**UNIVERSIDADE DE BRASÍLIA**
**FACULDADE DE CIÊNCIA DA INFORMAÇÃO**
**PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA INFORMAÇÃO**

Eduardo Wallier Vianna

# Segurança da informação digital: proposta de modelo para a Ciber Proteção nacional

Brasília – DF

2019

**UNIVERSIDADE DE BRASÍLIA**
**FACULDADE DE CIÊNCIA DA INFORMAÇÃO**
**PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA INFORMAÇÃO**

# Segurança da informação digital: proposta de modelo para a Ciber Proteção nacional

Eduardo Wallier Vianna

Tese apresentada à Faculdade de Ciência da Informação, do Programa de Pós-graduação em Ciência da Informação da Universidade de Brasília como requisito parcial para a obtenção do grau de Doutor em Ciência da Informação

**Área de concentração:** Gestão da Informação
**Linha de pesquisa:** Organização da Informação

**Orientador:** Prof. Dr. Renato Tarciso Barbosa de Sousa – UnB

Brasília – DF
2019

Ficha catalográfica


VED24s

Vianna, Eduardo Wallier
Segurança da informação digital: proposta de modelo para a Ciber Proteção nacional / Eduardo Wallier Vianna; orientador Renato Tarciso Barbosa Sousa . -- Brasília, 2019
292 p.

Tese (Doutorado - Doutorado em Ciência da Informação) -- Universidade de Brasília, 2019.

1. Segurança da Informação. 2. Segurança Cibernética. 3. Defesa Cibernética. 4. Gestão da Informação Digital. 5. Ciber Proteção. I. Sousa , Renato Tarciso Barbosa , orient. II. Título.

Faculdade de Ciência da Informação (FCI)
UnB Programa de Pós-Graduação em Ciência da Informação (PPGCINF)

**FOLHA DE APROVAÇÃO**

**Título:** "SEGURANÇA DA INFORMAÇÃO DIGITAL: PROPOSTA DE MODELO PARA A CIBER PROTEÇÃO NACIONAL"

**Autor (a):** Eduardo Wallier Vianna

**Área de concentração:** Gestão da Informação
**Linha de pesquisa:** Organização da informação

Tese submetida à Comissão Examinadora designada pelo Colegiado do Programa de Pós-graduação em Ciência da Informação da Faculdade de Ciência da Informação da Universidade de Brasília como requisito parcial para obtenção do título de **Doutor** em Ciência da Informação.

Tese aprovada em: 28 de fevereiro de 2019.

Renato Tarciso B. de Sousa

**Prof. Dr. Renato Tarciso Barbosa de Sousa**
Presidente (PPGCINF/UnB)

**Profª Drª Maria Manuela Gomes de Azevedo Pinto**
Membro Externo (U.Porto)

**Prof. Dr. Edison Ishikawa**
Membro Externo (CIC/UnB)

**Prof. Dr. Rogério Henrique de Araújo Júnior**
Membro Interno (PPGCINF/UnB)

**Profª Drª Lillian Maria Araújo de Rezende Álvares**
Suplente (PPGCINF/UnB)

**A minha família querida**

***Mônica, Aninha e Carlinhos***

razão do meu viver

amor incondicional

fonte inspiradora

porto seguro

**AGRADECIMENTOS**

À assistente do PPGCINF *Vívian Miatelo*
pela colaboração e solicitude.

Às professoras
*Maria de Lourdes Barbosa Vianna* e *Maria Manuela Pinto*
pelo especial desvelo e compartilhamento generoso dos seus conhecimentos.

A *colega do PPGCINF*
*Sonia Araújo de Assis Boeres*
pelo companheirismo e apoio imprescindíveis na realização desse desafio.

Ao meu Orientador, Professor *Renato Tarciso Barbosa de Sousa*
pela confiança no enfrentamento dos desafios, disponibilidade oportuna
e conhecimentos compartidos.

Aos *meus pais Regina Wallier Vianna e Bento Barbosa Vianna*,
pelas lições de vida que me transmitem e pelos exemplos de superação
e determinação na busca das convicções, aspirações e sonhos.

Ao *nosso **DEUS**,*
por tudo.

Muito obrigado

*O direito de errar é tão normal e humano quanto o dever de acertar.*

*Se queres a paz digital, prepara-te para a guerra cibernética.*

## RESUMO

Este estudo analisa a segurança da informação digital no ciberespaço de interesse nacional. No âmbito da Ciência da Informação, torna-se inevitável e desafiador avançar em estudos diversificados, tais como promover o debate e o desenvolvimento de procedimentos de segurança e de gestão da informação, particularmente em um espaço informacional típico, como o cibernético. No desenvolvimento desta pesquisa exploratória/descritiva, a construção do conceito de Ciber Proteção, *core* deste estudo, foi alicerçado nas vivências operacionais do autor e nas contribuições teóricas e metodológicas da Ciência da Informação, bem como inserida na realidade brasileira e orientada pelos anseios e objetivos de um Estado-Nação soberano como o Brasil. A Ciber Proteção possui, por premissa, contemplar a gestão da informação digital em toda sua extensão, independentemente da teoria ou da metodologia utilizada, integrando, particularmente: segurança da informação da informação em meio digital, segurança cibernética, preservação digital, infraestruturas críticas/estratégicas, gerenciamento de incidentes, defesa cibernética e soberania nacional. As atividades e inquéritos internacionais, bem como o estudo empírico, baseado em entrevistas com especialistas de destaque no cenário cibernético da Administração Pública Federal, possibilitaram a estruturação e a validação da proposta de um modelo nacional para a Ciber Proteção. O Modelo proposto resulta em dois grupos distintos: o primeiro abrange o diagnóstico, a análise e a visão sistêmica da proteção da informação no meio digital brasileira; o segundo grupo, tipicamente intervencionista, estrutura-se em três pilares: uma política nacional, uma entidade de Estado e um centro de competências em Ciber Proteção. Mais à frente, espera-se que os resultados obtidos com a presente pesquisa contribuam para a redução das vulnerabilidades e a mitigação das ameaças aos recursos informacionais em ambiente digital, nas organizações e instituições imbricadas com a Segurança e a Defesa do País.



**Palavras-chave:** Segurança da informação. Segurança cibernética. Defesa cibernética. Gestão da informação digital. Ciber Proteção.

## ABSTRACT

This study analyzes the security of digital information in cyberspace of national interest. In the field of Information Science it is inevitable and challenging to advance in diversified studies such as promoting the debate and development of security procedures and information management particularly in a typical information space such as cybernetics. In the development of this exploratory / descriptive research the construction of the concept of Cyber Protection core of this study was based on the operational experiences of the author and on the theoretical and methodological contributions of Information Science, as well as inserted in the Brazilian reality and guided by the aims and objectives of a sovereign nation-state like Brazil. Cyber Protection has as its premise to contemplate the management of digital information in all its extension regardless of the theory or methodology used integrating particularly: information security in the digital media, cybersecurity, digital preservation, critical/strategic infrastructures, management of incidents, cyber defense and national sovereignty.

International activities and surveys, as well as the empirical study based on interviews with leading experts in the cybernetic scenario of the Federal Public Administration, allowed the structuring and validation of the proposal of a national model for Cyber Protection. The proposed model results in two distinct groups: the first covers the diagnosis, analysis and systemic view of information protection in the Brazilian digital environment; the second group typically interventionist is structured in three pillars: a national policy, a State entity and a competence center in Cyber Protection. Further on, it is expected that the results obtained with this research contribute to the reduction of vulnerabilities and mitigation of the threats to the information resources in the digital environment, in organizations and institutions imbricated with the Security and Defense of the Country.



**Keywords**: Information security. Cyber security. Cyber defense. Management of digital information. Cyber Protection.


.

## LISTA DE FIGURAS


Figura 1 - Estruturas públicas e privadas na segurança dos GE.............................24
Figura 2 - Evolução das políticas e responsabilidades em SegInf ...........................36
Figura 3 - Influências e componentes da pesquisa ................................................41
Figura 4 - Desenho básico da pesquisa .................................................................42
Figura 5 - Bases para desenvolvimento da pesquisa..............................................43
Figura 6 - Percurso investigativo da pesquisa.........................................................46
Figura 7 - Sistemas estratégicos e estruturantes da APF .......................................49
Figura 8 - Comparação entre investigação empírica e investigação-ação ...............58
Figura 9 - Revisão da literatura ..............................................................................61
Figura 10 - Mosaico metodológico quadripolar........................................................72
Figura 11 - Formatos de arquivo utilizados nos órgãos públicos..............................89
Figura 12 - Organograma do NIC.br.........................................................................94
Figura 13 - Diagrama da Estratégia de Governança Digital ...................................107
Figura 14 - Estudo científico da GI – abordagem problemas .................................143
Figura 15 - Mapa de Caixas LOCKSS da Rede Cariniana.....................................155
Figura 16 - Mapa estratégico da ESIC (2015-2018)...............................................171
Figura 17 - Segurança cibernética e outras seguranças........................................173
Figura 18 - Exemplo de infraestruturas críticas no Brasil .......................................184
Figura 19 - Modelo de construção de conceito.......................................................192
Figura 20 - Triângulo do Conceito .........................................................................193
Figura 21 - Bússola da Ciber Proteção .................................................................197
Figura 22 - Entrantes da Ciber Proteção................................................................203
Figura 23 - Visão sistêmica preliminar da gestão da informação digital.................203
Figura 24 - Questão 1 - Desafios da informação no ciberespaço...........................217
Figura 25 - Questão 2 - Atuação governamental no ciberespaço ..........................218
Figura 26 - Questão 3 - Requisitos para a gestão segura da informação ..............219
Figura 27 - Questão 4 - Gestão da informação em estruturas heterogêneas .........220
Figura 28 - Questão 5 - Soluções políticas/regulatórias governamentais ..............221
Figura 29 - Questão 6 - Pontos-chave para otimização .........................................222
Figura 30 - Questão 7 - Entidade articuladora e normativa....................................223
Figura 31 - Questão 8 - Competências e centro aglutinador..................................224

Figura 32 - Elementos de um incidente de segurança ...........................................237
Figura 33 - Sistema de Gerenciamento de Incidentes de Redes (SGIR)................239
Figura 34 - Sistema Militar de Defesa Cibernética (SMDC) ...................................241
Figura 35 - Sistema de Proteção das Infraestruturas Críticas (SPIC) .....................243
Figura 36 - Sistema de Preservação da Informação Digital (SPID).........................245
Figura 37 - Sistema de Segurança da Informação e Cibernética (SSIC) ................248
Figura 38 - CICC e a abordagem Hélice Tríplice....................................................250
Figura 39 - Visão conceitual da Entidade Nacional de Ciber Proteção ...................253
Figura 40 - Política Nacional de Ciber Proteção – ciclo inicial................................257
Figura 41 - Modelo de Ciber Proteção Nacional.....................................................263
Figura 42 - Mandala do Modelo de Ciber Proteção Nacional..................................269

## LISTA DE QUADROS

Quadro 1 - Elementos norteadores da pesquisa ..................................................... 53
Quadro 2 - Análise documental ........................................................................ 63
Quadro 3 - Trabalhos acadêmicos correlatos.......................................................... 65
Quadro 4 - As hipóteses, as variáveis e os instrumentos de pesquisa ..................... 68
Quadro 5 - Aplicação do Método Quadripolar .......................................................... 70
Quadro 6 - Objetivos e caminhos metodológicos ..................................................... 73
Quadro 7 - Dimensões da Observação Participante ................................................. 74
Quadro 8 - Compartilhamento de resultados e melhores práticas ............................ 76
Quadro 9 - Descentralização da governança da Internet no Brasil ........................... 99
Quadro 10 - Modelos teóricos de Gestão de Informação....................................... 132
Quadro 11 - Gestão de documentos ..................................................................... 134
Quadro 12 - Síntese do conceito de Ciber Proteção .............................................. 194
Quadro 13 - Estudo empírico – levantamento de requisitos................................... 201
Quadro 14 - Estudo empírico – consolidação e validação dos requisitos ............... 205
Quadro 15 - Elementos do modelo de Ciber Proteção ........................................... 225
Quadro 16 - Normas complementares à IN 01/GSI ................................................ 246
Quadro 17 - Níveis de Decisão no MSCP .............................................................. 264

## LISTA DE TABELAS

Tabela 1 - Proteção da informação no ciberespaço ............................................... 207
Tabela 2 - Gestão da Informação segura e organizacional ..................................... 209
Tabela 3 - Modelo de Ciber Proteção – APF .......................................................... 211
Tabela 4 - Modelo de Ciber Proteção – Competências ........................................... 213

## ABREVIATURAS, SIGLAS E ACRÔNIMOS

| | |
|---|---|
| ABIN | Agência Brasileira de Inteligência |
| ABNT | Associação Brasileira de Normas Técnicas |
| AC | Autoridade Certificadora |
| ANATEL | Agência Nacional de Telecomunicações |
| APF | Administração Pública Federal |
| BNDES | Banco Nacional de Desenvolvimento Econômico e Social |
| BRAJIS | Brazilian Journal of Information Science: research trends |
| CASNAV | Centro de Análises de Sistemas Navais |
| CCDA | Centro de Coordenação de Defesa de Área |
| CCI | Ciências de Comunicação e de Informação |
| CDCiber | Centro de Defesa Cibernética |
| CEGSIC | Curso de Especialização em Gestão da Segurança da Informação e Comunicações |
| CEPESC | Centro de Pesquisa e Desenvolvimento para a Segurança das Comunicações |
| CERT.br | Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil |
| CGI.br | Comitê Gestor da Internet no Brasil |
| CGSI/CDN | Comitê Gestor de Segurança da Informação do Conselho de Defesa Nacional |
| CGTI | Coordenador Geral de Tecnologia da Informação |
| CI | Ciência da Informação |
| CICCR | Centros Integrados de Comando e Controle Regionais |
| CICTE/OEA | Comitê Interamericano Contra o Terrorismo da Organização dos Estados Americanos |
| COMSIC | Comunidade em Segurança da Informação e Criptografia |
| CONARQ | Conselho Nacional de Arquivos |
| CPD | Centro de Processamento de Dados/ Centro de Informática (UnB) |
| CREDEN | Câmara de Relações Exteriores e Defesa Nacional |
| CRFB | Constituição da República Federativa do Brasil |
| CS | Ciências Sociais |
| CSIRT | Computer Security Incident Response Team |
| CTC | Comitê Técnico Científico |
| CTI | Centro de Tecnologia da Informação Renato Archer |

| | |
|---|---|
| CTIR Gov | Centro de Tratamento de Incidentes de Segurança de Redes de Computadores da APF – Presidência da República |
| DATAGOVS | Ambientes de armazenamento controlados pelo governo |
| DATAPREV | Empresa de Tecnologia e Informações da Previdência Social |
| DATASUS | Departamento de Informática do Sistema Único de Saúde |
| DefCiber | Defesa Cibernética |
| DeltCI | *Dicionário Eletrônico de Terminologia em Ciência da Informação* |
| DMDC | Doutrina Militar de Defesa Cibernética |
| EaD | Ensino a Distância |
| e-ARQ Brasil | Modelo de requisitos para sistemas informatizados de gestão arquivística de documentos |
| EB | Exército Brasileiro |
| EEA | Entrevistado estrangeiro alfa |
| EGD | Estratégia de Governança Digital da Administração Pública Federal |
| e-gov | Governo eletrônico |
| $E^n$ | Entrevistado da APF número ... |
| EnaDCiber | Escola Nacional de Defesa Cibernética |
| ENCP | Entidade Nacional de Ciber Proteção |
| END | Estratégia Nacional de Defesa |
| ENISA | European Union Agency for Network and Information Security |
| ESIC | Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal 2015-2018 |
| ETIR | Equipe de Tratamento de Incidentes de Segurança de Redes de Computadores |
| EU/ISSO | European Union/União Europeia |
| FA | Forças Armadas |
| FCC | Faculdade de Ciência da Computação |
| FEBRABAN | Federação Brasileira de Bancos |
| FINEP | Financiadora de Estudos e Projetos |
| FIRST | Forum of Incident Response and Security Teams |
| FLUP | Faculdade de Letras da Universidade do Porto |
| GC | Gestão do Conhecimento |
| GI | Gestão da Informação |
| GRISB | Grupo de Resposta a Incidente de Segurança dos Bancos |
| GRN-7/ CBC3 | Grupo Relator de Normalização de Telecomunicações 7, da Comissão Brasileira de Comunicações 3 |
| GSI | Gabinete de Segurança Institucional da Presidência da República |

| | |
|---|---|
| GT | Grounded Theory |
| GTI | Grupo de Trabalho Interministerial |
| HSM | Hardware Security Module |
| IC | Infraestruturas Críticas |
| ICCYBER | Conferência Internacional de Perícias em Crimes Cibernéticos |
| ICP-Brasil | Infraestrutura de Chaves Públicas Brasileira |
| IME | Instituto Militar de Engenharia |
| ISO/IEC | International Organization of Standardization/International Electro-technical Commission |
| ITA | Instituto Tecnológico de Aeronáutica |
| ITI | Instituto Nacional de Tecnologia da Informação |
| LAAD | Latin America Aerospace and Defence |
| LACNIC | Registro de Endereçamento de Internet para América Latina e Caribe |
| LAI | *Lei de acesso à informação* |
| LGPDP | *Lei geral sobre a proteção de dados pessoais* |
| LNCC | Laboratório Nacional de Computação Científica |
| LV | Laboratório Virtual |
| MC | Ministério das Comunicações |
| MCI | Marco Civil da Internet |
| MCPN | Modelo de Ciber Proteção Nacional |
| MCTIC/MCTI | Ministério da Ciência, Tecnologia, Inovação e Comunicações |
| MD | Ministério da Defesa |
| MDIC | Ministério do Desenvolvimento, Indústria e Serviço |
| ME | Ministério dos Esportes |
| MEC | Ministério da Educação |
| MF | Ministério da Fazenda |
| MI | Ministério da Integração Nacional |
| MinC | Ministério da Cultura |
| MJ | Ministério da Justiça e Segurança Pública |
| MME | Ministério de Minas e Energia |
| MPOG | Ministério do Planejamento, Orçamento e Gestão |
| MRE | Ministério das Relações Exteriores |
| MS | Ministério da Saúde |
| MSCP | Macrossistema de Ciber Proteção |
| MT | Ministério dos Transportes, Portos e Aviação Civil |

| | |
|---|---|
| Mtur | Ministério do Turismo |
| NC | Normas Complementares do DSIC/GSI |
| NSA | National Security Agency – USA |
| OCDE | Organização para a Cooperação e Desenvolvimento Econômico |
| OEA | Organização dos Estados Americanos |
| ONU | Organização das Nações Unidas |
| OTAN | Organização do Tratado do Atlântico Norte |
| PD | Preservação Digital |
| PDCA | Plan (planejamento) – Do (fazer) – Check (checar) – Act (Atuar) |
| PNCP | Política Nacional de Ciber Proteção |
| PND | Política Nacional de Defesa |
| PNDA | Política Nacional de Dados Abertos |
| PNSIC | Política Nacional de Segurança de Infraestruturas Críticas |
| PNSI | Política Nacional de Segurança da Informação |
| PPGCINF | Programa de Pós-graduação em Ciência da Informação |
| PR | Presidência da República |
| RDC-Arq | Repositórios Arquivísticos Digitais Confiáveis |
| RENASIC | Rede Nacional em Segurança da Informação e Criptografia |
| RICI | *Revista Ibero-americana de Ciência da Informação* |
| RTIR | Request Tracker for Incident Response |
| SAE | Secretaria de Assuntos Estratégicos – Presidência da República |
| SBSeg | Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais |
| SCADA | Supervisory Control and Data Acquisition |
| SegCiber | Segurança Cibernética |
| SegInf | Segurança da Informação |
| SEGINFO | Workshop de Segurança da Informação |
| SemSIC | Seminários de SIC |
| SEPIN | Secretaria de Política de Informática. |
| SERPRO | Serviço Federal de Processamento de Dados |
| SETIC | Secretaria de Tecnologia da Informação e Comunicação do MCTIC |
| SGIR | Sistema de Gerenciamento de Incidentes de Redes |
| SI | Sistemas de Informação |
| SIC | Segurança da Informação e Comunicações |
| SIGA | Sistema de Gestão de Documentos de Arquivo |

| | |
|---|---|
| SISP | O Sistema de Administração dos Recursos de Tecnologia da Informação do MPOG |
| SLTI | Secretaria de Logística e Tecnologia da Informação do MPOG |
| SMDC | Sistema Militar de Defesa Cibernética |
| SPIC | Sistema de Proteção das Infraestruturas Críticas |
| SPID | Sistema de Preservação da Informação Digital |
| SSIC | Sistema de Segurança da Informação e Cibernética |
| TA | Tecnologia de Automação |
| TCU | Tribunal de Contas da União |
| TI | Tecnologia da Informação |
| TIC | Tecnologias da Informação e Comunicação |
| UA | Universidade de Aveiro |
| UFCG | Universidade Federal de Campina Grande |
| UFMG | Universidade Federal de Minas Gerais |
| UnB | Universidade de Brasília |
| UNCSD (Rio+20) | Conferência das Nações Unidas sobre Desenvolvimento Sustentável |
| UPORTO | Universidade do Porto |
| v. t. | ver também |
| W3C | World Wide Web Consortium |
| WEF | World Economic Forum |
| WICI | Workshop Internacional em Ciência da Informação |

## SUMÁRIO


**1 INTRODUÇÃO ........................................................................ 22**

1.1 Considerações Iniciais ........................................................................ 22

1.2 Contextualização da Tese ........................................................................ 25

1.3 Justificativas ........................................................................ 30

1.4 Desenho básico da pesquisa ........................................................................ 41

**2 PROPOSIÇÕES DA PESQUISA ........................................................................ 44**

2.1 Problema e Objetivos ........................................................................ 44

2.2 Delimitações da pesquisa ........................................................................ 45

*2.2.1 O universo investigado ........................................................................ 47*

*2.2.2 Administração Pública Federal ........................................................................ 48*

2.3 Hipóteses, Variáveis e a Tese ........................................................................ 50

*2.3.1 Hipóteses ........................................................................ 50*

*2.3.2 Variáveis ........................................................................ 51*

*2.3.3 Construção da Tese ........................................................................ 52*

**3 CAMINHOS METODOLÓGICOS ........................................................................ 55**

3.1 Trilhas investigativas ........................................................................ 56

3.2 Observação ........................................................................ 59

3.3 Levantamento para a Revisão da Literatura ........................................................................ 61

*3.3.1 Pesquisa Bibliográfica ........................................................................ 61*

*3.3.2 Análise documental ........................................................................ 62*

*3.3.3 Trabalhos acadêmicos correlatos ........................................................................ 64*

3.4 *Entrevistas* ........................................................................ 66

3.5 Abordagem Quadripolar ........................................................................ 68

**4. OBSERVAÇÃO PARTICIPANTE ........................................................................ 74**

4.1 Atividades realizadas ........................................................................ 74

4.2 Comunicação e registros da Observação Participante ........................................................................ 75

**5 O CIBERESPAÇO – UMA REALIDADE ........................................................................ 79**

5.1 Ciberespaço ........................................................................ 81

5.2 O ciberespaço e o contexto nacional ........................................................................ 86

*5.2.1 A governança da Internet no Brasil ........................................................................ 90*

5.2.1.1 Comitê Gestor da Internet no Brasil ........................................................................ 91

5.2.*1*.2 Marco Civil da Internet ........................................................................ 96

*5.2.2 Outros Instrumentos norteadores* ........ *100*
5.2.2.1 *Lei de Acesso à Informação* ........ 100
5.2.2.2 Política Nacional de Dados Abertos ........ 102
5.2.2.3 Privacidade e Proteção de Dados ........ 104
5.2.2.4 Estratégia de Governança Digital ........ 106
5.2.2.5 Estratégia Brasileira para a Transformação Digital ........ 109
**6 O AMBIENTE INFORMACIONAL ........ 114**
6.1 A INFORMAÇÃO NO MEIO DIGITAL ........ 114
*6.1.1 O papel transformador da informação digital* ........ *120*
*6.1.2 Novas Tecnologias da Informação e da Comunicação* ........ *123*
*6.1.3 O Estado digital e o poder cibernético* ........ *127*
6.2 GESTÃO DA INFORMAÇÃO E A CI ........ 130
*6.2.1 Aspectos inerentes à segurança na gestão em CI* ........ *133*
*6.2.2 Desafios da Gestão na Ciência da Informação* ........ *142*
6.3 PRESERVAÇÃO DIGITAL ........ 145
*6.3.1 A Preservação Digital e a Tecnologia da Informação* ........ *146*
*6.3.2 A PD governamental – uma abordagem* ........ *151*
**7 PROTEÇÃO DA INFORMAÇÃO NO CIBERESPAÇO ........ 157**
7.1 SEGURANÇA DA INFORMAÇÃO ........ 161
*7.1.1 Segurança da informação na Administração Pública Federal* ........ *163*
*7.1.2 A certificação da informação em meio digital* ........ *166*
*7.1.3 Estratégia de Segurança da Informação e Comunicações* ........ *171*
7.2 SEGURANÇA CIBERNÉTICA ........ 172
7.3 DEFESA CIBERNÉTICA ........ 174
7.4 GUERRA CIBERNÉTICA ........ 179
7.5 INFRAESTRUTURAS CRÍTICAS ........ 184
**8 A GÊNESE DA CIBER PROTEÇÃO ........ 190**
8.1 BASES DO CONCEITO CIBER PROTEÇÃO ........ 191
*8.1.1 A Teoria do Conceito* ........ *191*
*8.1.2 Construindo o conceito de Ciber Proteção* ........ *193*
8.2 CIBER PROTEÇÃO - UMA PROPOSTA CONCEITUAL ........ 195
**9 ESTUDO EMPÍRICO ........ 199**
9.1 LEVANTAMENTO PRELIMINAR DE REQUISITOS ........ 200
9.2 ESPECIALISTAS DA APF – DEMONSTRAÇÃO DE RESULTADOS ........ 205
9.3 ESPECIALISTAS DA APF - ANÁLISE DOS RESULTADOS ........ 216

*9.3.1. Q1 – Ciberespaço e seus desafios* ... *217*
*9.3.2 Q2 – Ciberespaço e a atuação governamental* ... *218*
*9.3.3 Q3 – Requisitos para a gestão segura da informação digital* ... *219*
*9.3.4 Q4 – Gestão da informação em estruturas heterogêneas* ... *220*
*9.3.5 Q5 – Soluções políticas/regulatórias governamentais* ... *221*
*9.3.6 Q6 – Pontos-chave para otimização* ... *222*
*9.3.7 Q7 – Entidade articuladora e normativa* ... *223*
*9.3.8 Q8 – Competências e centro aglutinador* ... *224*
**10 MODELO PARA A CIBER PROTEÇÃO NACIONAL - MCPN ... 225**
*10.1 CIBER PROTEÇÃO – ANÁLISE CONTEMPORÂNEA* ... 227
10.2 MACROSSISTEMA DA CIBER PROTEÇÃO - MSCP ... 235
*10.2.1 Sistema de Gerenciamento de Incidentes de Redes (SGIR)* ... *237*
*10.2.2 Sistema Militar de Defesa Cibernética (SMDC)* ... *239*
*10.2.3 Sistema de Proteção das Infraestruturas Críticas (SPIC)* ... *241*
*10.2.4 Sistema de Preservação da Informação Digital (SPID)* ... *243*
*10.2.5 Sistema de Segurança da Informação e Cibernética (SSIC)* ... *246*
10.3 AGENTES INTERVENIENTES ... 248
*10.3.1 Centro de Inovação e Competências Cibernéticas (CICC)* ... *249*
*10.3.2 Entidade Nacional de Ciber Proteção (ENCP)* ... *252*
*10.3.3 Política Nacional de Ciber Proteção (PNCP)* ... *254*
**11 CONSIDERAÇÕES FINAIS ... 259**
11.1 PRETÉRITO - PRIMÍCIAS DO ESTUDO ... 259
11.2 PRESENTE - VISÃO CONSOLIDADA DO MCPN ... 262
11.3 FUTURO – DESDOBRAMENTOS E CONCLUSÕES ... 268
**REFERÊNCIAS ... 274**
**APÊNDICE A - LEVANTAMENTO DE REQUISITOS ... 288**
**APÊNDICE B - ENTREVISTA ADMINISTRAÇÃO PÚBLICA FEDERAL ... 289**

# 1 INTRODUÇÃO

## 1.1 CONSIDERAÇÕES INICIAIS

Em meados da década de 1990, ao apresentar as características gerais que constituem a razão da existência e da evolução da Ciência da Informação (CI), Saracevic (1996) afirmou que a mesma está inexoravelmente ligada à tecnologia da informação (TI)[1], participando, ativa e deliberadamente, na evolução da sociedade da informação. O autor destacou o importante papel a desempenhar por sua forte dimensão social e humana, que ultrapassa a tecnologia, ressaltando a vocação da CI para a interdisciplinaridade[2] particularmente com a Ciência da Computação (CC). Na recuperação/comunicação da informação (“tornar mais acessível um acervo crescente de conhecimento”) e buscando a complementariedade entre as Ciências, o autor subentende que uma questão fundamental para a Computação: “o que pode ser (eficientemente) automatizado?” e que seja compartilhada com o escopo de estudo da Ciência da Informação.

Após duas décadas da afirmação de Saracevic (1996), vive-se em plena sociedade do conhecimento e das redes, onde a informação trafega em fluidos ambientes digitais e os dados são armazenados em sistemas de informação[3] computadorizados. Nesta nova realidade mundial, apoiado pelo uso massivo da rede mundial de computadores (Internet), sugere-se ampliar o questionamento de Saracevic para: “o que pode ser automatizado” **e como garantir a proteção[4] dessa informação?**

---

[1] Reconhecida neste estudo como sinônimo de TIC - Tecnologia da Informação e Comunicação**:** ativo estratégico que apoia processos de negócios institucionais, mediante a conjugação de recursos, processos e técnicas utilizados para obter, processar, armazenar, disseminar e fazer uso de informações (BRASIL, 2016a).

[2] Interdisciplinaridade - traduz-se na constante emergência de novas disciplinas que não são mais do que a estabilização institucional e epistemológica de rotinas de cruzamento de disciplinas. Este fenômeno não apenas torna mais articulado o conjunto dos diversos “ramos“ do saber [...] como o fazem dilatar, constituindo mesmo novos espaços de investigação, surpreendentes campos de visibilidade (POMBO, 2006, p. 210).

[3] Conjunto organizado de políticas, procedimentos, pessoas, equipamentos e programas computacionais que produzem, processam, armazenam e proveem acesso à informação (CONARQ, 2011).

[4] Proteção - entendida no seu aspecto mais abrangente como ato ou efeito de proteger: 1. tomar defesa de, 2. apoiar, 3. favorecer, 4. preservar do mal, 5. patrocinar, 6. resguardar, defender. Disponível em: <https://www.priberam.pt/dlpo/proteger>. Acesso em: 23 jan. 2018.

Em setembro de 2013, o Congresso Nacional brasileiro aprovou a proposta do *Livro Branco da Defesa Nacional* (LBDN), que se configura em um documento de caráter público, compreendendo a visão do governo e de parte da sociedade sobre a Defesa Nacional[5] do Brasil e seguindo uma prática das grandes democracias, incentivada pela Organização das Nações Unidas (BRASIL, 2012b).

De caráter inovador, o LBDN criou oportunidades para o debate sobre o tema desta pesquisa, em que:

> a **proteção do espaço cibernético** [grifo nosso] abrange um grande número de áreas, como a capacitação, inteligência, **pesquisa científica** [grifo nosso], doutrina, preparo e emprego operacional e gestão de pessoal. Compreende, também, a proteção de seus próprios ativos e a capacidade de atuação em rede (BRASIL, 2012b, p. 69).

Intrínseca e oportunamente alinhada ao LBDN, a edição conjunta da Política e da Estratégia Nacional de Defesa destacou a necessidade de uma Defesa [Segurança] Nacional moderna, fundada em princípios democráticos, capaz de atender às necessidades de uma nação repleta de riquezas e inserida num mundo turbulento e imprevisível como o atual, ressaltando ainda que: “Defesa não deve ser assunto restrito aos militares ou ao governo. Diferentemente, deve ser uma preocupação de toda a sociedade” (BRASIL, 2012c, p. 7).

Na prática, em operações reais e de alto risco, observa-se que ações típicas de Ciber Proteção[6], como defesa e de segurança cibernéticas, ocorrem simultaneamente[7]. Tal fato comprovou-se durante a realização dos chamados “Grandes Eventos” (GE) internacionais no Brasil, ocorridos a partir de 2012:

a) Conferência das Nações Unidas sobre Desenvolvimento Sustentável – UNCSD (Rio+20 em 2012), quando, pela primeira vez, um planejamento

---

[5] De acordo com a Política Nacional de Defesa: “o conjunto de medidas e ações do Estado, com ênfase no campo militar, para a defesa do território, da soberania e dos interesses nacionais contra ameaças preponderantemente externas, potenciais ou manifestas”. (BRASIL, 2012c, p. 12).
[6] Entendida, preliminarmente, como proteção da informação em meio digital no ciberespaço ou espaço cibernético. Sinônimo de proteção cibernética.
[7] No âmbito estrito do Ministério da Defesa, particularmente na Doutrina de Operações Conjuntas, o termo proteção cibernética caracteriza-se como ‘um conjunto de ações para neutralizar ataques e exploração cibernética contra dispositivos computacionais e redes de computadores e de comunicações, incrementando as ações de Segurança Cibernética em face de uma situação de crise ou conflito armado’ (BRASIL, 2011b).

operacional levou em consideração as ameaças advindas do espaço cibernético, com potencial para comprometer o comando e o controle das operações de segurança, assim como para afetar a imagem do Brasil[8];

b) Copa das Confederações (CopaConf 2013);

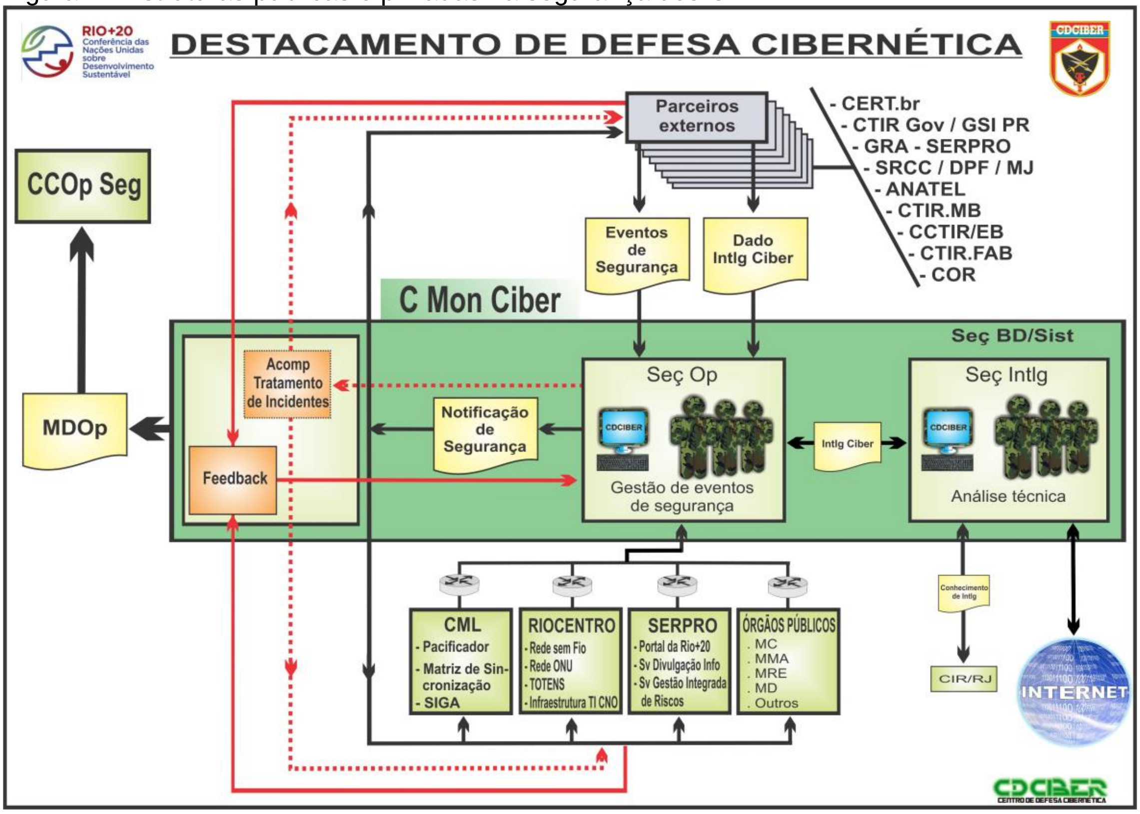
c) Jornada Mundial da Juventude (JMJ 2013);

d) Copa do Mundo de Futebol (FIFA 2014);

e) Jogos Olímpicos e Paralímpicos (Rio 2016).

Constatou-se, também, a participação de diversos atores governamentais e da sociedade civil, bem como a decorrente necessidade de articulação e de integração de uma gama de estruturas[9] heterogêneas públicas e privadas, como pode ser observado na figura 1.

Figura 1 - Estruturas públicas e privadas na segurança dos GE




Fonte: Vianna (2013)

---

[8] Informações adicionais em "A Segurança Cibernética na Conferência das Nações Unidas para o Desenvolvimento Sustentável" (VIANNA, 2013).
[9] Estrutura - tessitura organizacional de uma entidade qualquer pública ou privada, singular ou coletiva. In Dicionário Eletrônico de Terminologia em Ciência da Informação (DeltCI). Disponível em: <https://paginas.fe.up.pt/~lci/index.php/1716>. Acesso em: 25 abr. 2017.

O mosaico colaborativo e integrador experimentado com sucesso na Rio+20, em 2012, articulado por um órgão governamental *ad hoc*, foi sendo adaptado aos demais Grandes Eventos, incluindo os Jogos Olímpicos e Paralímpicos (Rio 2016). Não obstante a desarticulação do modelo cooperativo após a realização dos grandes eventos, os mesmos contribuíram para evidenciar a importância e a necessidade imprescindível da proteção da informação a trafegar no espaço cibernético, nas ações operacionais de segurança pública e de defesa nacional, bem como na salvaguarda das infraestruturas críticas estratégicas nacionais (IC)[10].

Como fatores de atração para o enfrentamento acadêmico do 'desafio da Ciber Proteção', além da ativa participação operativa e de planejamento nos eventos supracitados, foram consideradas a atualidade e a relevância do tema para a Ciência da Informação, nomeadamente pela inexorável internalização da imprescindibilidade que a informação em meio digital[11] possui, como vetor de sustentabilidade e de desenvolvimento socioeconômico do Estado[12] e da Sociedade brasileira.

## 1.2 Contextualização da Tese

Marshall McLuhan (1969), há mais de quatro décadas, mostrou como os meios de comunicação de massa afetam profundamente a vida física e mental do Homem, onde a 'mensagem' de qualquer meio (digital) ou tecnologia é a mudança que os mesmos introduzem nos procedimentos humanos. O autor, precursor da teoria da comu-

[10] Também conhecidas como Infraestruturas Estratégicas (IE), compreendem instalações, serviços, bens e sistemas que exercem significativa influência na vida de qualquer pessoa e na operação de setores fundamentais para o desenvolvimento e a manutenção de um país. Informações complementares sobre IC/IE em Fernandes (2012).

[11] Meio digital caracteriza-se como um conjunto de recursos com elevada capacidade de processamento e de armazenamento das informações, aliados à recuperação da mesma de forma instantânea. Considera-se que os meios digitais incorporam as tecnologias digitais: "referem-se às TIC, incluindo a Internet, tecnologias e dispositivos móveis, desenvolvimento de serviços e aplicações e análise de dados, utilizados para melhorar a geração, coleta, troca, agregação, combinação, análise, acesso, busca e apresentação de conteúdo digital" (OECD, 2014, p. 6).

[12] De acordo com o Código Civil brasileiro, Estado é uma pessoa de Direito Público formado por três elementos indissociáveis e indispensáveis: população, território e governo soberano. O Estado é concebido sob forma artificial para fins de proteção e de defesa, sendo comunidade e poder (SILVA, 2008).

nicação, formulou as bases da denominada ‘aldeia global’. Trata-se de um novo conceito de sociedade, completamente interconectada e dominada pelos novos meios de comunicação eletrônicos que aproximam pessoas de diferentes latitudes, permitindo que estas se comuniquem e se conheçam melhor. Ou seja, um ambiente de convergência, em que toda a evolução tecnológica estivesse a caminhar no sentido de formar um ambiente, onde a qualquer distância seja possível a comunicação direta e imediata. De certa forma, essa ‘aldeia global’ torna-se concretizada pelo uso de uma infraestrutura sistêmica de comunicação global, a Internet, e dos dispositivos de interação homem-sistemas como *smartphones, tablets* e computadores portáteis.

Por sua vez, Alvin Tofler (1980) traça características, análises e previsões sobre as transformações da civilização, impactada por aquilo que o escritor futurista denomina de “Terceira Onda” na maré da história, em sequência à Segunda Onda lançada pela revolução industrial, a qual, por sua vez, substituiu a revolução agrícola. Na Terceira Onda, Tofler antecipa o mundo tal como hoje o conhecemos, designando, como sociedade da informação, o último estágio da humanidade, uma aldeia global eletrônica, onde as pessoas podem acessar uma série infindável de serviços e informação, participar num mundo interativo e construir uma verdadeira comunidade baseada, não na geografia, mas em interesses comuns[13].

No final do século XX, após mais de uma década de pesquisas, o sociólogo Manuel Castells traçou com sua trilogia – A Era da Informação[14]: Economia, Sociedade e Cultura, o que se pode denominar de um novo paradigma[15] informacional, um ponto de descontinuidade histórica da mesma importância da Revolução Industrial do Século XVIII, propondo novos conceitos e perspectiva teórica, a fim de se compreenderem as tendências das sociedades no século atual.

---

[13] Pode-se considerar, como exemplo atual, a utilização das ‘redes sociais’ baseadas na Internet, acessada particularmente por *smartphones*.
[14] Considera-se como o período pós-era industrial, também conhecida como Era Digital ou Tecnológica, ou ainda denominada de 4ª Revolução Industrial, em que a informação destaca-se como força produtiva.
[15] Paradigma, em termos filosóficos, representa as formulações teóricas que servem implicitamente, por um período de tempo, para legitimar problemas e métodos de um campo do conhecimento (CUNHA; CAVALCANTI, 2008, p. 155). Aplicado às condições de produção das Ciências Sociais, paradigma pode consistir, genericamente, num modo de ver/pensar e de agir comum a uma ampla maioria de cientistas (dentro de seu campo disciplinar específico) de diferentes línguas e nacionalidades distribuídos por mais de uma geração (SILVA, 2006, p. 158).

Segundo Castells (1999), conhecimento[16] e informação estão diretamente ligados com o desenvolvimento econômico, ou melhor, são componentes fundamentais para a geração de riqueza e de poder na sociedade. Para Castells, as TIC suportam a formação de uma economia dual: informacional pois as empresas e nações dependem da sua capacidade de gerar, processar e aplicar de forma eficiente a informação; e global porque as principais atividades produtivas, o consumo e seus componentes estão organizados em escala mundial, diretamente ou mediante uma rede econômica de conexões.

Em 2009, ao prefaciar a 4ª edição do volume 1 – *A sociedade em rede*, o autor atualiza e ratifica o impacto das transformações em curso na Era da Informação:

> vivemos tempos confusos como muitas vezes acontece em tempos de transição histórica entre diferentes formas de sociedade. Tal acontece porque as categorias intelectuais que utilizamos para compreender o que acontece em nosso redor foram cunhadas em diferentes circunstâncias e dificilmente conseguirão compreender o que é novo referindo-se ao passado. [...] um conjunto de importantes transformações sociais, **tecnológicas** [grifo nosso] económicas [sic] e culturais que deram lugar a uma nova forma de sociedade, a sociedade em rede[17], [...] (CASTELLS, 2010, p. XXXVII).

Conforme a Teoria da Transição de Paradigmas analisada por Roberto Spolidoro (1996, 1998), cada uma dessas eras (industrial e da informação) corresponde a um paradigma social, definido como o padrão de percepção da realidade e de resposta aos seus desafios que caracteriza determinada sociedade. Dentre os axiomas adotados por essa teoria, destacam-se:

a) por suas características revolucionárias, as transições de paradigma social criam **ameaças** [grifo nosso] e oportunidades extraordinárias às gerações que as vivenciam;
b) os problemas trazidos por um novo paradigma só têm solução no âmbito do novo paradigma;
c) em um novo paradigma, urge questionarem-se conceitos e instrumentos herdados do paradigma exaurido;

---

[16] Conhecimento surge, no início da década de 1990, como um novo recurso relacionado ao poder socioeconômico, à gestão organizacional e à necessidade de tomadas de decisão mais céleres.
[17] Nova estrutura social em construção constituída por redes em todas as dimensões-chave da sua organização e prática social (CASTELLS, 2010, p. XXXVIII).

d) conceitos e instrumentos inovadores e revolucionários são essenciais [grifo nosso] para vencer os desafios de um novo paradigma;

e) as sociedades que não conseguem compreender e efetuar os 'saltos paradigmais' necessários podem condenar-se à estagnação ou à extinção.

Ao discutir o contexto[18] da mudança inerente à sociedade da informação, Kira Tarapanoff (2001) argumenta que a mesma representa uma profunda mudança na organização da sociedade e da economia, onde o digital torna-se o padrão e a informação assume contornos de estratégia e de área de segurança, sobretudo mundial. Para a autora, expressões como "sociedade global da informação" e "aldeia global" são questionadas, pois põe-se em risco a questão da soberania, particularmente nos Estados política e economicamente mais fracos.

