomunicações Internacionais (UIT)</p> <p>– As recomendações que emanam da Organização para Cooperação e Desenvolvimento Econômico (OCDE) no desenvolvimento digital.</p>	<p>Caribe, eLAC2015 (2011-2015), Lima, novembro de 2010.</p> <p>– Recomendações de órgãos como a União Telecomunicações Internacionais (UIT)</p> <p>– As recomendações que emanam da Organização para Cooperação e Desenvolvimento Econômico (OCDE) no desenvolvimento digital.</p> <p>– XI Conferência Regional sobre Mulheres na América Latina e no Caribe, organizado pela Comissão Econômica para a América Latina e o Caribe (CEPAL).</p>
ATOES PRINCIPAIS INSTITUCIONALIDADE	– Governo (Secretaria da Presidência, Ministério da	Grupo de Ação Digital (GAD), presidido pelo Coordenador de Governo TIC composta por	– Comitê de Ministros – Conselho Consultivo – Conselho Internacional	Grupos de trabalhos multissetoriais com a participação de diferentes	Grupos de trabalhos multissetoriais com a participação de diferentes

FATORES	AGENDAS DIGITAIS				
	Chile: “Hacia la sociedad de la información” 1999	Agenda Digital: “Te acerca al futuro” 2004-2006	Estratégia digital 2007-2012	Agenda Digital “Imagina Chile” 2013-2020	Agenda Digital 2020 “Chile digital para tod@s” 2015-2020
DA AGENDA DIGITAL	Economia, Subsecretaria de Telecomunicações). – Grupo de Trabalho Multidisciplinar proveniente do poder executivo, legislativo, sector privado, empresas.	instituições governamentais, organizações representantes do setor empresarial, acadêmico e outros poderes do Estado.	– Secretaria Executiva – Sector Privado – Sociedade Civil – Mesas Regionais TIC – Sector Público	atores do campo público, privado e acadêmico, "Diálogos Digital"	atores do campo público, privado e acadêmico.
OBJETIVOS ESPECÍFICOS	– Promover a universalização do Acesso. – Desenvolver novas capacidades competitivas. – Modernizar o Estado a serviço do cidadão	– Uma infraestrutura de informação sólida e segura em banda larga. – Uma força de trabalho alfabetizada digitalmente e uma mão de obra qualificada com padrões de excelência mundial em TIC. – Um Estado online ao serviço do cidadão. – Um e-commerce altamente desenvolvido. – Promover uma massa crítica de empresas de TIC capazes de competir internacionalmente.	– Aumentar a competitividade das empresas usando com intensidade as TIC. – Criar e fomentar uma nova cultura em TIC para aumentar a transparência e participação cidadã. – Promover o desenvolvimento de um governo de qualidade digital. – Aumentar a intensidade e profundidade de uso das TIC pelos alunos e pela sociedade civil.	– Incentivar a existência de uma infraestrutura TIC robusta, moderna e capaz de entregar serviços avançados com a qualidade necessária e com cobertura em todo o país. – Manter um mercado dinâmico e competitivo. – Maior inclusão digital da sociedade. – Estabelecer um quadro regulatório digital adequado e eficiente.	– Respeito total pelos direitos das pessoas que se relacionam com a Internet e TICs. – Obter uma conectividade universal que permita o acesso para todas as pessoas às redes de alta velocidade e qualidade. – Apoiar o uso e desenvolvimento de TICs para melhorar a qualidade de vida de todas as pessoas; contribuir para o desenvolvimento e

FATORES	AGENDAS DIGITAIS				
	Chile: “Hacia la sociedad de la información” 1999	Agenda Digital: “Te acerca al futuro” 2004-2006	Estratégia digital 2007-2012	Agenda Digital “Imagina Chile” 2013-2020	Agenda Digital 2020 “Chile digital para tod@s” 2015-2020
		<ul style="list-style-type: none"> – Um moderno quadro jurídico-regulatório que facilita o desenvolvimento da sociedade da informação. 		<ul style="list-style-type: none"> – Coordenar aos órgãos responsáveis pela promoção do desenvolvimento digital. – Gerar infraestrutura e condições de conectividade ideais em ensino. – Fomentar o desenvolvimento de competências digitais de graduados. – Gerar novos incentivos para treinamento contínuo em habilidades para o emprego. – Aprimorar os instrumentos de apoio direto para a inclusão das TIC no empreendedorismo e inovação. 	<ul style="list-style-type: none"> massificação da economia digital. – Posicionar as tecnologias a serviço da qualidade da educação. – Promover e sustentar o desenvolvimento de políticas públicas de desenvolvimento digital por meio de uma instância multissetorial que aborda o escopo e o impacto que tecnologia nas diferentes áreas da sociedade.