Em relação às tecnologias de redes digitais que caracterizam a Era da Informação, Castells (2010, p. XXXVIII) vaticina que as mesmas "estimularam as redes sociais e organizacionais de formas que possibilitaram a sua expansão e reconfiguração contínua [...], na medida em que as redes não param nas fronteiras de um Estado-Nação[19], a sociedade em rede constitui-se como um sistema global". O autor, buscando consolidar a consistência e relevância da sua investigação, atualiza o que considera serem os componentes-chave da sociedade em rede: (i) a revolução tecnológica, com a comunicação baseada na microeletrônica, dando suporte material às nossas vidas; (ii) as redes tornaram-se nas formas de organização predominantes em todos os domínios da atividade humana; (iii) a globalização intensificou-se e diversificou-se e (iv) as tecnologias da comunicação construíram a virtualidade como uma dimensão fundamental da nossa realidade.

---

[18] Interrelação de circunstâncias que acompanham um fato ou uma situação ou como a composição e o que envolve e condiciona um elemento que aí se destaca. Em ciência da informação, alguns autores concentraram a aplicação do conceito operatório em estudos de comportamento informacional, propondo a seguinte definição instrumental: uma unidade agregadora de elementos materiais (um edifício, um ou mais aposentos quaisquer que constitui cenário para a ação infocomunicacional), tecnológicos (mobiliário, material de escritório, computadores com ou sem ligação à Internet, etc.) e simbólicos (o estatuto e os papéis desempenhados pelas pessoas ou atores sociais) que envolvem o(s) sujeito(s) de ação infocomunicacional através de momentos circunstanciais delimitados cronologicamente (situação). (PASSARELLI *et al*, 2014, p. 91).

[19] Estado-Nação: território delimitado composto por um governo e uma população de composição étnico-cultural coesa (BRASIL, 2012b).

No âmbito da área de conhecimento da CI, torna-se primordial e desafiador avançar em estudos amplos e diversificados, tais como promover o debate e o desenvolvimento de procedimentos de segurança da informação[20] (SegInf), particularmente em um espaço informacional típico, como o cibernético.

Pretendeu-se, assim, atualizar uma das definições mais frequentemente usadas em Ciência da Informação, onde a CI ocupa-se com “a geração, coleta, organização, interpretação, armazenamento, recuperação, disseminação, transformação e uso da informação”, buscando como disciplina, “criar e estruturar um corpo de conhecimentos científico, tecnológico e de sistemas, relacionando à transferência **[segura]** da informação” (GRIFFITH, 1980 *apud* CAPURRO; HJORLAND, 2007, p. 186; grifo nosso).

Este estudo está inserido no contexto oriundo da Era da Informação e da sociedade em rede, intrinsicamente relacionado aos usos e possibilidades do ciberespaço e das TIC, bem como enquadra-se no novo paradigma da Ciência da Informação (Pós-Custodial, Informacional e Científico[21]).

Para fins desta pesquisa, considerou-se, ainda, que as atividades inerentes à Ciber Proteção (englobando as atividades de segurança e defesa cibernéticas) estão imbricadas no contexto abrangente da segurança da informação praticada no âmbito da CI, como observado pela Academia Latino-Americana da Segurança da Informação**: “**proteger as informações registradas, sem importar onde estejam situadas: impressas em papel, nos discos rígidos dos computadores ou até mesmo na memória das pessoas que as conhecem”[22].

---

[20] Entendida e conhecida no âmbito da Administração Pública Federal como SIC - Segurança da Informação e Comunicações.

[21] A ser detalhado em seção posterior nesta pesquisa.

[22] A Academia Latino-Americana de Segurança da Informação integra a iniciativa da Microsoft de Computação Confiável (*Trustworthy Computing*), lançada em 2002, que visa oferecer uma plataforma ao mercado e orientar os usuários, quanto à proteção de seus dados e ações. Disponível em: <http://www.technetbrasil.com.br/academia>. Acesso em: 09 jul. 2015.

## 1.3 Justificativas

Uma vez que o foco deste estudo abordou a segurança da informação (em meio digital) no ciberespaço, entende-se que tal assunto parece estar sendo abordado de forma esporádica e superficial na literatura em geral. Na realidade, no que concerne à segurança e à defesa do ciberespaço, percebe-se que grande parte das publicações são técnicas ou operacionais, ligadas à computação, às redes de comutação de dados e ao tratamento de incidentes computacionais ou, ainda, que relatam a ocorrência de ações adversas a sistemas informatizados. Neste contexto, soma-se a carência de gestão da informação (GI) e do conhecimento (GC)[23] produzidos no planejamento, no desenvolvimento e na desmobilização das atividades de proteção do ciberespaço realizadas pelas instituições governamentais, ao longo dos últimos anos, por ocasião dos Grandes Eventos[24].

Levando-se em conta a complexidade e a dinâmica do tema no cenário atual, nacional e mundial, bem como a soberania e a segurança do Estado brasileiro, percebeu-se a necessidade do crescimento da interação entre as áreas de atuação da Ciência da Informação e a proteção do ciberespaço, particularmente, no que tange às denominadas "soluções de segurança" centradas no uso massivo das TI. As mesmas possuem riscos inerentes e são incompletas, necessitando, no mínimo: (i) de **pessoas** qualificadas para adequá-las ao ambiente e às necessidades de segurança institucionais, bem como para responder às falhas ou os incidentes indesejados que possam comprometer a informação organizacional[25] e (ii) de **processos** peculiares para a gestão da informação e do conhecimento com segurança.

Com relação aos 'pilares' (tecnologia, pessoas e processos) que sustentam a segurança da informação, Kelson Côrte (2014, p. 163) conclui que:

> a definição dos requisitos de proteção que compõem os pilares [...] deve levar em consideração o valor da informação e os riscos a que ela está sujeita. [...]

---

[23] No caso, a GC trata (aprendizagem, distribuição e uso) do conhecimento organizacional, seja o mesmo explícito, tácito, tangível ou não.
[24] Evidências coletadas pelo autor, por meio de observação direta participativa nas atividades de defesa cibernética realizadas ao longo dos Grandes Eventos.
[25] No contexto da Ciência da Informação, pode-se, por exemplo, citar a realização do mapeamento das necessidades informacionais dos profissionais que atuam na gestão da segurança da informação do ciberespaço (VIANNA, 2015).

> como os sistemas de informação são formados por pessoas, processos e tecnologia, para protege-los é necessário atuar nessas três dimensões, simultaneamente, pelo fato de serem interdependentes. [...] O pilar pessoas continua sendo o que recebe menor atenção.

Paradoxalmente ao inexorável desenvolvimento tecnológico, o ser humano detém papel essencial no controle e na segurança do espaço cibernético (onde, invariavelmente, circula grande parte da informação em tempo real), devendo sua capacidade profissional ser objeto de constante estudo e aperfeiçoamento[26]. Sobre a importância do fator humano na Ciber Proteção, o lendário *hacker* Kevin Mitnick (Mitnick; Simon, 2006, p. 131) questiona: "Qual é o ativo mais valioso do mundo em qualquer organização? Não é o *hardware* de computador, não são os escritórios nem a fábrica, nem mesmo [...] o clichê da corporação: 'Nosso ativo mais valioso é nosso pessoal´" e traça uma interessante e atual analogia:

> na medida que os especialistas contribuem para o desenvolvimento contínuo de melhores tecnologias de segurança, tornando ainda mais difícil a exploração de vulnerabilidades técnicas, os atacantes se voltarão cada vez mais para a exploração do elemento humano. Quebrar a "firewall humana" quase sempre é fácil, não exige nenhum investimento além do custo de uma ligação telefônica e envolve um risco mínimo (MITNICK; SIMON, 2003, p. 4).

Considerando-se os "processos", argumenta-se que a Ciber Proteção possui um significativo componente informacional, associado com: (i) a representação, armazenagem e a preservação da informação, sua organização intelectual e encadeamentos; (ii) a busca e recuperação; (iii) a qualidade, o valor e o uso da informação e (iv) a gestão da informação e do conhecimento – todos tradicionalmente tratados pela Ciência da Informação. No caso, entende-se a CI como um campo de questões a serem estudadas, englobando, tanto a pesquisa científica quanto a prática profissional, pelos problemas que propõe e pelos métodos que escolheu, ao longo do tempo, para solucioná-los (SARACEVIC, 1996).

Na manutenção da segurança dos sistemas de informação, são necessárias atividades de gestão e de monitoramento diversificadas internas e externas à organização, voltadas aos processos e controles inerentes à proteção das informações.

No contexto da Administração Pública Federal (APF)[27], o Tribunal de Contas da União (TCU) vem realizando seguidos levantamentos de governança de Tecnologia

---

[26] Sobre os perfis e procedimentos realizados pelos agentes responsáveis pela segurança da Informação no espaço cibernético da APF ver Vianna; Fernandes (2015).

[27] Conjunto formado por órgãos e instituições do poder executivo federal, incluindo autarquias e fundações.

da Informação com o objetivo de avaliar a situação de governança de TI, nos órgãos e instituições do poder executivo e afins. Tais levantamentos abordam práticas de governança e de gestão de TI previstas em leis, regulamentos, normas técnicas e modelos internacionais de boas práticas (BRASIL, 2014e).

A análise dos levantamentos do TCU[28], por intermédio da Secretaria de Fiscalização de Tecnologia da Informação (SEFTI), realizados entre 2007 e 2016, permite mapear diversos problemas e vulnerabilidades inerentes ao ciberespaço da APF, contribuindo, por intermédio de governança adequada da área de TI, para a promoção da proteção a informações críticas, assim como para que as organizações atinjam seus objetivos institucionais.

O TCU, no seu primeiro levantamento, buscou avaliar a situação da governança de TI, a partir da coleta de informações em questionário disponibilizado a instituições representativas de diversos segmentos do governo federal. O levantamento de 2010, que, ao todo, avaliou 301 instituições, revelou que a situação da governança de TI nas organizações públicas era bastante heterogênea. Em relação à segurança da informação, de uma forma geral, verificou-se que seus processos de gestão ainda eram pouco implantados (BRASIL, 2010c). Avaliando os resultados de 2010 e comparando-os com o levantamento de 2007, merecem destaque as seguintes vulnerabilidades:

a) a área de segurança da informação continuou a chamar a atenção pelos altos índices de não conformidade, sugerindo que, de forma geral, as organizações públicas, além de não tratarem dos riscos aos quais estão expostas, desconhecem tais problemas;
b) nenhum dos indicadores relativos à segurança da informação, que envolveram a melhoria das características: confidencialidade, integridade e disponibilidade, apresentou avanço substancial;
c) a despeito das recomendações emitidas pelo TCU e das publicações normativas do Gabinete de Segurança Institucional da Presidência da República (GSI) sobre segurança da informação, a Administração Pública, de forma geral, continuou a desconhecer e a não proteger suas informações críticas adequadamente.

---

[28] Baseado no artigo: O gestor da segurança da informação no espaço cibernético governamental: grandes desafios, novos perfis e procedimentos, produzido pelo próprio pesquisador e por Jorge H. C. Fernandes (VIANNA; FERNANDES, 2015).

No prosseguimento desse tema, o levantamento de governança de TI 2012 (BRASIL, 2012e) questionou ao todo 349 organizações da APF, selecionadas a partir de critérios como a representatividade no orçamento da União, a estrutura de governança e a gestão de TI. No que se refere à segurança da informação, percebe-se que houve melhoria percentual discreta em apenas metade dos critérios questionados em relação a 2010. A partir da análise do relatório de 2012, destacam-se as seguintes vulnerabilidades:

a) menos da metade das instituições questionadas implementaram uma Política de Segurança da Informação (PSI);
b) 90% das instituições públicas federais ainda não realizam Análise de Riscos (AR) aos quais a informação crítica para o negócio está submetida, considerando-se os objetivos de disponibilidade, integridade, confidencialidade e autenticidade;
c) somente 17% das instituições possuem processo de classificação das informações, apesar da Lei 12.527/2011 (LAI), que regula o acesso a informações mantidas pelo Estado. A ausência de classificação pode implicar tratamento inadequado da informação, como a divulgação ostensiva de dados não públicos;
d) a proteção aos ativos de informação[29] permanece muito prejudicada, tendo em vista que 76% das instituições não implementaram os processos corporativos referentes ao Inventário dos ativos de informação (dados, *hardware, software* e instalações);
e) também foi avaliado o controle sobre elementos críticos da gestão de segurança da informação. A capacidade da alta administração da APF em controlar a gestão de processos e resultados de TI é baixa, tendo em vista que 72% das respostas concentraram-se na faixa inicial de capacidade.

[29] Refere-se aos meios de armazenamento, transmissão e processamento, sistemas de informação, bem como aos locais onde se encontram esses meios e as pessoas que a eles têm acesso-que afetam diretamente a consecução e a continuidade da missão do Estado e a segurança da sociedade (BRASIL, 2009).

O TCU exemplifica a necessidade da segurança, em face das Infraestruturas críticas estratégicas:

> uma gestão inadequada da segurança da informação pode causar prejuízos significativos à instituição e, ainda, no caso de entes públicos, afetar ou interromper serviços necessários à sociedade e aos cidadãos. A indisponibilidade de um sistema de uma operadora de energia elétrica, resultando na interrupção do fornecimento de energia, ou o acesso indevido à conta bancária de um cliente de uma instituição financeira são exemplos comuns dos prejuízos que uma falha de segurança da informação pode ocasionar (TCU, 2012e, p. 16).

O ciclo de 2014, além de atualizar o panorama traçado em 2012, trouxe como aprimoramento a mudança da escala de resposta do questionário, que antes era binária (sim ou não) e que passou a ter cinco categorias de resposta relativas ao nível de adoção da prática (não se aplica, não adota, iniciou plano para adotar, adota parcialmente, adota integralmente). No que tange à segurança da informação, como percebido em todos os levantamentos anteriores, o tema continua a ser de preocupação, por causa da baixa conformidade das organizações em relação aos normativos e às boas práticas aplicáveis. Analisando os dados levantados e em complemento aos já mapeados em anos anteriores, evidenciam-se as seguintes vulnerabilidades (BRASIL, 2014e):

a) é reduzido o número de organizações que monitoram a governança e o uso de TI. Apenas 37% das pesquisadas possuem estabelecida a prática de avaliar periodicamente seus sistemas de informação, enquanto 39% das organizações avaliam a gestão da segurança da informação;
b) 38% das organizações não dispõem de comitê de segurança da informação formalmente instituído (responsável por formular e conduzir diretrizes para a segurança da informação corporativa), colocando em risco a efetividade de suas ações de proteção à informação;
c) metade das organizações não possui gestor da segurança da informação formalmente designado, responsável pelas ações corporativas de segurança da informação;
d) quase a metade (48%) dos órgãos não normatiza o controle de acesso às informações e aos recursos e serviços de TI;
e) apenas 54% possuem política de cópias de segurança (*backup*), que são necessárias para garantir a disponibilidade das informações, em casos de falhas de sistemas ou pessoas.

Em relação ao Levantamento de governança de TI realizado no ano 2016 (TCU, 2017), a fim de se manter a comparabilidade com o levantamento anterior, não foram realizadas significativas alterações, sendo utilizado, essencialmente, o mesmo questionário do ciclo 2014 com ajustes na redação de alguns itens para melhorar o entendimento e acréscimo de duas novas questões, versando sobre abertura de dados e prestação de serviços públicos[30].

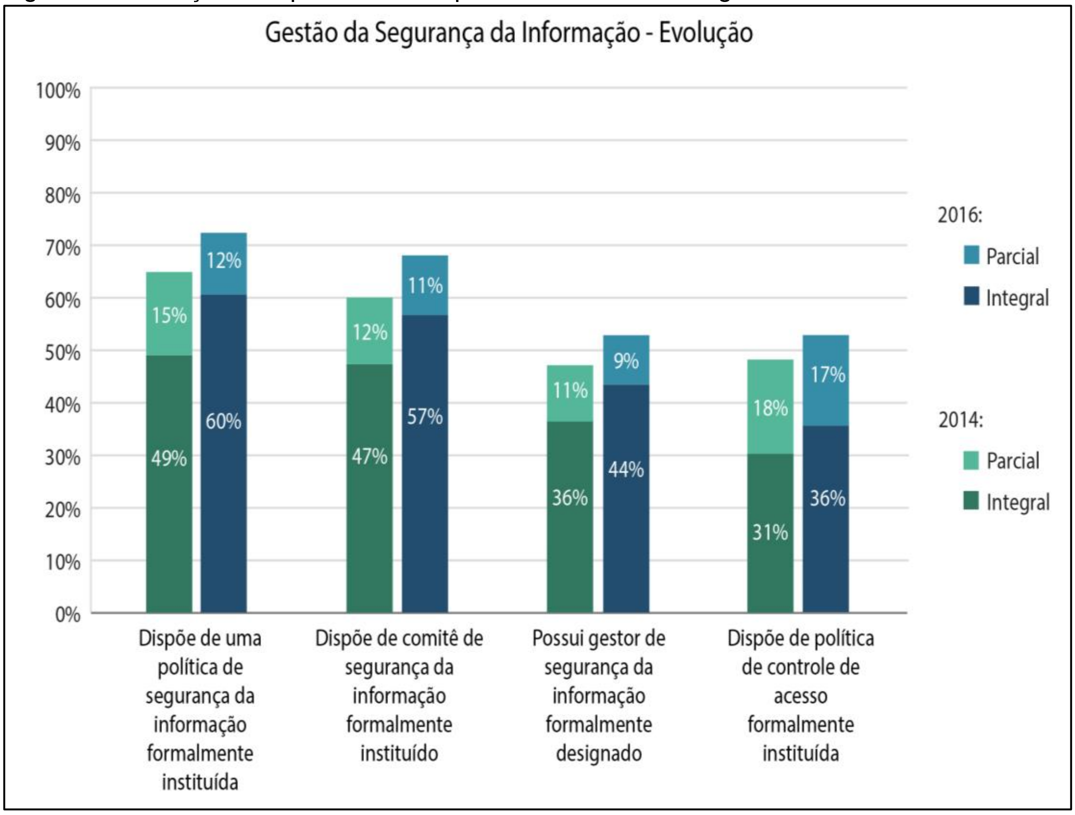
Genericamente, observou-se discreta evolução em relação ao ciclo de 2014. As organizações apresentaram maior capacidade de implementar estratégias e planos, porém menor capacidade no estabelecimento e manutenção de uma estrutura de liderança.

No que tange às novas questões, 63 % das organizações prestam serviços públicos diretamente ao cidadão (constante da Carta de Serviços), enquanto apenas 11 % das organizações publicam conjuntos de dados aderentes aos princípios de dados abertos. Interessante destacar-se que, entre as 12 razões para que os serviços passíveis de prestação sob a forma eletrônica não sejam assim prestados, o quesito “preocupações com segurança” ocupa a quinta colocação, após outras questões transversais como: falta de recursos humanos, financeiros, de infraestrutura e restrições legais.

Especificamente em relação à segurança da informação, a figura 2 sintetiza a evolução em relação às responsabilidades e políticas, onde os resultados “demonstram discreta evolução na gestão corporativa de segurança da informação, com crescimentos que variaram entre cinco e onze pontos percentuais na adoção integral das principais políticas e responsabilidades atinentes ao tema” (TCU, 2017, p. 40).

[30] Diversas visualizações sobre os dados coletados das organizações participantes e sobre o índice de governança de Tecnologia da Informação dessas organizações podem ser acessadas por meio da página do levantamento de governança de TI no portal do TCU. Disponível em: <http://www.tcu.gov.br/perfilgovti>. Acesso em: 05 dez. 2018.

Figura 2 - Evolução das políticas e responsabilidades em SegInf




Fonte: TCU (2017, p. 40)

De fato, considerando-se que um efetivo controle de acesso às informações em meio digital é imprescindível à proteção Cibernética, o avanço pouco significativo de quatro pontos no tocante à adoção de política de controle de acesso, aliado ao fato de que apenas 53% (17% parcialmente e 36% integralmente) das organizações tratam com seriedade do tema, demonstra reais fragilidades na gestão corporativa de segurança da informação, como atesta o próprio TCU:

> o nível de adoção das práticas apresentadas está muito distante do esperado, situação que revela a existência de lacunas na formulação de políticas e na atribuição de responsabilidades concernentes à gestão corporativa da segurança da informação, expondo a APF a diversos riscos, como indisponibilidade de serviços e perda de integridade de informações (2017, p. 41).

Em 10 anos de levantamentos e análises (2007 a 2017), o TCU considera que, apesar da considerável evolução na situação de governança e gestão de TI na APF, a mesma ainda está longe de ser aceitável, haja vista a relação cada vez mais intrínseca entre TI e negócio.

Em relação à gestão da segurança da informação, o Levantamento Integrado de Governança Organizacional Pública – ciclo 2018, destaca que

> 68% das organizações definiram, ao menos de forma parcial, alguma estrutura de segurança (EstrutSeg), porém vemos que somente 39% a implementam a gestão da segurança da informação (GestSeg). Tal situação sugere

> que a maior parte da APF limita-se a definir políticas e estruturas, mas tem dificuldade para implementá-las (TCU, 2018, p. 17).

De fato, o lento amadurecimento das práticas de gestão da segurança da informação demonstra a urgência e a importância de implementação de novas e abrangentes medidas intrínsecas à Ciber Proteção. Por exemplo, dentro do contexto supracitado, urge sensibilizar e comprometer os dirigentes dos órgãos APF, otimizando a efetiva implementação da segurança da informação, em toda a estrutura governamental, com os decorrentes impactos positivos na sociedade.

Às análises citadas anteriormente, soma-se a percepção de que as 'soluções de segurança' mais utilizadas pelas instituições públicas e privadas são baseadas nas Tecnologias de Informação[31]. De fato, as mesmas são, quase que exclusivamente, constituídas por aquisições de equipamentos (*hardware*) ou de aplicativos (*software*) de controle de acesso lógico a sistemas de informação ou redes de computadores, que, em sua maioria, não são fabricados ou desenvolvidos no Brasil[32]. Corroboram com esse entendimento Castells e Cardoso (2005, p. 254), ao afirmarem:

> em questões de defesa nacional, como no que diz respeito ao direito à privacidade, uma vez que, quando se usa um programa [TIC] proprietário, não há nenhuma forma de sabermos se ele não põe de alguma forma em risco a confidencialidade dos dados, por exemplo em favor das agências de informação dos países onde estão sediados os seus fabricantes.

Ao abordar as dificuldades inerentes à defesa do setor cibernético, Fernandes (2012, 2015) sinaliza sua dependência e interação com as diversas cadeias produtivas estrangeiras, ressaltando a dificuldade para uma nação conseguir produzir um produto cibernético que não possua algum componente fabricado no exterior. No caso, pode ser um *chip*, um módulo de *softwar*e, ou mesmo um serviço. O autor adverte que, além das vulnerabilidades que podem existir devido a falhas (não intencionais) no desenvolvimento, falhas/vulnerabilidades propositais podem estar inseridas nos componentes, o que poderia tornar todo um esforço de se produzir um sistema ciberneticamente seguro inútil.

---

[31] Atualmente, percebe-se crescente tendência para a compra e utilização dos denominados *Firewalls* UTM *(Unified Threat Management*) – Gerenciamento Unificado de Ameaças, que engloba várias funções de segurança em um único dispositivo: *firewall*, prevenção e detecção de intrusão, antivírus, VPN, *antispam*, filtragem de conteúdo *web*, bem como a geração de relatórios gerenciais.

[32] Maiores considerações sobre a dependência brasileira em *hardware* e *software* (componentes de um sistema computacional) ver Fernandes (2015).

Contribuíram, para fortalecer a relevância e oportunidade da pesquisa, dois eventos organizados pela Secretaria de Assuntos Estratégicos (SAE[33]) da Presidência da República. O primeiro, em dezembro de 2010, promoveu uma Reunião Técnica sobre Segurança e Defesa Cibernéticas, buscando-se identificar o papel das Forças Armadas e de outras instituições do Estado brasileiro, bem como de semelhantes órgãos públicos e privados envolvidos ou relacionados com o setor cibernético. Como consequência, foi esboçada uma proposta sistêmica, baseada nos anais do evento, em que a segurança teria um viés político, enquanto a defesa cibernética seria mais estratégica e operacional por meio da guerra cibernética (VIANNA, 2015).

O segundo evento, em 2013, referiu-se à realização do XIII Encontro Nacional de Estudos Estratégicos (XIII ENEE), cujo tema geral foi “O setor cibernético brasileiro: Contexto atual e perspectivas”. Dentre os consensos e apreciações do XIII ENEE, que ratificam as lacunas levantadas por este estudo, destacam-se:

a) necessidade de aprimoramento da coordenação político-estratégica institucionalizada, para promover a convergência de esforços dos diversos atores;
b) necessidade de se estreitar a interatividade interórgãos da administração pública federal e entre o governo e a sociedade, de modo geral;
c) segurança e defesa cibernética são assuntos estratégicos nacionais, cuja necessidade premente recai sobre a articulação entre governo, parceiros internacionais, **academia** [grifo nosso] e setor empresarial, como também sobre o investimento em capacitação de recursos humanos (BRASIL, 2013).

Interessante acrescentar-se que, em 2008, a Estratégia Nacional de Defesa (END) já reconhecia a importância da área acadêmica, em face da complexidade do setor cibernético, ao afirmar:

> a primeira prioridade do Estado na política dos três setores estratégicos será a formação de recursos humanos nas ciências relevantes. [...] não se limitará à ciência aplicada, de emprego tecnológico imediato. Beneficiará, também, a ciência fundamental e especulativa (BRASIL, 2008ª, p. 34).

Alia-se, aos fatos supracitados, a constatação de que o setor cibernético é ratificado pelo Congresso Nacional, em 2012, no primeiro eixo estruturante da END, como

---

[33] A SAE possuía como principais atribuições: o planejamento nacional de longo prazo e a discussão das opções estratégicas do País, sendo considerada em 2014, junto com o GSI, como órgão essencial da Presidência da República (VIANNA, 2015, p. 56).

uma das prioridades do Estado brasileiro, extrapolando a divisão entre desenvolvimento e defesa, entre o civil e o militar (BRASIL, 2012c).

Em escala global, os Encontros do Fórum Econômico Mundial (World Economic Fórum – WEF*)*, em suas análises sobre os riscos tecnológicos globais, vêm destacando nos últimos anos (WEF, 2015, 2016, 2017):

a) mau uso das novas tecnologias;

b) colapso das infraestruturas críticas da informação e das redes;

c) ataques cibernéticos em larga escala;

d) massiva incidência de fraudes e roubos de dados.

Somam-se, aos itens anteriores, a ameaça à interconectividade mundial (Internet) e a preocupação crescente com a privacidade[34] dos dados corporativos e individuais. Em 2016, o foco do WEF foi a denominada 4ª Revolução Industrial, baseada na acelerada e irreversível interconectividade global, onde a maneira de compartilhar, analisar e processar as informações tem profundas consequências políticas, econômicas e sociais na Era (da Informação) Digital. Na opinião do Professor Klaus Schwab, fundador e presidente executivo do WEF, essa nova era de inovação seria um conjunto de modernas tecnologias que estão integrando os mundos físico, digital e tecnológico, influenciando todas as disciplinas, economias e setores e, até mesmo, desafiando o significado de ser humano[35] .

Em 2017, o *Relatório de Riscos Globais* (GRR- *Global Risks Report*), que direciona a formulação de políticas e estratégias de governos e empresas, ressaltou como tendência crítica tecnológica o crescimento da ciberdependência e os ciber ataques. Dentre as maiores ameaças, destacam-se as fraudes cibernéticas, em particular o roubo de dados, devido à introdução das novas tecnologias (P.ex.: Internet das Coisas – IoT), bem como os ataques patrocinados por governos e orientados a interesses comerciais (WEF, 2017).

O GRR de 2018 (WEF, 2018) confirmou o crescimento dos riscos em ciber segurança tanto em quantidade (a quantidade de ataques a empresas dobrou em cinco

---

[34] Entende-se que uma sociedade democrática exige que os indivíduos possam se comunicar sem interferências indevidas, o que requer que suas comunicações sejam privadas e seguras (OEA, 2013).
[35] Disponível em <http://www.segs.com.br/info-ti/2677-privacidade-de-dados-dominou-discussao-sobre-4-revolucao-industrial-no-forum-economico-mundial-de-2016-em-davos.html>. Acesso em: 15 abr. 2016.

anos) quanto em potencial disruptivo. O crescimento da dependência cibernética afeta, prioritariamente, a seara dos Riscos Tecnológicos, em particular os ataques pedindo resgate (*ransomware*) e as infraestruturas críticas. Neste contexto, consequências decorrentes, em diferentes áreas, podem ser percebidas, tais como: roubo ou fraude em dados financeiros, terrorismo, interrupção de serviços afetando a sociedade e instabilidade governamental.

Considera-se, também, em relação aos processos informacionais, a percepção (construída a partir das atividades profissionais desenvolvidas no período de 2008 a 2018) de lacunas e oportunidades de melhoria, no que tange ao tratamento e gestão da informação e do conhecimento[36] pelas instituições governamentais imbricadas com a segurança e a defesa cibernéticas. Destaca-se que o simples somatório de ações isoladas de agências governamentais não se vem constituindo em política pública de segurança da informação no ambiente digital. De fato, por vezes, as normas e orientações, segmentadas por diversos órgãos da APF, vêm ocasionando mais ambiguidade do que efetividade nas atividades inerentes à proteção cibernética.

Considera-se, ainda, que lacunas de segurança vão existir, vulnerabilidades serão exploradas, ataques e ações maliciosas poderão acontecer, e que nem todos os atacantes serão descobertos ou responsabilizados pelos prejuízos e danos causados, direta ou indiretamente, aos cidadãos e às instituições.

Reconhecendo, portanto, o contexto dos sistemas de informação digitais e das redes de comunicação de dados como emergente, mutável, multifacetado e inovador, bem como indissociáveis ao desenvolvimento da sociedade, questionou-se o seguinte**: como estão gerenciadas as informações nas estruturas institucionais envolvidas diretamente com a proteção do espaço cibernético de interesse nacional?**

[36] No entendimento de Maria Manuela Pinto, a GC é referenciada como disciplina, teoria e prática, a par ou mesmo substituindo a GI, sendo relacionada com capital humano, qualidade, gestão do risco, *benchmarking*, boas práticas, gestão da mudança e da transformação dos sistemas (PINTO, 2015a, p. 400).

## 1.4 DESENHO BÁSICO DA PESQUISA

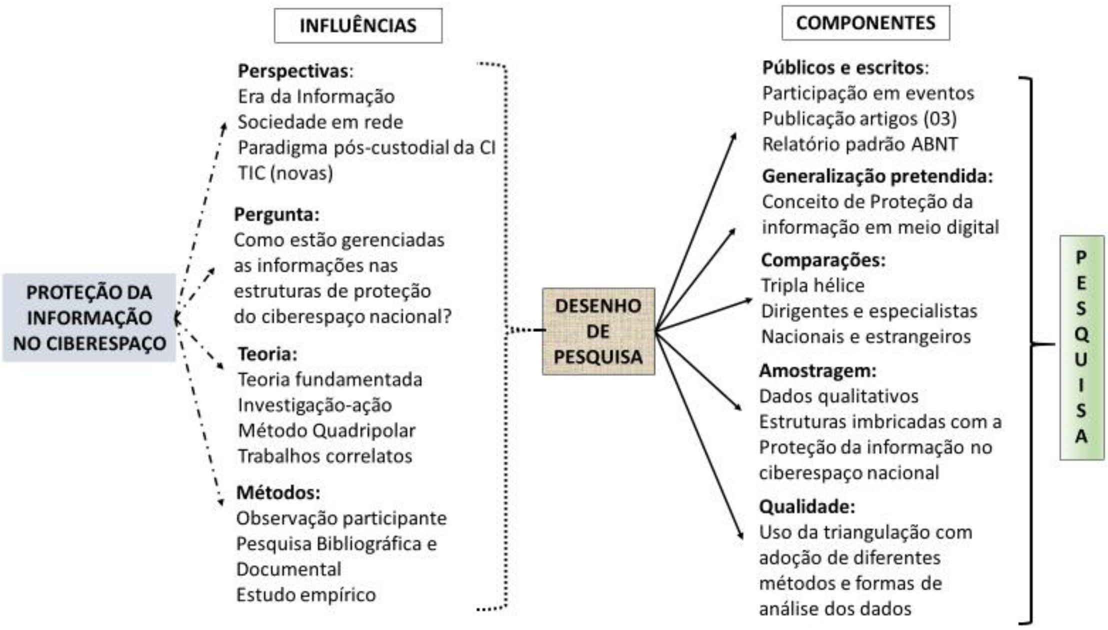
Objetivando propor uma resposta à pergunta basilar e motivadora em questão, optou-se por uma abordagem qualitativa[37], privilegiando a diversidade e o significado dos dados obtidos de diferentes formas e fontes.

Graham Gibbs alerta para as duas atividades ou práticas que envolvem a análise dos dados qualitativos, os quais foram levados em consideração na planificação desta pesquisa:

> em primeiro lugar, desenvolver uma consciência dos tipos de dados que podem ser examinados e como eles podem ser descritos e explicados; em segundo, desenvolver uma série de atividades práticas adequadas aos tipos de dados e às grandes quantidades que devem ser examinados (GIBBS, 2009, p. 17).

Assim, a pesquisa foi sendo construída no macrocontexto contemporâneo de uma sociedade da informação interligada tecnologicamente e aderente à Ciência da Informação que vivencia "novo" paradigma pós-custodial, informacional e científico. Na busca de respostas à pergunta base em questão, teorias e pesquisas anteriores foram parcialmente apropriadas e mescladas. Tais influências típicas de um estudo qualitativo conduziram à materialização de cinco grupos de componentes listados na figura 3, juntamente com o detalhamento dos quatro grupos de influências.

Figura 3 - Influências e componentes da pesquisa

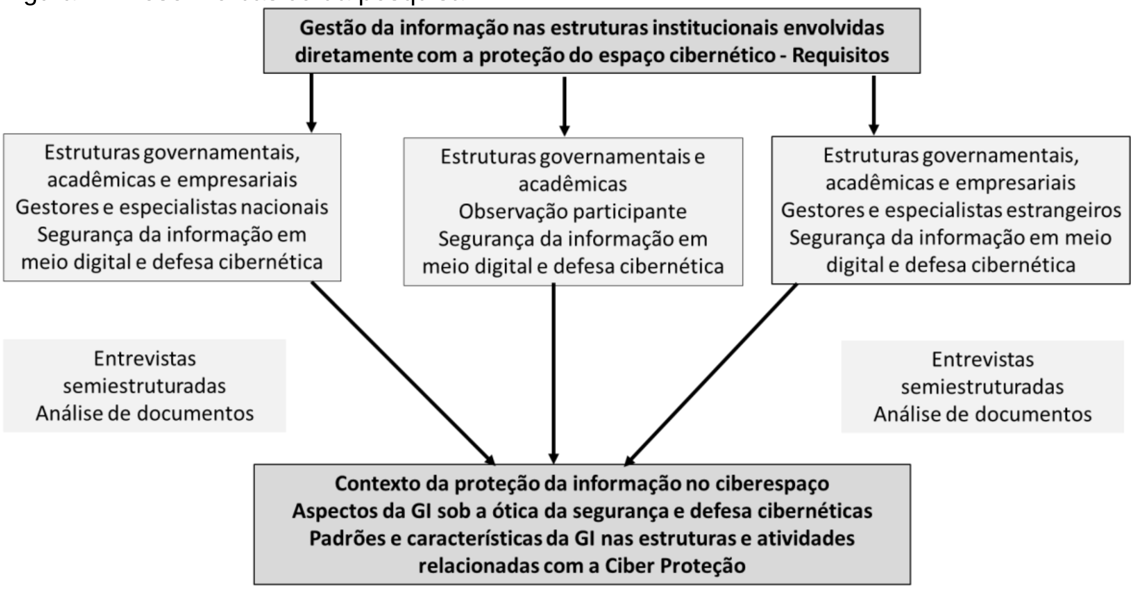



[37] O termo qualitativo significa quer o tipo de dados que uma investigação produz, quer os modos de atuação ou postulados que lhe são correlatos (SILVA; RIBEIRO, 2002, p. 86).

Fonte: adaptado de Flick (2009ª, p. 59-60)

No entendimento de Uwe Flick (2009ª, p. 150), um desenho de pesquisa seria um “plano sistemático para um projeto de pesquisa, incluindo quem integra à pesquisa (amostragem), quem ou o quê comparar em função de quais dimensões”. O desenho básico desta pesquisa, esboçado na figura 4, possui uma perspectiva transversal (contato empírico) por ocasião das entrevistas, aliado a uma dimensão retrospectiva no que tange à observação participante.

Figura 4 - Desenho básico da pesquisa




Fonte: adaptado de Flick (2009ª, p. 69)

Como fontes principais ou bases estruturantes para o desenvolvimento, a pesquisa encontra-se apoiada em vivências operacionais e estudos acadêmicos no Brasil e no exterior (P.ex.: o intercâmbio acadêmico, realizado em 2017, com a Universidade do Porto – Uporto/Portugal), sendo resumidas na figura 5, as quais serão apresentadas ao longo do estudo.

Figura 5 - Bases para desenvolvimento da pesquisa


Fonte: elaboração própria

A pesquisa desenvolve-se em mais dez capítulos. O capítulo 2 apresenta as proposições, delimitações e contribuições da pesquisa. Na sequência, o capítulo 3 define as perspectivas e abordagens metodológicas do estudo. No capítulo 4, caracteriza-se a realização da observação participante, pedra angular deste trabalho. Do capítulo 5 ao 7, é realizada a revisão da literatura estruturante, abrangendo os principais macrotemas estudados, nomeadamente: ciberespaço, ambiente informacional e proteção da informação. Avança-se, no capítulo 8, com a concepção do conceito de Ciber Proteção, núcleo do modelo proposto. O capítulo 9 é dedicado à demonstração e à análise dos resultados do estudo empírico, realizado por meio de entrevistas com especialistas. O capítulo 10 consolida a contextualização e o diagnóstico do fenômeno estudado, com o detalhamento dos sistemas alcançados pelo modelo, bem como apresentam-se os requisitos dos componentes da fase interventiva, ou seja, as três propostas transversais para a otimização, nomeadamente a elaboração de uma política de Estado, a organização de uma Entidade coordenadora e integradora supragovernamental e a estruturação de um ‘ciber’ centro de inovação e competências com representatividade nacional. Finalmente, o capítulo 11, consolida-se os aspectos basilares da pesquisa, bem como seus resultados, por meio de um Modelo de Ciber Proteção para a APF, concluindo-se a exposição de todo o processo de pesquisa e análise, com sugestões para estudos futuros.

# 2 PROPOSIÇÕES DA PESQUISA

A fim de se caracterizar não só com mais detalhamento o questionamento geral – **como estão gerenciadas as informações nas estruturas institucionais envolvidas diretamente com a proteção do espaço cibernético de interesse nacional?** Bem como proporcionar dimensionamento adequado ao escopo desta pesquisa, entendeu-se que:

a) no que tange ao gerenciamento (da informação), além de buscar-se uma perspectiva integradora, consideram-se, também, enquadrados: segurança, processos, serviços e normas inerentes ao fluxo informacional;
b) as informações estão relacionadas às atividades das estruturas institucionais quando envolvidas de modo direto e particular com o estabelecimento de políticas, estratégias, instruções normativas e outros instrumentos orientadores no contexto do ciberespaço de interesse nacional;
c) no ciberespaço de interesse nacional, desenvolvem-se as atividades que proporcionam sustentabilidade ao desenvolvimento e a sobrevivência da sociedade brasileira, bem como as ações de segurança e defesa imprescindíveis à soberania nacional;
d) estruturas institucionais referem-se aos órgãos que integram a Administração Pública Federal (APF) ou entidades que possuam representantes do governo federal (P.ex.: Conselhos, Comitês entre outros).

## 2.1 PROBLEMA E OBJETIVOS

No macrocontexto do questionamento deste estudo, formulou-se o problema[38] angular da pesquisa: no âmbito da Administração Pública Federal, quais seriam as

---

[38] Formular o problema consiste em dizer, de maneira explícita, clara, compreensível e operacional, qual a dificuldade com a qual nos defrontamos e que pretendemos resolver, limitando o seu campo e apresentando suas características. Desta forma, o objetivo da formulação do problema da pesquisa é tomá-lo individualizado, específico, inconfundível. (RUDIO, 1978, p. 75 *apud* LAKATOS; MARCONI, 2003).

maneiras mais efetivas de reduzir as vulnerabilidades e mitigar as ameaças aos recursos informacionais em meio digital e globalmente interconectados, indissociáveis ao desenvolvimento e à sobrevivência de um Estado-Nação?

A fim de subsidiar, nortear e construir solução para o problema supracitado, traçou-se o seguinte objetivo geral (OG): verificar a possibilidade de propor um modelo de gestão da informação nas estruturas institucionais relacionadas diretamente à proteção cibernética nacional, com a finalidade de reduzir as vulnerabilidades e mitigar as ameaças aos recursos informacionais digitais no ambiente da APF.

Para esquematizar a condução do estudo, estabeleceram-se os seguintes objetivos específicos (OE):

a) contextualizar a proteção da informação no ciberespaço;
b) analisar conceitos e perspectivas de gestão da informação, sob a ótica de segurança em meio digital e defesa do ciberespaço;
c) identificar os padrões e a situação da gestão da informação nas estruturas institucionais relacionadas com a Ciber Proteção;
d) definir os requisitos para um modelo de Ciber Proteção para a APF.

Assim, em sentido geral, pretendeu-se contribuir para a otimização do desempenho dos responsáveis pela gestão da proteção do ciberespaço, fornecendo subsídios para o planejamento de iniciativas e o aperfeiçoamento de atividades relacionadas com a segurança da informação em meio digital e a defesa cibernética nacionais, bem como com uma investigação desenvolvida nos domínios da Ciência da Informação situados não somente no nível interanalítico e transdisciplinar, mas também intercientífico.

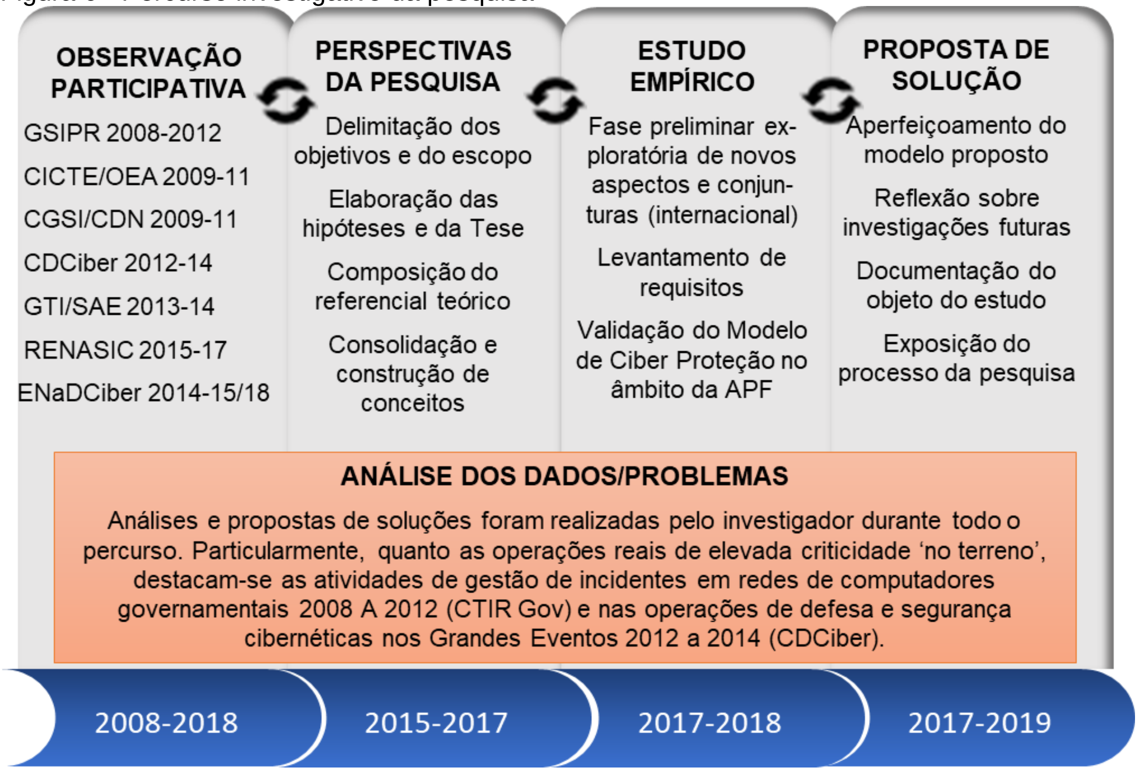
## 2.2 Delimitações da pesquisa

Ao referenciar o processo da pesquisa qualitativa, Flick entende que

> pode ser habilmente organizado em uma sequência linear de etapas conceituais, metodológicas e empíricas. Cada etapa pode ser tomada e considerada uma após a outra e separadamente. [...] há uma interdependência mútua das etapas isoladas do processo de pesquisa (FLICK, 2009b, p. 95).

De caráter híbrido e adaptativo, misto de preditivo, indutivo e explicativo, aliado à necessidade de um seletivo conhecimento teórico (estado da arte), a figura 6 sintetiza as fases e a cronologia do percurso investigativo, que se desenvolveu por aproximadamente 10 anos, no espaço temporal entre 2008 e 2018, culminando na formulação e apresentação do Modelo para a Ciber Proteção nacional.

Figura 6 - Percurso investigativo da pesquisa




Fonte: elaboração própria

O referido percurso reflete, também, o zelo em ampliar o cabedal prático experimentado no terreno, com as proposições teóricas elencadas (revisão da literatura). Demonstrou-se, ainda, a preocupação do autor com a qualidade da pesquisa, ao articular abordagens complementares, comumente denominadas de Triangulação[39], conjugando: (i) evidências e conjunto de dados geográfica e cronologicamente diferentes resultantes das observações participantes (no terreno) e das entrevistas/estudo empírico e (ii) metodologias e teorias de pesquisa diversificadas.