FATORES	AGENDAS DIGITAIS				
	Chile: “Hacia la sociedad de la información” 1999	Agenda Digital: “Te acerca al futuro” 2004-2006	Estratégia digital 2007-2012	Agenda Digital “Imagina Chile” 2013-2020	Agenda Digital 2020 “Chile digital para tod@s” 2015-2020
				<ul style="list-style-type: none"> - Promover um ambiente adequado para desenvolvimento nacional de soluções e ferramentas de TIC que apoiam todos os setores econômico. - Focar e alinhar os esforços TIC com as necessidades que contribuem para a competitividade de setores produtivos. - Modernizar o estado e a incorporação das TIC com uma perspectiva abrangente. - Incorporação de novas tecnologias em todos os setores produtivos. - Dirigir o desenvolvimento de conteúdo digital como um importante alavanca 	

FATORES	AGENDAS DIGITAIS				
	Chile: “Hacia la sociedad de la información” 1999	Agenda Digital: “Te acerca al futuro” 2004-2006	Estratégia digital 2007-2012	Agenda Digital “Imagina Chile” 2013-2020	Agenda Digital 2020 “Chile digital para tod@s” 2015-2020
				para promover a riqueza de nossas culturas.	
ÁREAS / LINHAS DE AÇÃO /EIXOS	<ul style="list-style-type: none"> - Educação e capacitação - Empresas e mercados - Tecnologias para aprofundar as redes e cadeias produtivas - Governo eletrônico 	<ul style="list-style-type: none"> - Acesso - Educação e capacitação - Governo eletrônico - Empresas - Indústria de TIC - Quadro jurídico-regulatório 	<ul style="list-style-type: none"> - Política tecnológica para o desenvolvimento digital. - Projetos e programas de desenvolvimento digital. - Estratégia de desenvolvimento da indústria TIC. - Desenho institucional 	<ul style="list-style-type: none"> - Conectividade e inclusão digital - Entorno para o desenvolvimento digital - Educação e capacitação - Inovação e empreendimento - Serviços e aplicativos digitais. 	<ul style="list-style-type: none"> - Direitos para o desenvolvimento Digital - Conectividade Digital - Governo Digital - Economia Digital - Competências Digitais
INICIATIVAS / AÇÕES ESPECÍFICAS	60	34	9	30	13/60

APÉNDICE B – Decreto presidencia N.001, Instrui a implementación da Política nacional de Cibersegurança



GAB.PRES. N° 001

ANT.: Decreto supremo N° 533, de 27 de abril de 2015, que crea el Comité Interministerial sobre Ciberseguridad.

MAT.: Instruye implementación de la Política Nacional sobre Ciberseguridad.

SANTIAGO, 27 ABR 2017

**DE: MICHELLE BACHELET JERIA
PRESIDENTA DE LA REPÚBLICA**

A: SEGÚN DISTRIBUCIÓN

I. ANTECEDENTES

1. El programa de Gobierno para el período 2014-2018 propone desarrollar una estrategia de seguridad digital que proteja a los usuarios privados y públicos, basado en el diagnóstico que la masificación en el uso de tecnologías de información y comunicaciones (TIC), conlleva riesgos que pueden afectar los derechos de las personas, la seguridad pública, las infraestructuras críticas, el gobierno digital, los intereses esenciales y la seguridad exterior de Chile.
2. En cumplimiento de ese compromiso, el 27 abril de 2015, mediante decreto supremo N° 533 de 2015 del Antecedente, instruí la creación del Comité Interministerial sobre Ciberseguridad (el Comité), de carácter permanente, el que tuvo por misión proponer una Política Nacional de Ciberseguridad (la Política) y asesorar en la coordinación de acciones, planes y programas de los distintos actores institucionales en la materia.
3. El Comité desempeñó sus funciones durante el año 2015 y en febrero de 2016, sometiendo a consulta pública un borrador de propuesta de Política Nacional de Ciberseguridad, de conformidad a lo dispuesto en la ley N° 20.500 sobre Participación Ciudadana en la Gestión Pública.
4. Mediante oficio conjunto MISP/MDN.GAB(P) N° 1421, de 21 de septiembre de 2016, del Ministro del Interior y Seguridad Pública y del Ministro de Defensa Nacional, me fue presentado el texto final de la Política Nacional de Ciberseguridad aprobado por el Comité Interministerial sobre Ciberseguridad, cuyas propuestas son objeto del presente instructivo.
5. La presente Política Nacional de Ciberseguridad constituye el primer instrumento de política pública del Estado de Chile que orientará la acción



del país en esta materia de ciberseguridad, con el objetivo de contar con un ciberespacio libre, abierto, seguro y resiliente.