Este complexo e rico arcabouço de dados qualitativos que proporcionou a revelação de novas dimensões da Ciber Proteção, favorecendo uma visão mais precisa

---

[39] Combinação de diferentes métodos, teorias, dados e/ou pesquisadores no estudo de um tema (FLICK, 2009a, p. 154).

do tema, foi sendo analisado à medida que coletado (união entre coleta e análise), em consonância com os esclarecimentos de Graham Gibbs:

> em alguns tipos de pesquisa [...], estimula-se a coleta de todos os dados antes do início de qualquer tipo de análise. A pesquisa qualitativa se diferencia nesse sentido porque não há separação entre conjunto de dados e análise de dados. A análise pode e deve começar no campo. À medida que coleta seus dados, por meio de entrevistas, notas de campo, aquisição de documentos e assim por diante, é possível iniciar sua análise [...] Com frequência, há dados em abundância que podem ser examinados [previamente], em documentos existentes e em estudos anteriores (GIBBS, 2009, p. 18).

### *2.2.1 O universo investigado*

Em termos de escopo (origem, desenvolvimento e destinação), o universo[40] deste estudo enquadra-se no macroambiente da Administração Pública Federal – APF.

Sobre o tamanho da amostragem, ainda que de forma não definitiva, Angrosino (2009, p. 68) esclarece que "o tamanho de uma amostra depende das características do grupo que você está estudando, de seus próprios recursos (isto é, suas limitações de tempo, mobilidade, acesso a equipamento etc.) e dos objetivos do estudo". Para o autor, a amostra deve refletir a heterogeneidade do grupo em estudo. Em complemento, Uwe Flick descreve, assim, o cerne da escolha da amostragem qualitativa:

> os pesquisadores qualitativos estão interessados nas pessoas que estão "realmente" envolvidas e têm experiência com a questão de estudo. [...] Assim, nossa amostra deve ser representativa, não no sentido estatístico ou por representar a realidade de uma população básica: nossos casos [entrevistados] devem ser capazes de representar a relevância do fenômeno que queremos estudar [...] estamos interessados na variedade de experiências e envolvimentos, de forma que não apenas devemos ter casos comparavelmente centrais ou fundamentais, como também a variabilidade no campo de estudo e as diferenças nos vínculos com a questão (FLICK, 2009ª, p. 48).

No caso desta tese, a alternativa de amostragem foi intencional, típica e flexível. Em complemento, os critérios de seleção não se basearam nas técnicas usuais como amostragem aleatória ou estratificação, mas pelos de vivência, evidências e *insights* forjados, principalmente, na observação participante do autor. Assim, a amostra do

---

[40] Segundo Gil (2008), universo ou população refere-se a um conjunto definido de elementos que possuem determinadas características, enquanto amostra seria o subconjunto do universo, por meio do qual se estabelecem ou se estimam as características do mesmo.

universo em questão (APF), onde foi realizado o estudo empírico, nomeadamente as entrevistas em profundidade, situou-se nas instituições imbricadas com a segurança da informação e a defesa do ciberespaço de interesse nacional, relacionadas a ministérios essenciais ao governo federal, ligados direta ou indiretamente à Ciber Proteção, tais como:

a) Casa Civil da Presidência da República;
b) Gabinete de Segurança Institucional da Presidência da República (GSI);
c) Ministério da Ciência, Tecnologia, Inovação e Comunicações (MCTIC);
d) Ministério da Defesa (MD);
e) Ministério da Educação (MEC);
f) Ministério da Justiça e Segurança Pública (MJ);
g) Ministério da Fazenda (MF);
h) Ministério do Planejamento, Orçamento e Gestão (MPOG).

### *2.2.2 Administração Pública Federal*

Como ressalta Maria Manuela Pinto (2015), depois do ‘salto tecnológico’ impunha-se a mudança fundamental que consistia na ‘mudança da estrutura organizacional da Administração Pública’ e a correspondente ‘mudança da cultura organizacional’, no âmbito de uma sociedade caracterizada pela capacidade de os seus membros (Cidadãos, Empresas e Estado) obterem e partilharem qualquer tipo de informação e conhecimento instantaneamente, a partir de qualquer lugar e na forma mais conveniente.

Infelizmente, nem sempre o entendimento correto ou simplesmente eivado de lógica sobrepõe- se aos interesses políticos e econômicos, ou mesmo a estrutura administrativa vigente suporta as mudanças ou minimamente admite o aceite célere das propostas de melhoria e adequação à nova realidade.

O elevado número de entidades da APF, ressaltou as imensas diferenças na qualificação de pessoal, nas práticas e nas políticas já estabelecidas; os diversos níveis de segurança implementados; a localização geográfica diversificada no território nacional e muitos outros fatores, inclusive os de natureza política, oferecendo um contexto rico e abrangente da realidade do governo eletrônico (*e-gov*) brasileiro (VIANNA, 2015).

Desafios crescentes do governo *on-line* (ampliação do *e-gov*), como a proteção de dados pessoais, o acesso à informação, inclusão digital e a implementação do teletrabalho ou trabalho em casa (*home office*) reforçam, para a sociedade brasileira, o papel fundamental da informação em meio digital, exigindo confiabilidade, integridade e disponibilidade da mesma.

Além dos fatores supracitados, contribui para incrementar a complexidade da APF a dimensão continental do Brasil, ocasionando a pulverização de órgãos. Também, ampliam-se as dificuldades, na operacionalização das medidas de Ciber Proteção, a diversidade dos sistemas estratégicos e estruturantes nacionais, conforme ilustrado na figura 7.

Figura 7 - Sistemas estratégicos e estruturantes da APF


Fonte: DEIST/STI-MPOG [41]

[41] Disponível em: <http://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-temporarias/parlamentar-de-inquerito/55a-legislatura/cpi-crimes-ciberneticos/documentos/audiencias-publicas/audiencia-publica-dia-29-03.16/apresentacao-leonardo-boselli-da-motta-diretor-do-departamento-de-infraestrutura-e-servicos-de-tecnologia-da-informacao-do-ministerio-do-planejamento-orcamento-e-gestao>. Acesso em: 16 nov. 2017.

Outro fator complicador é a criação e extinção de ministérios e a rotatividade de chefias e de gestores, bem como a subordinação dos órgãos, entidades, autarquias e afins, de acordo com ajustes político-partidários tempestivos, sem considerar as necessidades de conhecimento técnico dos ocupantes dos cargos ou os planos e os interesses estratégicos do país. A APF é uma plêiade heterogênea e instável de dezenas de ministérios, secretarias, colegiados, conselhos, institutos e centros, entre outros, sob a égide da Presidência da República[42].

## 2.3 HIPÓTESES, VARIÁVEIS E A TESE

### *2.3.1 Hipóteses*

As hipóteses formam um conjunto estruturado de argumentos e explicações o qual desempenha o papel fundamental na pesquisa de sugerir explicações para os fatos, que podem ser a solução para a questão da mesma. Possuem caráter provisório, pois dependem de ser confirmadas por observação ou experimentação, tornando-se, também, instrumentos importantes como guias na tarefa de investigação. De fato, as hipóteses auxiliam na definição da linha de chegada do pesquisador e orientam o planejamento dos procedimentos metodológicos. O processo de formulação das hipóteses requer criatividade e experiência na área, podendo surgir das seguintes fontes: observação, resultados de outras pesquisas, teorias e intuição (GIL, 2008; LAKATOS; MARCONI, 2003; LUNA, 1997).

Assim sendo, formularam-se duas hipóteses (H1 e H2), as quais possuem, como pedra angular, a premissa de que as atividades relativas à proteção cibernética no País devem ser assunto de Estado, tratadas de forma perene e estratégica com projetos contínuos e de longo prazo, buscando o bem maior do País e da Sociedade, evitando-se, assim, ações e omissões, sem o devido respaldo técnico-científico, episódicas, não aderentes às melhores práticas globais e imediatistas/fracionadas, típicas de governos voltados, prioritariamente, aos seus interesses conjunturais, político-partidários:

---

[42] Informações detalhadas e atualizadas disponíveis em:<https://siorg.planejamento.gov.br/siorg-cidadao-webapp/pages/listar_orgaos_estruturas/listar_orgaos_estruturas.jsf>. Acesso em: 16 nov. 2017.

**H1** – a manutenção e o desenvolvimento das atividades relativas à proteção cibernética no País são impactados significativamente por ações governamentais e

**H2** – a apresentação inadequada do arcabouço regulatório, relacionada à segurança e à defesa dos ambientes[43] digitais[44] de interesse nacional, compromete a efetividade das medidas de mitigação das vulnerabilidades nos sistemas de informação e o enfrentamento das ameaças do ciberespaço.

As hipóteses são supostas respostas ao problema a ser investigado, podendo ser aceitas ou rejeitadas somente depois de devidamente testadas. Assim, as hipóteses podem ser verdadeiras ou falsas, devendo conduzir à verificação empírica, que é o propósito da pesquisa científica. As hipóteses originam-se das mais diversas fontes, sendo que a observação dos fatos constitui o procedimento fundamental na construção das mesmas. O estabelecimento assimétrico de relações entre fatos no dia-a-dia fornece indícios para a solução dos problemas propostos pela ciência (GIL, 2008. P. 41-46).

### *2.3.2 Variáveis*

A fim de se verificar a sustentabilidade das hipóteses lançadas, foram estabelecidas cinco variáveis: V1 e V2 relacionadas à H1; e V3, V4 e V5 ligadas à H2. São elas:

V1 – valorização da segurança e da defesa cibernética pelo governo federal;

V2 – qualidade do fomento à Gestão da Informação segura por meio de diversos recursos (pessoal, financeiro e logísticos) pela APF[45];

[43] Ambiente ou meio ambiente – realidade geográfica, política, econômica, social e cultural que condiciona e envolve os contextos e as situações comportamentais relativas ao fluxo/experiência ótima e ao uso/reprodução de informação (PASSARELLI *et al*, 2014, p. 92).

[44] Digitais - caracterizados pela codificação em dígitos binários e acessados por intermédio de sistema computacional.

[45] Geralmente, limita-se minimamente à manutenção e não ao fortalecimento das estruturas já existentes.

V3 – efetividade (atualidade e pertinência) das normas em vigor[46];

V4 – nível de integração entre as estruturas envolvidas com a Ciber Proteção[47];

V5 – capacidade técnica – operacional dos atores envolvidos com a gestão e normatização do ciberespaço[48].

As variáveis levantadas envolvem relações assimétricas e imanentes, sendo, no entendimento de Gil (2008, p. 45), significativas nas Ciências Sociais[49]. Tomando por exemplo a H1, há inequívoca relação entre a valorização da segurança e da defesa cibernética e o aporte de recursos. À medida que se observa uma maior valorização e entendimento da necessidade das mesmas, justifica-se um maior aporte de recursos, não só para a manutenção, ampliação e aperfeiçoamento das organizações já existentes, mas também para a criação de novas estruturas. Isto não significa dizer que, necessariamente, uma variável cause outra, mas que o aporte de recursos pode derivar da respectiva valorização. No caso da H2, também é evidente o relacionamento entre as três varáveis. Observa-se que a elevação da capacidade técnica dos atores envolvidos pode ser obtida pelo compartilhamento de informações entre as estruturas envolvidas (bom nível de integração), o que é capaz de influir diretamente, na formulação, atualização e pertinência das normas publicadas.

### *2.3.3 Construção da Tese*

Fundamentou-se, de forma particular, a tese proposta neste trabalho na observação participativa do autor, alicerçada pela revisão da literatura e pelas análises das informações provenientes da pesquisa de campo, bem como na busca de alternativas mais efetivas para reduzir as vulnerabilidades e mitigar as ameaças do ciberespaço.

---

[46] Grande diversidade de órgãos normatizando, de forma isolada e compartimentada, causando conflito de responsabilidades, sobreposição de assuntos, conflito de diretivas etc., dificultando a gestão por parte dos integrantes da APF.
[47] Dependente de iniciativas dos próprios órgãos a integração funcionou com limitações e parcialmente apenas durante os grandes eventos.
[48] Limitadas e descentralizadas iniciativas na APF, aliadas à grande rotatividade dos profissionais que buscam melhores condições de trabalho e salários. Maiores informações ver Vianna (2015).
[49] De acordo com a Tabela de Áreas do Conhecimento do Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPQ), a Ciência da Informação (6.07.00.00-9) enquadra-se nas Ciências Sociais Aplicadas (6.00.00.00-7). Disponível em: <http://www.cnpq.br/documents/10157/186158/TabeladeAreasdoConhecimento.pdf>. Acesso em: 30 abr. 2017.

Como resultado, formulou-se a Tese de que: **uma política de ciber proteção nacional, alinhada com os objetivos soberanos do Estado-Nação e construída por uma entidade articuladora e normativa, autônoma e com representatividade nacional, colaboraria, efetivamente, para reduzir as vulnerabilidades e mitigar as ameaças aos recursos informacionais em ambiente-digital.**

A referida Tese e suas hipóteses/variáveis reforçam, em contexto nacional, o inexorável desafio na construção de políticas, estabelecimento de estratégias e na consolidação do pensamento em segurança e defesa, chegando-se, ainda, à necessidade de criação de uma nova ordem para lidar com o caos informacional e o estado de natural insegurança que caracterizam o ciberespaço. Os componentes e as características essenciais que compõem a política de ciber proteção estão contidas no modelo proposto ao final desta pesquisa.

O quadro 1 revisa os elementos norteadores da pesquisa, pavimentando a caminhada metodológica traçada no próximo capítulo.

Quadro 1 - Elementos norteadores da pesquisa

<table>
<tr><td colspan="2">TEMA<br>A proteção da informação no ciberespaço de interesse nacional</td></tr>
<tr><td colspan="2">PROBLEMA<br>No âmbito da Administração Pública Federal, quais seriam as maneiras mais efetivas de reduzir as vulnerabilidades e mitigar as ameaças aos recursos informacionais em ambiente digital e globalmente interconectado, indissociáveis ao desenvolvimento da sociedade e à sobrevivência de um Estado-Nação?</td></tr>
<tr><td colspan="2">QUESTÃO DA PESQUISA<br>Como estão gerenciadas as informações nas estruturas institucionais envolvidas diretamente com a proteção do espaço cibernético de interesse nacional?</td></tr>
<tr><td>Objetivo Geral<br>Verificar a possibilidade de propor um modelo de gestão da informação nas estruturas institucionais relacionadas diretamente à proteção cibernética nacional, com a finalidade de reduzir as vulnerabilidades e mitigar as ameaças aos recursos informacionais digitais no ambiente da APF</td><td>Objetivos Específicos<br>OE1 – Contextualizar a proteção da informação no ciberespaço<br>OE2 – Analisar conceitos e padrões de gestão da informação, sob a perspectiva de segurança e defesa do ciberespaço<br>OE3 – Identificar os padrões e a situação da gestão da informação nos órgãos e entidades relacionados diretamente com a Ciber Proteção<br>OE4- Definir os requisitos para um modelo de Ciber Proteção para a APF.</td></tr>
<tr><td colspan="2"></td></tr>
<tr><td>Hipóteses<br>H1- A manutenção e o desenvolvimento das atividades relativas à proteção cibernética no País são impactados significativamente por ações governamentais</td><td>Variáveis<br>V1 – Valorização da segurança e da defesa cibernética pelo governo federal<br>V2 – Fomento à Gestão da Informação segura por meio de diversos recursos (pessoal, financeiro e logísticos), pela APF</td></tr>
</table>

| | |
|---|---|
| **H2- A apresentação inadequada do arcabouço regulatório, relacionadas à segurança e à defesa dos ambientes digital de interesse nacional, compromete a efetividade das medidas de mitigação das vulnerabilidades e o enfrentamento das ameaças do ciberespaço** | **V3** – Efetividade (atualidade e pertinência) das normas em vigor<br>**V4** – Nível de integração entre as estruturas envolvidas com a Ciber Proteção<br>**V5** – Capacidade técnica – operacional dos atores envolvidos com a gestão e normatização do ciberespaço |
| **TESE DA PESQUISA**<br>**Uma política de ciber proteção nacional, alinhada com os objetivos soberanos do Estado-Nação e construída por uma entidade articuladora e normativa, autônoma e com representatividade nacional, colaboraria, efetivamente, para reduzir as vulnerabilidades e mitigar as ameaças aos recursos informacionais em Ambiente Digital.** | |

Fonte: elaboração própria

O próximo capítulo apresenta a metodologia e os métodos utilizados nesta pesquisa sobre o fenômeno da informação digital, particularmente sua gestão e proteção no ciberespaço de interesse nacional.

# 3 CAMINHOS METODOLÓGICOS

Em uma pesquisa, cabe à metodologia, aderente e alinhada ao contexto do estudo, apontar a direção para os procedimentos a serem adotados. Assim, esta pesquisa de cunho qualitativo, tipificada como descritiva-exploratória, desenvolveu-se no âmbito da Ciência da informação, direcionada à investigação de um problema social e transformador, fortemente acoplado à tecnologia da informação.

Assim, este estudo sustenta-se no novo paradigma da Ciência da Informação, nomeadamente pós-custodial[50], informacional e científico, associado à Era da Informação e às (novas) tecnologias da informação e da comunicação (TIC), que ora estamos vivenciando. Sobre os desafios digitais da Era da Informação, cabe destaque a análise de Fernanda Ribeiro:

> a tecnologia digital veio pôr em crise o paradigma tradicional, quanto mais não fosse pelo simples facto [SIC] de tornar evidente a separação entre informação e suporte (dois elementos que, em conjunto, formam aquilo que designamos de ‘documento’ e que materialmente são indissociáveis) e permitir perceber claramente que as duas ‘coisas’ podem ser pensadas, estudadas e conhecidas de forma separada. A tecnologia permitiu ‘desligar’ a informação do suporte e veio evidenciar que a mesma informação pode estar, simultaneamente, em suportes [meios] diversos e em locais diferenciados. Enfim, a tecnologia proporcionou a passagem da visão ‘documental’ para a visão ‘informacional’ e, por isso, contribuiu para o reforço da identidade epistemológica da CI (PINTO, 2009b, p. 8).

Neste paradigma emergente de uma conjuntura de transição notoriamente híbrida, complexa e sujeita a um ritmo intenso de inovação tecnológica e científica (a Sociedade pós-industrial, da informação, em rede etc.), percebe-se o dinamismo e a evolução da Ciência da Informação, particularmente pela transdisciplinaridade (biblioteconomia, Arquivística, Documentação, sistemas Informacionais etc.) e pela interdisciplinaridade com outras Ciências como as Humanas e Sociais, bem como as exatas e naturais. Complementando, Armando Malheiro recorda que as práticas interdisciplinares da CI

> são com as ciências que ajudam a contextualizar, quer a informação produzida, quer o correlativo processo comunicacional ou de recuperação/uso – a História, a Administração e o Direito, a Gestão e a Economia e a Auditoria e a Contabilidade. As questões relacionadas com a preservação do suporte material simples, ou o dispositivo tecnológico de registro / processamento de conteúdo (informação) [/ segurança da informação] implicam relações com as

[50] Expressão usada para designar a época atual e que evidencia as emergentes incursões teóricos-científicas num domínio marcadamente tecnicista (PINTO, 2009b, p. 19).

> ciências naturais (Física e Química) e com a engenharia eletrotécnica e informática (SILVA, 2006, p. 107)

Nesta nova conjuntura, a informação é entendida como representações mentais e emocionais que podem estar em diversos suportes e em mutação constante[51]. Diferencia-se, portanto, do paradigma anterior, tipicamente custodial, historicista, patrimonialista e tecnicista, que se preocupava mais fortemente com a custódia e a "ritualização" do documento[52], pelo estudo científico e pela intervenção teórico-prática na produção, no fluxo, na difusão e no acesso (comunicação) da Informação.

## 3.1 Trilhas investigativas

A tempestividade e relevância do tema, vinculado à sua célere dinâmica evolutiva e transformadora, remete, inicialmente, a uma investigação exploratória[53]. Porém, devido aos aspectos de descrição, detalhamento e explicitação das características do fenômeno supracitado, aliados, particularmente, pela efetiva interação do autor do estudo com o tema e atuação 'no terreno', há aproximação, também, da pesquisa descritiva[54]. Nesse sentido, Gil (2008) observa que tais pesquisas podem acabar servindo para proporcionar uma nova visão do problema o que as aproxima das demais exploratórias, devido, por vezes, à atuação prática do pesquisador.

No entendimento de Cervo, Bervian e Silva (2007), a pesquisa descritiva observa, registra, analisa e relata fatos ou fenômenos sem manipulá-los. Busca, também, conhecer situações do comportamento humano, cujo registro não consta de documentos.

A pesquisa qualitativa baseia-se: (i) na apropriação de várias abordagens teóricas e metodológicas resultantes de diferentes linhas de desenvolvimento, (ii) nas

---

[51] cf. *Dicionário Eletrônico de Terminologia em Ciência da Informação* (DeltCI). Disponível em: < https://paginas.fe.up.pt/~lci/index.php/1751>. Acesso em: 25 abr. 2017.

[52] Informações adicionais sobre esse novo paradigma da Ciência da Informação consultar Pinto (2009a) e Silva (2006).

[53] Gil (2008, p. 27) afirma que as pesquisas exploratórias têm como principal finalidade desenvolver, esclarecer e modificar conceitos e ideias [...]. Habitualmente envolvem levantamento bibliográfico e documental, entrevistas não padronizadas e estudos de caso.

[54] Segundo Vergara (1998, p.45), a investigação exploratória é realizada em área na qual há pouco conhecimento acumulado e sistematizado, enquanto a pesquisa descritiva expõe características de determinada população ou de determinado fenômeno, podendo, também, estabelecer correlações entre variáveis e definir sua natureza.

perspectivas dos participantes e sua diversidade, considerando a subjetividade dos pesquisadores e sujeitos estudados como parte integrante do processo investigativo e (iii) nas reflexões, observações, impressões e sentimentos dos pesquisadores que se tornam dados, constituindo parte da interpretação (FLICK, 2009ª, p. 23-25).

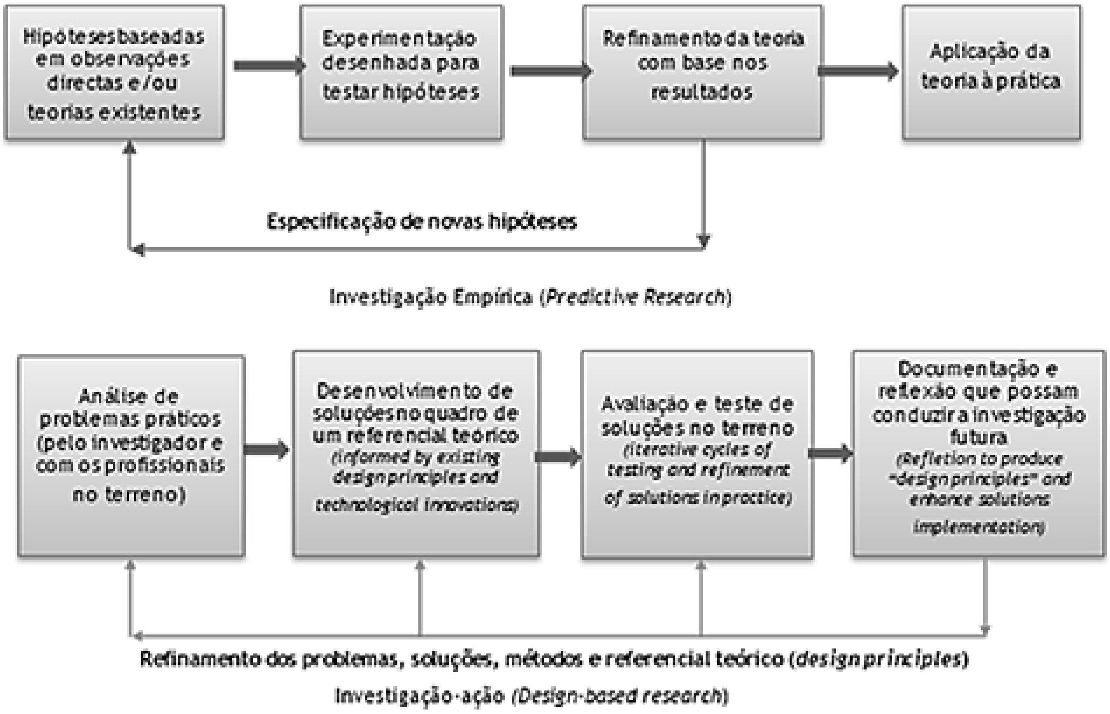
Segundo Minayo (2007), a pesquisa qualitativa permite a revelação de processos sociais ainda pouco conhecidos referentes a grupos particulares, propiciando a construção de novas abordagens, bem como a revisão e criação de novos conceitos e categorias. Assim, durante o levantamento dos dados, envolver análise numérica foi minimizada, devido à apreciação teórica das questões envolvidas no estudo (enfoque mais holístico).

Maria Manuela Pinto, ao analisar a produção científica no âmbito das Ciências Sociais, em particular quanto ao desenvolvimento da investigação qualitativa na gestão da informação, destaca:

> a Teoria Fundamentada, também designada por *Grounded Theory* (GT), que remete para a ideia de fundamentado ou enraizado na superficialidade da realidade a investigar. [...] A GT é referenciada na bibliografia popular como uma popular técnica de análise qualitativa, envolvendo os seguintes passos: 1) Formulação da questão-investigação; 2) Amostragem teórica; 3) Registro de entrevistas e contatos; 4) Agrupamento e codificação de dados; 5) Desenvolvimento de categorias conceituais; 6) Permanente comparação; 7) Análise de significado/interpretação; 8) Desenvolvimento de teoria.
>
> A investigação empírica/'positivista' (*predictive research*) [...], baseando-se em situações/pressupostos já conhecidos, envolvendo geralmente, alguma forma de decisão ou condição relacionada ao comportamento humano.
>
> A investigação-ação () [...] essencialmente prática e aplicada, que se rege pela necessidade de resolver problemas reais e em que não se considera a distinção de dois momentos: o da produção do conhecimento, que é levado a cabo pelo investigador, e o da aplicação desse conhecimento pelos profissionais no terreno, dado em que se assume a sua integração (PINTO, 2015, p. 555, 564 e 565).

Durante a análise das abordagens investigativas supracitadas, a autora busca condensá-las e compará-las graficamente de acordo com a figura 8.

Figura 8 - Comparação entre investigação empírica e investigação-ação




Fonte: Pinto (2015, p. 565)

Segundo Flick (2009ª), a abordagem da Teoria Fundamentada dá prioridade aos dados e ao campo de estudo sobre as suposições teóricas, as quais são descobertas e formuladas ao se lidar com o campo, onde a amostragem teórica provê uma orientação constante ao pesquisador para direcionar o processo de coleta, organização e interpretação dos dados com o objetivo de oferecer sustentação teórica. Observou-se, também, o procedimento denominado “comparação constante”, em que os dados recém coletados são comparados de forma contínua a outros elementos trabalhados anteriormente, de forma a desvendar novos e produtivos rumos para a pesquisa.

O emprego da GT, nesta pesquisa, faz-se aderente às caracterizações de Graham Gibbs:

a) é uma forma indutiva de pesquisa qualitativa;

b) seu foco central está em gerar, de maneira indutiva, ideias teóricas novas ou hipóteses a partir de dados, em vez de testar teorias especificadas de antemão;

c) a coleta e a análise são realizadas juntas;

d) a comparação constante e a amostragem teórica são usadas para sustentar a descoberta sistemática da teoria a partir dos dados fundamentados nas observações em vez de geradas no abstrato;

e) a amostragem dos contextos e entrevistados é guiada pela necessidade de testar os limites de explicações em desenvolvimento (GIBBS, 2009).

Ao abordar a Teoria Fundamenta como nova perspectiva à pesquisa exploratória no contexto da CI, Kelley Gasque afirma que a estratégia para a coleta de dados acontece de forma gradual onde

> muitas técnicas de coleta de dados podem ser utilizadas na Teoria Fundamentada, como a observação participante, entrevistas, discursos, cartas, biografias, autobiografias, pesquisa na biblioteca. Independentemente do método utilizado, sublinha-se que a abordagem se concentra firmemente na interpretação dos dados. (GASQUE, 2007, p. 93).

Assim, foi utilizada uma combinação sistematizada e parcial entre os métodos Investigação Empírica, Teoria Fundamentada, Investigação-ação e Método Quadripolar. Dessa forma, buscou-se uma maior clarificação do percurso investigativo seguido pelo autor, iniciado antes do período formal de elaboração da pesquisa acadêmica.

A referida combinação, ajustada aos tempos e movimentos (cronologia) vivenciados, visa, tão somente[55], esclarecer a adequação dos principais métodos/metodologias de pesquisa utilizados à realidade ao estudo, bem como tornar mais transparente e fidedigno o planejamento e a cronologia investigativa, proporcionando maior sustentabilidade acadêmico-científica.

## 3.2 Observação

De acordo com Gil (2008, p. 100): “desde a formulação do problema, passando pela construção da hipótese, coleta, análise e interpretação de dados, a observação desempenha papel imprescindível no processo de pesquisa”. A observação participante, ou ativa, consiste em fazer parte real do conhecimento na vida da comunidade, do grupo ou de uma situação determinada, tendo, como uma das principais vantagens, possibilitar o acesso a dados que o grupo considera de domínio privado.

No período de 2008 a 2018, de fato, significativa parcela das constatações de ordem prática neste estudo foi construída **no terreno**, a partir da participação ativa do

[55] Não faz parte do escopo desta Tese discutir/propor métodos ou ferramentas adicionais para a pesquisa qualitativa.

autor em diversas atividades operacionais, de coordenação e de planejamento em organizações públicas e privadas relacionadas com a segurança e a defesa do espaço cibernético, destacando-se:

a) assessor em segurança da informação do Gabinete de segurança Institucional da Presidência da República (GSI), como integrante do Departamento de Segurança da Informação e Comunicações (DSIC);

b) coordenador-geral do Centro de Tratamento de Incidentes de Segurança de Redes de Computadores da Administração Pública Federal da Presidência da República – CTIR Gov;

c) instrutor do Programa de Segurança Cibernética do Comitê Interamericano Contra o Terrorismo da Organização dos Estados Americanos CICTE/OEA;

d) membro do Comitê Gestor de Segurança da Informação do Conselho de Defesa Nacional – CGSI/CDN[56];

e) coordenador-executivo de segurança cibernética da Conferência das Nações Unidas sobre Desenvolvimento Sustentável (UNCSD – Rio+20);

f) assessor no planejamento e nas operações do Centro de Defesa Cibernética (CDCiber) do Exército Brasileiro/Ministério da Defesa;

g) integrante do Grupo de Trabalho Interministerial (GTI) sobre segurança e defesa do espaço cibernético nacional, coordenado pela Secretaria de Assuntos Estratégicos – SAE;

h) relator do Projeto Defesa Cibernética na Defesa Nacional – viabilidade e concepção da Escola Nacional de Defesa Cibernética – EnaDCiber;

i) colaborador da Rede Nacional em Segurança da Informação e Criptografia – RENASIC;

j) assessor de gestão do conhecimento de Defesa Cibernética na EnaDCiber.

As experiências e evidências colhidas foram particularmente úteis na escolha, amplitude e aprofundamento dos temas revisados e das fontes pesquisadas, bem como na consolidação das reflexões inerentes à revisão da literatura, detalhada a seguir.

---

[56] O CDN é um órgão de consulta do Presidente da República nos assuntos relacionados à soberania nacional e à defesa do Estado democrático de direito, cuja secretaria-executiva é exercida pelo GSI.

## 3.3 Levantamento para a Revisão da Literatura

De forma abrangente, tendo por meta a segurança da informação no meio digital, esta revisão abrange três macrotemas: ciberespaço, ambiente informacional digital e Proteção da Informação em meio digital, sintetizados na figura 9.

Figura 9 - Revisão da literatura

| **TEMAS** | | |
|---|---|---|
| CIBERESPAÇO | INFORMAÇÃO | PROTEÇÃO |
| - Cibernética | - Informação no meio digital | - Segurança e Defesa Nacional |
| - Rede de computadores | - Fluxos informacionais | - Segurança da informação |
| - Internet | - Gestão da Informação | - Segurança cibernética |
| - Plataformas digitais | - Gestão de documentos | - Defesa cibernética |
| - Novas TIC | - Preservação digital | - Guerra cibernética |
| - Governança da Internet no Brasil | - Sistemas de informação digitais | - Infraestruturas Críticas / Estratégicas |
| - Marcos regulatórios nacionais e internacionais | - Papel das TIC | - Ciber Proteção |

Fonte: elaboração própria

No desenvolvimento desta seção, buscou-se o entendimento de Alda Alves, quando afirma que

> a literatura revista deve formar com os dados um todo integrado: o referencial teórico servindo à interpretação e às pesquisas anteriores, orientando a construção do objeto e fornecendo parâmetros para comparação com os resultados e conclusões do estudo em questão (ALVES, 1992, p. 56).

Assim sendo, grandes áreas como Administração, Arquivologia, Cibernética, Ciência da Computação, Comunicação, Segurança e Defesa Nacional, Relações Institucionais, entre outras, foram objeto de revisão da literatura (compreendendo pesquisa bibliográfica e análise documental), no período entre 2015 a 2018, majoritariamente em língua portuguesa, seguida da inglesa e espanhola. Especial atenção foi dada aos trabalhos acadêmicos correlatos brasileiros e portugueses.

### *3.3.1 Pesquisa Bibliográfica*

Para Alves (1992), a revisão crítica de teorias e pesquisas no processo de produção de novos conhecimentos é aspecto essencial à construção do objeto da pesquisa. Na revisão da bibliografia, a autora supõe que o pesquisador já esteja trabalhando/praticando o assunto em curso, bastando direcionar seu esforço na atualização e integração desses conhecimentos.

Assim, a pesquisa bibliográfica consistiu no uso de fontes (livros, artigos científicos, reportagens, relatórios de empresas etc.) das quais foram coletados dados sobre dois eixos principais: gestão da informação digital e proteção da informação no ciberespaço.

Foram revisados temas típicos da Ciência da Informação e outros transdisciplinares, a saber: informação digital, tecnologia da informação, sistemas de informação, gestão, preservação, segurança da informação e das comunicações, cibernética, rede mundial de computadores (Internet), Segurança e Defesa Nacional, governo eletrônico e infraestruturas críticas, compondo um *corpus* diversificado, mutável e complexo.

Tal *corpus* incorporou a delimitação de conceitos-chave, tais como: ciberespaço, informação, meio digital, gestão da informação, segurança da informação, documento digital, preservação digital, Cibersegurança, defesa cibernética, guerra cibernética, infraestruturas críticas/estratégicas de informação, ativos de informação, entre outros, possibilitando a concepção do conceito angular desta tese – a Ciber Proteção.

### *3.3.2 Análise documental*

No entendimento de Uwe Flick (2009b, p. 237), "os documentos podem ser instrutivos para a compreensão das realidades sociais em contextos institucionais". Na análise documental, buscou-se uma amostra representativa dos documentos nacionais e oficiais relacionados à proteção da informação em meio digital, ou seja, um *corpus* voltado à construção de uma realidade específica, nomeadamente a Ciber Proteção na APF.

Utilizaram-se, prioritariamente, documentos primários, a fim de garantir a autenticidade, origem e representatividade das informações, considerando-se que os mesmos foram construídos dentro de uma realidade singular (segurança/defesa cibernéticas) e com objetivos específicos no tempo (a partir do ano 2000, com o Decreto n. 3505) e no espaço (Brasil/APF). O quadro 2 apresenta os principais documentos analisados.

Quadro 2 - Análise documental

| NOME | ORIGEM | ANO |
|---|---|---|
| Decreto 3505 – instituiu Política de Segurança da Informação nos órgãos e entidades da APF | GSI/Presidência da República | 2000 |
| Medida Provisória 2.200-2 – deu início à implantação do sistema nacional de certificação digital da ICP-Brasil | Presidência da República | 2001 |
| Modelo de governança da Internet no Brasil | MCTIC/Presidência da República | 2003 |
| Estratégia Nacional de Defesa (END) | SAE/Presidência da República | 2008 |
| Instrução Normativa n. 1 – disciplina a gestão da segurança da informação e comunicações na APF | GSI/Presidência da República | 2008 |
| Política de Segurança da ICP-Brasil (DOC-ICP-02 – V 3.0, de 01 de dezembro de 2008) | ITI/Casa Civil | 2008 |
| Livro verde: segurança cibernética no Brasil | GSI/Presidência da República | 2010 |
| Guia de referência para a segurança das infraestruturas críticas da informação | GSI/Presidência da República | 2010 |
| Brasil 2022 | SAE/Presidência da República | 2010 |
| e-ARQ Brasil: modelo de requisitos para sistemas informatizados de gestão arquivística de documentos. | Arquivo Nacional/CONARQ/MJ | 2011 |
| Lei de acesso à informação (LAI) | Congresso Nacional | 2011 |
| Tendência Global em Segurança e Defesa Cibernética: reflexões sobre a proteção dos interesses brasileiros no ciberespaço. | SAE/Presidência da República | 2011 |
| Lei n. 12.598 – estabelece normas especiais para as compras, as contratações e o desenvolvimento de produtos e de sistemas da área estratégica de defesa | Congresso Nacional | 2012 |
| Livro Branco da Defesa Nacional (LBDN) | Congresso Nacional | 2012 |
| Política Cibernética de Defesa (PCD) | Presidência da República/MD | 2012 |
| Política Nacional de Defesa (PND) e a Estratégia Nacional de Defesa (END). | Congresso Nacional | 2012 |
| Marco Civil da Internet (MCI) | Congresso Nacional | 2014 |
| Portaria Interministerial n. 1421 – instituiu o Programa de Pesquisa, Desenvolvimento e Inovação em Defesa Cibernética | Ministério da Defesa/Ministério da Ciência, Tecnologia e Inovação | 2014 |
| Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da APF 2015-2018. | GSI/Presidência da República | 2015 |
| Diretrizes para a Implementação de Repositórios Arquivísticos Digitais Confiáveis – RDC-Arq | Arquivo Nacional/CONARQ/MJ | 2015 |
| Política Pública de Inclusão Digital | Tribunal de Contas da União | 2015 |
| Estratégia de Governança Digital para a APF 2016-2019 | MPOG/Presidência da República | 2016 |

| | | |
|---|---|---|
| Decreto n. 8771 – regulamenta o MCI quanto à degradação de pacotes e de tráfego de dados, proteção de dados por provedores, entre outros aspectos | Presidência da República | 2016 |
| Política de Governança Digital | MPOG/Presidência da República | 2016 |
| Política Nacional de Dados Abertos | MPOG/CGU/Presidência da República | 2016 |
| Plano Nacional de Internet das Coisas/ Cartilha de Cidades | MCTI/MPOG/ Presidência da República | 2018 |
| Decreto n. 9283 – incentiva a inovação e a pesquisa científica e tecnológica no ambiente produtivo. | Presidência da República | 2018 |
| Estratégia Brasileira para a Transformação Digital (E-Digital) | Presidência da República | 2018 |
| Decreto n. 9319 – institui o Sistema Nacional para a Transformação Digital – SinDigital | MCTI/ Presidência da República | 2018 |
| Lei n. 13.709 sobre a proteção de dados pessoais (LGPDP), altera o MCI/LAI | Congresso Nacional | 2018 |
| Decreto n. 9.573 – aprovou a Política Nacional de Segurança de Infraestruturas Críticas (PNSIC) | GSI/ Presidência da República | 2018 |
| Decreto n. 9637 – instituiu a Política Nacional de Segurança da Informação(PNSI), no âmbito da APF | GSI/ Presidência da República | 2018 |

Fonte: elaboração própria

### *3.3.3 Trabalhos acadêmicos correlatos*

O tema é ainda muito incipiente, atual, instável e com rápidas mudanças de cenários e atores. A proteção da informação em meio digital necessita de periódicas atualizações, devido à obsolescência e às constantes evoluções de *hardware* e *software*, bem como de constantes revisões nos processos informacionais e de preservação. Devido, ainda, ao frenético surgimento de novas formas de ataque e de artefatos maliciosos, o tema apresenta-se carente de bibliografia e estudos atualizados, particularmente em termos nacionais. O quadro 3 resume os principais trabalhos consultados ao longo da pesquisa, sendo organizado em duas áreas centrais: a primeira - Ciber Proteção, compreendendo ciberespaço, cibernética, TIC, Internet, Segurança e Defesa Nacional, SIC, defesa cibernética, IC entre outros e a segunda – Gestão da Informação, abrangendo - Informação no meio digital, Fluxos informacionais, Gestão de documentos, Preservação digital e Sistemas de informação digitais.

Quadro 3 - Trabalhos acadêmicos correlatos

| MACROTEMAS | TÍTULO | AUTOR/ANO |
|---|---|---|
| CIBER PROTEÇÃO | Ciência, Tecnologia e Inovação no Setor Cibernético: Desafios e Oportunidades | FERNANDES, Jorge H. C Relatório Técnico-2013 |
| CIBER PROTEÇÃO | Colaborações dos estudos de cibercultura para a ciência da informação. | LINS, Greyciane Souza. Tese-2013 |
| CIBER PROTEÇÃO | Designing a Method for Discovering Expertise in Cyber Security Communities: an ontological approach | FONTENELE, Marcelo Paiva Tese-2016 |
| CIBER PROTEÇÃO | Diretrizes para melhoria da política de segurança da informação da infraestrutura de chaves públicas brasileira | PORTO, Luís Carlos de Oliveira Monografia-2014 |
| CIBER PROTEÇÃO | Políticas Nacionais de Segurança Cibernética: o regulador das telecomunicações | JUNIOR, Sérgio A. G. A. Dissertação-2011 |
| CIBER PROTEÇÃO | Projeto Conceitual para a Escola Nacional de Defesa Cibernética (ENaDCiber) | ISHIKAWA E. *et al* Relatório-2015 |
| CIBER PROTEÇÃO | Segurança da informação baseada no valor da informação e nos pilares tecnologia, pessoas e processos | CÔRTE, Kelson Tese - 2014 |
| CIBER PROTEÇÃO | Segurança e Defesa Cibernéticas para Reduzir Vulnerabilidades nas Infraestruturas Críticas Nacionais | FERNANDES, Jorge H. C Relatório Técnico-2012 |
| GESTÃO DA INFORMAÇÃO | A Gestão da Informação nas Universidades Públicas Portuguesas: Reequacionamento e proposta de modelo | PINTO, Maria Manuela Gomes de Azevedo Tese-2015 |
| GESTÃO DA INFORMAÇÃO | Competências necessárias para equipes de profissionais de preservação digital | BOERES, Sonia Araújo de Assis Tese-2017 |
| GESTÃO DA INFORMAÇÃO | Contribuições das abordagens positivista e pragmática do estudo do conceito para o modelo conceitual FRSAD. | MELO, Maria Antônia Fonseca. Dissertação-2013 |
| GESTÃO DA INFORMAÇÃO | Gestão da informação para a tomada de decisão em uma instituição de ensino superior privada | SILVA, Gleiciane Rosa da Dissertação-2016 |
| GESTÃO DA INFORMAÇÃO | Gestão da informação: estudo comparativo de modelos sob a ótica integrativa dos recursos de informação | MARTINS, Sergio de Castro Dissertação-2014 |
| GESTÃO DA INFORMAÇÃO | Gestão da preservação de documentos arquivísticos: proposta de um modelo conceitual | INNARELLI, Humberto Celeste Tese-2015 |
| GESTÃO DA INFORMAÇÃO | Sobre uma Arquitetura da Informação do Governo Brasileiro: a AIGov-BR/ | NEVES, Odilon Júnior Tese-2013 |

| GESTÃO DA INFORMAÇÃO | Os Repositórios Institucionais das Universidades Federais do Brasil: Um Modelo de Política de Preservação Digital | Silva Júnior, Laerte Pereira da Tese-2017 |
|---|---|---|

Fonte: elaboração própria

## 3.4 *ENTREVISTAS*

Esta etapa da investigação exploratória consistiu na realização de entrevistas em profundidade (*in depth interview*) com pesquisadores/especialistas em segurança da informação no ciberespaço.

No entendimento de Angrosino (2009, p. 61-62), "as entrevistas são uma extensão lógica da observação", particularmente aquelas em profundidade que têm por objetivo "sondar significados, explorar nuances, capturar áreas obscuras que podem escapar às questões de múltipla escolha que meramente se aproximam da superfície do problema". Cervo, Bervian e Silva (2007) reforçam a pertinência da técnica empregada no estudo empírico, ao afirmarem que, para viabilizar a operação de coleta de dados em uma pesquisa qualitativa, são utilizados, como principais instrumentos: a observação, a entrevista e o formulário.

A entrevista é uma técnica de coleta de dados típica de uma pesquisa qualitativa, onde é possível confrontar as narrativas dos entrevistados com a bibliografia e a documentação estudadas. Foi a mesma utilizada, também, com a finalidade de avaliar as análises e conclusões realizadas pelo autor, particularmente baseadas na experiência e nas evidências coletadas no curso da observação participante, bem como ampliar, otimizar e validar uma gama de requisitos inerentes ao modelo de gestão da informação pretendido. Não obstante, em sentido amplo, buscou-se mapear, coletar e analisar qualitativamente o conhecimento adquirido no planejamento, na execução e na normatização (gestão) das atividades relacionadas à Ciber Proteção.

As entrevistas semiestruturadas foram organizadas de modo a reconstruir as teorias subjetivas[57] dos entrevistados sobre a proteção da informação, em meio digital

[57] O termo "teoria subjetiva" refere-se ao fato de os entrevistados possuírem uma reserva complexa de conhecimento sobre o tópico do estudo. [...] Esse conhecimento inclui suposições que são explícitas e imediatas, que podem ser expressas pelos entrevistados de forma espontânea ao responderem a uma pergunta aberta, sendo as mesmas complementadas por suposições implícitas (FLICK, 2009b, p. 149).

brasileiro, organizadas por meio de pautas e de perguntas com resposta aberta, questões relacionadas aos objetivos e hipóteses do estudo, bem como outras sobre o conceito de Ciber Proteção.

As entrevistas desta pesquisa foram realizadas com profissionais experientes, também sendo conhecidas como “entrevista com especialistas”. No entendimento de Flick, (2009b), o maior interesse em relação a um entrevistado, reside na sua capacidade em um determinado campo específico, onde o guia de entrevista possui uma função diretiva mais forte, a fim de evitar uma conversa personalista, centrada nas atividades realizadas pelo entrevistado ou mesmo do tipo palestra.

Caracterizou-se, ainda, o perfil dos entrevistados escolhidos sob três aspectos: (i) técnico - especialização e prática em segurança da informação, (ii) gestão - experiência gerencial em organizações relacionadas à TIC e (iii) ético/moral - comprometimento com a Ciber Proteção nacional.

Destaca-se, aqui, o uso da amostragem teórica[58], quando o pesquisador (que possui conhecimento teórico sobre o objeto que abordará, como os conceitos, as principais características da estrutura e dos processos), deve, inicialmente, deixar o seu conhecimento em "estado de suspensão", ou seja, estar aberto ao novo, ao inesperado, percebendo, com maior clareza, a relevância dos conceitos em determinado contexto ao longo do processo de pesquisa (FLICK, 2009b; GASQUE, 2007).

Nesse sentido, aplicou-se como estratégia a definição gradual da amostra, de acordo com a relevância e tipicidade dos entrevistados e não conforme sua representatividade. De acordo com Vergara (1998, p. 49), a amostra não probabilística por tipicidade é “constituída pela seleção de elementos que o pesquisador considere representativos da população-alvo, o que requer profundo conhecimento dessa população [universo]”.

As entrevistas foram efetivadas em momentos e com objetivos distintos.

O primeiro, considerado como preliminar e exploratório, desenvolveu-se por ocasião da realização do intercâmbio com a Universidade do Porto, no período de maio a junho de 2017, seguindo o estipulado no Apêndice A. Escolheram-se, pois, especialistas dotados de substancial capacidade decisória, orientadora ou normativa, ligados às áreas de segurança e de gestão da informação em meio digital.

---

[58] Etapa inicial da Teoria Fundamentada, também designada por *Grounded Theory* (GT).

O segundo momento foi efetuado exclusivamente nos órgãos essenciais da Administração Pública Federal brasileira, sendo que, preliminarmente, foi realizado um pré-teste contemplando dois representantes com as mesmas características da amostra.

Buscou-se, nesse contexto, contemplar entrevistados com vivências acadêmicas, empresariais, operacionais e de gestão no ambiente da APF, particularmente nas estruturas orgânicas das instituições nacionais envolvidas com a proteção da informação em meio digital (segurança e a defesa cibernéticas), compondo um *corpus* de experiências empíricas, com vista a validar o modelo de Ciber Proteção.

As entrevistas seguiram o planejado no Apêndice B e foram realizadas no período de outubro a dezembro de 2017.

Estabelecendo ligação entre as perspectivas da pesquisa e a metodologia, o quadro 4 correlaciona as hipóteses, as variáveis e os instrumentos de averiguação.

Quadro 4 - As hipóteses, as variáveis e os instrumentos de pesquisa

| **HIPÓTESES** | **VARIÁVEIS** | **ENTREVISTA (Questões)** |
|---|---|---|
| H1 - A manutenção e o desenvolvimento das atividades relativas à proteção cibernética no País são impactados significativamente por ações governamentais | V.1 - valorização da segurança e da defesa cibernética pelo governo federal<br>V.2 - fomento à Gestão da Informação segura por meio de diversos recursos (pessoal, financeiro e logísticos), pela APF | Q1 a Q4 |
| H2- A apresentação inadequada do arcabouço regulatório, relacionada à segurança e à defesa do ambiente digital de interesse nacional, compromete a efetividade das medidas de mitigação das vulnerabilidades nos sistemas de informação e o enfrentamento das ameaças do ciberespaço | V3 - efetividade (atualidade e pertinência) das normas em vigor<br>V4 nível de integração entre as estruturas envolvidas com a Ciber Proteção<br>V5 - capacidade técnica – operacional dos atores envolvidos com a gestão e normatização do ciberespaço | Q5 a Q8 |

Fonte: elaboração própria

## 3.5 Abordagem Quadripolar

O Método Quadripolar decorre da proposta metodológica contida no livro *Dynamique de la recherche en sciences sociales: les pôles de la pratique méthodologique*

(Dinâmica da pesquisa em ciências sociais: os polos da prática metodológica) apresentada pelos belgas Paul De Bruyne, Jacques Herman e Marc De Schoutheete em 1974. Trata-se, sinteticamente, de uma metodologia qualitativa com uma dinâmica de investigação baseada em quatro polos, pensada para as Ciências Sociais.

O Observatório de Ciência da Informação da Universidade do Porto, em seu dicionário[59], ao referenciar o Método Quadripolar, sustenta que o mesmo nasceu como resposta alternativa ao positivismo e à dicotomia redutora entre “quantitativo" e “qualitativo", como um instrumento operativo de uma dinâmica de investigação instauradora de novo paradigma nas Ciências Humanas e Sociais. A dinâmica investigativa resulta de uma interação entre quatro polos:

a) polo epistemológico **-** opera a permanente construção do objeto científico e a definição dos limites da problemática de investigação, dando-se uma constante reformulação dos parâmetros discursivos, dos paradigmas (correntes de pensamentos/filosóficas/modos de pensar) e dos critérios de cientificidade que orientam todo o processo de investigação;

b) polo teórico **-** centra a racionalidade do sujeito que conhece e aborda o objeto, bem como a postulação de leis, a formulação de hipóteses, as teorias e conceitos operatórios e a consequente confirmação ou invalidação do “contexto teórico" elaborado;

c) polo técnico **-** consuma, por via instrumental, o contato com a realidade objetivada, aferindo-se a capacidade de validação do dispositivo metodológico, sendo, aqui, que se desenvolvem operações cruciais como: a observação de casos e de variáveis, a avaliação retrospectiva e prospetiva, a infometria e até a experimentação mitigada ou ajustada ao campo de estudo de fenomenalidades humanas e sociais, sempre tendo em vista a confirmação ou refutação das leis postuladas, das teorias elaboradas e dos conceitos operatórios formulados;

d) polo morfológico **-** formaliza os resultados da investigação levada a cabo, através da representação do objeto em estudo e da exposição de todo o processo de pesquisa e análise que permitiu a construção científica em torno dele.

---

[59] *cf. Dicionário Eletrônico de Terminologia em Ciência da Informação* (DeltCI). Disponível em: <https://paginas.fe.up.pt/~lci/index.php/1738>. Acesso em: 25 abr. 2017.

De acordo com Armando Malheiro Silva (2014), o método quadripolar tem sido utilizado como ferramenta de suporte à investigação em Ciência da Informação 'aplicada'. Com suas diferentes instâncias metodológicas, que submetem a pesquisa a exigências específicas, aponta para uma abordagem global do processo de pesquisa, mostrando, por sua dinâmica interna, que a prática científica se desenvolve holisticamente, com vista a construir progressivamente o seu objeto. Segundo o autor, não se trata de momentos separados ou um esquema sequencial, pelo contrário, são etapas que se articulam de forma estreita e flexível, num movimento elíptico e aberto, nunca linear ou redutor, apresentando uma dinâmica investigativa e de conhecimento que resulta da interação dinâmica dos seus quatro polos, garantindo flexibilidade e continuidade na estratégia da investigação.

A aplicação do Método Quadripolar, além de auferir qualidade pela triangulação, assegura a cientificidade deste estudo, aperfeiçoou e materializou o desenho inicial da pesquisa (seção 1.4), bem como forneceu enquadramento investigativo, conforme estruturado no quadro 5.

Quadro 5 - Aplicação do Método Quadripolar

| POLO | DESCRIÇÃO | ENQUADRAMENTO INVESTIGATIVO |
|---|---|---|
| EPISTEMOLÓGICO | Vigilância crítica (auto-exame) e equacionamento dos domínios da pesquisa (aparato teórico e institucional) com o macroenquadramento da problemática da investigação | - Inserido no atual paradigma pós-custodial, informacional e científico, associado ao dinamismo da Era da Informação e das (novas) tecnologias da informação e da comunicação (TIC), bem como seu impacto na sociedade em rede<br>- Busca equacionamento dos seguintes domínios: ciberespaço, informação, ambiente digital, segurança e defesa cibernética, instituição governamental, preservação, tecnologia e proteção cibernética gestão da informação<br>- Abordagem centrada no impacto/necessidade da proteção da informação (digital) na sustentação e no desenvolvimento de um Estado-Nação |

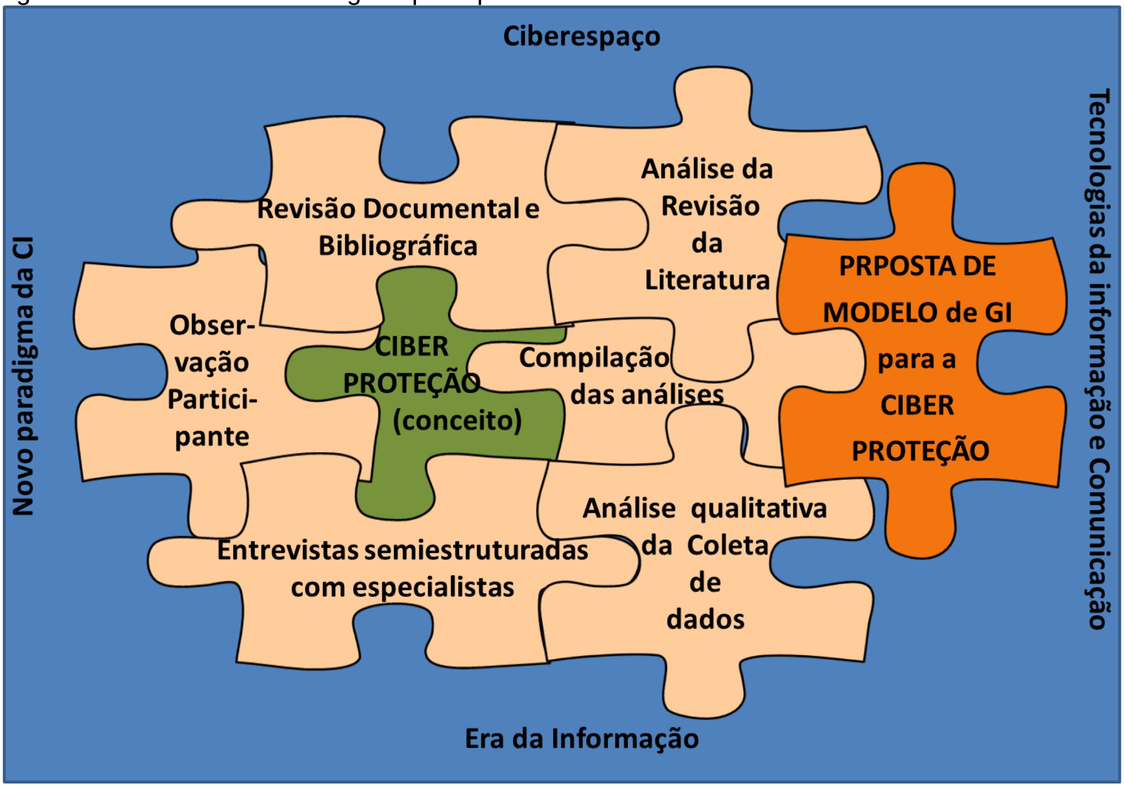
| | | |
|---|---|---|
| TEÓRICO | Elaboração dos instrumentos norteadores (hipóteses, variáveis, conceitos, pressupostos) aliado à interpretação dos fatos, especificação de requisitos e definição das soluções | - Potencializa o valor da informação no ambiente digital institucional nacional<br>- Reflete o estado da arte relativo à segurança da informação no ciberespaço, reforçando a necessidade de discussão do tema no escopo da Ciência da Informação<br>- Gestão da informação, na perspectiva do campo científico da Ciência da Informação, colocando sob análise as práticas de segurança e preservação da informação em meio digital, em contexto estratégico-nacional, de uma sociedade e instituições governamentais<br>- Construção do conceito de Ciber Proteção, contribuindo para a contextualização do objeto de estudo<br>- Elaboração de um Modelo de amplitude nacional, com características visões sistêmicas, holísticas e estratégicas intrínsecas da Ciber Proteção |
| TÉCNICO | Investigador toma contato, por via instrumental, com a realidade objetivada. Operacionalizam-se instrumentos metodológicos, com caraterísticas qualitativas e operacionais | - Realiza uma exploração da problemática supracitada em função da observação participante<br>- Revisa a literatura (pesquisas bibliográficas e documentais) em três macrotemas, nomeadamente ciberespaço, ambiente informacional e proteção da informação em meio digital<br>- Busca soluções a partir da revitalização de conceitos<br>- Aplica metodologias de levantamento de dados<br>- Analisa qualitativamente por meio da técnica de análise de conteúdo<br>- Consolida os requisitos para um modelo de gestão da informação<br>- Almeja validar o Modelo proposto por intermédio de entrevistas em profundidade. |
| MORFOLÓGICO | Estruturação, formatação e redação de todo o processo de construção do objeto científico. Comunicação por meio do relatório de investigação | - Apresenta por escrito todo os processos de construção e delimitação do objeto de estudo, de estruturação da pesquisa e de análise dos dados, bem como os resultados obtidos na revisão da literatura, observação participante e no estudo empírico<br>- Descreve os elementos norteadores da investigação, propondo e consolidando conceitos, perspectivas e recomendações<br>- Apresenta proposta de Modelo para a Ciber Proteção |

Fonte: elaboração própria

Conforme ficou caracterizado no método Quadripolar, há uma necessária integração e retomada cíclica entre as etapas. Porém, percebe-se que o Polo Epistemológico se desenvolveu, substancialmente, na fase ‘inicial’ da pesquisa formal, fornecendo base segura e arcabouço sólido para o desenvolvimento e consolidação dos demais polos, enquanto o Polo Morfológico materializou-se mais para o final da mesma, intercalado pela maturação do Polo Teórico revestido de um viés mais descritivo.

Não obstante, o Polo Técnico, de cunho descritivo e exploratório, tornou-se naturalmente mais complexo e extenso, sendo necessário explicitar o emprego das múltiplas técnicas investigativas. A figura 10 resume de forma gráfica aspectos metodológicos da pesquisa sustentados pelo Método quadripolar.

Figura 10 - Mosaico metodológico quadripolar




Fonte: elaboração própria

Neste capítulo, sinteticamente, foi apresentado o conjunto de métodos e técnicas utilizados que possibilitasse mapear e analisar tanto o conhecimento registrado na literatura e em fontes documentais, como aquele adquirido por atores envolvidos no planejamento e na execução das atividades de segurança e defesa cibernéticas. Em relação à sistematização das atividades realizadas e ao alcance dos objetivos estabelecidos, o quadro 6 relaciona os objetivos específicos (OE) e os caminhos metodológicos adotados.

Quadro 6 - Objetivos e caminhos metodológicos

| OBJETIVOS ESPECÍFICOS | MÉTODOS DE COLETA | FONTE | DADOS A SEREM COLETADOS |
|---|---|---|---|
| OE1-Contextualizar a proteção da informação no ciberespaço | Análise Documental<br>Pesquisa Bibliográfica<br>Observação participante<br>Entrevista | Literatura especializada (livros, periódicos, artigos, teses, anais de eventos).<br>Estruturas relacionadas às atividades de proteção cibernética | Características, peculiaridades, atividades, marcos legais etc., referentes à proteção da informação no ciberespaço<br>Considerações em relação ao conceito de Ciber Proteção desenvolvido |
| OE2-Analisar conceitos e padrões de gestão da informação, sob a perspectiva de segurança e defesa do ciberespaço | Análise Documental<br>Pesquisa Bibliográfica<br>Observação participante<br>Entrevista | Literatura especializada (livros, periódicos, artigos, teses, anais de eventos).<br>Estruturas relacionadas às atividades de proteção cibernética | Padrões, conceitos e melhores práticas de gestão segura da informação |
| OE3-Identificar os padrões e a situação da gestão da informação nos órgãos e entidades relacionados diretamente com a Ciber Proteção | Observação participante<br>Entrevista | Estruturas relacionadas às atividades de proteção cibernética | Situação atual da segurança em meio digital nacional e internacional<br>Características da gestão da informação nas estruturas ligadas à Ciber Proteção |
| OE4- Definir os requisitos para um modelo de Ciber Proteção para a APF. | Análise Documental<br>Pesquisa Bibliográfica<br>Observação participante<br>Entrevista | Literatura especializada (livros, periódicos, artigos, teses, anais de eventos).<br>Estruturas relacionadas às atividades de proteção cibernética | Sistemas/Modelos adotados, planejados (ou necessários) de gestão da informação e do conhecimento nas estruturas ligadas à Ciber Proteção |

Fonte: elaboração própria

Objetivou-se, assim, prover e avaliar a estruturação de requisitos para um modelo de gestão da informação nos órgãos e entidades públicos relacionados diretamente com a Ciber Proteção. Consideraram-se, também, de grande valia e diferencial para esta pesquisa, as evidências e experiências operacionais vivenciadas pelo autor por meio de observação participante explorada no próximo capítulo.

# 4. OBSERVAÇÃO PARTICIPANTE

A vivência operacional do autor, nos campos da segurança e da defesa cibernéticas, norteou a formulação do problema, a concepção da tese, a tipificação do universo da pesquisa, incluindo o discernimento sobre a amostra escolhida e, particularmente, a proposição das hipóteses.

## 4.1 ATIVIDADES REALIZADAS

No presente estudo, o pesquisador realizou as referidas observações de forma natural, ou seja, pertencendo efetivamente aos grupos/organizações suprarreferenciados. O quadro 7 apresenta, sinteticamente, características relevantes da observação participante realizada entre 2008 e 2018.

Quadro 7 - Dimensões da Observação Participante

| **AÇÃO PRINCIPAL** | **ESPAÇO FÍSICO** | **PRINCIPAIS ATORES ENVOLVIDOS** | **ATIVIDADES/EVENTOS EM DESTAQUE** | **PERÍODO** |
|---|---|---|---|---|
| Implementação (conscientização, pesquisa e regulação) de SIC (DSIC) | DSIC Sede das oficinas | Servidores federais da Administração Pública | Congressos e seminários de SIC; Oficinas de implementação da IN 01/GSI e de suas Normas Complementares | 2008 a 2012 |
| Gestão de incidentes de segurança em redes de computadores (CTIR Gov) | CTIR Gov DSIC GSI | Integrantes dos CSIRTs nacionais e internacionais; FEBRABAN; ANATEL | Implementação de Sistema de *Workflow* – RTIR; Colóquios, Fóruns e acordos de cooperação técnicos (P.ex.: LACNICs; GRN-7/CBC3; FIRST; GRISB) | 2009 a 2011 |
| Compartilhamento de melhores práticas sobre segurança cibernética (CICTE/OEA) | América latina e Caribe | Integrantes dos CSIRTs dos Países membros da OEA | *Workshops* (organização e participação) Missões de assistência técnica (instrutor) | 2009 a 2011 |
| Normatização/regulação em SIC (CGSI/CDN) | CDN; GSI; DSIC | Organizações integrantes do Comitê Gestor – GSI | Elaboração de Normas Complementares a IN 01 (P.ex.: NC 05, 08 e 20) | 2009 a 2011 |
| Coordenação executiva e planejamento da segurança cibernética (UNCSD) | CDCiber; Riocentro | EB; MB; FAB; MD; GSI; Serpro; ANATEL; NIC.br/CGI; ABIN; MTur; MRE; MJ; MinC; ONU, IC do RJ | Planejamento, operacionalização e desmobilização da Conferência das Nações Unidas Rio + 20 | 2012 |

| | | | | |
|---|---|---|---|---|
| Planejamento, coordenação e integração de segurança e de defesa cibernéticas (CDCiber) | CDCiber; CCDA; CI-CCR; Destacamentos Def Ciber | EB; MB; FAB; MD; GSI; MPOG; MC; MCTIC; ANATEL; NIC.br/CGI; MinC; ABIN; MTur; MRE; ME; MJ; MinC, IC dos Estados sede | Planejamento, execução e desmobilização da Copa das Confederações, JMJ, Copa do Mundo e Operações conjuntas do MD; Organização de Seminários de Def Ciber | 2012 a 2014 |
| Proposta de plano estratégico para políticas públicas voltadas à segurança e defesa do espaço cibernético nacional (GTI) | SAE/PR | SAE; MD; MRE; MEC; MDIC; MPOG; MC; MCTIC; GSI; ANATEL; NIC.br/CGI; Dataprev; Serpro | Avaliação diagnóstica; levantamento de riscos; reuniões do GTI | 2013 a 2015 |
| Projeto de estruturação da Escola Nacional de Defesa Cibernética (EnaDCiber) | CPD da UnB | UnB, MD, CDCiber | Jornadas/Seminários Termos de referências Estudo sobre ecossistema de Def Ciber | 2014 a 2015 |
| Projeto Laboratórios Virtuais de segurança da informação e criptografia (RENASIC) | RENASIC Instituições Executoras | MD, CDCiber; MCTIC, FINEP; ITA; UFMG; UnB; CASNAV; LNCC; IME; UFCG; CTI | Seminários; visitas técnicas; Revista ENIGMA; COMSIC | 2015 a 2017 |
| Assessor de gestão do conhecimento | ENaDCiber | ComDCiber, MD, MEC, MCTIC, EB; MB; FAB, CDCiber | Conteudista e revisor de cursos, de trilhas do conhecimento e de itinerários formativos | 2018 |

Fonte: elaboração própria

O quadro descreve, além das dimensões espaço e tempo, situações que auferem confiabilidade científica ao estudo, particularmente pela forma sistematizada de participação nas atividades de gestão de incidentes na APF e nos grandes eventos, inseridos, em ambos os casos, nas atividades operacionais, compartilhando objetivos similares e integrantes comuns.

## 4.2 Comunicação e registros da Observação Participante

Em termos de organização sistematizada, comunicação acadêmica e científica durante o período da participação ativa, registra-se o seguinte:

a) artigo sobre governo eletrônico e segurança da informação (OEA/2010);

b) conteudista, do módulo ETIR, no Curso de Fundamentos em Gestão de Segurança da Informação e Comunicações - CFGSIC, para servidores públicos, a cargo DSIC (GSI/2010)[60];

c) monografia sobre os procedimentos de segurança cibernética para o gerenciamento de incidentes em redes de computadores da administração pública federal - CEGSIC (UnB/2011);

d) apresentação de trabalho sobre procedimentos para a gestão da segurança da informação em redes de computadores no WICI (UnB/2013);

e) capítulo sobre a segurança cibernética na Conferência das nações unidas para o desenvolvimento sustentável – RIO+20 (UFSC/2013);

f) artigo sobre a identificação das necessidades de informação dos profissionais de segurança da informação (BRAJIS/2013);

g) orientação de trabalhos de conclusão de curso (TCC) e ensino (professor) na Pós-graduação em Segurança da Informação (IESB/2015-18);

h) dissertação de mestrado sobre o comportamento informacional na gestão da segurança cibernética da administração pública federal (UnB/2015);

i) artigo sobre a segurança dos sistemas de informação no espaço cibernético (RICI/2017);

j) artigo sobre a proteção da informação em ambientes digitais – tendências e perspectivas (ENANCIB/2018).

No que tange ao compartilhamento de resultados e melhores práticas colhidas em campo, bem como da publicidade dos estudos, experiências e vivências, o quadro 8, apresenta um resumo das participações em *workshops*, seminários, palestras, eventos e atividades diversas nacionais e internacionais relacionadas à Ciber Proteção.

Quadro 8 - Compartilhamento de resultados e melhores práticas

| **EVENTO** | **ATIVIDADE** | **ANO** |
|---|---|---|
| Encontro internacional de CSIRTs nacionais-CERT CC, Japão | apresentação sobre Brazilian`s CSIRT (inserção do CTIR Gov como ponto focal nacional) | 2009 |

[60] Informações complementares disponíveis em: <https://trompowsky.org.br/ft-e-gabinete-de-seguranca-institucional-da-presidencia-firmam-parceria-para-realizacao-de-treinamento/>. Acessado em: 08 jan. 2017.

| | | |
|---|---|---|
| Joint OAS Hemispheric Workshop Developing a National Framework for Cyber Security/OEA, Brazil | coordenador do exercício de Segurança Cibernética para os membros dos 34 países participantes e moderador no painel sobre gestão de incidentes | 2009 |
| *Taller Avanzado* - CICTE/OEA, Chile | instructor sobre Manejo de un Equipo de Respuesta a Incidentes de Seguridad Cibernética (CSIRT) Nacional | 2009 |
| VIII FÓRUM de TIC Dataprev | Apresentação sobre o Tratamento de Incidentes em Rede na Administração Pública Federal | 2009 |
| SICGOV | organização e desenvolvimento de oficinas de tratamento de incidente | 2009 - 2010 |
| SICGOV | Painel sobre SIC e a gestão de incidentes de segurança em redes de computadores | 2009 - 2010 |
| Subcomissão de fraudes na Internet | colaborador da FEBRABAN | 2009 - 2011 |
| GRISB | colaborador no tratamento e resposta a incidentes | 2009 - 2011 |
| SemSIC | capacitação de integrantes da APF em segurança da informação | 2009 - 2011 |
| CICTE/OEA, Peru | instructor na Misión de asistencia técnica en materia de seguridad cibernética | 2010 |
| Overview of creating and managing CSIRTs/CERT program/CERT.br | organização do *Workshop* de Gerência de Tratamento de Incidente em Rede na APF | 2010 |
| SBSeg (Simpósio) | painel sobre Segurança da Informação Corporativa: Desafios atuais e futuros | 2010 |
| *Taller* - CICTE/OEA, Panamá | instrutor do sobre manejo de equipos de respuesta a incidentes de seguridad cibernetica – CSIRTS | 2010 |
| *Taller* - CICTE/OEA, Uruguai | instructor sobre Mejores Prácticas en Seguridad Cibernética | 2010 |
| ICCYBER | conferência sobre Incidentes de Segurança em Redes na Administração Pública Federal | 2011 |
| II Fórum da Internet no Brasil | painel sobre o novo ativismo em rede, ciber guerra e segurança informacional | 2012 |
| US – Brazil Internet and ICT Working Group | apresentação sobre Cyber defense actions during the United Nations Conference on Sustainable Development – Rio+20 | 2012 |
| II Seminário Internacional de Ciência, Tecnologia e Inovação | conferência sobre a evolução da Segurança Cibernética na Copa das Confederações e na Jornada Mundial da Juventude | 2013 |
| IX *Workshop* Internacional em Ciência da Informação (WICI) | apresentação de uma minuta de procedimentos para a gestão de incidentes de segurança nas redes de computadores da Administração Pública Federal. | 2013 |
| XIII Encontro Nacional de Estudos Estratégicos (ENEE) | painel sobre segurança e defesa cibernética: gerenciamento de riscos e recuperação de desastres. | 2013 |

| | | |
|---|---|---|
| III Seminário de Segurança - LAAD | apresentação sobre Segurança cibernética em Grandes Eventos | 2014 |
| SEGINFO - *Workshop* de Segurança da Informação | apresentação sobre a atuação do Centro de Defesa Cibernética nos Grandes Eventos | 2014 |
| I Jornada de Discussões dos Projetos ENaDCiber e SHCDCiber | organização e participação nos debates do segmento da ENaDCiber e revisão do estudo sobre o ecossistema de ciber defesa | 2014 |
| Data Center Dynamics Converge | apresentação sobre a defesa cibernética no Brasil: desafios e perspectivas | 2015 |
| II Jornada de Discussões dos Projetos ENaDCiber e SHCDCiber | apresentação dos resultados e coordenação das sessões de Grupos Focais sobre: o Perfil do Egresso, Cursos, Grade Curricular, Metodologias de Ensino, Pesquisa, Projetos e o Ensino para pessoas com Altas Capacidades (*Hackers*). | 2015 |
| Summer Doctoral Consortium SDC'17 (Universidades do Porto e de Aveiro, Portugal) | apresentação da visão sistêmica preliminar da proposta do modelo para a Ciber Proteção governamental ao Programa doutoral em informação e comunicação em Plataformas Digitais - ICPD | 2017 |
| XIX ENANCIB | apresentação oral – GT8: A proteção da informação em ambientes digitais – tendências e perspectivas | 2018 |

Fonte: elaboração própria

Nos três capítulos seguintes, teorias de diversas áreas do conhecimento e diferentes linhas de pesquisa, correlatas ou não à própria Ciência da Informação, foram emprestadas e relacionadas para compor o ferramental epistemológico e teórico, o que norteou tanto a forma como o problema foi observado, quanto ao delineamento da abordagem dos objetivos, consolidação de conceitos e averiguação das hipóteses.

## 5 O CIBERESPAÇO – UMA REALIDADE

As próximas seções traçam um esboço entre o ciberespaço e a realidade brasileira, abordando as principais características do espaço cibernético imbricadas nesta pesquisa, bem como o modelo de governança da Internet adotado pelo Brasil, seus principais atores e marcos regulatórios.

O termo ‘ciber’ (do inglês *cyber*) remete à: cibernética, realidade virtual e ciberespaço. No entendimento de Cunha e Cavalcanti (2008, p. 80), *ciber* é um prefixo utilizado para criar termos que se referem às mudanças sociais, tecnológicas, culturais e científicas decorrentes da utilização dos computadores e, também, relacionados com a Internet.

O termo 'cibernética' deriva do grego *kybemytiky* ou *Kubernites* e significa arte de governar navios (ou homens), isto é, dirigi-los por meio da comunicação e do controle. No campo científico e, partindo de análises comportamentais, Wiener (1968, 1995) apresenta cibernética como o estudo capaz de amalgamar a comunicação e o controle das máquinas, seres vivos e grupos sociais; considerando-se que, do ponto de vista da transmissão da informação, não há distinção entre máquinas e seres humanos. Norbert Wiener, prossegue seus estudos, ao esclarecer que

> o propósito da cibernética é o de desenvolver uma linguagem e técnicas que nos capacitem, de fato, a haver-nos como problema de contrôle [sic] e da comunicação em geral, e a descobrir o repertório de técnicas e ideias adequadas para classificar-lhe as manifestações específicas sob a rubrica de certos conceitos (WIENER, 1968, p. 17).

No contexto da Ciência da Informação, Greyciane Lins ressalta a importância da informação para a cibernética[61], a partir do conceito sinteticamente apresentado por Wiener. No entendimento da autora, o termo (informação) designa o conteúdo daquilo que se permuta com o mundo exterior em um processo de ajuste às contingências do meio ambiente. A informação, portanto, seria a base da teoria cibernética, pois está relacionada aos conceitos de energia e controle. De fato, o próprio conceito de cibernética de Wiener está relacionado às ações de controle e comunicação da informação em humanos e máquinas, ou seja, não apenas as ações realizadas com

---

[61] A classificação de cibernética como ciência é controversa, podendo enquadrar-se como: Interciência (novas disciplinas constituídas na confluência de várias disciplinas de diferentes áreas de conhecimento), interdisciplina ou mesmo como disciplina universal, visando à reordenação da hierarquia tradicional das ciências (POMBO, 2006, p. 212).

o uso de computadores (LINS, 2013). A pesquisadora, no campo da cibercultura, conclui que o objetivo da cibernética seria:

> compreender a sociedade por meio dos processos comunicacionais utilizando a informação como energia que promove seu funcionamento. A percepção é a de que sistemas em geral funcionam da mesma maneira, e assim homens e máquinas podem comunicar-se e comunicar entre si (LINS, 2013, p. 37).

Em relação à cibercultura, convém acrescer que, no início da década de 2000, Manuel Castells (2007, p. 240) afirmava que vivíamos em um tipo de cultura da virtualidade real a qual

> é virtual porque está construída principalmente através de processos virtuais de comunicação em base eletrônica. É real (e não imaginária) porque é a nossa realidade fundamental, a base material com que vivemos a nossa existência, construímos os nossos sistemas de representação, fazemos nosso trabalho, nos relacionamos com os outros, obtemos informação, formamos nossa opinião, actuamos [sic] politicamente e alimentamos os nossos sonhos.

No tocante ao ‘espaço’, entre múltiplas definições, conceitos e contextos destaca-se o informacional: “a soma de informações numa determinada área de interesse. Esse espaço pode ser tão grande como a Internet ou pequeno como um disco rígido de computador de um indivíduo” e o filosófico: “meio ideal, caracterizado pela exterioridade das suas partes, no qual se localizam os nossos perceptos (isto é, objetos de percepção) e que contém, por consequência, todas as extensões finitas” (CUNHA; CAVALCANTI, 2008, p. 155).

Reforça-se, todavia, a inserção no paradigma da era da informação e da sociedade em rede, cuja característica-espacial-chave é a ligação em rede entre o local e o global. Consideram-se, assim, fundamentais os aportes de Manuel Castells, onde o espaço (e o tempo) é considerado dentro da teoria social, como expressão da sociedade, sendo definido como “suporte material de práticas sociais de tempo compartilhado”. Levando em consideração que os fluxos representam e dominam nossa organização social, vida econômica, política e simbólica, o autor apresenta uma nova espacialidade denominada ‘espaço de fluxos’[62] como “o suporte material das práticas

[62] Para Castells (2010, p. LXXII, 549), o espaço de fluxos conquistou a lógica do espaço de lugares (local cuja forma, função e significado são independentes dentro das fronteiras da contiguidade física - dinâmica da matéria), criando uma arquitetura espacial global de megacidades que se interligam, enquanto as pessoas continuam a encontrar significados em lugares e a criar as suas próprias redes nos espaços de lugares.

sociais simultâneas comunicadas a distância. Tal definição envolve a produção, transmissão e processamento de fluxos de informação". O novo conceito de espaço deveu-se ao

> desenvolvimento da comunicação digital com base na microeletrônica, redes avançadas de telecomunicação, sistemas de informação e o transporte computadorizado que transformaram a espacialidade da interação social ao introduzir a simultaneidade, ou qualquer enquadramento temporal escolhido, nas práticas sociais, independentemente da localização dos atores envolvidos no processo de comunicação (CASTELLS, 2010, p. LVI-LVII, 534-535).

Entende-se, pois, que espaço é uma realidade com componentes tangíveis e intangíveis, fidelizada a atividades humanas e ações temporais.

## 5.1 Ciberespaço

Cunha e Cavalcanti (2008, p. 80), buscando, no seu dicionário, definir de forma clara e sucinta os termos utilizados pelos profissionais da ampla e multifacetada área de ciência da informação, apresentam ciberespaço como:

a) espaço-tempo eletrônico criado pelas redes de comunicação e computadores multimídia;
b) o terreno não físico criado pelos sistemas computacionais e pelas redes de comunicações;
c) termo criado por Willian Gibson, em *Neuro romancer* de 1984, para relacionar o mundo e a sociedade que se reúnem ao redor do computador. Dessa forma, seria uma rede futurística de computadores (atual Internet) que as pessoas usariam, conectando seus cérebros à mesma;
d) metáfora que descreve o terreno não físico criado por sistemas de computador.

O *Tesauro Brasileiro de Ciência da Informação*[63] (Pinheiro; Ferrez, 2014) esclarece que o termo Ciberespaço possui relação de equivalência (USE) com Internet e

---

[63] Em outubro de 2014, o Instituto Brasileiro de Informação em Ciência e Tecnologia (IBICT) lançou o respectivo tesauro com a expectativa de que o mesmo seja instrumento fundamental para consistência

está classificado na categoria (CAT) 5.4 Redes de Comunicação e Informação, Internet, *Web*.

De acordo com Maria Manuela Pinto[64], o termo ciberespaço refere-se a um espaço virtual composto por cada computador e utilizador conectados numa rede mundial. Este termo poderá incluir a rede global de infraestruturas de tecnologias de informação interligadas entre si, especialmente as redes de telecomunicações, bem como os sistemas informáticos de processamento de dados, nomeadamente a última geração de *Big Data* e *Cloud Computing*, e, ainda, a Internet e os novos conteúdos interativos (redes sociais e os novos *media* digitais) ressalta a necessidade de se clarificar o conceito matricial de ciberespaço tipificando o entendimento de espaço e lugar onde:

> o espaço é o onipresente digital mas que quando as instituições, organizações e pessoas se apropriam dele e colocam, assim, a sua marca própria, fazem dele um 'lugar' seu, um '*locus'* (local do marcador genético) que varia, necessariamente, de acordo com as especificidades de quem o 'toma' …, daí uma maior orientação ao contexto que a objetos!

Na análise da autora, com o ciberespaço constituiu-se um novo espaço de sociabilidade que é não presencial e que possui impactos importantes na produção de valor, nos conceitos éticos e morais e nas interações humanas, importando, sobretudo, o ciberespaço como nova arma e como novo desafio à segurança de um Estado-Nação. Abre-se, portanto, a oportunidade de se refletir sobre o real papel do ciberespaço e de se conceberem políticas, estratégias, táticas e sistemas para os desafios em que se coloca à nova ordem mundial.

Para o Ministério da Defesa do Brasil, o espaço cibernético é composto de dispositivos computacionais conectados em redes, **ou não** [grifo nosso], onde as informações digitais transitam e são processadas e/ou armazenadas (BRASIL, 2014b). Ainda no escopo da defesa de um Estado-Nação, o Departamento de Defesa dos Estados Unidos (Department of Defense - DoD) define espaço cibernético como

> um domínio global dentro do ambiente de informações que consistem das redes interdependentes de infraestruturas de Tecnologia da Informação e

---

de terminologia e de vocabulário de determinado campo do conhecimento, assumindo um papel central na recuperação da informação no Brasil e em países lusófonos.

[64] Intercâmbio realizado (via e-mails e entrevistas presenciais), com a professora Maria Manuela Gomes de Azevedo Pinto, diretora do Centro de Investigação em Comunicação, Informação e Cultura Digital - Porto (CIC.Digital) - Universidade do Porto, entre abril e julho de 2017.

> seus dados residentes, incluindo a Internet, redes de telecomunicações, sistemas de computador, processadores e controladores embutidos[65] (ESTADOS UNIDOS, 2016, tradução nossa).

Interessante ressaltar-se que o chamado ciberespaço, mesmo quando tratado no contexto da segurança nacional, não se encontra restrito ao uso da Internet ou dos computadores, como corrobora o *Manual de Estrutura de Segurança Cibernética Nacional da Organização do Tratado do Atlântico Norte* - OTAN (*National Cyber Security Framework Manual* - NATO): "o ciberespaço é mais do que a Internet, incluindo não somente o *hardware*, *software* e sistemas de informação, mas também as pessoas e a interação social no âmbito dessas redes"[66]. Em 2016, a OTAN, durante a Cimeira de Varsóvia, declarou o ciberespaço como um novo domínio operacional, tão relevante como o ar, a terra e o mar (KLIMBURG, 2012, p. 8, tradução nossa).

Nas suas Disposições Preliminares, o *Marco Civil da Internet* define Internet, também conhecida por rede mundial de computadores, como: “o sistema constituído do conjunto de protocolos lógicos, estruturado em escala mundial para uso público e irrestrito, com a finalidade de possibilitar a comunicação de dados entre terminais por meio de diferentes redes” (BRASIL, 2014a, p. 1).

Sobre o surgimento da Internet, Demi Getschko[67] afirma que, na década de 1970, formas mais simples e alternativas de conexão de redes começavam a cair no gosto da comunidade acadêmica e ganhavam adeptos. Dentre esses padrões alternativos, destacou-se a pilha de quatro níveis (protocolos) chamada de TCP/IP (*Transmission Control Protocol/Internet Protocol*). O TCP/IP preocupou-se em “diluir controle, aumentar redundância, manter simplicidade, garantir abertura. **Privilegiar acesso, uso, robustez e serviço [...], sobre segurança na aplicação, controle e autenticação do usuário** [grifo nosso]” (CGI.br, 2016b).

Ao refletir sobre a criação da rede mundial de computadores, o Castells (1999, 2007) ressaltou que a Internet transformou a contemporaneidade ao permitir, pela pri-

---

[65] *Cyberspace - A global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.*
[66] *Cyberspace is more than the internet, including not only hardware, software and information systems, but also people and social interaction within these networks.*
[67] Foi o responsável pela primeira conexão TCP/IP brasileira, em 1991. Integra o Comitê Gestor da Internet no Brasil (CGI.br) desde 1995, sendo, atualmente, “Representante de notório saber em assunto da Internet”.

meira vez, a comunicação de muitos com muitos instantaneamente e em escala global. Para o sociólogo, a Internet nasceu basicamente de um projeto militar para desenvolver uma rede interativa de computadores, baseado em protocolos abertos e fomentado pela agência ARPA (Advanced Research Projects Agency), vinculada ao Ministério da Defesa dos EUA, ao findar do ano de 1969. O projeto, inicialmente denominado ARPANET-INTERNET, contou com o apoio das Universidades e Centros de Estudos, bem como de estudantes autônomos (conhecidos na atualidade como *Hackers*). Passada uma década, pressões comerciais aliadas ao crescimento de redes de empresas privadas e de redes cooperativas sem fins lucrativos consolidaram a privatização total da Internet.

Neste contexto, a Internet nasceu aberta, com verificação mínima de acesso e facilidade de expansão. Essas características inerentes ao protocolo TCP/IP, aliadas às facilidades de acesso por meio de estruturas de *hiperlinks* (*Web*), proporcionam à Internet potencialidades quase que ilimitadas, porém dentro de um ambiente inseguro para transações comerciais, uso governamental ou mesmo para manutenção da privacidade pessoal.

Na visão de Castells (2010, p. XLIX-LI):

> nos anos 2000 testemunhamos uma crescente convergência entre a Internet e as comunicações sem fios e múltiplas aplicações que distribuem os meios de comunicação através de redes sem fios, multiplicando, assim, pontos de acesso à Internet. [...] o seu vasto leque de aplicações é o tecido comunicacional das nossas vidas em várias áreas: no trabalho, nas ligações pessoais, na informação, no entretenimento, nos serviços públicos, na política e na religião [... distribuindo-se] por todos os patamares da vida social.

Ao abordar as possibilidades advindas da rede mundial de computadores, a Organização dos Estados Americanos declarou:

> o acesso à Internet, pela sua natureza multidirecional e interativa, sua velocidade e alcance global a um relativo baixo custo, e seus princípios de desenho descentralizado e aberto, possui um potencial inédito para a realização efetiva do direito a buscar, receber e difundir informações em sua dupla dimensão, individual e coletiva. Além disso, a Internet atua como uma plataforma para a realização de outros direitos humanos, como o direito a participar na vida cultural e a gozar dos benefícios do progresso científico e tecnológico, o direito à educação, o direito à reunião e associação, os direitos políticos, o direito à saúde, entre outros (OEA, 2013, p. 16-17).

Na visão do professor Gustavo Mirapalheta, dentre as possibilidades possíveis, oriundas dos milhares de dados que transitam além das fronteiras físicas e chegam a outros países, os governos encontram-se em uma encruzilhada. A Internet tornou as fronteiras físicas mais tênues, diminuindo sua capacidade de controle, e eles, para manter esta capacidade, precisarão abrir mão justamente de parte da mesma. Sobre a interação entre o ciberespaço e os governos observa:

> devemos pensar o fluxo de informações na Internet como uma gigantesca cadeia de suprimentos virtual. [..., cuja] gestão requer coordenação dos diversos atores envolvidos. Sendo assim, algum nível de coordenação intergovernamental terá de existir para que se possam implementar regras que evitem o manuseio de informações de maneira indevida (CGI.br, 2016a, p. 21).

Vint Cerf, cocriador do TCP/IP, afirmou, na 20ª edição do Congresso Mundial de Tecnologia da Informação - WCTI 2016, que a Internet é uma obra inacabada e insegura, haja vista que a criatividade para o seu uso parece ser infinita. No quesito segurança, ressaltou as crescentes vulnerabilidades dos *softwares* nas plataformas móveis e a importância dos acordos transnacionais e cooperativos para combater os crimes na rede mundial de computadores, bem como a da necessidade do uso intensivo da criptografia para a autenticação (WCTI, 2016).

Sobre as inovadoras possibilidades do ciberespaço, aliadas à força da natureza digital da informação, não obstante sua importância no nível estratégico-governamental de um Estado-Nação, destaca-se a hiperconectividade em tempo real (*real time*). Essa enxurrada informacional instantânea afeta sobremaneira o indivíduo, gerando um novo paradigma denominado *onlife*[68], onde, na tentativa de expressar o sentido de experiência contemporânea de uma realidade hiperconectada, a relação *online/offline* não faz mais sentido. De acordo com o filósofo da informação Luciano Floridi (2015), um dos mentores do "*The onlife manifesto*"[69], a crescente penetração das TIC produz as seguintes transformações:

a) embaçamento da distinção entre realidade e virtualidade;
b) embaçamento das distinções entre humano, máquina e mundo físico;
c) inversão da escassez de informações para a abundância de informação;
d) mudança da primazia das entidades à primazia das interações.

A seção, a seguir, tratará das peculiaridades do espaço cibernético brasileiro, contemplando o governo eletrônico e a governança da Internet no país.

---

[68] O projeto *onlife* desenvolve questões relativas ao significado humano em face de uma sociedade computacional interconectada via Internet que, juntamente com os desdobramentos oriundos da revolução digital, inserem-se no contexto do ciberespaço.
[69] Maiores informações disponíveis em: <https://www.academia.edu/9742506/The_Onlife_Manifesto_-_Being_Human_in_a_Hyperconnected_Era>. Acesso em: 21 nov. 2016.

## 5.2 O CIBERESPAÇO E O CONTEXTO NACIONAL

O governo brasileiro utiliza, em larga escala, as mais diversas possibilidades dos sistemas de informação automatizados e de redes de comunicação de dados. Nesse sentido, o governo vem disponibilizando aos cidadãos um crescente acervo de páginas, documentos, dados, aplicações e serviços *on-line*, interligados por meio da rede mundial de computadores. Tais iniciativas, conhecidas genericamente como governo eletrônico (*e-gov*), apoiam as mais diversificadas ações governamentais nas três esferas do poder, adotando soluções multifacetadas, fortemente suportadas nas tecnologias de informação, inseridas no contexto do espaço cibernético.

A Organização para a Cooperação e Desenvolvimento Econômico - OCDE (Organisation for Economic Co-operation and Development- OECD)[70], faz distinção entre governo eletrônico (*E-Government*) e Governo digital (*Digital Government*):

> e-Gov refere-se ao uso pelos governos de tecnologias de informação e comunicação (TIC), e em particular a Internet, como uma ferramenta para alcançar um governo melhor.
>
> governo digital refere-se ao uso de tecnologias digitais, como parte integrante das estratégias de modernização dos governos, para criar valor público. Baseia-se num ecossistema governamental digital compreendido por atores governamentais, organizações não governamentais, empresas, associações de cidadãos e indivíduos que apoiam a produção e o acesso a dados, serviços e conteúdos por meio de interações com o governo[71] (OECD, 2014, p. 6).