II. MOTIVOS

Chile requiere de una Política Nacional de Ciberseguridad por las siguientes razones:

- a. Para resguardar la seguridad de las personas en el ciberespacio. Es necesario brindar a las personas un nivel de seguridad que les permita el normal desarrollo de sus actividades personales, sociales y comunitarias en el ciberespacio, junto con el ejercicio de derechos fundamentales como la libertad de expresión, el acceso a la información, la protección de la vida privada y la propiedad.
- b. Para proteger la seguridad del país. Es necesario promover el resguardo de las redes y sistemas informáticos del sector público y privado, especialmente aquellas que son esenciales para el adecuado funcionamiento del país, velando por la continuidad operacional de los servicios básicos.
- c. Para promover la colaboración y coordinación entre instituciones. Es necesario mejorar las instancias de comunicación, coordinación y colaboración entre instituciones, organizaciones y empresas, de los sectores público y privado, nacional e internacional, con el propósito de fortalecer la confianza y entregar una respuesta común a los riesgos que se originan en el ciberespacio.
- d. Para gestionar los riesgos del ciberespacio. Es necesario considerar el desarrollo de procesos de análisis y gestión de riesgos que permitan identificar las vulnerabilidades, amenazas y riesgos implícitos en el uso, procesamiento, almacenamiento y transmisión de la información, junto a la generación de las capacidades para la prevención y la recuperación ante incidentes de ciberseguridad que se presenten, configurando un ciberespacio estable y resiliente.

III. OBJETIVOS DE LA POLÍTICA PARA EL AÑO 2022

La Política contiene los lineamientos estratégicos del Estado de Chile en materia de ciberseguridad, con una mirada que apunta al año 2022, y sus objetivos esenciales son:

1. El país contará con una infraestructura de la información robusta y resiliente, preparada para resistir y recuperarse de incidentes de ciberseguridad, bajo una óptica de gestión de riesgos.
2. El Estado velará por los derechos de las personas en el ciberespacio
3. Chile desarrollará una cultura de la ciberseguridad en torno a la educación, buenas prácticas y responsabilidad en el manejo de tecnologías digitales.
4. El país establecerá relaciones de cooperación en ciberseguridad con otros actores y participará activamente en foros y discusiones internacionales.



5. El país promoverá el desarrollo de una industria de la ciberseguridad, que sirva a sus objetivos estratégicos.

IV. INSTRUCCIONES

Teniendo presente los Antecedentes, Motivos y Objetivos previamente expuestos, he resuelto: Aprobar la Política Nacional de Ciberseguridad propuesta por el Comité Interministerial sobre Ciberseguridad; así como también los compromisos adoptados por los Ministerios y Servicios integrantes de éste. Además, he resuelto instruir a las secretarías de Estado que realicen los estudios pertinentes para el fortalecimiento de nuestras instituciones y legislación aplicable, para lo que deberán adoptar las medidas necesarias para cumplir con los compromisos asumidos, dentro del ámbito de sus competencias.

Para ello, el Comité Interministerial sobre Ciberseguridad actuará como instancia de coordinación en la implementación de la Política Nacional sobre Ciberseguridad y sus medidas de política pública, por parte de sus integrantes, en ejercicio de sus competencias legales.

Por ello deberán participar en una o más instancias de colaboración multisectorial con los representantes de los sectores públicos y privados, incluyendo organizaciones no gubernamentales, organizaciones gremiales e instituciones de educación superior, entre otras, que posean incidencia en la materia del presente instructivo.

Saluda atentamente a Ud.



MICHELLE BACHELET JERIA

Presidenta de la República

DISTRIBUCIÓN

1. Sr. Ministro del Interior y Seguridad Pública
2. Sr. Ministro de Relaciones Exteriores
3. Sr. Ministro de Defensa Nacional
4. Sr. Ministro de Hacienda
5. Sr. Ministro Secretario General de la Presidencia
6. Sra. Ministra Secretaria General de Gobierno
7. Sr. Ministro de Economía, Fomento y Turismo
8. Sr. Ministro de Desarrollo Social
9. Sra. Ministra de Educación
10. Sr. Ministro de Justicia y Derechos Humanos
11. Sra. Ministra del Trabajo y Previsión Social
12. Sr. Ministro de Obras Públicas
13. Sra. Ministra de Salud
14. Sra. Ministra de Vivienda y Urbanismo
15. Sr. Ministro de Agricultura
16. Sra. Ministra de Minería