Na Administração Pública Federal (APF) brasileira, as ações de governo digital começaram a ser estruturadas no início da década de 2000, sob a denominação de “governo eletrônico”. Elas tinham a finalidade de priorizar o uso das tecnologias da informação e comunicação, para democratizar o acesso à informação. Buscava-se não só ampliar o debate e a participação popular na construção das políticas públicas,

---

[70] A OCDE conta com 35 países membros, empenhados em promover a democracia e a economia de mercado, que, no quadro das suas valências, apoia os Governos no exercício de comparabilidade de experiências, boas práticas e de coordenação das suas políticas, bem como numa procura de respostas e soluções para problemas comuns. Disponível em: <https://www.dges.gov.pt/pt/pagina/ocde>. Acesso em: 31 out. 2018.

[71] *E-Government refers to the use by the governments of information and communication technologies (ICTs), and particularly the Internet, as a tool to achieve better government - Digital Government refers to the use of digital technologies, as an integrated part of governments’ modernization strategies, to create public value. It relies on a digital government ecosystem comprised of government actors, non-governmental organizations, businesses, citizens’ associations and individuals which supports the production of and access to data, services and content through interactions with the government.*

mas também aprimorar a qualidade e a efetividade dos serviços e informações (BRASIL, 2016a).

O Comitê Gestor da Internet no Brasil (CGI.br), por meio do Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (CETIC.br), do Núcleo de Informação e Coordenação do Ponto BR (NIC.br), vem realizando pesquisas sobre o *e-gov* nacional há mais de uma década. Os resultados das pesquisas oferecem estatísticas e indicadores sobre o acesso e o uso das tecnologias de informação e comunicação no âmbito da administração pública.

A pesquisa publicada em 2010, intitulada - *Dimensões e características da Web brasileira: um estudo do '.gov.br'* -, revelou baixo grau de maturidade na gestão da *Web* do governo brasileiro[72]. Tal fato, de certa forma, originou-se da pressão sofrida pelos administradores públicos para que acelerassem a acessibilidade dos serviços digitais à população, em detrimento da complexidade da máquina pública e das especificidades técnicas de segurança. Neste contexto, a grande quantidade de administradores de sítios espalhados geograficamente leva ao questionamento de que, em prol da rapidez na prestação ou disponibilização de algum serviço ou informações, as soluções (desenvolvimento das aplicações e programas voltados para a Internet) não são exaustivamente testadas e validadas, apresentando vulnerabilidades no seu desenvolvimento, na sua implementação ou não recebendo a devida manutenção/atualização periódica de segurança (VIANNA, 2015).

Dada a importância de acompanhar e compreender o processo de adoção das TIC pela administração pública no Brasil, desde 2013, o CETIC.br realiza a pesquisa TIC Governo Eletrônico, com o objetivo de coletar indicadores sobre o uso das tecnologias no setor público brasileiro, nos três níveis de governo e nos poderes Executivo, Legislativo, Judiciário e no Ministério Público (CETIC.br, 2018, p. 122).

---

[72] Informações adicionais sobre segurança, riscos e ameaças em relação à implantação do governo eletrônico disponíveis em Vianna (2010).

Na pesquisa TIC Governo Eletrônico 2015, além de medir a existência de infraestrutura e gestão de TI nas organizações públicas, a TIC Governo Eletrônico 2015[73] investigou:

a) a presença dos órgãos na Internet por meio de *websites* e redes sociais;
b) a disponibilização por eles de informações e mecanismos de interação *on-line* para a sociedade;
c) a provisão de serviços públicos pela Internet e recursos oferecidos por meio de dispositivos móveis;
d) a criação de novos indicadores, envolvendo questões relacionadas à gestão de TI, planos de TI, computação em nuvem[74], comitê de governança de TI, entre outros (CETIC.br, 2016, p. 28).

Entre os resultados obtidos pela pesquisa iniciada em 2015, de interesse particular para este trabalho, destacam-se:

a) a maior parte dos órgãos públicos federais (97%) e estaduais (83%) e menos da metade das prefeituras (41%) possui uma área ou departamento responsável pela gestão de TI;
b) *websites* adaptados para dispositivos móveis são disponibilizados pela metade dos órgãos públicos federais, por cerca de 42% dos órgãos estaduais e por apenas 24% das prefeituras brasileiras;
c) aplicativos criados pelo órgão público para dispositivos móveis foram citados por 33% dos órgãos federais, 20% dos estaduais e em somente 4% das prefeituras;
d) 68% dos órgãos públicos federais e 59% dos estaduais possuem processos de tratamento de incidentes;

---

[73] Com o objetivo de gerar indicadores comparáveis internacionalmente, a pesquisa TIC Governo Eletrônico incorpora os indicadores-chave propostos pelo consórcio internacional *Partnership on Measuring ICT for Development* e introduz novos indicadores relacionados à infraestrutura e gestão das TIC, e-serviços, disponibilização de informações públicas e canais de comunicação e participação pela Internet (CETIC.br, 2016, p. 28).
[74] Computação em nuvem (*cloud computing*) - modelo computacional que permite acesso por demanda, e independentemente da localização, a um conjunto compartilhado de recursos configuráveis de computação (rede de computadores, servidores, armazenamento, aplicativos e serviços), provisionados com esforços mínimos de gestão ou interação com o provedor de serviços (BRASIL, 2012a, p. 3).

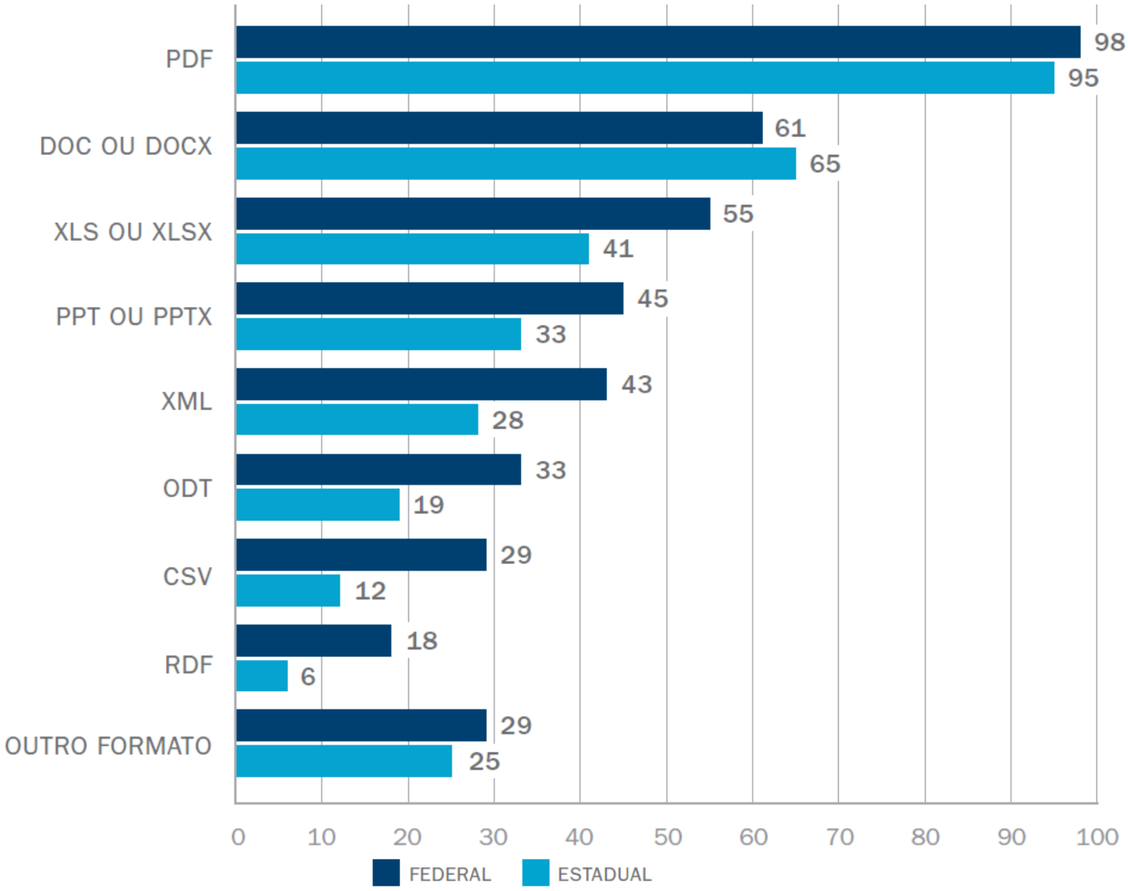
e) 79 % dos órgãos públicos federais e 44 % dos estaduais possuem plano de segurança da informação formalmente instituído;

f) aplicações de certificação digital[75] já foram utilizadas por 90% dos órgãos públicos federais e em menor proporção por aqueles de nível estadual (64%);

g) dentre os serviços públicos medidos pela pesquisa, o mais ofertado pelos *websites* foi o *download* de documentos ou formulários, cujas proporções observadas foram de 91% e 79%, respectivamente.

No que tange à gestão de documentos, destaca-se a utilização de diversos formatos de arquivo, que são disponibilizados nos sítios (*website*s) governamentais consolidados na figura 11.

Figura 11 - Formatos de arquivo utilizados nos órgãos públicos




Fonte: CETIC.br (2016, p. 164)

[75] Possibilita a troca eletrônica e segura de informações entre as organizações e outros usuários.

Percebe-se, na figura 11, que a maioria dos governos (estaduais ou federais) utilizam formatos de arquivos proprietários (P.ex.: pdf, doc e xls) que podem comprometer a preservação digital se forem descontinuados pelas empresas detentoras da tecnologia.

Sob a crescente demanda por um “governo digital”, a pesquisa complementa:

> as tecnologias de informação e comunicação são reconhecidas como agentes de mudança no setor público e como instrumentos que viabilizam a implementação de processos inovadores na gestão. Por outro lado, também geram cada vez mais as pressões sobre os gestores públicos para que o governo se adapte ao novo ambiente da economia digital. Essa pressão pode estar associada ao uso cada vez maior de tecnologias pelos cidadãos e empresas, também à preferência por serviços transacionais *on-line* e à conveniência dos ambientes virtuais (CETIC.br, 2016, p. 27).

A terceira edição da pesquisa TIC Governo Eletrônico, em 2017, indicou que a maior parte dos órgãos federais e estaduais e das prefeituras com *websites* não oferecem ferramentas transacionais aos cidadãos, tais como fazer inscrições e matrículas ou emitir documentos e licenças. No contexto da incorporação de novas tecnologias, a Pesquisa levantou que, entre os órgãos públicos federais, *e-mail* e *software* de escritório foram as soluções em nuvem mais utilizadas - ambas estavam presentes em 19% dos órgãos com área ou departamento de TI, seguidas por armazenamento de arquivos ou banco de dados (12%) e capacidade de processamento (12%). Em relação aos dispositivos moveis, a pesquisa constatou que 76% dos órgãos federais e 56% dos estaduais possuíam *website* adaptados para os mesmos, bem como, no que se refere aos recursos para comunicação, 19% dos órgãos federais disponibilizaram o envio de mensagens via aplicativos como WhatsApp e Telegram e 15% enviaram SMS aos cidadãos (CETIC.br, 2018, p. 128 e 131).

### *5.2.1 A governança da Internet no Brasil*

Em relação à história da Internet (ou do ciberespaço) no Brasil, Demi Getschko[76] adianta que:

> começa no final dos anos 1980, mais precisamente em setembro de 1988, quando uma conexão internacional dedicada e perene ligou a então ainda incipiente iniciativa brasileira de redes acadêmicas ao mundo. Seus primeiros usuários, pesquisadores, alunos e professores, tiveram acesso à maravilha

[76] Atual Diretor-Presidente do Núcleo de Informação e Coordenação do Ponto BR (NIC.br/CGI.br).

> do correio eletrônico, a bases de dados no exterior e, mesmo, ao acesso à rede mundial de computadores (GETSCHKO, 2009, p. 49).

A evolução da Internet brasileira pode ser traduzida em algumas datas significativas, tendo a primeira acontecido em abril de 1989, quando o País ganhou aquela que seria sua principal identidade digital na Internet: o <.br>, tal fato possibilitou aos brasileiros registrar endereços no domínio próprio do Brasil. Outras datas importantes aconteceram com o desdobramento desse processo, a partir da necessidade de gerenciar os domínios brasileiros, bem como de administrar o bloco de endereços de internet brasileiros. Assim, em 1994, o Brasil ganhou da Autoridade para Atribuição de Números da Internet – IANA (Internet Assigned Numbers Authority) cerca de quatro milhões de endereços IP (protocolo de Internet) que foram, na época, gerenciados pela reduzida equipe de Registro.br, que operava na Fundação de Amparo à Pesquisa do Estado de São Paulo (FAPESP).

#### 5.2.1.1 Comitê Gestor da Internet no Brasil

Em 1995, uma iniciativa do Ministério de Ciência e Tecnologia e do Ministério das Comunicações criou, por intermédio da Portaria Interministerial n. 147, de 31 de maio, o Comitê Gestor da Internet no Brasil (CGI.br) para coordenar e integrar as iniciativas relacionadas à rede mundial de computadores no Brasil. De acordo com Demi Getschko:

> a criação do CGI.br em 1995 mostrava o quanto o Brasil de então já entendia de Internet, ao criar um órgão não regulador, mas orientador da expansão da rede, composto por representantes dos variados setores da sociedade, e ao classificar a Internet como ‘serviço de valor adicionado’ sobre a estrutura de comunicações, mas sem com ele se confundir (CGI.br, 2016b).

O Comitê Gestor da Internet no Brasil é um modelo multissetorial de governança da Internet, contando com a participação de representantes do governo, da academia, do setor empresarial e do terceiro setor. O CGI.br possibilita a participação de múltiplos interessados nos debates, envolvendo a implantação, administração e uso da Internet no país.

O Decreto n. 4.829, de 03 de setembro de 2003 (Brasil, 2003), atualizou o decreto n. 145, de 1995, dispondo sobre o modelo de governança da Internet no Brasil e determinando as seguintes atribuições ao CGI.br:

a) estabelecer diretrizes estratégicas relacionadas ao uso e desenvolvimento da Internet no Brasil;

b) estabelecer diretrizes para a organização das relações entre o Governo e a sociedade, na execução do registro de Nomes de Domínio, na alocação de Endereço IP (*Internet Protocol*) e na administração pertinente ao Domínio de Primeiro Nível (*ccTLD - country code Top Level Domain*), <**.**br**>**, no interesse do desenvolvimento da Internet no País;

c) propor programas de pesquisa e desenvolvimento relacionados à Internet, que permitam a manutenção do nível de qualidade técnica e inovação no uso, bem como estimular a sua disseminação em todo o território nacional, buscando oportunidades constantes de agregação de valor aos bens e serviços a ela vinculados;

d) promover estudos e recomendar procedimentos, normas e padrões técnicos e operacionais, para a segurança das redes e serviços de Internet, bem assim para a sua crescente e adequada utilização pela sociedade;

e) articular as ações relativas à proposição de normas e procedimentos relativos à regulamentação das atividades inerentes à Internet;

f) ser representado nos fóruns técnicos nacionais e internacionais relativos à Internet;

g) adotar os procedimentos administrativos e operacionais necessários para que a gestão da Internet no Brasil se dê segundo os padrões internacionais aceitos pelos órgãos de cúpula da Internet, podendo, para tanto, celebrar acordo, convênio, ajuste ou instrumento congênere;

h) deliberar sobre quaisquer questões a ele encaminhadas, relativamente aos serviços de Internet no País;

i) aprovar o seu regimento interno.

Dentro dos princípios de múltiplas partes interessadas *(multistakeholder),* quanto à transparência e democracia, o CGI.br é integrado por 21 membros titulares a saber:

a) Ministério da Ciência e Tecnologia, que o coordenará;

b) Casa Civil da Presidência da República;

c) Ministério das Comunicações;

d) Ministério da Defesa;

e) Ministério do Desenvolvimento, Indústria e Comércio Exterior;
f) Ministério do Planejamento, Orçamento e Gestão;
g) Agência Nacional de Telecomunicações;
h) Conselho Nacional de Desenvolvimento Científico e Tecnológico;
i) Fórum Nacional de Secretários Estaduais para Assuntos de Ciência e Tecnologia;
j) notório saber em assuntos de Internet;
l) quatro representantes do setor empresarial ((i) provedores de acesso e conteúdo da Internet; (ii) provedores de infraestrutura de telecomunicações; (iii) indústria de bens de informática, de bens de telecomunicações e de *software*; e (iv) setor empresarial usuário);
m) quatro representantes do terceiro setor;
n) três representantes da comunidade científica e tecnológica.

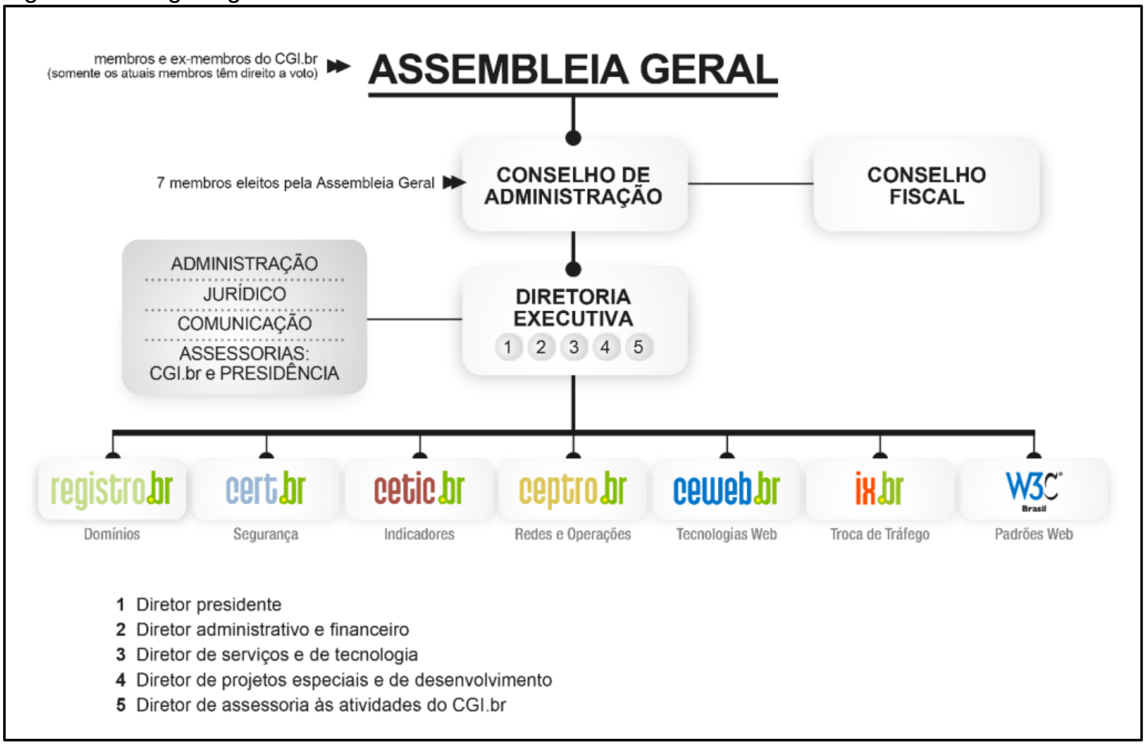
Nesse contexto, em meados de 2003, o NIC.br (Núcleo de Informação e Coordenação do Ponto BR) foi, formalmente, estabelecido como pessoa jurídica, com a finalidade de implementar as decisões e os projetos do CGI.br. Dentre suas atribuições estão as seguintes:

a) o registro e manutenção dos nomes de domínios que usam o <.br>, e a distribuição de números de Sistema Autônomo (ASN) e endereços IPv4 e IPv6 no País, por meio do Registro.br;
b) o tratamento e resposta a incidentes de segurança em computadores, envolvendo redes conectadas à Internet no Brasil, atividades do Cert.br;
c) projetos que apoiem ou aperfeiçoem a infraestrutura de redes no País, como a interconexão direta entre redes (IX.br) e a distribuição da Hora Legal brasileira (NTP.br). Esses projetos estão a cargo do Ceptro.br;
d) a produção e divulgação de indicadores, estatísticas e informações estratégicas sobre o desenvolvimento da Internet no Brasil, sob responsabilidade do Cetic.br;
e) promover estudos e recomendar procedimentos, normas e padrões técnicos e operacionais, para a segurança das redes e serviços de Internet, bem assim para a sua crescente e adequada utilização pela sociedade;
f) viabilizar a participação da comunidade brasileira no desenvolvimento global da *Web*, atividade desenvolvida pelo Ceweb.br;

g) o suporte técnico e operacional ao LACNIC (Registro de Endereços da Internet para a América Latina e Caribe).

A figura 12 apresenta o organograma do NIC.br, considerado o braço executivo do CGI.br.

Figura 12 - Organograma do NIC.br




Fonte: NIC.br (Disponível em: <http://www.nic.br/sobre/#composicao>)

Dessa forma, o NIC.br é uma entidade civil, de direito privado e sem fins de lucro, que possui como atividades permanentes: coordenar o registro de nomes de domínio, responder e tratar incidentes de segurança no Brasil, estudar e pesquisar tecnologias de redes e operações, produzir indicadores sobre as tecnologias da informação e da comunicação, implementar e operar os Pontos de Troca de Tráfego (PTT), viabilizar a participação da comunidade brasileira no desenvolvimento global da *Web* e subsidiar a formulação de políticas públicas, e, ainda, abrigar o escritório do W3C no Brasil.

Em março de 2009, o CGI.br publicou a resolução 2009/003[77], que aprovou os “Princípios para a Governança e Uso da Internet no Brasil”, a saber:

[77] Disponível em: <http://www.cgi.br/resolucoes/documento/2009/003>. Acesso em: 19 out. 2016.

a) liberdade, privacidade e direitos humanos - o uso da Internet deve guiar-se pelos princípios de liberdade de expressão, de privacidade do indivíduo e de respeito aos direitos humanos, reconhecendo-os como fundamentais para a preservação de uma sociedade justa e democrática;

b) governança democrática e colaborativa - a governança da Internet deve ser exercida de forma transparente, multilateral e democrática, com a participação dos vários setores da sociedade, preservando e estimulando o seu caráter de criação coletiva;

c) universalidade - o acesso à Internet deve ser universal para que ela seja um meio para o desenvolvimento social e humano, contribuindo para a construção de uma sociedade inclusiva e não discriminatória em benefício de todos;

d) diversidade - a diversidade cultural deve ser respeitada e preservada e sua expressão deve ser estimulada, sem a imposição de crenças, costumes ou valores;

e) inovação - a governança da Internet deve promover a contínua evolução e ampla difusão de novas tecnologias e modelos de uso e acesso;

f) neutralidade da rede - filtragem ou privilégios de tráfego devem respeitar apenas critérios técnicos e éticos, não sendo admissíveis motivos políticos, comerciais, religiosos, culturais, ou qualquer outra forma de discriminação ou favorecimento;

g) inimputabilidade da rede - o combate a ilícitos na rede deve atingir os responsáveis finais e não os meios de acesso e transporte, sempre preservando os princípios maiores de defesa da liberdade, da privacidade e do respeito aos direitos humanos;

h) funcionalidade, segurança e estabilidade - a estabilidade, a segurança e a funcionalidade globais da rede devem ser preservadas de forma ativa, através de medidas técnicas compatíveis com os padrões internacionais e de estímulo ao uso das boas práticas;

i) padronização e interoperabilidade - a Internet deve basear-se em padrões abertos que permitam a interoperabilidade e a participação de todos em seu desenvolvimento;

j) ambiente legal e regulatório - o ambiente legal e regulatório deve preservar a dinâmica da Internet como espaço de colaboração.

Interessante destacar-se o pioneirismo do CGI.br, sua atualidade, bem como a aderência do entendimento da Organização dos Estados Americanos com os princípios brasileiros:

> sendo a Internet um meio de comunicação social especial e singular [...] a sua governança se torna um assunto de particular relevância. [destacando a] importância do processo multipartite e democrático na governança da Internet, no qual prevaleça o princípio de cooperação reforçada para que todos os pontos de vista relevantes possam ser considerados e nenhum ator assuma a sua regulação de forma exclusiva (OEA, 2013, p. 58).

Em nosso país, o CGI.br coordena e integra as atividades e serviços de internet, seguindo o modelo de múltiplas partes interessadas. É uma experiência inovadora em relação à participação da sociedade nas decisões com base nos princípios de multilateralidade, transparência e democracia. A contribuição do CGI.br, por meio de sua estrutura operacional e executiva, o NIC.br, em prol do desenvolvimento da Internet no Brasil, também ocorre por meio de inúmeras outras atividades regulares, tais como: o Fórum da Internet, a Escola de Governança da Internet no Brasil, o Observatório da Internet, as câmaras técnicas, além de participações em eventos relacionados ao contexto digital no país e no exterior.

Os dez princípios supracitados serviram de inspiração para a proposição de um marco regulatório que estabelecesse condições básicas e essenciais para o futuro da Internet no país, denominado Marco Civil da Internet, o qual será abordado na próxima seção.

#### 5.2.*1*.2 Marco Civil da Internet

No Brasil, a regulação técnica e civil para a Internet consolidou-se em 23 de abril de 2014, ao ser sancionada a Lei n. 12.965, conhecida como *Marco Civil da Internet* (MCI). O MCI estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil e determina as diretrizes para atuação da União, dos Estados, do Distrito Federal e dos Municípios em relação à matéria, bem como destaca:

a) o reconhecimento da escala mundial da rede;
b) os direitos humanos, o desenvolvimento da personalidade e o exercício da cidadania em meios digitais;
c) a proteção dos dados pessoais e da privacidade;

d) a preservação da estabilidade, **segurança** [grifo nosso] e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas;
e) a importância da Internet para a promoção do desenvolvimento humano, econômico, social e cultural (BRASIL, 2014a).

O MCI busca regular, de forma técnica e dentro do Direito Civil, o uso e o desenvolvimento da Internet no país, sendo apelidada no ambiente digital como a "Constituição da Internet no Brasil".

De acordo com o CGI.br[78]:

> a iniciativa partiu da percepção de que o processo de expansão do uso da Internet por empresas, governos, organizações da sociedade civil e por um crescente número de pessoas colocou novas questões e desafios relativos à proteção dos direitos civis e políticos dos cidadãos. Nesse contexto, era crucial o estabelecimento de condições mínimas e essenciais não só para que o futuro da Internet seguisse baseado em seu uso livre e aberto, mas que permitissem também a inovação contínua, o desenvolvimento econômico e político e a emergência de uma sociedade culturalmente vibrante.

O MCI afirma que o acesso à rede mundial de computadores é essencial ao exercício da cidadania, bem como aborda a garantia do direito à privacidade e à liberdade de expressão nas comunicações por intermédio da Internet (BRASIL, 2014a).

De acordo com Marques *et al* (2015), a proposta de uma regulação civil para a Internet mobilizou, a partir de meados de 2007, setores da sociedade que defendiam primeiramente uma regulação civil, para que depois a rede fosse tratada criminalmente, no caso, o então projeto de lei nº 84/1999, popularmente conhecido como 'lei Azeredo', que abordava os crimes virtuais. Curiosamente, todo o processo de formulação da lei foi marcado pelo amplo debate público feito, justamente, por meio de processos de consulta pública *online*, via Internet. Para os autores citados:

> o Marco Civil da Internet é um marco jurídico importante para a garantia da liberdade de expressão *online* no Brasil. Entre outros pontos, o texto garante a neutralidade da rede, protege a privacidade na Internet, isenta provedores de responsabilidade por conteúdos gerados por terceiros e ainda visa estimular a inclusão digital.

Em relação ao usuário da Internet, o MCI busca assegurar:

---

[78] Disponível em: <http://www.cgi.br/media/docs/publicacoes/4/CGI-e-o-Marco-Civil.pdf>. Acesso em: 19 out. 2016.

a) inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação;
b) inviolabilidade e sigilo do fluxo de suas comunicações pela Internet e suas comunicações privadas armazenadas;
c) proteção de seus dados pessoais, abrangendo a coleta, o uso, o armazenamento e o tratamento dos mesmos;
d) acesso às medidas e aos procedimentos de segurança e de sigilo implementados pelos provedores de acesso (BRASIL, 2014a).

No que concerne à atuação do Poder Público, o MCI reforça o dever constitucional do Estado na prestação da educação, em particular para o uso seguro, consciente e responsável da Internet, como ferramenta para o exercício da cidadania, a promoção da cultura e o desenvolvimento tecnológico. Nesta conjuntura governamental, ressaltam-se as seguintes diretrizes:

a) estabelecimento de mecanismos de governança multiparticipativa, transparente, colaborativa e democrática, com a participação do governo, do setor empresarial, da sociedade civil e da **comunidade acadêmica** [grifo nosso];
b) promoção da interoperabilidade entre sistemas e terminais diversos, inclusive entre os diferentes âmbitos federativos e diversos setores da sociedade;
c) publicidade e disseminação de dados e informações públicos, de forma aberta e estruturada;
d) otimização da infraestrutura das redes e estímulo à implantação de centros de armazenamento, gerenciamento e disseminação de dados no País [...] (BRASIL, 2014a).

Ao analisar o *Marco Civil da Internet*, Marques *et al* (2015) chamam a atenção para o desenho institucional com relação à governança da Internet no Brasil. De acordo com os autores, há uma multiplicidade de órgãos responsáveis por decidir as políticas e medidas administrativas, sintetizados no quadro 9, o que torna, na prática, complexa a implementação do marco legal.

Quadro 9 - Descentralização da governança da Internet no Brasil

| ÓRGÃOS E INSTITUIÇÕES | RESPONSABILIDADE |
|---|---|
| Agência Nacional de Telecomunicações (Anatel) | Autorização para prestação de serviço por parte dos provedores de acesso à Internet |
| Comitê Gestor da Internet no Brasil (CGI.br)/Registro.br | Administração e registro de domínios <.br> |
| Ministério das Comunicações | Promoção de políticas de inclusão digital do Governo Federal |
| Ministério da Educação | Utilização para fins educacionais |
| Ministério do Desenvolvimento Agrário | Inclusão da população rural |
| Ministério da Integração Nacional | Implantação de ‘Quiosques’ dos cidadãos |
| Ministério da Ciência, Tecnologia e Inovação | Fomento ao desenvolvimento tecnológico |
| Serviço de processamento de dados do governo federal (SERPRO) | Processamento de dados pessoais do cidadão (P.ex.: imposto de renda) |
| Núcleo de Informação e Coordenação do Ponto BR (NIC.br/CGI.br) | Promoção de estudos sobre o uso de Internet no Brasil, incluindo destaque em ações que versem sobre promoção da racionalização da gestão e da expansão |
| Instituto Brasileiro de Geografia e Estatística (IBGE) | Realização de pesquisas econômicas do setor da Tecnologia da Informação e Comunicação |
| Ministério da Justiça | Condução do processo de regulamentação da Lei |

Fonte: adaptado de Marques *et al* (2015)

O Decreto n. 8771, de 11 de maio de 2016, visa regulamentar o MCI em relação às hipóteses admitidas quanto à discriminação de pacotes de dados na internet e de degradação de tráfego, indicar procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, apontar medidas de transparência na requisição de dados cadastrais pela administração pública e estabelecer parâmetros para fiscalização e apuração de infrações. O responsável pela comutação, transmissão ou roteamento deverá adotar medidas de transparência para explicar aos usuários as alterações ocorridas no tráfego de dados contratado. Em relação à proteção, o referido decreto define, como requisitos técnicos indispensáveis, o tratamento de questões de segurança de redes, tais como restrição ao envio de mensagens em massa (*spam*) e controle de ataques de negação de serviço, assim também a previsão de mecanismos de autenticação de acesso aos registros, usando, por exemplo, sistemas de autenticação dupla para assegurar a individualização do responsável pelo tratamento dos registros.

### *5.2.2 Outros Instrumentos norteadores*

#### 5.2.2.1 *Lei de Acesso à Informação*

Uma sociedade bem informada tem melhores condições de acompanhar e reivindicar seus direitos mais básicos como: saúde, educação, segurança, entre outros. Por isso, o acesso à informação confiada e produzida pelo Estado é mais que um direito do cidadão. A *Constituição da República Federativa do Brasil* de 1988 (CF/88), no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216, regulamenta o direito ao acesso à informação pela sociedade brasileira, direito esse respeitado em vários países (MARQUES; VIANNA, 2013).

Com o objetivo de regular o disposto na CF/88, foi sancionada a Lei n. 12.527, de 18 de novembro de 2011, conhecida como *Lei de Acesso à Informação* (LAI).

A LAI estabeleceu que o Estado brasileiro oferecesse acesso rápido e fácil às informações que estão sob sua guarda e que essas informações devessem ser apresentadas de forma clara, objetiva e de fácil entendimento, empregando, sempre que possível, as Tecnologias de Informação e Comunicação, no caso utilizadas como sinônimo de TI. A implantação da LAI e suas consequências de uma maior transparência nas informações são sentidas, de forma concreta, no combate à corrupção e na busca por melhores serviços públicos (VIANNA; FERNANDES, 2015).

De acordo com a LAI, o acesso à informação é a regra, o sigilo é a exceção, ou seja, todas as informações produzidas ou custodiadas pelo poder público e não classificadas como sigilosas são públicas e, portanto, acessíveis a todos os cidadãos, estabelecendo ainda como padrões: o requerente não precisa dizer nem por quê e nem para que deseja a informação, fornecimento gratuito, salvo custo de reprodução e criação de procedimentos e prazos que facilitem o acesso.

Não obstante, de acordo com o artigo 23 da citada lei, são passíveis de classificação sigilosa as informações que podem:

a) pôr em risco a defesa e a soberania nacionais ou a integridade do território nacional;
b) prejudicar ou pôr em risco a condução de negociações ou as relações internacionais do país, ou as que tenham sido fornecidas em caráter sigiloso por outros Estados e organismos internacionais;
c) pôr em risco a vida, a segurança ou a saúde da população;
d) oferecer elevado risco à estabilidade financeira, econômica ou monetária do país;
e) prejudicar ou causar risco a planos ou operações estratégicas das Forças Armadas;
f) prejudicar ou causar risco a projetos de pesquisa e desenvolvimento científico ou tecnológico, assim como a sistemas, bens, instalações ou áreas de interesse estratégico nacional;
g) pôr em risco a segurança de instituições ou de altas autoridades nacionais ou estrangeiras e seus familiares;
h) comprometer atividades de inteligência, bem como as de investigação ou fiscalização em andamento, relacionadas com a prevenção ou repressão de infrações (BRASIL, 2011a).

De acordo com Dirlene Barros e Georgete Rodrigues (2016, p. 16-17), no quesito da 'transparência passiva', a LAI está impossibilitada de ser cumprida em sua totalidade, em função da elevada quantidade dos acervos em estado precários e mal gestados, particularmente nos Estados e Municípios. As autoras entendem que:

> o engajamento do AN poderia ser mais intenso, como, por exemplo, pelo desenvolvimento do monitoramento da LAI, o que convergiria na construção de uma política arquivística, de forma a incidir, diretamente, no primeiro problema de implantação da LAI, a gestão documental.

### 5.2.2.2 Política Nacional de Dados Abertos

A LAI teve papel precursor nas iniciativas de dados abertos do governo executivo. De acordo com o Portal Brasileiro de Dados Abertos[79]:

> dados são abertos quando qualquer pessoa pode livremente acessá-los, utilizá-los, modificá-los e compartilhá-los para qualquer finalidade, estando sujeito a, no máximo, a exigências que visem preservar sua proveniência e sua abertura.

Ainda, segundo o Portal, três leis foram propostas para os dados abertos governamentais, mas que podem ser aplicadas aos mesmos de forma geral: (i) se o dado não pode ser encontrado e indexado na Web, ele não existe, (ii) se não estiver aberto e disponível em formato compreensível por máquina, ele não pode ser reaproveitado e (iii) se algum dispositivo legal não permitir sua replicação, ele não é útil. Como princípios basilares para a abertura de dados governamentais, têm-se os seguintes:

a) completos - todos os dados públicos são disponibilizados. Dados são informações eletronicamente gravadas, incluindo, mas não se limitando a documentos, bancos de dados, transcrições e gravações audiovisuais. Dados públicos são aqueles que não estão sujeitos a limitações válidas de privacidade, segurança ou controle de acesso, reguladas por estatutos;
b) primários - os dados são publicados na forma coletada na fonte, com a mais fina granularidade possível, e não de forma agregada ou transformada;
c) atuais - os dados são disponibilizados o quão rapidamente seja necessário para preservar o seu valor;
d) acessíveis - os dados são disponibilizados para o público o mais amplo possível e para os propósitos os mais variados possíveis;
e) processáveis por máquina - os dados são razoavelmente estruturados para possibilitar o seu processamento automatizado;
f) acesso não discriminatório - os dados estão disponíveis a todos, sem que seja necessária a respectiva identificação ou registro;
g) formatos não proprietários - os dados estão disponíveis em um formato sobre o qual nenhum ente tenha controle exclusivo;

---

[79] Disponível em: <http://dados.gov.br/pagina/sobre>. Acesso em: 19 set. 2018.

h) livres de licenças - os dados não estão sujeitos a regulações de direitos autorais, marcas, patentes ou segredo industrial. Restrições razoáveis de privacidade, segurança e controle de acesso podem ser permitidas na forma regulada por estatutos.

No entendimento do Tribunal e Contas da União[80]:

> a abertura de dados relacionados a políticas públicas permite avalição de desempenho da respectiva área, seja de forma direta (porque se espera a divulgação de índices de desempenho), ou indireta (por serem subsídio para compor quadro de análise). Esses mesmos dados possibilitam o uso por empresas, organizações não governamentais, pesquisadores e demais interessados, que poderão criar as próprias visualizações e aplicativos, algo em que as organizações governamentais podem não ter recursos necessários ou interesse para desenvolver.

Em maio de 2014, o Ministério do Planejamento Orçamento e Gestão (MPOG) publicou o *Plano de Dados Abertos* (PDA). O PDA foi o documento orientador para as ações de implementação e promoção de abertura de dados, inclusive geoespacializados, obedecendo a padrões mínimos de qualidade, de forma a facilitar o entendimento e a reutilização das informações, organizando o planejamento referente à implantação e à racionalização dos processos de publicação de dados abertos nas organizações públicas[81].

O Decreto n. 8777, publicado no mês de maio de 2016, estabeleceu regras para disponibilização de dados abertos no âmbito do Poder Executivo Federal, por meio da *Política Nacional de Dados Abertos* (PNDA). De acordo com o Ministério da Transparência, Fiscalização e Controladoria-Geral da União (CGU) [82], a PNDA visa contribuir para o aumento da transparência do governo, criando melhores possibilidades de: controle social das ações governamentais, combate à corrupção, controle dos gastos públicos e da qualidade do gasto, assim como obtenção de informações para monitorar e avaliar as políticas públicas. Quanto à gestão da Política, o órgão responsável pela coordenação das ações será o Ministério do Planejamento, Desenvolvimento e

---

80 Dados abertos na Administração Pública Federal. Disponível em: <http://portal.tcu.gov.br/lumis/portal/file/fileDownload.jsp?inline=1&fileId=8A8182A14E1CA3E4014E1CFD9C525B33>. Acesso em: 19 out. 2016.

81 Disponível em: <http://www.planejamento.gov.br/tema/governo-aberto/plano-de-dados-abertos-pda#plano_acao>. Acesso em: 28 maio 2017.

82 Disponível em: <http://www.governoaberto.cgu.gov.br/noticias/2016/copy_of_disponivel-2a-fase-da-consulta-publica-do-decreto-do-202a200emarco-civil202c-da-internet>. Acesso em: 28 maio 2017.

Gestão, por meio da Infraestrutura Nacional de Dados Abertos – INDA. Os principais objetivos de tal Política são:

a) promover a publicação de dados contidos em bases de dados de órgãos e entidades da administração pública federal direta, autárquica e fundacional sob a forma de dados abertos;
b) aprimorar a cultura de transparência pública;
c) franquear aos cidadãos o acesso, de forma aberta, aos dados produzidos ou acumulados pelo Poder Executivo federal, sobre os quais não recaia vedação expressa de acesso;
d) fomentar o controle social e o desenvolvimento de novas tecnologias destinadas à construção de ambiente de gestão pública participativa e democrática, bem como à melhor oferta de serviços públicos para o cidadão.

A implementação da Política de Dados Abertos ainda não se mostra efetiva, pois carece da execução do Plano de Dados Abertos (PDA), no âmbito de cada órgão ou entidade da administração pública federal, direta, autárquica e fundacional, bem como da plena inserção dos PDA na Infraestrutura Nacional de Dados Abertos (INDA).

#### 5.2.2.3 Privacidade e Proteção de Dados

Em agosto de 2018, foi sancionada a Lei n. 13.709 sobre a proteção de dados pessoais (LGPDP), alterando o *Marco Civil da Internet*, como também complementando a *Lei de Acesso à Informação*. A LGPDP dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade, assim como o livre desenvolvimento da personalidade da pessoa natural, possuindo por fundamentos:

a) o respeito à privacidade;
b) a autodeterminação informativa;
c) a liberdade de expressão, de informação, de comunicação e de opinião;
d) a inviolabilidade da intimidade, da honra e da imagem;
e) o desenvolvimento econômico e tecnológico e a inovação;

f) a livre iniciativa, a livre concorrência e a defesa do consumidor;

g) os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais (BRASIL, 2018c).

Dessa forma, toda pessoa natural tem assegurada a titularidade de seus dados pessoais (informação relacionada à pessoa natural identificada ou identificável) e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade. A LGPDP dá especial atenção ao tratamento de dados considerados como:

> toda operação realizada com dados pessoais, como as que se referem à coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração (BRASIL, 2018c).

Dentre os princípios do tratamento de dados pessoais, destacam-se, entre outros: (i) o livre acesso, a transparência, **a segurança** e a responsabilização. Nestes aspectos, a LGPDP alerta que os sistemas de informações utilizados para o tratamento de dados pessoais devem ser estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança, de tal maneira que o formato do dado armazenado favoreça o exercício do direito de acesso.

Em síntese, a LGPDP é aplicada a serviços digitais ou não, tanto públicos quanto privados, valendo para toda a organização brasileira ou estrangeira que coleta dados em território nacional. Não obstante, a LGPDP não se aplica para: fins particulares ou não econômicos, ou com finalidade artística, jornalística ou acadêmica, bem como para o caso de tratamento de informação que visa à segurança pública, defesa nacional, segurança do Estado ou investigações criminais.

### 5.2.2.4 Estratégia de Governança Digital

O reconhecimento da importância do Setor Cibernético nacional ratificou-se, também, na publicação, no início de 2016, do Decreto n. 8638, de 15 de janeiro, instituindo a *Política de Governança Digital*[83], no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional (APF). Em relação à referida Política, destacam-se os seguintes princípios e diretrizes:

a) priorização de serviços públicos disponibilizados em meio digital - sempre que possível, os serviços públicos serão oferecidos em meios [ambientes] digitais, sendo disponibilizados para o maior número possível de dispositivos e plataformas;

b) governo como plataforma - o governo deve constituir-se como uma plataforma aberta, sobre a qual os diversos atores sociais possam construir suas aplicações tecnológicas para a prestação de serviços e o desenvolvimento social e econômico do país, permitindo a expansão e a inovação;

c) autosserviço[84] como a forma prioritária de prestação de serviços públicos disponibilizados;

d) os dados serão disponibilizados em formato aberto, amplamente acessível e utilizável por pessoas e máquinas, **assegurados os direitos à segurança e à privacidade** [grifo nosso].

Ainda, em âmbito do poder executivo federal, a Portaria n. 68, de 7 de março de 2016, do Ministério do Planejamento, Orçamento e Gestão (MPOG) aprovou a *Estratégia de Governança Digital da Administração Pública Federal* (EGD), para o período de 2016-2019, que estabelece os objetivos estratégicos, metas e indicadores para a tecnologia da informação dar suporte às atividades-fim dos órgãos da APF, de acordo com o estabelecido pela Política de Governança Digital, publicada em janeiro de 2016. A EGD busca a ampliação das ferramentas e a disseminação do governo

---

[83] Governança Digital – a utilização pelo setor público de recursos de tecnologia da informação e comunicação com o objetivo de melhorar a disponibilização de informação e a prestação de serviços públicos, incentivar a participação da sociedade no processo de tomada de decisão e aprimorar os níveis de responsabilidade, transparência e efetividade do governo (BRASIL, 2016a).

[84] Serviço público disponibilizado em meio digital que pode ser utilizado pelo próprio cidadão, sem auxílio do órgão ou da entidade ofertante do serviço (BRASIL, 2016a).

eletrônico, na construção de canais de prestação de serviços 100% digitais, possuindo como propósito basilar:

> orientar e integrar as iniciativas relativas à governança digital na administração direta, autárquica e fundacional do Poder Executivo Federal, contribuindo para aumentar a efetividade da geração de benefícios para a sociedade brasileira por meio da expansão do acesso às informações governamentais, da melhoria dos serviços públicos digitais e da ampliação da participação social (BRASIL, 2016b, p. 7).

Aderente ao contexto da denominada era digital, a EGD busca inovar-se ao adotar as seguintes definições: (i) serviços públicos digitais - conjunto de ações do Estado que envolvem interação em meios digitais com a sociedade para atendimento direto às suas necessidades, visando ao alcance de direitos ou possibilitando o cumprimento de um dever; e (ii) tecnologias digitais - referem-se às TIC, incluindo a Internet, tecnologias e dispositivos móveis, desenvolvimento de serviços e de aplicações e análise de dados, utilizados para melhorar a geração, coleta, troca, agregação, combinação, análise, acesso, busca e apresentação de conteúdo digital. A EGD possui três eixos de atuação: acesso à informação, prestação de serviços e participação social, bem como uma gama de princípios sintetizados na figura 13.

Figura 13 - Diagrama da Estratégia de Governança Digital


Fonte: Brasil (2018d, p. 96) E-Digital

De acordo com a *Estratégia de Governança Digital*, o *e-Gov* passa a se enquadrar na definição de governança digital:

> utilização, pelo setor público, de tecnologias da informação e comunicação com o objetivo de melhorar a informação e a prestação de serviços, incentivando a participação dos cidadãos no processo de tomada de decisão e tornando o governo mais responsável, transparente e eficaz (BRASIL, 2016b, p. 7).

Ainda, no âmbito da EGD, dentre os aspectos que motivam o governo digital destacam-se [85]:

a) demanda social – em que se observa a pressão da sociedade incluída, aliada à experiência preliminar com serviços privados e redes sociais e baixa tolerância para a "jornada da papelada", especialmente por jovens;

b) economia - transações *online* tendem a ser muito mais econômicas e ágeis para o Estado e para o cidadão (pessoa física ou jurídica), com melhor aproveitamento de recursos humanos, bem como potencial redução de custos em aluguel de locais para armazenamento de documentos e papéis;

c) integração e convergência - menor fragmentação do governo para o cidadão em suas interfaces de interação, com entrada e autenticação do mesmo para a solicitação de informações uma única vez;

d) segurança e privacidade - proteção de dados pessoais;

e) transparência e controle social - acompanhamento do atendimento, buscando-se a satisfação do cidadão;

f) qualidade de serviços - padronização de atendimento, a fim de ampliar a confiança no governo.

Quanto à interação com a presente pesquisa, os temas segurança e privacidade enquadram-se entre os nove princípios orientadores da EGD: "os serviços públicos digitais devem propiciar disponibilidade, integridade, confidencialidade e autenticidade dos dados e informações, além de proteger o sigilo e a privacidade pessoais dos cidadãos na forma da legislação". Tanto segurança como privacidade consolidam-se no Objetivo Estratégico 03 da EGD: "Garantir a disponibilidade, integridade, confidencialidade e autenticidade dos ativos de informação custodiados pelo Estado, bem

---

[85] Disponível em: <http://www.planejamento.gov.br/apresentacoes/2016/apresentacao-ministro-seminario-100-pc-digital.pdf>. Acesso em: 19 nov. 2016.

como a proteção da informação pessoal e da propriedade intelectual" (BRASIL, 2018d, p. 28-29). Tal objetivo desdobra-se em 14 Iniciativas Estratégicas, onde se destacam:

a) contribuir para o aumento da capacidade de resiliência[86] dos ativos de informação e das infraestruturas críticas;
b) implantar e fortalecer as equipes de tratamento de incidentes de segurança nas redes de computadores do Estado;
c) desenvolver uma política nacional de Segurança da Informação e Comunicação[87] (SIC) e de Segurança Cibernética (SegCiber);
d) estabelecer mecanismos mais eficazes para viabilizar a efetiva classificação da informação nos órgãos da APF;
e) promover a cooperação nacional e internacional com setor produtivo e acadêmico, visando à troca de experiências e ao fortalecimento dos temas de SIC e de SegCiber;
f) ampliar e fortalecer as ações de sensibilização e capacitação dos servidores (técnicos e membros da alta administração) em SIC;
g) melhorar a taxonomia da área de SIC, inclusive com definições de limites relacionados ao uso de dados da sociedade por parte do Estado, à privacidade e ao sigilo das informações do cidadão (BRASIL, 2016b, p. 29).

#### 5.2.2.5 Estratégia Brasileira para a Transformação Digital

A dimensão do desafio nacional, no que tange ao espaço cibernético, pode ser caracterizada no capítulo introdutório da *Estratégia Brasileira para a Transformação Digital* (E-Digital), como:

> as tecnologias digitais estão cada vez mais presentes na vida de todos: em casa, no trabalho, nas escolas, nos meios de comunicação e nas relações

[86] No caso de um incidente de segurança cibernético, seria a capacidade de continuar operando mesmo na presença de falhas ou ataques. Para tanto, torna-se fundamental identificar o que é crítico e o nível de uso aceitável. Informações adicionais disponíveis em: <https://www.symantec.com/content/en/us/enterprise/white_papers/b-cyber-resilience-blueprint-wp-0814.pdf>. Acesso em: 29 jan. 2017. No caso das IC, seria a "capacidade de as infraestruturas críticas serem recuperadas após a ocorrência de situação adversa" (BRASIL, 2018a).

[87] Na opinião do autor, a adição do termo comunicações, na prática, em nada se desalinha da Segurança da Informação praticada no âmbito da CI.

> sociais. Para que o Brasil possa tirar pleno proveito da revolução digital, colhendo todos os benefícios que a sociedade da informação e do conhecimento tem a oferecer, a economia nacional deve se transformar, com dinamismo, competitividade e inclusão, absorvendo a digitalização em seus processos, valores e conhecimento (BRASIL, 2018d).

A E-Digital compõe o Sistema Nacional para a Transformação Digital (SinDigital), sendo instituída pelo Decreto n. 9.319, de 21 de março de 2018 (BRASIL, 2018d). A Estratégia visa à harmonização das iniciativas do Poder Executivo federal ligadas ao ambiente digital, com o objetivo de aproveitar o potencial das tecnologias digitais para promover o desenvolvimento econômico e social sustentável e inclusivo, com inovação, aumento de competitividade, de produtividade e dos níveis de emprego e renda no País.

A E-Digital baseia-se nas seguintes diretrizes: (i) engajamento permanente com a comunidade científica, o setor produtivo e a sociedade civil e (ii) fortalecimento da articulação e da cooperação entre os diferentes órgãos e entidades do Poder Público com competências relacionadas à temática digital, sendo estruturada em dois grandes grupos de eixos temáticos: eixos habilitadores e eixos de transformação digital. Os eixos habilitadores visam criar um ambiente propício para o desenvolvimento da transformação digital da economia brasileira, com iniciativas essenciais para alavancar a digitalização, incluindo:

a) infraestrutura e acesso às tecnologias de informação e comunicação - objetiva promover a ampliação do acesso da população à Internet e às tecnologias digitais, com qualidade de serviço e economicidade;
b) pesquisa, desenvolvimento e inovação - objetiva estimular o desenvolvimento de novas tecnologias, com a ampliação da produção científica e tecnológica, e buscar soluções para desafios nacionais;
c) confiança no ambiente digital - objetiva assegurar que o ambiente digital seja seguro, confiável, propício aos serviços e ao consumo, com respeito aos direitos dos cidadãos;
d) educação e capacitação profissional - objetiva promover a formação da sociedade para o mundo digital, com novos conhecimentos e tecnologias avançadas, e prepará-la para o trabalho do futuro;
e) dimensão internacional - objetiva fortalecer a liderança brasileira nos fóruns globais relativos a temas digitais, estimular a competitividade e a presença

das empresas brasileiras no exterior, assim como promover a integração regional em economia digital.

Em relação ao eixo temático habilitador de maior relevância para este trabalho, nomeadamente 'Confiança no ambiente digital', destaca-se que a ação governamental deve estar focada em duas áreas: (i) proteção de direitos e privacidade e (ii) defesa e segurança no ambiente digital. Os objetivos a serem alcançados incluem aprimorar os mecanismos de proteção de direitos no meio digital e fortalecer a segurança cibernética no País, com as decorrentes ações estratégicas:

a) editar uma política nacional de segurança cibernética, incluindo a definição de uma instância nacional responsável pela articulação de um sistema nacional de segurança cibernética, envolvendo os setores público e privado;
b) consolidar o marco legal de segurança cibernética, harmonizando as disposições de direito penal e processual já existentes na legislação brasileira e avançando na previsão de novos instrumentos de investigação para o mundo digital;
c) elaborar planos nacional e subnacionais de prevenção, resposta a incidentes e mitigação de ameaças cibernéticas, inclusive no âmbito de infraestruturas críticas;
d) estabelecer mecanismos de cooperação entre entes governamentais, entes federados e setor privado com vista à adoção de melhores práticas, compartilhamento de informações, adoção de padrões adequados de segurança, coordenação de resposta a incidentes e proteção da infraestrutura crítica;
e) treinar agentes públicos em segurança e mitigação de riscos cibernéticos e desenvolver parcerias para o treinamento de recursos humanos do setor privado;
f) realizar campanhas educacionais amplas para expandir a conscientização da população sobre o tema da segurança da informação;
g) formar recursos humanos especializados e investir em pesquisa e desenvolvimento na área de defesa e segurança cibernética, com vista a promover a autonomia tecnológica nacional em termos de competências e produtos;

h) reforçar instrumentos de cooperação internacional entre autoridades e entre provedores de acesso e conteúdo atuantes em diferentes países, de maneira a garantir a aplicação da lei no ambiente digital, especialmente nos casos em que o caráter transnacional dos crimes e ameaças cibernéticos força o envolvimento de mais de uma jurisdição (BRASIL, 2018d, p. 43-44)

Além disso, no contexto da Ciber Proteção, destaca-se uma ação estratégica do eixo temático Pesquisa, Desenvolvimento e Inovação, que prioriza áreas onde o investimento em Desenvolvimento Experimental e Inovação em TIC poderá trazer ganhos de competitividade ao País. No caso, trata-se da Segurança e defesa com o desenvolvimento de plataformas que garantam a interoperabilidade e a coordenação entre os sistemas de comando e controle das três forças de Defesa nacional, utilizando, em particular, ferramentas de radiocomunicação; bem como investimentos no desenvolvimento, por empresas nacionais, de protocolos de comunicação, criptografia e equipamentos de segurança. Destaca-se, também, uma estratégia do eixo Educação e Capacitação Profissional que almeja promover maior interação entre o setor privado e as instituições de ensino (universidades, institutos de pesquisa e de capacitação profissional e técnica), a fim de incorporar as demandas e necessidades das empresas digitais do futuro, aplicando conceitos como *lifelong learning* e educação vocacional.

As ações específicas em prol do segundo grande eixo - Transformação Digital, tanto no governo quanto no setor produtivo, foram assim agrupadas: (i) transformação digital da economia - objetiva estimular a informatização, o dinamismo, a produtividade e a competitividade da economia brasileira, de forma a acompanhar a economia mundial; e (ii) cidadania e transformação digital do Governo - tornar o Governo federal mais acessível à população e mais eficiente em prover serviços ao cidadão, em consonância com a Estratégia de Governança Digital. Dentre os objetivos da transformação digital, no contexto da proteção cibernética, requerem especial atenção aqueles que se propõem a:

a) promover um ambiente jurídico-regulatório que estimule investimentos e inovação, a fim de conferir segurança aos dados tratados e adequada proteção aos dados pessoais;

b) reconhecer o potencial transformador das aplicações da Internet das Coisas, devendo ser estabelecidos ações e incentivos destinados à contínua evolução e disseminação dos dispositivos e das tecnologias digitais associadas;
c) conceder amplo acesso à informação e a dados abertos governamentais, que possibilitem o exercício da cidadania e a inovação em tecnologias digitais;
d) adotar tecnologia de processos e serviços governamentais em nuvem, como parte da estrutura tecnológica dos diversos serviços e setores da administração pública;
e) apoiar a formação e a capacitação profissional em habilidades necessárias para o desenvolvimento e a utilização das novas tecnologias digitais relacionadas aos dispositivos conectados.

Dentre as ações estratégicas do Eixo supracitado, destacam-se: implementar um sistema de autenticação única ao cidadão, agregando os principais níveis de segurança em uma única ferramenta; promover o aumento da interação entre centros públicos de pesquisa e empresas, e a articulação entre as infraestruturas de pesquisa nacionais e linhas de fomento voltadas ao desenvolvimento de dispositivos conectados; e avaliar os potenciais impactos sociais e econômicos [proteção] de tecnologias digitais disruptivas, como Inteligência Artificial e *Big Data*.

O próximo capítulo apresenta entendimentos sobre a informação em meio digital e a sua gestão, tendo como viés a segurança da informação. Estes entendimentos, juntamente com a preservação digital e as TIC, são peças basilares na construção do conceito desenvolvido de Ciber Proteção.

# 6 O AMBIENTE INFORMACIONAL

Uma das características do termo informação é a polissemia. Segundo Capurro e Hjorland (2007), quase toda a disciplina científica usa o conceito de informação dentro de seu próprio contexto/situação e com relação a fenômenos específicos. Em consequência, diferentes conceitos de informação dentro da Ciência da Informação refletem tensões entre uma abordagem subjetiva e outra objetiva[88].

Neste sentido, os referidos autores (2007, p. 153 e 164) declaram: “propomos que as definições científicas de termos como informação dependem das funções que damos a elas em nossas teorias”, de modo que a questão “o que é informação? não pode ser feita sem referência a uma situação".

No caso do presente estudo, o referido “contexto/situação” contempla as transformações em curso na Era da Informação, particularmente a sociedade em rede e o ciberespaço, assuntos que se encontram no cerne desta tese e que foram aprofundados em seções anteriores.

## 6.1 A INFORMAÇÃO NO MEIO DIGITAL

Optou-se pela abordagem objetiva da informação, alinhada, principalmente, às seguintes categorizações: (i) informação como um recurso de Sandra Braman (1989, 2006, 2014)[89] e (ii) Informação-como-coisa de Michael K. Buckland (1991)[90]. Resgata-se, também, o ponto de vista etimológico latino da palavra informação: *informatio* – ação de formar, forma, modelar, esboço. Assim, estruturas informacionais externas ao indivíduo (objetos físicos) afetam, objetivamente, o ambiente individual e social ao compartilhar informação.

---

[88] Informação objetiva seria aquela disponível coletivamente em sistemas informatizados, enquanto a informação subjetiva seria assimilada individualmente (análise e síntese individual), aproximando-se do “conhecimento”.

[89] A autora delineia seis categorias/definições para informação: (i) como um recurso, (ii) como uma mercadoria, (iii) como uma percepção de padrão, (iv) como uma força social constitutiva, (v) como um agente, e (vi) como um recipiente de possibilidade.

[90] O autor identifica três principais usos da palavra “informação”: (i) Informação-como-processo, (ii) informação-como-conhecimento, e (iii) informação-como-coisa.

Para Braman, a informação como recurso favorece o reconhecimento da natureza finalística dos sistemas de informação, enfatizando-se os usos que as pessoas (físicas ou jurídicas) fazem da mesma, em vez de seus efeitos sobre os indivíduos e a sociedade. Na visão da autora, a informação é um recurso quando seus criadores, processadores e usuários, são vistos como entidades distintas e isoladas, bem como quando é percebida como algo que a referida entidade deve possuir para o seu funcionamento. Assim, a informação como recurso torna-se insumo para a tomada de decisão, como componente do processo produtivo, e favorece a articulação de leis e regulamentos específicos.

Não obstante, convém listar algumas das propriedades da informação segundo Armando Malheiro:

a) estruturação pela ação (humana e social) – o ato individual e/ou coletivo funda e modela estruturalmente a informação;
b) integração dinâmica – o ato informacional está implicado ou resulta sempre tanto das condições e circunstâncias internas, como das externas do sujeito da ação;
c) pregnância – enunciação (máxima ou mínima) do sentido ativo, ou seja, da ação fundadora e modeladora da informação;
d) quantificação – a codificação linguística, numérica, figurativa é valorável [sic] ou mensurável quantitativamente;
e) reprodutividade – a informação é reprodutível sem limites, possibilitando a subsequente retenção/memorização;
f) transmissibilidade – a (re) produção informacional é potencialmente transmissível ou comunicável (SILVA, 2006, p. 25).

No entendimento de Buckland, o uso da informação-como-coisa representaria a informação-como-conhecimento; onde o termo "informação" é atribuído para objetos tangíveis, como dados e documentos, sendo, os mesmos considerados pela sua capacidade de informar, ou seja, possuem condições de comunicar e partilhar a informação.

Considera-se, então, apenas o lado objetivo da análise de Braman e Buckland, ou seja, a informação como um elemento tangível (recurso/coisa), endossada pela percepção de Capurro e Hjorland:

> a distinção mais importante [em relação aos conceitos de informação] é aquela entre informação como objeto ou coisa (por exemplo, número de ***bits*** [grifo nosso]) e informação como um conceito subjetivo, informação como signo; isto é, como dependente da interpretação de um agente cognitivo (CAPURRO; HJORLAND, 2007, p. 193).

Gleick (2013) recorda que, em 1948, Claude Shannon utilizou o neologismo “bit” (versão mais curta de dígitos binários sugerida por J. W. Tukey) na sua monografia: “Uma teoria matemática da Comunicação”. Assim, o *bit* juntou-se à polegada e ao minuto como uma quantidade determinada, tornando-se uma unidade fundamental de medida. Ou seja, no entendimento de Shannon, o *bit* seria “uma unidade de medida da informação”, como se a mesma fosse mensurável e quantificável. Na opinião de Gleick, a Teoria da Informação de Shannon construiu uma ponte entre a informação e os computadores, bem como com o ciberespaço, propiciando o processamento de informações, junto com o armazenamento e o acesso às mesmas.

Contemporaneamente, o Arquivo Nacional da Austrália (AUSTRÁLIA, 2016), em seu Glossário, exemplificou informação como: “uma sequência de *bits* (os dados) acompanhada de uma descrição de como interpretar uma sequência de *bits*, como números que representam as observações de temperatura medidas em graus Celsius (a informação representada)”[91]. O NAA considera a informação como qualquer tipo de conhecimento que possa ser trocado, sendo que, nesse intercâmbio, a mesma é representada por dados.

O progresso na tecnologia da informação aumenta as possibilidades de criação e utilização de informação como um ativo tangível. Grande parte da informação em sistemas de informação[92] deve ser processada, estruturada e registrada por ser codificável e transformável, bem como devidamente modelada e organizada, a fim de prover conteúdo estável e seguro.

Para Buckland (1991), informação-como-coisa é a única forma de informação com que os sistemas de informação se relacionam diretamente, podendo, inclusive, ser falsificada, alterada, escondida ou destruída. No caso desta pesquisa, considera-

---

[91] *A string of bits (the data) accompanied by a description of how to interpret a string of bits as numbers representing temperature observations measured in degrees Celsius (the representation information*) (AUSTRÁLIA, 2016).

[92] A informação pode ser identificada, descrita e representada em sistemas de informação para diferentes domínios de conhecimento (CAPURRO; HJORLAND, 2007, p. 192).

se que, nos sistemas de informação automatizados, dígitos binários (*bits*) representam a forma física dos objetos informativos[93].

A fim de se ampliar o entendimento de qual "tipo de informação" trata esta pesquisa, documentos, recursos, objetos (entre outras caracterizações da informação considerada) não são estudados apenas sintaticamente como códigos binários passíveis de quantificação que geram símbolos/signos/sinais como, por exemplo, letras, números, caracteres matemáticos etc. Possuem os mesmos uma semântica própria, com significado para o 'receptor', representando 'coisas' do mundo, pensamentos do homem, devendo ser preservados por um determinado período histórico.

Em relação às características da informação organizacional, Choo (2006) afirma que as organizações podem ser encaradas como sistemas interpretadores das informações ambientais e/ou como complexos sistemas processadores de informação. Dessa forma, as organizações processam a informação para diminuir a incerteza e a ambiguidade, usando-a em três arenas básicas: na criação de significados para o entendimento do seu ambiente, na construção de conhecimentos, para suprir suas lacunas de conhecimento e desenvolver novas competências, e na tomada de decisões para escolher formas de ação.

Dentro desse entendimento, as informações necessitam de proteção própria, particularmente considerando-se o ciberespaço. Assim, seguem-se as atividades maliciosas mais usuais que podem incidir sobre um sistema de informação (SI), a saber:

a) interrupção indesejada dos serviços prestados pelo SI - ação deliberada que causa indisponibilidade no acesso às informações[94];

b) uso não autorizado de informação sigilosa - ação que atinge diretamente a confidencialidade e a privacidade das informações disponibilizadas;

c) furto de informação sigilosa ou ostensiva - ação criminosa que torna a informação indisponível, mesmo que temporariamente;

---

[93] Em consonância, também, com o proposto pelo físico alemão Rolf Landauer, que dedicou sua carreira ao estabelecimento das bases físicas da Informação. Landauer afirmou: "A informação é inevitavelmente física", tendo em vista que a computação exige objetos físicos e obedece às leis da Física, bem como não poderia existir sem "algum tipo" de encarnação (GLEICK, 2013, p. 370).

[94] Incluindo-se também a inserção prévia de códigos maliciosos pelos próprios fabricantes de *hardware* e *software*.

d) extorsão / sequestro da informação - tipo de ação em expansão, conhecido como *ransomware*[95], em que artefatos maliciosos, enviados em grande parte por *e-mails* de *phishing*, sequestram o ingresso a computadores e arquivos, cobrando pagamento para a liberação do acesso à informação sequestrada;

e) modificações nas propriedades e atributos da informação - ação intencional ou não, que altera os dados de identificação como autoria, data de criação, formato, classificação etc.;

f) adulteração da informação disponibilizada - ação que compromete diretamente a integridade, a autenticidade e a credibilidade da informação, ocasionando prejuízos aos usuários e responsáveis pelos SI.

Os questionamentos supracitados, relacionados ao 'uso' da informação, remetem, inquestionavelmente, à assimetria e à complementariedade presentes no relacionamento entre informação e comunicação.

Apesar de não serem objeto deste estudo, os fluxos informacionais conduzem inexoravelmente ao âmago da CI e fazem aflorar, naturalmente, a sua natureza interdisciplinar, trazendo novas motivações e necessidades no que se refere ao aperfeiçoamento da organização, tratamento, disponibilização e uso da informação, bem como à monitoração e à segurança dos fluxos e dos processos inerentes aos sistemas informacionais.

Em relação aos denominados fluxos de informação, convém, preliminarmente, recordarem-se os dois sentidos do conceito Informação, na visão de Anthony Wilden, que reforçam o entendimento do mesmo nesta pesquisa:

> o primeiro estritamente técnico ou tecnológico: informação como quantidade mensurável em bit (*binary digit*) [...]. O segundo sentido pertence a uma abordagem diversa [...] sempre qualitativo antes de ser quantitativo [...]. A informação apresenta-nos em estruturas, formas, modelos, figuras e configurações; em ideias e ídolos; em índices, imagens e ícones; no comércio e na mercadoria; em continuidade e descontinuidade; em sinais, signos, significantes e símbolos; em gestos, posições e conteúdos; em frequências, entonações, ritmos e inflexões; em presenças e ausências; em palavras, em acções [sic] e em silêncio; em visões e em silogismos. É a organização a própria variedade (WILDEN *apud* SILVA, 2006, p. 53).

---

[95] *Ransomware* é um tipo de código malicioso que torna inacessíveis os dados armazenados em um equipamento, geralmente usando criptografia, e que exige pagamento de resgate (*ransom*) para restabelecer o acesso ao usuário (CERT.br, 2016).

Considera-se, de igual forma, a célebre definição de Ciência da Informação de Harold Borko: “disciplina que investiga as propriedades e comportamento da informação e as forças que regem o **fluxo informacional** [grifo nosso] e os meios de processamento da informação, otimização do acesso e uso [...]” (BORKO, 1968, p. 3).

Na análise de Armando Malheiro, a própria CI é derivada e relacionada a vários campos como: a matemática, a lógica, a linguística, a psicologia, a tecnologia computacional, as operações de pesquisa, as artes gráficas, as comunicações, a biblioteconomia, a gestão e outros campos similares”. Remete, também, ao fenômeno infocomunicacional[96] (informação + comunicação) que contempla três eixos cruciais: (i) a produção da informação dos mais diversos tipos e em quaisquer suportes, (ii) a recepção/uso de informação dos mais diversos tipos e em quaisquer contextos e (iii) a ocorrência ou não de condições efetivas de interação/comunicação. Ainda, segundo o autor, ao se estudar o comportamento humano em face do fenômeno e do processo infocomunicacional, geralmente, depara-se com as seguintes questões: “Como se fornece, ‘sem ruído’ a informação para quem dela precisa? Como se geram as necessidades de quem a busca? Como se satisfaz, sem condicionar à partida, o ‘manancial’ desconhecido do utilizador (e desconhecido até para o próprio) das suas necessidades concretas de informação? (SILVA, 2006, p. 105, 140 e 246).

Quanto aos fluxos de informação e de comunicação, Manuel Castells, no contexto da sociedade em rede, esclarece o seguinte:

> as mudanças radicais no domínio da comunicação, motivadas pela revolução nas tecnologias da informação, agravam o sentimento de desorientação. A transição dos *mass media* tradicionais para um sistema de redes de comunicação horizontal, organizado em torno da Internet e da comunicação sem fios, introduziu uma multiplicidade de padrões de comunicações que estão na origem de uma transformação cultural fundamental à medida que a virtualidade se torna uma dimensão essencial a nossa realidade. [...] [constituindo] uma nova cultura alicerçada na comunicação multimodal e no **processamento digital da informação** [grifo nosso]. [...] na medida em que as redes não param na fronteira do Estado-Nação, a sociedade em rede constituiu-se como um sistema global [...] as instituições do Estado-Nação perderam gradualmente a sua capacidade de controlar e regular os fluxos globais da riqueza e da informação (CASTELLS, 2010, p. XXXVIII).

[96] Para maiores esclarecimentos, consultar os diversos estudos, estratégias e aplicações transnacionais da Infocomunicação por diversos profissionais da informação organizados em Passarelli *et al* (2014).

### *6.1.1 O papel transformador da informação digital*

Em sentido amplo, considera-se a informação como um recurso fundamental e indispensável no desenvolvimento individual e no das sociedades, não obstante ser componente estratégico para as tomadas de decisão de um Estado soberano.

Segundo Uhlir (2006), o uso da informação e do conhecimento para o fortalecimento dos cidadãos, nos campos cultural e científico, deveria ser uma das principais metas de qualquer sociedade. Como facilitador, no caso, tem-se a informação oriunda das áreas de governo produzida e disponibilizada por meio da Internet.

Em relação ao papel alavancador da informação, Capurro e Hjorland (2007, p. 149) vaticinaram: "é lugar-comum considerar-se informação condição básica para o desenvolvimento econômico, juntamente com o capital, o trabalho e a matéria prima; mas o que torna a informação especialmente significativa na atualidade é a sua natureza digital".

Não obstante, convém ressaltar-se o impacto da informação digital na vida cotidiana e privada do indivíduo. Nesse aspecto, no que tange ao uso das tecnologias da informação e à intimidade das pessoas, o arquivista Ramón Alberch comenta que o direito à privacidade pode tornar-se facilmente vulnerável no ciberespaço:

> um retorno eficiente sobre o investimento dedicado às ferramentas informáticas [de TI] deve implicar um esforço significativo, destinado a superar uma série de problemas relacionados com as suas vulnerabilidades e sua capacidade de causar danos à privacidade dos indivíduos, bem como à sua rápida obsolescência [...]. Da mesma forma, deve garantir que a informação contida nos suportes de dados tenha eficácia jurídica, como também promover a **segurança e a confiança** [grifo nosso] nas comunicações eletrônicas (ALBERCH, 2003, p. 187, tradução nossa)[97].

Ao abordar o futuro da sociedade inserida no ambiente cibernético (digital), Lemos e Lévy (2010) preveem que as novas e libertárias modalidades e mídias de compartilhamento da informação estejam produzindo mudanças globais na esfera política sem precedentes. Tal fato deve-se, particularmente, à liberdade de expressão e de comunicação permitidas pelo ciberespaço, bem como à possibilidade de colaboração

---

[97] *Una rentabilización eficiente de la inversión dedicada a las herramientas informáticas debe comportar un serio esfuerzo dirigido a superar una serie de problemas referidos a su vulnerabilidad y su poder lesivo en cuanto a la intimidad de las personas, así como su rápida obsolescencia [...]. Asimismo, se debe conseguir que las informaciones contenidas en los soportes informáticos tengan un valor de eficacia jurídica, como también fomentar la seguridad y la confianza en la comunicación electrónica.*

em rede em escala mundial. Para os referidos autores, ciberespaço não significa somente a infraestrutura material de comunicação digital, mas o grande fluxo de informações que trafegam nele, assim como as pessoas que acessam e alimentam esse ambiente, sendo, na atualidade, um dos principais provedores de informação.

Na análise de Jane Fountain (CASTELLS; CARDOSO, 2005, p. 167) "as tecnologias de informação contribuíram para a alteração da comunicação, particularmente no tocante à sua dimensão e conteúdo, proporcionando a partilha de informação mais complexa e em maior volume".

Ainda sobre a característica transformadora da TI, Marta Pinheiro complementa:

> as tecnologias de informação deste século são qualitativamente diferentes daquelas do passado no que tange à capacitação dos Estados em proteger seu sistema nacional de segurança e ter ao mesmo tempo, pela transparência, a sociedade como aliada. A mobilidade na comunicação e o acesso à informação têm um novo potencial político, em suas dimensões geográficas e de comunicação, pelas interfaces técnicas, dentro de uma ação social que atinge os diferentes grupos da sociedade (PINHEIRO, 2012, p. 75).

Ao considerar a TI e as políticas públicas, o Comitê Gestor da Internet no Brasil alerta:

> a ampliação do uso de tecnologia pelos órgãos públicos no Brasil, em especial a partir dos anos 1990, provocou transformações importantes na governança do Estado, em especial na redefinição dos canais de interação com a sociedade. Também é importante ressaltar que a compreensão do uso que os governos fazem das TIC, especialmente da Internet, é um desafio que exige uma atuação multidimensional das organizações públicas, e deve envolver aspectos como a infraestrutura e a gestão de tecnologia, a oferta de serviços pelos meios digitais, o acesso à informação via Internet e os mecanismos de comunicação e participação digital do cidadão na tomada de decisão pública (CGI.Br, 2016b, p. 180).

Em termos globais, a Organização das Nações Unidas para a Educação, a Ciência e a Cultura (UNESCO)[98], ao longo dos anos, tem priorizado temas como a comunicação, o conhecimento e a informação, considerados molas propulsoras do desenvolvimento sustentável. Para a UNESCO (2010, 2016), essas questões devem ser, igualmente, as ferramentas básicas, permitindo que as pessoas desfavorecidas possam melhorar suas condições de vida. Um elemento essencial da estratégia da

---

[98] A missão da UNESCO consiste em contribuir para a construção de uma cultura da paz, para a erradicação da pobreza, para o desenvolvimento sustentável e para o diálogo intercultural, por meio da educação, das ciências, da cultura e da comunicação e informação.

UNESCO consiste em promover o acesso à informação e ao conhecimento, em particular, por meio de uma gama de atividades que incluem a criação de oportunidades de formação nas Tecnologias da Informação e da Comunicação (TIC). A Organização, também, incentiva o debate sobre os desafios políticos, éticos e sociais, associados à emergência de uma sociedade mundial do conhecimento, além de elaborar diretrizes e projetos para a promoção de um acesso equitativo à informação.

Em relação ao Brasil, a UNESCO reconhece o avanço trazido pela *Lei de Acesso à Informação* (LAI) de 2011 e a necessidade de se reduzirem assimetrias informacionais no país, sugerindo:

a) desenvolver políticas, regulamentações e ações para melhoria da gestão documental das informações públicas [grifo nosso];
b) aumentar a familiaridade e efetividade dos brasileiros com as novas TIC;
c) aumentar o fornecimento de meios para maior conectividade no país;
d) promover o uso de TIC nas escolas, visando à diminuição da exclusão digital (UNESCO, 2016).

Percebe-se que os itens a) e b) apresentam oportunidades de melhoria no que tange à efetivação de medidas e atividades de proteção, enquanto os dois últimos itens podem potencializar riscos e ampliar vulnerabilidades já latentes.

No âmbito nacional, percebe-se que há uma compreensão abrangente, quanto ao reconhecendo das tecnologias da informação, como agentes de transformação na esfera do poder público. Assim o CGI.br considera que:

> Internet e as aplicações de governo eletrônico podem favorecer os governos ao aumentar a sua capacidade de resposta aos cidadãos, ao melhorar a prestação de serviços públicos e ao possibilitar a criação de mecanismos de participação democrática. Dessa forma, os ganhos potenciais advindos da otimização dos processos internos de governo e melhoria da eficiência e qualidade dos serviços dependem, fundamentalmente, do uso de soluções tecnológicas para criar um paradigma de eficiência da máquina pública e de relacionamento do governo com a sociedade, baseado em transparência, eficiência, qualidade dos serviços públicos e controle social (CETIC.BR, 2016, p. 27).

Carlos Alvares, ao abordar as TIC como parte da estratégia para o desenvolvimento e a segurança digital [da informação no espaço cibernético] no setor público, adverte:

> o sector [sic] público assenta numa complexa infraestrutura informacional que, como resultado do crescimento da interconectividade, é vulnerável a ameaças em número e variedade crescentes. A protecção [sic] eficaz desta infraestrutura essencial no sector [sic] público exige a definição de uma estratégia de segurança da infraestrutura digital, com a finalidade de diminuir a

> vulnerabilidade, mitigar os estragos, acelerar tempos de recuperação no caso de pequenos erros ou actividades [sic] maliciosas, e ser capaz de identificar as causas ou as fontes dessas actividades [sic] por análise ou pesquisa (CASTELLS; CARDOSO, 2005, p. 388).

Tratando-se de informação governamental e segurança, vale recordarem-se as considerações do Tribunal de Contas da União, quando da conclusão sobre o levantamento de governança de Tecnologia da Informação, em 2014:

> a informação é um ativo muito importante para qualquer instituição, podendo ser considerada, atualmente, o recurso patrimonial mais crítico. Informações adulteradas, não disponíveis, sob conhecimento de pessoas de má-fé ou de concorrentes, podem comprometer significativamente, não apenas a imagem da instituição perante terceiros, como também o andamento dos próprios processos institucionais. É possível inviabilizar a continuidade de uma instituição, se não for dada a devida atenção à segurança de suas informações (BRASIL, 2014e).

Na próxima seção, explora-se o uso das TIC, não apenas na qualidade elementar de suporte, mas como vetor potencializador e transformador da informação.

### *6.1.2 Novas Tecnologias da Informação e da Comunicação*

As 'novas' tecnologias de informação e comunicação (NTIC) possuem características aglutinadora, disruptiva e futurista, particularmente ao se levar em consideração as possiblidades do ciberespaço e os ambientes informacionais, refletindo, assim, tendências e oportunidades de negócio, em ambiente privado, ou mesmo, no contexto público/governamental. Como ponto de partida, basta recordar-se o profundo e duradouro impacto na produção, armazenamento, uso e comunicação da informação, que vem sendo causado pela dupla computador pessoal-internet, iniciado nas últimas décadas do século passado.

Para Manuel Castells, as novas tecnologias de informação e comunicação, que respaldam a era da informação e suportam as sociedades em rede, apresentam três características distintivas:

a) são autoexpansíveis – capacidade de processamento e comunicação, em termos de volume, complexidade e velocidade;
b) têm uma quase ilimitada capacidade de recombinação – através da digitalização e da comunicação recorrente;
c) são flexíveis em termos de distribuição – pelos sistemas de digitalização e interação em rede (CASTELLS, 2004, *apud* SANTOS, 2014).

Além disso, destaca-se que as TIC podem influenciar (potencializar ou reduzir) o poder de dominação em todas os domínios de uma nação (social, econômico, político, militar etc.):

a) por meio da exclusividade na produção de *hardware* ou *software*;

b) pelo domínio/restrição de acesso às comunicações globais (P.ex.: provedores de internet);

c) através do controle dos meios de comunicação e das mídias de massa - 1 para N (P.ex.: Tv digital);

d) por intermédio das comunicações interativas - N para N (P.ex.: redes sociais como *WhatsApp, Facebook* etc.).

Ao analisar a hibridação do humano pelas tecnologias eletrônicas, Moisés Martins (2014) ressalta que as plataformas eletrônicas [digitais] inscrevem-se no quadro de uma artificialização e uniformização crescentes da experiência estética de massas pela tecnologia, associando tanto a ideologia do conformismo como a distribuição social do comodismo.

No cenário europeu, particularmente na França, Alex Mucchielli destaca e analisa as NTIC como um dos quatro ‘domínios de estudo’ das ciências de comunicação e de informação (CCI):

> as NTICs constituem um tópico privilegiado de estudo que foi disputado pelas CICs (interdisciplina situada no campo das Ciências Sociais e Humanas), tecnólogos e engenheiros. Encadeia-se neste “domínio” uma variedade de aspectos que correspondem a segmentos de análise fecunda e tipicamente interdisciplinar: digitalização das informações; multimídia e interatividade; acesso a “conhecimento representacional” através da imagem; as redes (a “Numéris” da France Télécom e a Internet); o “cibermundo”; o diálogo homem-computador ou máquina de comunicação; a informação-documentação eletrônica; o ensino e a formação baseada nas TICs; imaginação das TICs; o mito das mudanças psicológicas e sociais provocadas pela tecnologia (MUCCHIELLI, 2006 *apud* SILVA; RAMOS, 2014, p. 53).

Ainda neste contexto, Brasilina Passarelli aponta que, sob a presença indiscutível do ‘eletrônico’ nos tempos de hoje, vive-se uma ambiência digital, uma mediação tecnológica assim categorizada:

> é num ambiente imbuído de e imerso em tecnologia (digital) que se produz, se usa e se armazena/preserva informação e, concomitantemente, ocorre a troca de mensagens entre pessoas ou a interação homem-máquina, que está na base e/ou faz parte integrante do processo comunicacional. A tecnologia medeia esse processo e entra em simbiose com ele, constituindo-se não como um simples canal transmissor de mensagens (informação), mas sim como um *locus,* um ambiente ou, dito de outra forma, como um sistema onde

> a informação e a comunicação têm o seu lugar privilegiado (PASSARELLI *et al*, 2014, p. 116).

Desde a década de 1990, a rede mundial de computadores vem se expandindo não somente em tamanho, capilaridade, compartilhamento de informações e serviços, mas, também, em oportunidades e desafios; ocasionando um grande impacto sobre os relacionamentos pessoais, as organizações, os governos, a cultura e o comércio mundial. Inovações, oportunidades e riscos do espaço ciberespaço caminham lado a lado. Dentre as tendências mais promissoras e mais perigosas, destaca-se a Internet das coisas – IoT (*Internet of Things).* A IoT integra, junto com outras tecnologias físicas e digitais (P.ex.: Inteligência artificial e computação cognitiva), a denominada Indústria 4.0 ou quarta Revolução Industrial.

A evolução é de tal forma vertiginosa que já se alude a uma terceira vaga do ciberespaço, que se desenvolve em torno da IoT. Na *Internet of things* ou mesmo das *moving things*, em que a Internet, para além de conectar pessoas e coisas, passa a fazer parte das próprias coisas, no limite, de todas elas, afetando relações entre pessoas, empresas e o todo social (PINTO, 2017)[99].

Pode-se, então, considerar a IoT como uma revolução tecnológica informacional (suportada pelas TIC), com a finalidade de conectar, à Rede Mundial de Computadores, dispositivos eletrônicos (físicos ou virtuais) utilizados no dia-a-dia da sociedade.

Na IoT, têm-se: carros, utensílios domésticos (geladeiras, máquinas de lavar, fogões etc.), televisões, relógios, roupas, câmeras de vídeo e de TV, aparelhos hospitalares, entre outros, conectados à Internet, que podem representar ameaças graves à sociedade, pois qualquer dispositivo em rede mundial corre o risco de ter seu controle sequestrado, demandando, também, proteção de dados e sigilo de informações pessoais (CGI.br, 2016a).

Nestes aspectos convergentes da segurança com a privacidade, o relatório “Tendências de Ciber segurança", da empresa TÜV Rheinland[100], esclarece que, em 2016, o advento do vírus Mirai provou que os dispositivos da Internet das Coisas estão

---

[99] Intercâmbio realizado (via *e-mails* e entrevistas presenciais), com a professora Maria Manuela Gomes de Azevedo Pinto, diretora do Centro de Investigação em Comunicação, Informação e Cultura Digital - Porto (CIC.Digital) - Universidade do Porto, entre abril e julho de 2017.

[100] Empresa mundial de certificações, inspeções, treinamentos e gerenciamento de projetos, maiores esclarecimentos, disponíveis em: <https://www.itforum365.com.br/seguranca/8-desafios-de-ciberseguranca-que-vao-tirar-o-sono-das-empresas-nos-proximos-meses/. Acesso em: 18 jan. 2018.

expostos à exploração de vulnerabilidades críticas, podendo ser, efetivamente, transformados em *botnets* (grupo de computadores -robôs – conectados à Internet). Dessa forma, como os dispositivos e sistemas estão diretamente conectados às redes abertas, o impacto das violações de dados estende-se muito além da simples monetização de dados para as ameaças “cinéticas”, por exemplo no campo da saúde e da segurança pública.

Não obstante as possíveis vulnerabilidades e ameaças decorrentes, o Ministério da Ciência, Tecnologia, Inovação e Comunicações, em parceria com o BNDES, preparou o estudo "Internet das Coisas: um plano de ação para o Brasil", que deve ser consolidado como um Plano Nacional. O Plano em construção almeja o aceleramento da implantação da IoT, como instrumento de desenvolvimento sustentável da sociedade brasileira, capaz de aumentar a competitividade da economia, fortalecer as cadeias produtivas nacionais e promover a melhoria da qualidade de vida. Todo o estudo do BNDES está embasado no pressuposto que a IoT vem ganhando espaço, não por causa do surgimento de tecnologias disruptivas, mas pela evolução de um conjunto de tecnologias já disponíveis, que estão se tornando mais acessíveis, possibilitando sua adoção em massa.

Os aprendizados do referido Estudo estão sintetizados na "Cartilha de Cidades", lançada em janeiro de 2018 (BNDES, 2018). Segundo tal estudo, até 2025, no mundo, a Internet das Coisas terá um impacto econômico de US$ 4 a 11 trilhões, maior do que robótica avançada, tecnologias *cloud* e até mesmo internet móvel. No Brasil, o impacto esperado é de US$ 50 a US$ 200 bilhões por ano, valor que representa cerca de 10% do PIB brasileiro.

O Estudo, em questão, considera, também, a segurança da informação como aspecto fundamental para a viabilidade técnica, econômica e social das soluções em IoT, sobressaindo-se os seguintes aspectos:

a) a preocupação com a segurança dos dispositivos tecnológicos utilizados nas soluções de IoT, pois estes são comumente compostos de *hardware* e *software* vulneráveis;
b) a necessidade de adoção de medidas de privacidade e segurança da informação no armazenamento de dados pessoais;
c) o grau de segurança de infraestruturas consideradas críticas, como redes de saneamento básico e energia elétrica;

d) a tendência de aumento da conectividade de sistemas essenciais [IC], considerando-se o potencial impacto social causado por um possível ataque ou falha de segurança;
e) a certificação voluntária sobre a segurança de dispositivos ligados à Internet das Coisas (BNDES, 2018, p. 45).

Neste contexto, como exemplo de ameaças, por meio de equipamentos IoT, pode-se citar o crescimento dos ataques de negação de serviço (DDoS) no Brasil e no mundo, onde os principais vetores de ataques são as *botnets*, redes formadas por equipamentos infectados ou invadidos, como câmeras de segurança e roteadores domésticos para o estabelecimento de redes sem fio (*wireless*). No caso, os atacantes, de forma simples e com baixo custo, aproveitam-se, principalmente, de senhas fracas ou padrão desses equipamentos para invadi-los, particularmente por meio de protocolos de comunicação como o SSDP (*Simple Service Discovery Protoco*l).

Na próxima seção, será abordado o papel da informação na construção e consolidação de um Estado-Nação, sob os mais diversificados aspectos da nacionalidade em ambiente digital.

### *6.1.3 O Estado digital e o poder cibernético*

No início do século XXI, ao apresentar governança e formas de governo no ciberespaço (ciberdemocracia), Pierre Levy profetizava:

> a rede telefónica [sic] mundial, a televisão por satélite, a multiplicação dos canais televisivos e, mais recentemente, a interligação mundial dos computadores, que integra todos os *media* anteriores num meio de comunicação interativa original, leva ao nascimento de um *novo espaço público*. Este novo espaço redefine radicalmente as condições de governação e vai, provavelmente, gerar novas formas políticas, ainda dificilmente previsíveis (LEVY, 2002, p. 29).

Ao analisar a sociedade em rede, Manuel Castells e Gustavo Cardoso alertam que o mundo contemporâneo está sendo transformado por intermédio da globalização e da “informacionalização[101]”, determinadas pelas redes de riqueza, tecnologia e poder. Nesse sentido, os mecanismos atuais de controle social e de representação política vêm se transformando pela repentina aceleração no tempo histórico, aliada à abstração do poder em uma rede de computadores (CASTELLS; CARDOSO, 2005).

Segundo Braman (2006), quando se fala em controle de bases e técnicas do poder informacional, refere-se ao exercício do poder sob ordem da informação, ou seja, do poder capaz de modelar o comportamento do indivíduo pela manipulação das bases informacionais do poder instrumental (via força física), estrutural (via regras e instituições) e simbólico (via imagens, ideias e palavras).

Como contraponto, Sergio Silva (2008) identifica uma flexibilidade relativa nas políticas convencionais governamentais, justamente em virtude do advento e do crescimento do uso de novas tecnologias de informação. Segundo Silva (2008, p. 24): “estudar a informação nas formações políticas modernas e contemporâneas significa conhecer o papel do Estado e de suas agências de informação e reconhecer a existência de mediação informacional nas relações entre Estado e políticas públicas”. O autor ratifica “uma certa flexibilidade nas fronteiras territoriais tradicionais e nas políticas convencionais das nações que acabam afetando a noção que se tem de Estado”.

Em relação, particularmente, à caracterização de um Estado no cenário atual, considera-se que o mesmo foi redefinido. O Estado burocrático passou a denominar-se Estado informacional, que controla a informação e seus fluxos em uma nova forma particular de poder. Por conseguinte, o Estado-Nação moderno estabelece a convergência entre inovação tecnológica e política, colocando o controle da informação, o tratamento, os fluxos e a sua utilização para exercício de uma nova natureza de poder (BRAMAN, 2006; PINHEIRO, 2012).

Pinheiro (2012), ao discutir os papéis do Estado moderno - informacional, reforça nosso entendimento sobre a necessidade aperfeiçoar a gestão da informação em meio digital:

> as informações do país continuam a ser controladas e armazenadas, mas sem um tratamento objetivo, sobrepostas de forma difusa em novos formatos ou suportes, como **legalização**, **proteção** [ grifo nosso] e comunicação – apesar de interpretadas e reconhecidas, principalmente nos discursos, como um tema fundamental para a governança em regimes políticos democráticos (PINHEIRO, 2012, p. 66).

---

[101] Paradigma tecnológico que substituiu/absorveu o industrialismo, constituindo-se na base material do início das sociedades do século XXI (CASTELLS, 1999, 2003).

Segundo Sandra Braman, do ponto de vista das mutações do Estado, podem-se verificar três indícios de mudanças de natureza informacional:

a) a absorção por parte de alguns Estados do controle de técnicas de poder informacional já utilizadas por empresas e por outros atores não governamentais;
b) o desenvolvimento de técnicas para expandir o uso das entidades do setor privado como agentes reguladores, transformando-os em centros particulares de poder para proposições do Estado;
c) a adoção pelos Estados de aspectos característicos de organizações caracterizadas como organismos em rede (*networked*) (BRAMAN, 2006).

Para Jane Fountain, o Estado virtual (informacional/digital) é “intersetores, interagências e intergovernamental”. A pesquisadora destaca três aspectos interessantes ligados ao “novo relacionamento” entre a informação e os governos na era da informação:

a) as trocas de informação informais através da Internet, entre profissionais dentro e fora do Governo, operam uma forte mudança nos processos associados à tomada de decisão e criação de políticas públicas;
b) todas estas mudanças [trocas de informação] alteram os tipos de diálogo entre os oficiais do governo;
c) as trocas de informação diárias e informais estão entre as mais importantes e, potencialmente, mais passíveis de causar mudança na forma de governação e elaboração de políticas (CASTELLS; CARDOSO, 2005, p. 167).

Segundo Sérgio Silva, dentro do contexto de um Estado e suas políticas de governo, destaca-se:

> o uso da informação é parte do processo de construção democrática, de novas formas de organizar a vida, de controlar o poder e de compartilhar destinos. A informação, ou a sua inexistência, ou ainda a sua indisponibilidade, é elemento fundamental para a participação democrática (SILVA, 2008, p. 28).

Sobre tal “mundo de mudanças”, Marta Pinheiro avalia que esse novo contexto mundial seja regido pelo paradigma técnico e econômico das tecnologias de informação, sendo fortemente marcado pelo crescimento de rivalidades econômicas. A articulista considera “o surgimento de novas forças geográficas mundiais, nas quais o mercadológico e o político fundem-se e, pela dimensão financeira, domina--se o bélico, a ciência e a tecnologia” (PINHEIRO, 2012, p. 62).

Em síntese, destaca-se no cenário mundial, um novo domínio ou poder – o cibernético, que, dentre outras, possui as seguintes caraterísticas:

a) não é definido territorialmente, ou seja, sem limites físicos;
b) as ferramentas de segurança e defesa estão disponíveis para os possíveis oponentes;
c) depende da criatividade humana, gerando assimetria entre ataque e defesa;
d) não existe sistema que possa ser considerado totalmente seguro.

Não obstante, o controle de técnicas informacionais, nomeadamente o do gerenciamento da informação sob sua tutela, pode, além de proporcionar menos insegurança institucional, auxiliar um Estado-Nação a otimizar seu relacionamento com os cidadãos e a promover o desenvolvimento sócio-cultural-econômico da sociedade, bem como a repensar a sua base de poder e representatividade global.

Na presente pesquisa, considera-se que essa nova natureza de poder, trata-se de uma nova dimensão de poder nacional, o cibernético. Tal poder para ser reconhecido positivamente, tanto nacionalmente como no contexto globalizado, deve ser precedido no âmbito das instituições públicas e privadas pelo domínio e pela adoção perene das melhores práticas de gestão da informação em meio digital, tema a ser discutido na próxima seção.

## 6.2 Gestão da Informação e a CI

A Gestão da Informação (GI) pode ser entendida, sumariamente, como o gerenciamento do conjunto de atividades e de mecanismos relativos à produção, armazenamento e acesso à informação[102], ou, ainda, como um ‘ambiente’, envolvendo

> a intervenção dos gestores para implementar recursos de informação para fins organizacionais, [...] a identificação das necessidades da Organização, a

---

[102] Definição livre e propositalmente minimalista inspirada na proposição de Brian Detlor: “*Information management concerns the control over how information is created, acquired, organized, stored, distributed, and used as a means of promoting, efficient and effective information access, processing, and use by people and organizations”*. Disponível em: <http://www.sciencedirect.com/science/article/pii/S0268401209001510>. Acesso em: 25 jun. 2017.

> identificação e avaliação de recursos de informação e o desenvolvimento e implementação dos recursos necessários para responder às necessidades (PINTO, 2016, p. 4).

Na análise de Kira Tarapanoff, toda mudança, para que seja implementada, depende da gestão/gerenciamento (*management).* Assim, coube à gestão disseminar as novas tecnologias nos ambientes de trabalho e domésticos, bem como proporcionar a criação de empresas em rede, favorecendo, inclusive, a globalização da economia. Na opinião da autora: "a gestão da informação, aquisição, armazenamento, análise e uso provê a estrutura para o suporte ao crescimento e desenvolvimento de uma organização inteligente, adaptada às exigências e novidades da ambiência em que se encontra" (TARAPANOFF, 2001, p. 57).

Na busca de entendimento comum, o *Dicionário Eletrônico de Terminologia em Ciência da Informação* caracteriza a GI como:

> lidar, administrar, encontrar soluções práticas desde a génese [sic] até ao efeito multiplicador do fluxo da informação e compreende um conjunto diversificado de atividades, a saber: produção, tratamento, registo e guarda, comunicação e uso da informação. [...] A vasta e complexa problemática ligada à produção da informação (do meio ambiente à estrutura produtora, a operacionalização e utilidade da memória orgânica, os atores, os objetivos, as estratégias e os ajustamentos à mudança) em contexto orgânico institucional e informal constitui o núcleo duro da Gestão de Informação propriamente dita[103].

Gleiciane Silva recorda que há diversas abordagens[104] sobre GI na literatura que sofrem influência do contexto em que estavam inseridas, não sendo possível uma perspectiva universal e unânime sobre o significado, conteúdo e uso da Gestão da Informação (SILVA, 2016).

Ao analisar modelos genéricos de gerenciamento da informação, envolvendo necessidades organizacionais e reconhecendo a informação como uma ferramenta valiosa para os ofícios profissionais, Cavalcante, Silva e Freire (2013) apresentam, no quadro 10, um interessante resumo de alguns modelos de gestão e informação.

---

[103] Dicionário Eletrônico de Terminologia em Ciência da Informação (DeltCI). Disponível em: <https://paginas.fe.up.pt/~lci/index.php/1770>. Acesso em: 25 abr. 2017.
[104] Detalhamento sobre a visão de diversos teóricos sobre a GI disponível em Silva (2016, p.62ss).

Quadro 10 - Modelos teóricos de Gestão de Informação

| CHOO | MORAIS | DAVENPORT | MCGEE E PRUSAK |
|---|---|---|---|
| 1) Identificação de necessidades | 1) Determinação da necessidade | 1)Determinação das exigências | 1) Identificação de necessidades e requisitos |
| 2) Aquisição de informação | 2) Obtenção | 2) Obtenção | 2) Coleta/entrada de informação |
| 3) Organização e armazenagem de informação | 3) Processamento | - | 3) Classificação e Armazenamento/Tratamento e Apresentação da Informação |
| 4) Desenvolvimento de produtos e serviços | - | - | 4) Desenvolvimento de produtos e serviços de informação |
| 5) Distribuição da informação | 5) Distribuição | 5) Distribuição | 5) Distribuição e disseminação de informação |
| 6) Uso da informação | 6) Utilização | 6) Utilização | 6) Análise e uso de informação |

Fonte: Cavalcante, Silva e Freire (2013, p. 15)

No entendimento de Armando Malheiro da Silva, o estudo científico da GI, no contexto da CI, percorre diversos momentos e aspectos, com destaque para:

> as necessidades e funções das entidades (instituições e organizações) produzem e recebem informação (**documentos** [grifo nosso]), organizam processos, controlam a circulação da informação (documentos simples e processos), conservam os suportes informativos e/ou seus registros, temporária ou definitivamente e consultam a informação seletivamente; [...];
>
> no estudo dos tipos documentais, seu valor, vigência, tipo e qualidade da sua informação para colaboração entre os serviços produtores de informação e o arquivo;
>
> na preparação de informações para a resolução de qualquer assunto ou para estudos [...] (SILVA, 2009a, p. 246).

Na visão de Wilson (2002, *apud* Silva, 2016), há o uso ambíguo da expressão Gestão da Informação na literatura de diversas áreas do conhecimento, tais como: ciência da informação, ciência da computação, administração e negócios estratégia empresarial, de modo que a GI deve levar em consideração:

a) o valor da informação;

b) a qualidade;

c) a posse;

d) o uso da informação;

e) a Segurança da informação [grifo nosso].

Ao relacionar a gestão com a segurança, Fernandes e Rodrigues (2013. p. 15) argumentam que:

> a gestão da informação tem fundamentos em todas as áreas da organização e para garantir satisfação das expectativas de continuidade, ou simplesmente de segurança, a gestão da informação lança mão de elementos organizacionais, humanos, físicos e tecnológicos, integrados por meio de arquitetura e engenharia de sistemas de tecnologia da informação, ou forma mais geral através de uma abordagem cibernética. O controle das informações [...], sendo necessário para o alcance de garantias para o desempenho organizacional, cria limitações às ações dos agentes que executam processos na organização. [...] É importante que todos os agentes que atuam na organização recebam uma clara mensagem da alta administração quanto à forma de tratar a informação com segurança, pois é central para o controle dos negócios e alcance da missão institucional. As responsabilidades individuais dos agentes devem ser alinhadas com a visão de segurança e a questão da segurança da informação deve ser embutida na cultura organizacional. A mensagem que comunica essa necessidade é usualmente estabelecida por uma política.

Diante de inúmeras e diferentes formas de abordagens da GI, infere-se, portanto, quanto à necessidade de se aprofundarem entendimentos referentes à gestão da informação, bem como de documentos e objetos digitais[105], sobre a temática central da pesquisa, qual seja, a segurança da informação em meio digital no contexto da CI.

### *6.2.1 Aspectos inerentes à segurança na gestão em CI*

Ao estudar pontos de convergência entre a Ciência da Informação e a Arquivologia, no que tange aos conceitos de informação e de documento, Rondinelli (2013, p. 25) destaca a materialidade (conteúdo fixado num suporte) e a funcionalidade (ensino, aprendizagem, registro e comunicação da informação, testemunho de fatos e ações).

Não obstante, ao abordar a recuperação da informação, sob o entendimento de “recuperação de documentos”, Capurro e Hjorland (2007, p. 182) afirmam: “Semântica, significado, texto e documentos estão muito mais relacionados às teorias sobre linguagem e literatura, enquanto informação está muito mais relacionada às teorias sobre computação e controle”.

---

[105] Propositalmente, este estudo não contemplou a ‘Gestão de Recursos de Informação’, por adotar que, “sob o termo ‘recursos de informação’, não só são incluídos os documentos eletrônicos de todos os tipos, mas também as atividades e serviços de informação (entre outros: os *records management*, a gestão de bibliotecas, reprografia, os centros de dados), [...] etc.” (PINTO, 2015, p. 379).

Ao identificar a concepção material da informação (como coisa (algo) registrada em um suporte), Buckland (1991) entende que documentos e textos não seriam somente documentos textuais e em papel, mas também imagens, tabelas de números e sons, tanto no meio convencional quanto no eletrônico/digital. Para Buckland:

> o registro do conhecimento ocorre a partir do uso de recursos tecnológicos, das redes formais de comunicação, da infraestrutura da instituição e do registro da informação e estabelece a relação entre *information-as-thing* e *document*. [...] a informação registrada é a base do documento formal e sistematizado (1997, 1998 *apud* INNARELLI, 2015).

Na busca por fundamentos para o conceito de "gestão de documentos", em contexto amplo e globalizado, Jardim (2015) compilou vários conceitos e definições do referido termo em diversas línguas e "tradições arquivísticas", a saber: inglês, espanhol, francês e português.

O quadro 11 resume o levantamento do autor, grupando seus aspectos teóricos e práticos, no que tange à frequência de termos associados ao objeto, às ações e aos objetivos inerentes à gestão de documentos, por língua/tradição arquivística.

Quadro 11 - Gestão de documentos

| **LÍNGUAS** | **OBJETO** | **AÇÕES** | **OBJETIVOS** |
|---|---|---|---|
| INGLESA (EUA, Inglaterra, Canadá e Austrália) | Produção, manutenção, uso e destinação de documentos | Planejamento, controle e direção | Economia e eficiência |
| FRANCESA (França, Canadá [Quebec e Montreal]) | Produção, conservação, uso e destinação de documentos | Controle | Eficácia |
| ESPANHOLA (Espanha, Colômbia, Costa Rica e México) | Produção, uso, manutenção, controle físico e intelectual de documentos íntegros, autênticos e confiáveis | Controle, planejamento, e análise da produção, tramitação, uso e informação contidos nos documentos | Eficiência e estabelecimento de normas |
| PORTUGUESA (Brasil e Portugal) | Produção, tramitação, classificação, uso, avaliação e arquivamento | Controle | Eficácia, eficiência e racionalização |

Fonte: adaptado de Jardim (2015)

Ao analisar o quadro resumo de gestão de documentos à luz da segurança da informação no espaço cibernético, percebe-se que:

1) o "uso" e a "produção" são comuns a todas as línguas no quesito Objeto, sendo também, essenciais para o estabelecimento de medidas preventivas de Ciber Proteção;
2) o "controle", berço e essência da Cibernética, encontra-se presente em todas as línguas no que se refere às Ações;

3) a busca pela efetividade (eficiência + eficácia) alinha-se perfeitamente com o objetivo de redução das vulnerabilidades em Tecnologia da Informação, quesito basilar da Ciber Proteção.

Ao tratar de gestão de documentos, Joaquin Llansó esclarece que existem três modelos básicos:

a) modelos primários - aqueles que atingiram um tal desenvolvimento que vêm diretamente influenciar outros modelos;
b) modelos de segunda geração - os que receberam uma influência de modelos estrangeiros, oriundos de compartilhamento de tradições administrativas e arquivísticas comuns;
c) modelos de assimilação - os que adotaram, *a priori*, elementos de outros modelos exteriores à sua tradição administrativa e arquivística de origem (LLANSÓ SANJUAN, 2011, p. 47, tradução nossa).

Sobre modelos para a gestão de documentos, Jardim (2015, p. 31) conclui que "a ampliação do ambiente [meio] digital e todas as suas consequências, na produção, conservação e uso dos documentos daí decorrentes, colocaram efetivamente em cheque a noção de ciclo vital[106] [bem como a teoria das três idades[107]], especialmente a partir dos anos de 1990".

No entendimento de Jardim (2015, p. 35), o "mapeamento das mudanças decorrentes da emergência e ampliação do uso das tecnologias da informação e comunicação, em diferentes cenários sociais nas últimas décadas do século passado", aliado aos "novos modos de produção, uso e conservação de documentos arquivísticos, associados a várias reconfigurações, na gestão das organizações públicas e privadas", fez emergir a teoria/modelo do *records continuum*[108].

[106] Sucessivas fases por que passam os documentos arquivísticos, da sua produção à guarda permanente ou eliminação (CONARQ, 2014).
[107] Ideia [teoria] de que os documentos arquivísticos, em função dos seus usos e valores para a organização produtora ou para terceiros, podem ser objeto de intervenção em uma ou mais fases: corrente, intermediária e permanente (JARDIM, 2015, p. 32).
[108] Toda a extensão da existência de um documento. Refere-se a um regime consistente e coerente dos processos de gestão a partir do momento da produção de documentos [...], mediante a preservação e utilização dos documentos e arquivos (JARDIM, 2015, p. 36).

As informações geradas, comunicadas e armazenadas em meio digital possuem características peculiares como seu suporte, formas de recuperação e comunicação. Convém, então, destacarem-se dois termos definidos pelo Conselho Nacional de Arquivos (CONARQ, 2014): documento eletrônico e objeto digital. O primeiro trata-se da “informação registrada, codificada em forma analógica ou em dígitos binários, acessível e interpretável por meio de equipamento eletrônico”. No caso do objeto digital: é “uma ou mais cadeias de *bits* que registram o conteúdo do objeto e de seus metadados associados”.

Em relação aos metadados, literalmente entendidos como “dados sobre dados”, o *Tesauro Brasileiro de Ciência da Informação* (Pinheiro e Ferrez, 2014) estabelece as seguintes relações hierárquicas:

a) metadados administrativos - usados na gerência e administração de recursos informacionais. Ajudam com o monitoramento, acesso, reprodução, digitalização e cópia de segurança de recursos digitais;
b) metadados descritivos - informação estruturada que representa e descreve, de forma sintética, o conteúdo de recursos ou objetos de informação, para fins de seu registro e recuperação;
c) metadados de direitos - facilitam o gerenciamento dos direitos legais de um recurso informacional, tais como: direito autoral e licença para reprodução;
d) metadados descritivos - informação estruturada que representa e descreve, de forma sintética, o conteúdo de recursos ou objetos de informação para fins de seu registro e recuperação;
e) metadados estruturais - definem a organização interna dos objetos digitais, sendo importantes para a sua visualização e navegação;
f) metadados de preservação - informações necessárias para garantir a longa duração do armazenamento e a usabilidade de conteúdos digitais.

Ainda sobre metadados, Lídia Alvarenga (2001, p. 5 e 17), ao pesquisar o tema, no campo das bibliotecas digitais, esclarece que:

> no novo contexto de produção, organização e recuperação de objetos digitais, as metas de trabalho não se restringem à criação de representações simbólicas dos objetos físicos constantes de um acervo, mas compreendem estabelecimento dos denominados metadados, muitos dos quais podem ser extraídos diretamente dos próprios objetos [digitais], constituindo-se esses em chaves de acesso a serviço dos internautas.

> [...] os metadados incluem pontos de acesso expressos igualmente nos próprios textos, nas imagens e registros sonoros, presentes no meio digital, muitos desses não sendo passíveis de marcação do texto como nos padrões baseados nas linguagens de marca mais tradicionais HTML e SGML.

Neste contexto, a anatomia do objeto digital é percebida em três níveis pelo Conselho Nacional de Arquivos (2014, p. 27):

a) nível físico - refere-se ao objeto digital como fenômeno físico que registra as codificações lógicas dos *bits* nos suportes. Por exemplo, no suporte magnético, o objeto físico é a sequência do estado de polaridades (negativa e positiva) e, nos suportes ópticos, é a sequência de estados de translucidez (transparência e opacidade);

b) nível lógico - refere-se ao objeto digital como um conjunto de sequências de *bits*, que constitui a base dos objetos conceituais;

c) nível conceitual - refere-se ao objeto digital que se apresenta de maneira compreensível para o usuário, como, por exemplo, o documento visualizado na tela do computador (CONARQ, 2014, p. 27).

Surge, então, o documento digital que, de acordo com o próprio CONARQ (2014), caracteriza-se como a “informação registrada, codificada em dígitos binários e acessível por meio de sistema computacional”. Para Bodê (2016, p. 505), a mais importante característica definidora de documentos digitais seria a “não existência de uma ligação necessária e definitiva entre o conteúdo de um documento e seu respectivo suporte documental no qual esse conteúdo era registrado”.

No presente estudo, o documento digital pode também ser considerado arquivístico, ou seja, acumulado (produzido ou recebido) no curso de uma atividade prática, como instrumento ou resultado da mesma e retido para ação ou referência, bem como incorporado a um sistema de arquivos [sistema de informação automatizado] (CONARQ, 2011).

Dessa forma, adota-se, nesta tese, a definição operacional de Ernesto Bodê para documento digital:

> um documento digital é o equivalente a uma sequência de códigos binários registrados em algum tipo de tecnologia de memória. Organizados de acordo com determinado formato de arquivo computacional e mensurado através da quantidade de *bytes* total desse arquivo. Dependendo do tipo de conteúdo, haverá outras características específicas como a representação de cores, som ou texto. A interpretação desses códigos para humanos ocorrerá através de sistemas computacionais de *software* e *hardware* (BODÊ, 2016, p. 511).

Ao questionar o entendimento do termo ‘documento’, a partir do contexto digital, Rosely Rondinelli afirma:

> a nítida fisicalidade dos documentos foi substituída por dígitos binários, invisíveis aos olhos humanos, fixados em bases magnéticas e ópticas; a leitura antes direta, passou a ser indireta, isto é, dependente de *hardware* e *software*; a visualização simultânea do suporte e da informação deixou de existir; e, como se não bastasse, ainda há base de dados e os hipertextos, ou seja, “documentos” aparentemente ilimitados (RONDINELLI, 2011, p. 27).

Admite-se que tanto o *hardware* como o *software* integrante de um sistema de informação pode ser comprometido, bem como a rede de comunicação de dados. Assim, nesta tese, não há, para fins de Ciber Proteção, distinção entre documentos digitalizados[109] (P.ex.: conversão de documentos analógicos para digital por meio de um escâner) e documento (nato) digital. Tal entendimento encontra suporte na afirmação de Ernesto Bodê (2016, p. 504):

> o documento digital é um artefato bastante novo em nosso mundo e sua presença proeminente ocorreu somente nas últimas décadas. Estamos aqui nos referindo tanto ao documento digital que já nasce nesta forma, como também aos documentos digitais oriundos de processos de digitalização a partir de outros documentos em suportes documentais tradicionais, como o papel comum ou o papel fotográfico.

Neste contexto, inerente à segurança dos documentos digitais, destacam-se os quesitos seguintes:

a) controle de acesso - físico e lógico;
b) acessibilidade - garantia de localização, recuperação, apresentação e interpretação;
c) autenticidade - transmissão e preservação sem adulteração/corrupção, por meio do controle dos processos de criação, manutenção e custódia;
d) fixidez - a transmissão de uma informação do documento está vinculada ao conteúdo em si e à sua disposição formal;
e) preservação digital - conjunto de ações gerenciais e técnicas exigidas para superar as mudanças tecnológicas e as fragilidades [vulnerabilidades] dos suportes.

---

[109] O Glossário do Conselho Nacional de arquivos entende por digitalização: “Processo de conversão de um documento para o formato digital, por meio de dispositivo apropriado” (CONARQ, 2014, p. 18).

Ao debater o documento arquivístico ante a realidade digital, Rondinelli (2013) demonstra uma convergência conceitual em relação a dois pontos: (i) natureza (origem e constituição) a partir de pessoas jurídicas e (ii) organicidade (elo intelectual das ações)[110].

Além do exposto, no âmbito dos documentos arquivísticos, registram-se como características relevantes para este trabalho: a autenticidade e a acurácia apontadas pelo Projeto InterPARES 2 (2007)[111]:

> autenticidade refere-se ao fato de que os documentos arquivísticos são o que eles dizem ser e que não foram adulterados ou corrompidos de qualquer outra forma. [...] refere-se à confiabilidade dos documentos enquanto tais. [...] A **autenticidade é colocada em risco sempre que os documentos arquivísticos são transmitidos através do tempo e do espaço** [grifo nosso].
>
> acurácia é o grau de precisão, correção, verdade e ausência de erros e distorções existentes nos dados contidos nos materiais. Para assegurar a acurácia, deve-se **exercer controle sobre os processos de produção, transmissão** [grifo nosso]**,** manutenção e preservação dos materiais.

Innarelli reforça, ainda, que o documento arquivístico digital:

> nada mais é que um documento digital tratado, gerenciado e preservado como um documento arquivístico [e] deve ser preservado ao longo do tempo, independentemente de sua fase no ciclo vital, em conjunto com todas as suas características arquivísticas e tecnológicas, as quais são imprescindíveis para o seu acesso, manifestação, compreensão e garantia de autenticidade (INNARELLI, 2015, p. 89-90 e 94).

Em relação à gestão dos documentos (*records management),* adota-se a definição da Sociedade dos Arquivistas Americanos - SAA (Society of American Archivists): "O controle sistemático e administrativo dos documentos durante seu ciclo de vida para garantir a eficiência e a economia na sua criação, uso, tratamento, controle manutenção e destinação"[112] (SAA, 2005, p. 334).

Vale destacar-se que o segundo parágrafo, do Art. 216, da *Constituição da República Federativa do Brasil* (CRFB) determina: “Cabem à administração pública, na

---

[110] A autora infere que os documentos digitais gerados, no curso de atividades desempenhadas por pessoas físicas ou jurídicas e em suporte diferenciados, também podem ser documentos arquivísticos.
[111] O Projeto InterPARES – *International Research on Permanent Authentic Records in Electronic Systems* – (Pesquisa Internacional sobre Documentos Arquivísticos Permanentes Autênticos em Sistema Eletrônicos) começou em 1998. Trata-se de um projeto interdisciplinar e multinacional de pesquisa que explora questões relativas a documentos arquivísticos digitais e a dados confiados à Internet.
[112] *The systematic and administrative control of records throughout their life cycle to ensure efficiency and economy in their creation, use, handling, control, maintenance, and disposition*.

forma da lei, a gestão da documentação governamental e as providências para franquear sua consulta a quantos dela necessitem"[113].

Neste contexto governamental, o Arquivo Nacional, subordinado ao Ministério da Justiça, tem por finalidade implementar e acompanhar a política nacional de arquivos públicos e privados e sua consequente regulamentação (Lei n. 8159/1991 e Decreto n. 4553/2012), sendo, portanto, o órgão central do Sistema de Gestão de Documentos de Arquivo (SIGA). O SIGA foi criado em 2003, com as seguintes finalidades:

a) garantir ao cidadão e aos órgãos e entidades da Administração Pública Federal, de forma ágil e segura, o acesso aos documentos de arquivo e às informações neles contidas, resguardados os aspectos de sigilo e as restrições administrativas ou legais;
b) integrar e coordenar as atividades de gestão de documentos de arquivo desenvolvidas pelos órgãos setoriais e seccionais que o integram;
c) disseminar normas relativas à gestão de documentos de arquivo;
d) racionalizar a produção da documentação arquivística pública;
e) racionalizar e reduzir os custos operacionais e de armazenagem da documentação arquivística pública;
f) preservar o patrimônio documental arquivístico da administração pública federal;
g) articular-se com os demais sistemas que atuam direta ou indiretamente na gestão da informação pública federal[114].

Ainda no âmbito governamental, o Arquivo Nacional vincula o Conselho Nacional de Arquivos, órgão colegiado que possui como destinação definir a política nacional e arquivos públicos e privados, bem como ser o órgão central do Sistema Nacional de Arquivos (SINAR). Em 2006, o CONARQ lançou o e-ARQ BRASIL destinado a colocar parâmetros nos sistemas informatizados de gestão arquivística de documentos (SIGAD). O SIGAD é descrito como "um conjunto de procedimentos e operações técnicas, característico do sistema de gestão arquivística e documentos, processado por computador" (CONARQ, 2011).

---

[113] Disponível em: <https://www.senado.gov.br/atividade/const/con1988/CON1988_05.10.1988/art_216_.asp>. Acesso em: 22 jan. 2018.
[114] Disponível em: < http://siga.arquivonacional.gov.br/index.php/finalidade>. Acesso em: 17 out. 2018.

O e-ARQ descreve um conjunto de exigências a serem cumpridas por um programa de gestão arquivística de documentos, a saber:

a) organicidade - o documento arquivístico caracteriza-se pelas relações que mantém com os demais documentos do órgão ou entidade e que refletem suas funções e atividades. Os documentos arquivísticos não são coletados artificialmente, mas estão ligados uns aos outros por um elo que se materializa no plano de classificação, que os contextualiza no conjunto ao qual pertencem;

b) unicidade - o documento arquivístico é único no conjunto documental ao qual pertence. Podem existir cópias em um ou mais grupos de documentos, mas cada cópia é única em seu lugar, porque o conjunto de suas relações com os demais documentos do grupo é sempre único;

c) confiabilidade[115] - um documento arquivístico confiável é aquele que tem a capacidade de sustentar os fatos que atesta. A confiabilidade está relacionada ao momento em que o documento é produzido e à veracidade do seu conteúdo. Para tanto, há que ser dotado de completeza[116] e ter seus procedimentos de produção bem controlados;

d) autenticidade - um documento arquivístico autêntico é aquele que é o que diz ser, independentemente de se tratar de minuta, original ou cópia, e que é livre de adulterações ou qualquer outro tipo de corrupção. Enquanto a confiabilidade está relacionada ao momento da produção, a autenticidade está ligada à transmissão do documento e à sua preservação e custódia. Em um documento autêntico devem ser garantidas sua identidade[117] e integridade[118];

e) acessibilidade - um documento arquivístico acessível é aquele que pode ser localizado, recuperado, apresentado e interpretado (CONARQ, 2011, 2014).

---

[115] No caso, confiabilidade é sinônimo de fidedignidade, tradução do termo em inglês *reliability*.
[116] Completeza refere-se à presença, no documento arquivístico, de todos os elementos intrínsecos e extrínsecos exigidos pela organização produtora e pelo sistema jurídico-administrativo ao qual pertence, de maneira que esse mesmo documento possa ser capaz de gerar consequências.
[117] Identidade refere-se a atributos que caracterizam o documento arquivístico e o distinguem dos demais. Esses atributos constituem-se nos elementos intrínsecos da forma documental e nas anotações.
[118] Integridade refere-se ao estado dos documentos que se encontram completos e não sofreram nenhum tipo de corrupção ou alteração não autorizada nem documentada.

Levando-se em consideração que um dos focos da presente pesquisa trata das entidades governamentais, percebe-se alinhamento natural com os documentos que surgem no decorrer das atividades (criação e registro) de uma pessoa jurídica, gerando um vínculo orgânico e perene entre eles. Destaca-se, assim, o valor primário do documento: “Valor atribuído a documento em função do interesse que possa ter para a entidade produtora, levando-se em conta a sua utilidade para fins administrativos, legais e fiscais” (CONARQ, 2014, p. 34).

No entendimento de Innarelli (2015), o documento arquivístico digital trouxe novos problemas e desafios, principalmente no que diz respeito à sua preservação ao longo do tempo, tema abordado na próxima seção.

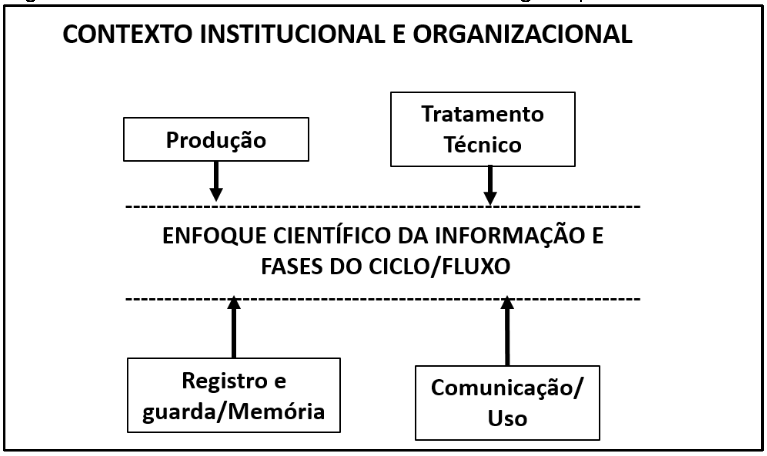
### *6.2.2 Desafios da Gestão na Ciência da Informação*

A transição para a denominada era digital, aliada ao novo paradigma (Pós-Custodial, Informacional e Científico) da CI, vem trazendo complexos desafios para a Gestão da informação, mas também excelentes oportunidades de amadurecimento, ampliação e solidificação das bases da GI e da própria Ciência da Informação.

Evocando a dinâmica transdisciplinar da ciência da Informação, Silva (2009a) propõe o estudo científico da gestão da informação, por meio de uma abordagem dos problemas relativos às principais fases do ciclo/fluxo infocomunicacional, sintetizados na figura 14 e que compreende um conjunto de quatro atividades:

a) produção - definição da lógica processual, dos objetivos ao se produzir a informação e do suporte para os registros, além das consultas às fontes de informação e da introdução dos dados;
b) tratamento técnico - utilização de formas de classificação e de indexação que permitam localizar e identificar a informação;
c) registro e guarda/memória - inserção e armazenamento de Informação e dos metadados (materialização - analógica ou digital - do conhecimento);
d) comunicação/uso - disseminação (por meio de plataformas digitais) e instrumentos de recuperação da informação.

Figura 14 - Estudo científico da GI – abordagem problemas




Fonte: Silva (2009a, p. 243)

A gestão da informação em meio digital suporta-se em uma base tecnológica estruturada para que se produza, armazene, recupere, dissemine, comunique e se transforme a informação, denominada 'Plataforma Digital'. Segundo Cunha e Cavalcanti (2008, p. 284), plataforma (*platform*), no âmbito da informática, refere-se a "conjuntos de equipamentos, sistema operacional e programas que são processados em um sistema informático". No campo das ciências da comunicação e da informação (CCI), entende-se:

> como o 'espaço de inscrição e de transmissão' da informação humana e social visível no *écran* do computador e gravada/inscrita no respectivo disco rígido e memória, de forma que possa ser comunicada. Trata-se de um 'espaço' tecnológico que, na essência, continua a ser constituído de *hardware* e *software*, mas no qual convergem diversas tecnologias e serviços com o fim de torná-lo um instrumento de mediação infocomunicacional". A plataforma digital não se esgota, pois, num mero registro tecnológico, embora seja sinônimo ou equivalente ao sentido que se dá a um sistema informático, mas vai mais além, porque ganha sua plena inteligibilidade dentro de sistema de informação (PASSARELLI *et al*, 2014, p. 116).

De acordo com a *Estratégia Brasileira para a Transformação Digital*, não há uma definição padrão e única de "plataforma digital". De forma genérica, o termo refere-se a variados serviços e a funcionalidades disponibilizados pela Internet tais como: mecanismos de busca, mídia social, plataformas de comércio eletrônico, lojas de aplicativos *online*, *sites* de comparação de preço, entre outros.

De forma genérica, as plataformas podem ser definidas pelas características em comum, como:

a) capacidade de facilitar transações diretas ou indiretas entre usuários e de extrair valores dessas transações;
b) habilidade de coletar, usar e processar grandes quantidades de dados pessoais e não pessoais, com a finalidade de otimizar a experiência do usuário;

c) capacidade de construir redes nas quais cada usuário adicional aprimora a experiência de todos os demais usuários – “efeito rede”;
d) habilidade de criar e moldar novos mercados em arranjos mais eficientes, que tragam benefícios a todos os usuários, atuando de maneira disruptiva sobre os mercados tradicionais;
e) habilidade de organizar novas formas de participação social baseada na coleta, processamento, alteração e edição de informação;
f) dependência das tecnologias de informação como meio de alcançar as capacidades acima (BRASIL, 2018d, p. 75).

Na avaliação de Maria Manuela Pinto, a gestão da informação caracteriza-se como área de estudo transversal e interdisciplinar com interesses na representação da informação, no comportamento informacional dos consumidores e na produção/concessão das plataformas digitais, contemplando, assim, três dimensões, nomeadamente: a social e humana, a informacional e a tecnológica. A investigadora sintetiza GI da seguinte forma:

> consiste no estudo, conceção, implementação e desenvolvimento dos processos e serviços inerentes ao Fluxo Infocomunicacional, permitindo a construção de Modelos de Operacionalização de máxima eficiência e rentabilização” (PINTO, 2015, p. 547).

A supracitada autora, no decorrer de sua investigação acerca da Gestão da Informação na perspectiva da CI, apresenta, analiticamente, a GI como um conjunto de processos desenvolvidos de forma contínua e interatuando em dois níveis, nomeadamente: ‘Ação’ e ‘Diagnóstico’. O primeiro nível compõe-se de: (i) comunicação e usos, (ii) armazenamento e preservação, (iii) processamento e avaliação e (iv) produção e criação; enquanto o nível diagnóstico abrange: (i) concepção/manutenção, plataformas informacional e tecnológica e processos, e (ii) análise e alinhamento institucional/organizacional estratégico, tático e operacional (PINTO, 2015, p. 548-549).

No entendimento deste pesquisador, os desafios da GI na CI, que se refletem diretamente no presente estudo, concentram-se, justamente, na integração entre teoria e prática, assim como na interação entre diagnóstico (passado), a situação atual eivada de dinamismo (presente) e as projeções ou tendências especulativas (futuro), bem como na viabilidade da ação (presente/futuro), encontrando alinhamento e respaldo nas investigações da pesquisadora antes citada.

## 6.3 Preservação Digital

Neste subcapítulo, a Preservação Digital (PD) foi analisada como um dos vetores norteadores da Ciber Proteção, sendo reconhecida como um conjunto de práticas imprescindíveis ao funcionamento administrativo da Organização que produziu a informação/documento digital, assim como base fundamental para as relações econômicas, sociais e históricas (memória e patrimônio cultural)[119] de um Estado-Nação.

Ao relacionar preservação digital com memória, história e cultura, a historiadora social Maria Tavares adverte que:

> em comparação com os vestígios históricos registrados em suportes duráveis, os conteúdos informacionais digitais, para que venham a se constituir em referências de sua época, dependerão não só dos métodos de análise vinculados a saberes específicos para sua interpretação ou decodificação, mas dependerão também de estratégias continuadas que garantam a legibilidade futura de dados diante do caráter de superação acelerada das tecnologias (TAVARES, 2012, p. 13).

O entendimento do termo ‘preservação’ está alinhado à definição do Arquivo Nacional da Austrália (AUSTRÁLIA, 2016): “[...] Preservação engloba o monitoramento ambiental, **segurança** [grifo nosso], criação, armazenamento, manuseio e planejamento de desastres para os registros em todos os formatos, incluindo documentos digitais “[120].

De acordo com o *Glossário de Documentos Arquivísticos Digitais* do CONARQ (2014, p. 29), preservação digital seria um: “conjunto de ações gerenciais e técnicas exigidas para superar as mudanças tecnológicas e a fragilidade dos suportes, garantindo o acesso e a interpretação de documentos digitais pelo tempo que for necessá-

---

[119] De acordo com o Art. 216 da Constituição da República Federativa do Brasil, constituem patrimônio cultural brasileiro os bens de natureza material e imaterial, tomados individualmente ou em conjunto, portadores de referência à identidade, à ação, à memória dos diferentes grupos formadores da sociedade brasileira, explicitando, no seu primeiro parágrafo, que o Poder Público, com a colaboração da comunidade, promoverá e protegerá o patrimônio cultural brasileiro, por meio de inventários, registros, vigilância, tombamento e desapropriação, e de outras formas de acautelamento e preservação. Disponível em: <https://www.senado.gov.br/atividade/const/con1988/CON1988_05.10.1988/art_216_.asp>. Acesso em: 22 jan. 2018.

[120] *Preservation encompasses environmental control, security, creation, storage, handling, and disaster planning for records in all formats, including digital records.*

rio”. Cunha e Cavalcanti (2008, p. 290) compilam PD como: "processo de armazenamento, em condições adequadas para uso, de documentos ou objetos produzidos em formato digital".

Com relação à visão sistêmica do modelo de Ciber Proteção, encontra-se a definição de Maureen Pennock para preservação digital:

> conjunto de ações e intervenções requeridas para garantir o acesso (contínuo e confiável) aos objetos digitais autênticos, ao longo do tempo em que forem considerados válidos. Isso abrange tanto as atividades técnicas quanto as questões estratégicas e organizacionais que implicam a sobrevivência e o gerenciamento de material digital (PENNOCK, 2006d *apud* MÁRDERO ARELLANO, 2017)[121].

Neste sentido, Sergio Silva (2008) destaca a tendência mundial de considerar a preservação no seu sentido amplo e abrangente, envolvendo opções políticas e tecnológicas, como a formatação de suportes por meio da digitalização. Tais medidas possibilitariam a transmissão e comunicação da informação ao longo do tempo, garantindo a disponibilidade do suporte. Segundo o pesquisador, a preservação contínua e em longo prazo precisa acontecer no momento da produção da informação e acompanhá-la ao longo de todo o seu percurso funcional de trâmite e utilização.

### *6.3.1 A Preservação Digital e a Tecnologia da Informação*

No que tange à infraestrutura tecnológica necessária ao gerenciamento da preservação digital, Márdero Arellano (2008, p. 153) constata que a mesma se refere "à combinação de estratégias (procedimentos, protocolos, documentação, redes, **medidas de segurança** [grifo nosso], *workflow)*, o pessoal [...], os equipamentos (*hardware, software* e mídias de armazenamento) e outros meios [...]".

No contexto de que informação digital necessita de igual, ou mesmo, maior cuidado de preservação do que a analógica, Santos corrobora:

> a tecnologia que permitiu a expansão do uso de correspondências eletrônicas e das redes sociais elevou exponencialmente a produção documental, todavia, pela fragilidade dessas tecnologias e a falta de controle dos usos desses recursos tornaram voláteis muitos registros de interesse institucional (SANTOS, 2012, p. 123).

---

[121] Disponível em: <https://www.slideshare.net/redecariniana/os-desafios-da-preservao-de-documentos-digitais>. Acesso em: 22 jan. 2018.

Referindo-se à gestão da preservação de documentos arquivísticos digitais, Humberto Innarelli alerta:

> o menosprezo em relação aos documentos arquivísticos, pode, no caso do digital, ser mais crítico, pois, diferentemente dos convencionais, os documentos são "pulverizados" na forma de dígitos binários, tornando-se "virtuais" nas mãos de seus gestores e preservadores, fator que atualmente é motivo de preocupação por parte dos profissionais de arquivo e das próprias instituições [...]. Agora, aparentemente, com o documento digital e a dita "virtualização" dos mesmos, tudo "foge" do controle e as variáveis de gestão e preservação parecem intermináveis. Neste sentido, a preservação digital é um grande desafio a ser superado, pois o conhecimento registrado em documentos arquivísticos digitais depende das nossas ações tomadas no presente (INNARELLI, 2015, p. 95).

Nesse contexto, Howard Besser, dentre os fatores causadores de problemas na longevidade digital, destaca:

> normalmente, a informação digital é codificada e para que seja visualizada requer um *software* aplicativo que roda em determinado sistema operacional, que, por sua vez, necessita de uma plataforma de *hardware* específica. Normalmente, é armazenada em dispositivos físicos (como um *drive* de disco rígido, disco flexível ou CD-ROM), que requer um tipo específico de *driver* conectado a um tipo específico de computador (BESSER, 2010, p. 59).

No que se refere às tecnologias utilizadas em conjunto com a informação, Gleick (2013, p. 20) propõe a seguinte reflexão:

> à sua época, cada nova tecnologia da informação levou a avanços em seu armazenamento e sua transmissão. Da prensa de tipos móveis surgiram novos modelos de organizadores da informação: dicionários, enciclopédias, almanaques – compêndios de palavras, classificadores de fatos, árvores do conhecimento. As tecnologias da informação dificilmente se tornam obsoletas. Cada nova tecnologia traz para as suas antecessoras um alento.

A reflexão de Gleick está repleta de sentido, mas, também, no nosso entendimento, traz complexas transformações seguidas de inéditos desafios no que tange à preservação da informação, em especial nas bases de dados dos sistemas automatizados.

Complementando, Márdero Arellano (2008) descreve algumas estratégias de preservação em curto prazo (cópias da sequência de *bits*, rejuvenescimento, replicação, preservação da tecnologia) e de médio e longo prazo (migração, canonização, emulação) compiladas a seguir:

a) cópias da sequência de *bits* - preservar a sequência básica de dados binários que representa a informação armazenada no sistema de informação digital, garantindo que o arquivo continue exatamente o mesmo com o passar do tempo enquanto a mídia física evolui;

b) rejuvenescimento (*refreshing*) - envolve mover periodicamente um arquivo de uma mídia física de armazenamento para outra, a fim de evitar a decadência física ou a obsolescência do meio;

c) replicação - uma forma de proteção contra a perda por via múltiplas cópias. As cópias de segurança já são tradicionais, mas não protegem contra uma queda organizacional;

d) preservação da tecnologia – refere-se ao computador, aos sistemas operacionais, à aplicação de *softwar*e original e a um considerável investimento em equipamento e pessoal;

e) migração - é muito mais complexa do que apenas transferir o *bitstream* de uma mídia para outra. A estrutura interna e o conteúdo do material devem ser preservados e transferidos igualmente para que, dessa forma, o "novo" objeto seja uma representação fiel do original;

f) canonização - determina a manutenção das características essenciais de um documento na conversão de um formato para outro, com a criação de uma representação de um objeto digital que mantém todos seus atributos-chave;

g) emulação - desenvolvimento de técnicas para garantir a longevidade do *software*, como encapsulamento de documentos, seus metadados, *software*, e especificações de emulador de forma a assegurar sua coesão e prevenir sua corrupção.

Ainda sobre problemas de preservação digital, particularmente do uso da Internet, Ramón Alberch destaca:

> o uso de sistemas de hipertexto e multimídia para difusão permite que o usuário navegue entre o conteúdo de um aplicativo, ligando-se com outros documentos, registros e programas. Devemos também dizer que o uso de páginas *web* como fonte de informações requer um esforço de atualização quase contínuo de seus conteúdos. A natureza torrencial e mutante das informações publicadas na Internet sugere que muito do que é introduzido pode ter uma duração altamente efêmera (ALBERCH, 2003, p. 166, tradução nossa) [122].

---

[122] *El uso de sistemas hipertexto y multimedia para la difusión permite al usuario navegar entre el contenido de una aplicación y enlazar con otros documentos, fichas y programas. También hay que decir que el uso de páginas web como fuente de información requiere un esfuerzo de actualización casi continua de sus contenidos. El carácter torrencial y cambiante de las informaciones puestas en Internet hace pensar que una buena parte de lo que se introduzca puede tener una duración altamente efímera.*

De fato, levantamento realizado pela empresa BigWeb[123], em 2015, constatou que o tempo médio de vida útil de um sítio na internet (*site*) é de apenas três meses. A pesquisa foi realizada por intermédio da plataforma BigData Corp, analisando e correlacionando dados de mais de 90 milhões de *sites* e 320 bilhões de páginas *web*. No caso, considerou-se que um *site* está "morto" quando não possui atividade, como postagem ou atualização, durante um mês inteiro.

No entendimento de Tavares, o tema da preservação digital, também, está ligado à dominância e à transversalidade do meio eletrônico nas práticas cotidianas da vida, constatando que:

> duas vertentes de preservação estão em debate: a que remete ao uso das tecnologias digitais para preservar e disseminar conteúdos originariamente contidos em suportes materiais, portanto tratados como documentos, e a segunda que se reporta à profusa produção de informação digital elaborada em sistemas informatizados, em computadores pessoais ou dispositivos móveis, que será irrecuperável no futuro diante da própria obsolescência tecnológica dos meios em que a informação foi gerada (TAVARES, 2012, p. 9).

Em entrevista concedida a *Revista Acervo*, Luciana Duranti, fundadora e diretora do Projeto InterPARES, ao abordar as ameaças futuras ou que ainda persistem sobre o impacto das TI nos princípios e práticas arquivísticas, elencou diversas inquietações. Dentre aquelas, intrinsicamente, relacionadas com o tema da presente tese, destacam-se:

a) o impressionante volume de dados e de documentos arquivísticos, bem como sua avaliação e destinação;
b) a confiabilidade de dados e de documentos arquivísticos nos novos e emergentes contextos, com destaque para o ambiente de nuvem (incluída a questão da jurisdição);
c) a habilidade para controlar o que as pessoas (continuam sendo o elo mais fraco da corrente) fazem no curso normal de suas atividades;
d) os conflitos de direitos (direito ao acesso e à privacidade, direito à memória e ao esquecimento, direito à propriedade intelectual e econômica, direito ao conhecimento etc.);

---

[123] Disponível em: <http://convergecom.com.br/tiinside/webinside/02/09/2015/tempo-medio-de-vida-util-de-um-site-e-de-apenas-tres-meses-diz-estudo/>. Acesso em: 04 nov. 2016.

e) a necessidade de manutenção e preservação de ambientes híbridos;

f) a crescente adoção pelas instituições de políticas que permitem aos empregados usarem seus próprios dispositivos e suas próprias nuvens (BYOD e BYOC[124]) (DURANTI, 2015, p. 12).

Dentre as principais preocupações, Duranti destaca o uso da "nuvem" para armazenar e gerenciar os documentos arquivísticos, o que está crescendo a cada dia:

> preservação permanente em um ambiente de nuvem está muito relacionada à custódia e ao controle. Os arquivos têm que proteger a identidade e a integridade dos materiais pelos quais são responsáveis e por meio dos quais os produtores – indivíduos, corporações e governos – são responsabilizados. [...]Em geral, a identidade, a integridade e o histórico da preservação de documentos arquivísticos digitais são verificados por meio de metadados. Em um ambiente de nuvem, os metadados de identidade (por exemplo, nomes do autor, do destinatário e outros interessados, nome da ação ou assunto, data de produção e de recebimento, código de classificação ou número de registro, forma documental, formato tecnológico etc.) acompanham o documento ao qual estão relacionados desde a produção, uma vez que nascem junto com ele e, com ele, constituem o "documento arquivístico". No entanto, os metadados de gestão – que são relacionados ao uso e às ações realizadas nos documentos ao longo do tempo, bem como às consequentes transformações tecnológicas e estruturais dos documentos à medida que passam da produção, uso e manutenção para a preservação (frequentemente por meio de criptografia, conversões e migrações etc.) – são adicionados pelo provedor de nuvem que armazena os documentos (DURANTI, 2015, p. 15-16).

Para Vint Cerf (WCTI, 2016), considerado "um dos pais da Internet", a preservação é uma questão fundamental que pode afetar o futuro da Internet, levando a uma situação de perda de memória, a qual denominou de "a era negra da Internet". No seu entendimento, diversas atividades já deveriam estar em curso, de forma global e cooperativa, visando, basicamente, assegurar:

a) a disponibilidade de mecanismos de "leitura";

b) que os arquivos digitais antigos possam rodar nos novos *softwares* que serão desenvolvidos;

c) a emulação de *hardware*, sistemas operacionais e *softwares* em máquinas virtuais;

d) um padrão mundial de documentos digitais que perdure por décadas;

---

[124] Traga seu próprio equipamento e traga sua própria nuvem - BYOD (*Bring your own device*) e BYOC (*Bring your Own Cloud).* Informações adicionais disponíveis em: <https://www.ibm.com/developerworks/community/blogs/ctaurion/entry/sua_empresa_esta_preparada_para_o_byod?lang=en>. Acesso em: 11 nov. 2016.

e) a continuidade dos domínios de conteúdos na Internet, que atualmente não são *links* permanentes e podem ser alterados.

Na oportunidade, Vint Cerf, também, destacou que a longevidade do mundo digital está diretamente relacionada à capacidade de preservação de arquivos, pois se acredita que os “*bits*” são indestrutíveis, além de subestimar o que realmente será importante daqui a cem anos, ou seja, como definir corretamente quais documentos devem ser conservados para as futuras gerações (WCTI, 2016).

Tais observações de Vint Cerf vêm reforçar a relevância da abordagem interativa dos temas: segurança no ciberespaço e preservação digital ao longo da pesquisa, pois eles constituem a base para a consolidação do conceito de Ciber Proteção, pedra angular desta tese.

### *6.3.2 A PD governamental – uma abordagem*

Ao tratar das complicações inerentes à preservação arquivística governamental, Sergio Silva (2008, p. 12) aponta que, em um primeiro momento, as perdas dos registros digitais acontecem da mesma forma que os convencionais: “ocorrem no universo microscópio, em um processo lento e silencioso, sendo, no início, imperceptíveis”. Segundo o autor, a grande diferença reside em que a preservação dos registros digitais “não contempla a possibilidade do acaso, pois depende de escolhas e decisões anteriores, que remetam ao momento em que a informação é produzida”.

No ano de 2004, a *Carta para preservação do patrimônio arquivístico digital do Conselho Nacional de Arquivos*, ao abordar a fragilidade intrínseca do armazenamento digital, já alertava:

> a tecnologia digital é comprovadamente um meio mais frágil e mais instável de armazenamento, comparado com os meios convencionais de registrar informações, tendo um impacto profundo sobre a gestão dos documentos digitais no presente para que se tenha garantia de acesso no futuro (CONARQ, 2004, p. 3).

Passada uma década, o mesmo CONARQ aprovou as *Diretrizes para a Implementação de Repositórios Arquivísticos Digitais Confiáveis* (RDC-Arq), para o arquivamento e manutenção dos documentos arquivísticos[125] em formato digital em todo o seu ciclo de vida, de forma a garantir: a autenticidade (identidade e integridade), a confidencialidade, a disponibilidade e a preservação desses documentos, tendo em vista a perspectiva da necessidade de manutenção dos acervos documentais por longos períodos de tempo ou, até mesmo, permanentemente.

O CONARQ, objetivando garantir o acesso de longo prazo a documentos arquivísticos autênticos por meio da implementação do RDC-Arq, estabeleceu os seguintes Princípios de preservação digital:

a) focar especificamente em documentos arquivísticos e não em objetos digitais de forma genérica;
b) focar em documentos arquivísticos digitais autênticos;
c) pressupor que a autenticidade dos documentos arquivísticos digitais está sob ameaça, principalmente, no momento da transmissão no espaço (entre pessoas e sistemas) e no tempo (atualização/substituição de *hardware* e *software* usados para armazenar, processar e comunicar os documentos);
d) reconhecer que a preservação digital é um processo contínuo, que começa na concepção do documento;
e) reconhecer que a autenticidade dos documentos arquivísticos digitais tem por base os procedimentos de gestão e preservação e a confiança tanto no repositório como no órgão responsável pela guarda desses documentos;
f) arbitrar o que se considera como documento original, uma vez que a preservação digital implica a necessidade de conversão de formatos e atualização de suportes;
g) reconhecer que a elaboração de manuais e os procedimentos de preservação desempenhados pelo repositório digital apoiam a presunção de autenticidade desses documentos;

[125] Os documentos arquivísticos caracterizam-se por registrarem e apoiarem as atividades do órgão ou entidade, servindo de evidência dessas atividades, bem como de fonte de informação para a pesquisa, e para assegurar os direitos dos cidadãos.

h) reconhecer que o registro, em metadados, das intervenções de preservação em cada documento apoia a presunção de autenticidade desses documentos;

i) reconhecer que a autenticidade dos documentos digitais deve ser avaliada e presumida no momento de sua submissão ao repositório;

j) reconhecer que o repositório digital é responsável pela manutenção permanente da autenticidade dos documentos a ele submetidos;

k) distinguir claramente a autenticidade e autenticação de documentos, considerando que a primeira é a qualidade de o documento ser verdadeiro, e a segunda é uma declaração dessa qualidade, feita, em um dado momento, por uma pessoa autorizada para tal. (CONARQ, 2015, p. 10-11).

Em decorrência do exposto, os arquivos devem dispor de repositórios digitais[126] confiáveis para a gestão, a preservação e o acesso de documentos digitais, levando-se em consideração que os mesmos sofrem diversas ameaças decorrentes da fragilidade inerente aos objetos digitais, da facilidade de adulteração no momento da transmissão em rede (entre pessoas e sistemas) e da rápida obsolescência tecnológica, particularmente quanto ao *hardware*/*software* usados para armazenar, processar e comunicar os documentos (CONARQ, 2015).

Em complemento, Charlley Luz (2016) considera que a fidedignidade e autenticidade do documento arquivístico é garantida pela credibilidade em sua cadeia de custódia por meio de sistemas de informação de arquivo confiáveis, tanto na gestão como na guarda permanente. Tal tarefa requer que as informações geradas no documento, além daquelas sobre seu contexto de criação sejam preservadas, desde a gênese documental por meio de diferentes técnicas de empacotamento e identificação dos conjuntos documentais.

---

[126] É um ambiente de armazenamento e gerenciamento de materiais digitais. Esse ambiente constitui-se de uma solução informatizada em que os materiais são capturados, armazenados, preservados e acessados. É formado por elementos de *hardware*, *software* e metadados, bem como por uma infraestrutura organizacional e procedimentos normativos e técnicos.

Ainda no contexto governamental da PD, particularmente no da pesquisa, destaca-se a Rede de Serviços de Preservação Digital – Cariniana[127], do Instituto Brasileiro de Informação em Ciência e Tecnologia (IBICT). A rede Cariniana surgiu da necessidade de se criar, no IBICT[128], uma rede de serviços de preservação digital de documentos eletrônicos brasileiros, com o objetivo de garantir seu acesso contínuo a longo prazo. A Cariniana possui mais de 10 grupos de pesquisa em áreas diversificadas, por exemplo *Big data*, Curadoria, Preservação e Políticas. Desse modo, integra conteúdos digitais das instituições de maneira consorciada, promovendo o compartilhamento de estudos e pesquisas.

O projeto de implantação da Rede de preservação digital foi elaborado em uma infraestrutura descentralizada, utilizando recursos de computação distribuída, baseada na participação das instituições detentoras desses documentos e de sua infraestrutura e em ambiente padronizado e de segurança que garanta o acesso permanente e o armazenamento monitorado dos documentos digitais[129]. Para tanto, no início do ano de 2013, o IBICT aderiu ao Programa LOCKSS[130], como um processo ativo de preservação onde cópias são validadas automaticamente em diferentes locais.

De acordo com Miguel Márdero Arellano (2017, p. 219), coordenador da Rede Cariniana,

> a adoção de um modelo de rede de preservação digital é uma alternativa para organizações que querem coletar, armazenar, preservar e oferecer acesso à sua coleção em cópias digitais. Também é essencial combinar essas redes com os padrões internacionais já testados e promover a preservação digital da produção científica a longo prazo.

---

[127] Exemplos adicionais de repositórios de dados de pesquisa nacionais: (i) Repositório de Dados do Programa de Pesquisa de Biodiversidade da Amazônia Ocidental (PPBIO), (i) Repositório de Dados do Programa de Pesquisas Ecológicas de Longa Duração (PELD), (iii) Portal GEOINFO de infraestrutura de dados espaciais da Embrapa, (iv) Portal da Biodiversidade (SISBio) e o (v) CarpeDIEN (Dados e Informações em Engenharia Nuclear) (COSTA; CUNHA; BOERES, 2017).

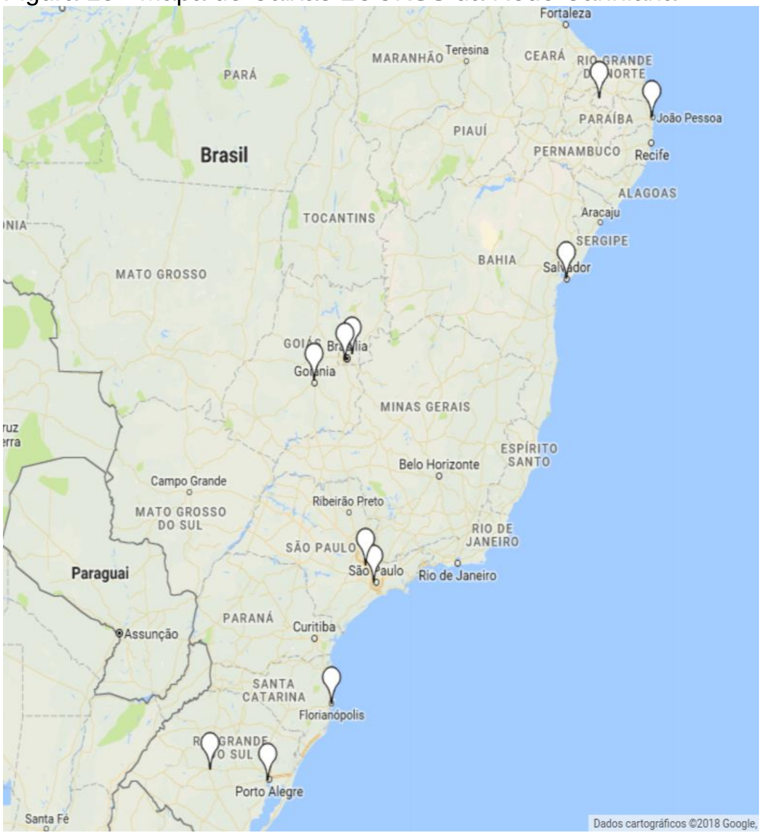
[128] Órgão nacional de informação, unidade de pesquisa do Ministério da Ciência, Tecnologia e Inovação, realiza estudos no campo da ciência da informação e temas relacionados. Maiores informações em: http://www.ibict.br/sobre-o-ibict. Acesso em: 22 jan. 2018.

[129] Informações complementares disponíveis em: <http://cariniana.ibict.br/index.php/inicio>. Acesso em: 22 jan. 2018.

[130] LOCKSS - *Lots Of Copies Keep Stuff Safe* é um programa da Universidade de Stanford, EUA, que fornece *softwares* livres de preservação digital premiados e de baixo custo para bibliotecas e editoras, com vista à preservação de conteúdos digitais permanentes e originais, assim como à garantia de acesso a esses acervos. Maiores esclarecimentos disponíveis em: <http://cariniana.ibict.br/index.php/inicio>. Acesso em: 22 jan. 2018.

Em 2015, iniciaram-se os trabalhos para a criação de um serviço de preservação de dados na rede Cariniana. O projeto do serviço de PD de dados de pesquisa da Cariniana está direcionado à replicação de cópias dos dados armazenados nos repositórios das instituições parceiras. Obtém-se, assim, a guarda segura de pelo menos quatro cópias dos documentos digitais em instituições geograficamente distantes[131], por meio do sistema de arquivamento por 'caixas', baseando-se no padrão LOCKSS. Tais 'caixas' estão situadas no próprio IBICT e em universidades públicas, de acordo com a figura 15, tendo seus metadados verificados por um servidor *web* localizado na Stanford University.

Figura 15 - Mapa de Caixas LOCKSS da Rede Cariniana




Fonte: <http://cariniana.ibict.br/index.php/mapa-da-rede-lockss>

Ainda, segundo o coordenador da rede Cariniana, no quesito preservação digital, há grande distância entre as propostas de iniciativas internacionais emergentes e a situação real no Brasil, particularmente em razão da insuficiência de recursos e do planejamento inadequado das práticas para permitir o acesso de longo prazo. Márdero

[131] Disponível em: http://cariniana.ibict.br/index.php/2014-07-15-17-27-30. Acesso em: 22 jan. 2018.

Arellano (2017) reforça que a aplicação de políticas públicas voltadas para a preservação do patrimônio digital, convocando os setores públicos e privados, envolvidos com a produção e proteção especial dos documentos em formato digital, é condição fundamental para a democratização da informação no país e a preservação da memória nacional.

Nota-se que a adoção de um modelo de preservação digital traz, inclusive, elementos como: atuação em rede, redundância de base de dados, controle de acesso físico e lógico e atenção especial às vulnerabilidades e possibilidades do *hardware* e do *software,* típicos da proteção cibernética, bem como quando se observa que os conteúdos em meio digital necessitam de autenticidade, integridade e de acessibilidade a longo prazo. Percebe-se, então, um estreitamento da *interface* entre gestão da informação e preservação digital com a proteção da informação no ciberespaço, assunto a ser tratado na próxima seção.

# 7 PROTEÇÃO DA INFORMAÇÃO NO CIBERESPAÇO

No contexto desta tese, onde se levam em consideração os temas tratados anteriormente, nomeadamente as peculiaridades do ciberespaço de interesse nacional e a informação digital com suas oportunidades e desafios, adotam-se as caracterizações da Segurança Nacional brasileira, tendo como base a *Política Nacional de Defesa* (PND) (BRASIL, 2012c).

Assim, entende-se Segurança como: "condição que permite ao País preservar sua soberania e integridade territorial, promover seus interesses nacionais, livre de pressões e ameaças, e garantir aos cidadãos o exercício de seus direitos e deveres constitucionais". No que concerne à Defesa, adota-se a seguinte definição: “conjunto de medidas e ações do Estado, com ênfase no campo militar, para a defesa do território, da soberania e dos interesses nacionais contra ameaças preponderantemente externas, potenciais ou manifestas” (BRASIL, 2012c, p. 15).

Em 18 de dezembro de 2008, a Presidência da República, por meio do Decreto n. 6.703, aprovou a *Estratégia Nacional de Defesa* (END), que, no seu bojo, trouxe os seguintes tópicos relacionados à temática da presente pesquisa:

a) identifica três setores de importância estratégica para a Defesa Nacional: o espacial, o **cibernético** [grifo nosso] e o nuclear;
b) os órgãos e entidades da Administração Pública Federal (APF) deverão considerar, em seus planejamentos, ações que concorram para fortalecer a Defesa Nacional [grifo nosso];
c) **todas as instâncias do Estado deverão contribuir para o incremento do nível de Segurança Nacional** [grifo nosso], com ênfase sobre [...] o aperfeiçoamento dos dispositivos e procedimentos de segurança que reduzam a vulnerabilidade dos sistemas relacionados à Defesa Nacional contra ataques cibernéticos;
d) resguardados os interesses de segurança do Estado quanto ao acesso a informações, serão estimuladas iniciativas conjuntas entre organizações de pesquisa das Forças Armadas, **instituições acadêmicas nacionais** [grifo nosso] e empresas privadas brasileiras (BRASIL, 2008a).

No contexto da END, a Defesa Nacional exterioriza-se pela aplicação do poder nacional em ações que, de forma lesiva, possam afetar a identidade e os interesses nacionais, tais como: soberania, paz social, progresso, democracia, integração e integridade do patrimônio nacional.

Ainda em 2008, foi criada, no Gabinete de Segurança Institucional da Presidência da República (GSI), a Rede Nacional de Segurança da Informação e Criptografia (RENASIC)[132].

A RENASIC possui como propósito elevar a competência brasileira em Segurança da Informação e Criptografia ao nível dos países mais desenvolvidos em Ciência e Tecnologia, pelo estabelecimento e efetivo aumento da integração das pesquisas brasileiras que acontecem nas universidades, institutos de pesquisa, órgãos governamentais e empresas.

Dentre os objetivos da RENASIC destacam-se:

a) estabelecimento de um nível de excelência das pesquisas nacionais nas áreas de Segurança da Informação e de Criptografia;
b) fortalecimento e integração das pesquisas no Brasil, diminuindo a atual fragmentação das competências e estabelecendo uma agenda de pesquisa e de projetos conjuntos nessas áreas;
c) melhoria do estado da arte, na teoria e prática, da segurança e da criptografia no Brasil, igualando-a aos grandes centros internacionais;
d) estabelecimento de Laboratórios Virtuais (Projeto RENASIC) que visem fomentar a pesquisa entre os membros da RENASIC;
e) desenvolvimento de uma infraestrutura comum que inclui:
   - ferramentas para a avaliação dos algoritmos de criptografia
   - ambientes de avaliação para *hardware* e *software* criptográficos
   - instrumentação física e lógica para análise de ataques secundários (*side-channel atacks*)
   - ferramentas para avaliação dos esquemas de defesa cibernética e forense computacional

[132] A RENASIC passou a integrar o Comando do Exército/Ministério da Defesa (EB/MD) a partir de 2011. Informações adicionais disponíveis em: <http://www.renasic.org.br/>. Acesso em: 24 nov. 2016.

O Projeto RENASIC é composto de oito subprojetos ou áreas de atuação, com um total de 39 metas e 151 atividades. Cada um desses subprojetos é gerenciado por um Laboratório Virtual (LV)[133], a saber:

a) VIRTUS - Técnicas Simétricas - Criação de um sistema de criptoanálise nacional e de ferramentas para a proteção de sistemas móveis;
b) ASTECA - Técnicas Assimétricas - Desenvolvimento de um produto de segurança corporativa;
c) PROTO – Protocolos Criptográficos Seguros – Desenvolvimento de sistemas de criptografia por chave única;
d) LATIM – Implementações Seguras - Desenvolvimento de um sistema de gestão de identidades e outro de defesa contra ataques laterais;
e) LAPAD - acesso ao processamento de alto desempenho à comunidade científica nacional;
f) QUANTA - Computação, Informação e Criptografia Quânticas;
g) LAPROJ - Acompanhamento de Projetos e Desenvolvimento de componente básico (*hardware*) do Sistema KeyBITS;
h) LABIN – Inteligência de Redes – Análise do tráfego de redes e proteção de pacotes sigilosos;
i) SALTAR - Sistema de Análise de Link e Tráfego de Dados em Redes de Comunicações;
j) LASEC2 – Desenvolvimento de ferramentas para Segurança Eletrônica, de Comunicações e Cibernética.

No final do ano de 2009, o Decreto n. 7.009, de 12 de novembro, inclui o tema segurança cibernética nos objetivos da Câmara de Relações Exteriores e Defesa Nacional – CREDEN[134] do Conselho de Governo. Tal inclusão foi consequência direta dos trabalhos desenvolvidos pelo Grupo Técnico de Segurança Cibernética instituído

---

[133] Além dos grupos de desenvolvimento no âmbito dos Laboratórios Virtuais, fazem parte da estrutura da RENASIC: um Comitê Diretor, um Comitê Técnico Científico e Entidades Associadas que podem ser: governamentais ou privadas; pequenas, médias ou grandes; nacionais ou internacionais.

[134] A CREDEN assessora o Conselho de Governo e possui como finalidade tratar de matérias como a cooperação internacional em assuntos de segurança e defesa, segurança para infraestruturas críticas, segurança da informação e segurança cibernética (BRASIL, 2015).

pela Portaria CREDEN n. 45, de 8 de setembro de 2009, com o objetivo de propor diretrizes e estratégias para a segurança cibernética, no âmbito governamental.

Passados quatro anos, o Congresso Nacional aprovou as propostas da *Política Nacional de Defesa* (PND), atualizando em 2013 a Estratégia Nacional de Defesa (END) e aprovando o *Livro Branco da Defesa Nacional* (LBDN).

A *Política Nacional de Defesa* é o documento condicionante de mais alto nível do planejamento de ações destinadas à defesa nacional, sendo voltada, essencialmente, para ameaças externas à segurança, bem como pressupondo que a defesa do país é inseparável do seu desenvolvimento. A PND estabelece objetivos e orientações para o preparo e o emprego dos setores militar e civil em todas as esferas do Poder Nacional, sendo, portanto, de interesse de todos os segmentos da sociedade brasileira e um dever de todos os brasileiros. Dentre as suas orientações, destaca-se:

> para se opor a possíveis ataques cibernéticos, é essencial aperfeiçoar os dispositivos de segurança e adotar procedimentos que minimizem a vulnerabilidade dos sistemas que possuam suporte de tecnologia da informação e comunicação ou permitam seu pronto restabelecimento (BRASIL, 2012c, p. 34).

De acordo com a PND, os avanços da tecnologia da informação, a utilização de satélites, o sensoriamento eletrônico e outros aperfeiçoamentos tecnológicos trouxeram maior eficiência aos sistemas administrativos e militares, sobretudo nos países que dedicam maiores recursos financeiros à Defesa. Em consequência, criaram-se vulnerabilidades que poderão ser exploradas, com o objetivo de inviabilizar o uso dos sistemas de interesse nacional ou facilitar a interferência à distância.

No seu primeiro eixo estruturante, a *Estratégia Nacional de Defesa* define que as três forças armadas devem operar em rede entre si e em ligação com o monitoramento do território, do espaço aéreo e das águas jurisdicionais brasileiras. O provimento de tecnologia de comunicação, para assegurar essa capacidade de atuar em rede, é efetuado no âmbito do Setor Cibernético de Defesa, que, da mesma forma que com os setores nuclear e espacial, transcende “a divisão entre desenvolvimento e defesa, entre o civil e o militar” (BRASIL, 2012c, p. 49).

O cenário cibernético nacional permaneceu em constante evolução, destacando-se o Grupo de Trabalho Interministerial (GTI) sobre segurança e defesa do espaço cibernético nacional em 2013.

O GTI, coordenado pela Secretaria de Assuntos Estratégicos da Presidência da República (SAE), objetivou elaborar uma proposta de Plano Estratégico, para promover ou subsidiar o aperfeiçoamento das políticas públicas voltadas à segurança e à defesa do espaço cibernético nacional (BRASIL, 2013). Na sua composição, observa-se um grupo heterogêneo composto por instituições de governo, agências reguladoras, empresas públicas e entidades civis, exemplificadas a seguir:

a) Ministério da Defesa;
b) Ministério das Relações Exteriores;
c) Ministério do Planejamento, Orçamento e Gestão;
d) Ministério da Ciência, Tecnologia e Inovação;
e) Gabinete de Segurança Institucional da Presidência da República;
f) Agência Nacional de Telecomunicações (ANATEL);
g) Serviço Federal de Processamento de Dados (SERPRO);
h) Telecomunicações Brasileiras (TELEBRAS);
i) Núcleo de Informação e Coordenação do Ponto BR do Comitê Gestor da Internet no Brasil (NIC.br/CGI.br).

Destacam-se, ainda, como insumos evolutivos da Ciber Proteção, não só a implantação de medidas que visavam à potencialização da Defesa Cibernética Nacional em 2014 (P.ex.: o projeto de criação da EnaDCiber e a implantação do ComDCiber), mas também os marcos normativos do GSI em 2015, do MPOG em 2016/2018 e do MCTIC em 2018.

## 7.1 Segurança da Informação

No entendimento de Fernandes (2012), a segurança pode ser obtida por meio da associação de uma hierarquia de controles a um sistema. Para o autor, um sistema seguro é modelado por subsistemas hierarquicamente organizados, cada qual com controles que monitoram e regulam não só a função mais exterior do sistema, mas também todo o complexo arranjo interno do mesmo.

De acordo com o Conselho Nacional de Arquivos - CONARQ (2011, 2014), segurança é um dos requisitos para sistemas informatizados de gestão arquivística de documentos e caracteriza-se pela preservação de diversas propriedades, tais como:

integridade e disponibilidade, que, de acordo com as normas internacionais da "família" ISO/IEC 27000[135], formam, com a confidencialidade, a tríade da segurança da informação (CID). Percebe-se, assim, um elo intrínseco com questões relacionadas à gestão da Informação como: coleta, organização, estocagem, recuperação, interpretação, transmissão, transformação e uso da informação.

Em termos gerais, a Norma ISO/IEC 27000 (2014, tradução nossa) descreve as propriedades que devem ser preservadas/garantidas, a fim de se proporcionar segurança informacional. Tais propriedades são assim definidas:

a) confidencialidade (*confidentiality*) - propriedade de que a informação não esteja disponível ou revelada a indivíduos, entidades ou processos não autorizados;
b) integridade (*integrity*) - propriedade de exatidão e completeza;
c) disponibilidade (*availability*) - propriedade de estar acessível e utilizável sob demanda de uma entidade autorizada;
d) autenticidade *(authenticity)* - propriedade de que uma entidade é o que a mesma diz ser;
e) responsabilidade *(accountability)* - propriedade na qual o responsável pela informação deve prestar contas da mesma;
f) não repúdio (*non-repudiation*) - capacidade de comprovar a ocorrência de uma reivindicação de um evento ou ação e suas entidades originárias;
g) confiabilidade (*reliability*) - propriedade de que o comportamento e o resultado acham-se consistentes com a intenção.

Segundo o *Tesauro Brasileiro de Ciência da Informação*, a segurança da informação:

> está relacionada à proteção e à preservação da informação e tem por finalidade evitar alterações, intencionais ou não, nos seus atributos de confidencialidade, integridade, disponibilidade e autenticidade. Não está restrita aos recursos computacionais e independe da forma como as informações/dados se apresentam: eletrônica, impressa etc. (PINHEIRO e FERREZ, 2014).

Compilando, várias fontes por meio da interdisciplinaridade para as áreas de: informática, redes de comunicação de dados, Biblioteconomia e Arquivologia, Cunha

---

[135] Maiores informações sobre a série ISO/IEC 27000 que aborda temas sobre gestão de segurança da informação, gestão de riscos e, mais recentemente, sobre segurança cibernética consultar Vianna (2015).

e Cavalcanti (2008) definem segurança da informação como um conjunto de procedimentos para proteção do acervo informacional de uma organização contra o acesso à informação ou ao seu uso por pessoas não autorizadas.

Ainda, no âmbito da Área do conhecimento da CI, segurança da informação seria assegurar que a produção, seleção, organização, interpretação, armazenamento, recuperação, disseminação, transformação e uso da informação estivessem livres de perigos e incertezas (CAPURRO, 2003; RAMOS, 2006).

De acordo com Márdero Arellano[136], ao se definir política de segurança da informação, devem ser considerados aspectos legais, organizacionais, humanos e tecnológicos, de modo a garantir a autenticidade dos documentos digitais e o sigilo da informação, bem como a proteção contra perdas, acidentes e intervenções não autorizadas. Segundo o autor, são elementos fundamentais e orientadores de uma política sobre o tema:

a) Autenticidade: verificação de que o objeto é ou não o que se afirma sobre ele durante um processo de seleção;
b) Integridade: verificada com medidas como encriptação: assinaturas digitais, verificação de fixidez etc.;
c) Confiabilidade: credibilidade de um documento de sustentar o fato ao qual se refere, estabelecida pelo exame da completeza, da forma do documento e do grau de controle exercido no processo de sua produção;
d) Proveniência: confirmação e reunião de evidências do tempo, do lugar e da pessoa responsável pela criação, produção ou descoberta do objeto.

### *7.1.1 Segurança da informação na Administração Pública Federal*

A atividade de segurança da informação é complexa e heterogênea, particularmente no ambiente governamental, tendo sido, inicialmente, regulada pelo Decreto Presidencial n. 3.505, de 13 de junho de 2000 (BRASIL, 2000), que instituiu a *Política de Segurança da Informação* (PSI) nos órgãos e entidades da administração pública

[136] Disponível em: <http://cariniana.ibict.br/index.php/2014-07-15-17-27-30>. Acesso em: 22 jan. 2018.

federal (APF). Em consequência, desde aquela época, grupos de trabalho, estabelecidos pelo Comitê Gestor de Segurança da Informação (CGSI) instituído pelo mesmo decreto, vêm estudando as diretrizes então apontadas no referido decreto e buscando soluções para sua efetiva implementação (VIANNA, 2015). Naquela ocasião, a segurança da informação foi definida como:

> proteção dos sistemas de informação contra a negação de serviço a usuários autorizados, assim como contra a intrusão, e a modificação desautorizada de dados ou informações, armazenados, em processamento ou em trânsito, abrangendo, inclusive, a segurança dos recursos humanos, da documentação e do material, das áreas e instalações das comunicações e computacional, assim como as destinadas a prevenir, detectar, deter e documentar eventuais ameaças a seu desenvolvimento (BRASIL, 2000).

No ensejo de despertar a atenção para os aspectos da segurança de tecnologia da informação nas organizações governamentais, o Tribunal de Contas da União (TCU) compilou um guia de boas práticas quanto à segurança da informação no ano de 2007. Nesse guia, o TCU observa que a referida segurança visa garantir a integridade, confidencialidade, autenticidade e disponibilidade das informações processadas pela organização:

a) integridade - consiste na fidedignidade de informações. Sinaliza a conformidade de dados armazenados com relação às inserções, alterações e processamentos autorizados efetuados, bem como a conformidade dos dados transmitidos pelo emissor com os recebidos pelo destinatário. A manutenção da integridade pressupõe a garantia de não violação dos dados com intuito de alteração, gravação ou exclusão, seja ela acidental ou proposital;
b) confidencialidade - consiste na garantia de que somente pessoas autorizadas tenham acesso às informações armazenadas ou transmitidas por meio de redes de comunicação. Manter a confidencialidade pressupõe assegurar que as pessoas não tomem conhecimento de informações, de forma acidental ou proposital, sem que possuam autorização para tal procedimento;
c) autenticidade - consiste na garantia da veracidade da fonte das informações. Por meio da autenticação, é possível confirmar a identidade da pessoa ou entidade que presta as informações;
d) disponibilidade - consiste na garantia de que as informações estejam acessíveis às pessoas e aos processos autorizados, a qualquer momento requerido, durante o período acordado entre os gestores da informação e a área de informática. Manter a disponibilidade de informações pressupõe garantir

> a prestação contínua do serviço, sem interrupções no fornecimento de informações para quem de direito (TCU, 2007).

A Instrução Normativa n. 1, do Gabinete de Segurança Institucional da Presidência da República (IN 01/GSI), de 13 de junho de 2008 (BRASIL, 2008b), disciplinou a gestão de Segurança da Informação e Comunicações (SIC) na Administração Pública Federal, direta e indireta, determinando, entre outros assuntos, no seu Art. 5º, que aos órgãos e entidades da APF compete coordenar as ações de segurança da informação e comunicações, aprovar Política de Segurança da Informação e Comunicações e implementar equipe de tratamento e resposta a incidentes em redes computacionais (ETIR)[137].

Neste contexto, a IN 01/GSI definiu, no âmbito da APF, SIC e a sua gestão, respectivamente, como:

> ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações.
>
> ações e métodos que visam à integração das atividades de gestão de riscos, gestão de continuidade do negócio**,** tratamento de incidentes, tratamento da informação, conformidade, credenciamento, **segurança cibernética** [grifo nosso], segurança física, segurança lógica, segurança orgânica e segurança organizacional aos processos institucionais estratégicos, operacionais e táticos, não se limitando, portanto, à tecnologia da informação e comunicações (BRASIL, 2008b, p. 2).

Ampliando o escopo de atuação, a IN 01/GSI gerou um arcabouço de 21 normas complementares (NC)[138], que evidenciam a diversidade de áreas de atuação da gestão de SIC.

[137] Conhecido também como *Computer Security Incident Response Team* – CSIRTs (Time de Resposta a Incidentes de Segurança em Computadores) ou CERT - *Computer Emergency Response Team* (Time de Resposta a Emergência em Computadores). Informações complementares acerca dos procedimentos e ações referentes à gestão de incidentes de segurança nas redes de computadores da Administração Pública Federal consultar Vianna (2011).

[138] Disponível em: <http://dsic.planalto.gov.br/legislacaodsic/23-dsic/legislacao/53-normas-complementares>. Acesso em: 29 jan. 2017.

### *7.1.2 A certificação da informação em meio digital*

Uma das formas de se garantir a segurança no intercâmbio de informações, em meio digital e nas transações na Internet, é o uso da denominada certificação digital[139].

A certificação digital contribui para a SegInf, particularmente nos quesitos da autenticidade e do não repúdio. Neste contexto, Autenticidade é entendida como a qualidade de um documento ser o que diz ser, independentemente de se tratar de minuta, original ou cópia e que é livre de adulterações ou de qualquer outro tipo de corrupção; enquanto não repúdio permite a garantia de que o emissor de uma mensagem ou a pessoa que executou determinada transação de forma eletrônica não poderá, posteriormente, negar sua autoria, visto que somente aquela chave privada poderia ter gerado tal assinatura digital.[140].

No Brasil, a responsabilidade pela Certificação Digital cabe ao Instituto Nacional de Tecnologia da Informação (ITI), autarquia federal vinculada à Casa Civil da Presidência da República, por intermédio da Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil, desempenhar o papel de Autoridade Certificadora Raiz – AC-Raiz, assim como o encargo de credenciar e descredenciar os demais participantes da cadeia, supervisionar e fazer auditoria dos processos.

A ICP-Brasil é integrada por diversos entes ou autoridades: (i) Autoridade Certificadora Raiz da ICP-Brasil (AC-Raiz) como primeira autoridade da cadeia de certificação, (ii) Autoridade Certificadora (AC) como uma entidade, pública ou privada, subordinada à hierarquia da ICP-Brasil, responsável por emitir, distribuir, renovar, revogar e gerenciar certificados digitais, (iii) Autoridade de Registro (AR) sendo responsável pela interface entre o usuário e a Autoridade Certificadora. Vinculada a uma AC, e tendo por objetivo o recebimento, a validação, o encaminhamento de solicitações de emissão ou revogação de certificados digitais e identificação, de forma presencial, de seus solicitantes e (iv) Autoridade Certificadora do Tempo (ACT) sendo uma entidade

---

[139] Atividade de reconhecimento em meio eletrônico que se caracteriza pelo estabelecimento de uma relação única, exclusiva e intransferível entre uma chave de criptografia e uma pessoa física, jurídica, máquina ou aplicação". Disponível em: <http://www.iti.gov.br/glossario>. Acessado em: 17 jan. 2018.
[140] Disponível em: <http://www.iti.gov.br/glossario>. Acessado em: 17 jan. 2018.

na qual os usuários de serviços de Carimbo do Tempo confiam para emissão dos mesmos[141].

Produzida pelo ITI, a *Política de Segurança da ICP-Brasil* (DOC-ICP-02 – V 3.0, de 01 de dezembro de 2008) tem por finalidade estabelecer as diretrizes de segurança que deverão ser adotadas pelas entidades participantes da Infraestrutura de Chaves Públicas Brasileira. Na visão de Porto (2014), o DOC-ICP-02 deveria nortear todos os itens referentes à prática de certificação, incluindo a segurança física e lógica da infraestrutura, dos sistemas e dos ativos criptográficos, acompanhando o avanço tecnológico com o objetivo de evitar qualquer vulnerabilidade, ameaça e risco que possa comprometer a confiabilidade do sistema.

A Medida Provisória n. 2.200-2, de 24 de agosto de 2001, deu início à implantação do sistema nacional de certificação digital da ICP-Brasil, significando que o Brasil possui uma infraestrutura pública, mantida e auditada por um órgão público, no caso, o ITI, que segue regras de funcionamento estabelecidas pelo Comitê Gestor da ICP-Brasil, cujos membros, representantes dos poderes públicos, sociedade civil organizada e pesquisa acadêmica, são nomeados pelo Presidente da República. São competências do ITI:

a) adotar as medidas necessárias e coordenar o funcionamento da ICP-Brasil;
b) estabelecer a política, os critérios e as normas técnicas para o credenciamento das AC, das AR e dos demais prestadores de serviço de suporte à ICP-Brasil, em todos os níveis da cadeia de certificação;
c) estabelecer a política de certificação e as regras operacionais da AC-Raiz;
d) homologar, auditar e fiscalizar a AC-Raiz e os seus prestadores de serviço;
e) delegar atribuições à AC-Raiz, primeira autoridade da cadeia de certificação;
f) estabelecer diretrizes e normas técnicas para a formulação de políticas de certificados e regras operacionais das AC e das AR e definir níveis da cadeia de certificação;
g) aprovar políticas de certificados, práticas de certificação e regras operacionais, credenciar e autorizar o funcionamento das AC e das AR, bem como autorizar a AC-Raiz a emitir o correspondente certificado;

[141] Informações complementares disponíveis em: < http://www.iti.gov.br/icp-brasil/57-icp-brasil/76-como-funciona>. Acesso em: 18 jan. 2018.

h) identificar e avaliar as políticas de ICP externas, negociar e aprovar acordos de certificação bilateral, regras de interoperabilidade e outras formas de cooperação internacional, certificar, quando for o caso, sua compatibilidade com a ICP-Brasil, observado o disposto em tratados, acordos ou atos internacionais; atualizar, ajustar e revisar os procedimentos e as práticas estabelecidas para a ICP-Brasil, garantir sua compatibilidade e promover a atualização tecnológica do sistema e a sua conformidade com as políticas de segurança[142].

Em relação à Infraestrutura de Chaves Públicas Brasileira, Luís Carlos Porto esclarece:

> a adoção da certificação digital ICP-Brasil propicia a realização de mudanças em diversos setores da sociedade e promove o desenvolvimento de novos produtos e novos processos, pois provoca mudanças sociais trazendo benefícios, como por exemplo: a validade jurídica dos documentos eletrônicos.
>
> outra vertente que caracteriza a certificação digital no Brasil é a importância que ela traz na desmaterialização dos procedimentos de governo. Nesta vertente pode reduzir tempo e etapas nos processos, reduzir custos com deslocamento e outros. Pode beneficiar pessoa jurídica ou física, tanto na esfera governamental como na privada, garantindo assim melhorias, agilidade, confiabilidade, disponibilidade, autenticidade e não repúdio, assim como tornar a comunicação mais eficiente e segura, promovendo maior controle de gestão (PORTO, 2014, p. 27).

O uso da certificação digital confere uma assinatura (digital) ao usuário, através de um sistema de criptografia assimétrica e da assinatura eletrônica, com segurança jurídica (pois equipara assinatura digital à semelhante de próprio punho), proporcionando, por exemplo, a tramitação e assinatura eletrônica de documentos oficiais. Dentre os vários sistemas estruturantes nacionais, localizados em infraestruturas críticas, destacam-se:

a) Atendimento Virtual (e-CAC0 - sistema da Receita Federal que possui diversos serviços protegidos por sigilo fiscal;

b) Bacenjud - sistema acessado com certificado digital que interliga a Justiça ao Banco Central e às instituições bancárias;

---

[142] Disponível em: <http://www.iti.gov.br/icp-brasil>. Acessado em: 17 jan. 2018.

c) CNH Digital - a Carteira Nacional de Habilitação é um documento eletrônico que tem a mesma validade do documento impresso, podendo ser apresentada em aparelhos eletrônicos, como *smartphones* e *tablets*, aos agentes de trânsito, que verificarão a autenticidade do documento através da leitura do QR-Code apresentado;

d) *Diário Oficial da União* (DOU) - o documento passou a ser publicado no Portal da Imprensa Nacional assinado com certificado digital ICP-Brasil em agosto de 2009;

e) Escritório Digital - integra os sistemas processuais dos tribunais brasileiros e permite ao usuário centralizar, em um único endereço eletrônico, a tramitação dos processos de seu interesse no Judiciário;

f) eSocial - por meio do sistema, acessado com certificado digital, empregadores devem comunicar ao Governo, de forma unificada, as informações relativas aos trabalhadores, como vínculos, contribuições previdenciárias, folha de pagamento, comunicações de acidente de trabalho, aviso prévio, escriturações fiscais e informações sobre o FGTS;

g) Nota Fiscal Eletrônica (NF-e) - o documento que substitui a nota fiscal eletrônica em papel;

h) Passaporte Eletrônico - o novo passaporte eletrônico agilizará a verificação de autenticidade do passaporte brasileiro em postos de controle migratório no exterior e proporcionará maior segurança aos viajantes brasileiros;

i) Processo Judicial Eletrônico (PJ-e) - sistema desenvolvido para automação do Judiciário, em que os acessos e as assinaturas das petições devem ser feitos com certificado digital;

j) Simples Nacional - canal de acesso virtual, com certificado digital, a serviços referentes a tributos relacionados às Microempresas e Empresas de Pequeno Porte;

l) Siscomex - facilita o acesso aos serviços e sistemas governamentais, bem como à legislação pertinente às operações de comércio exterior;

m) Sistema de Pagamentos Brasileiro (SPB) - gerencia o processo de compensação e liquidação de pagamentos por meio eletrônico, interligando as instituições financeiras credenciadas ao Banco Central do Brasil. Utiliza certificados digitais da ICP-Brasil para autenticar e verificar a identidade dos participantes em todas as operações realizadas;

n) Sistema de Registro e Licenciamento de Empresas (RLE) - integra a Administração Pública da União, dos estados e dos municípios, de forma a proporcionar, num processo único, simplificado, previsível e uniforme, a abertura, as licenças de funcionamento e, se for necessário, a baixa de empresas;

o) Sistema Público de Escrituração Digital (Sped) - a ferramenta da Receita Federal do Brasil possibilita o envio, com certificado digital, de informações de natureza fiscal e contábil para os órgãos de registro e para os fiscos das diversas esferas[143].

Na prática, a ICP-Brasil é uma cadeia hierárquica de confiança, fortemente suportada por criptografia[144], que viabiliza a emissão de certificados digitais para identificação virtual do cidadão e das instituições/empresas. A certificação digital, nos sistemas de informação digitais, robustece a segurança, caracterizando a importância da identificação do usuário, bem como provendo integridade, confidencialidade, autenticidade e não repúdio às atividades executadas.

Sintetizando, segurança da informação zela por manter íntegros os processos informacionais que servem à organização em um determinado contexto, seguindo os requisitos gerados pela mesma, além daqueles emanados dos indivíduos usuários dos sistemas de informação. A seção que se segue procura enquadrar a segurança cibernética no escopo da segurança da informação.

---

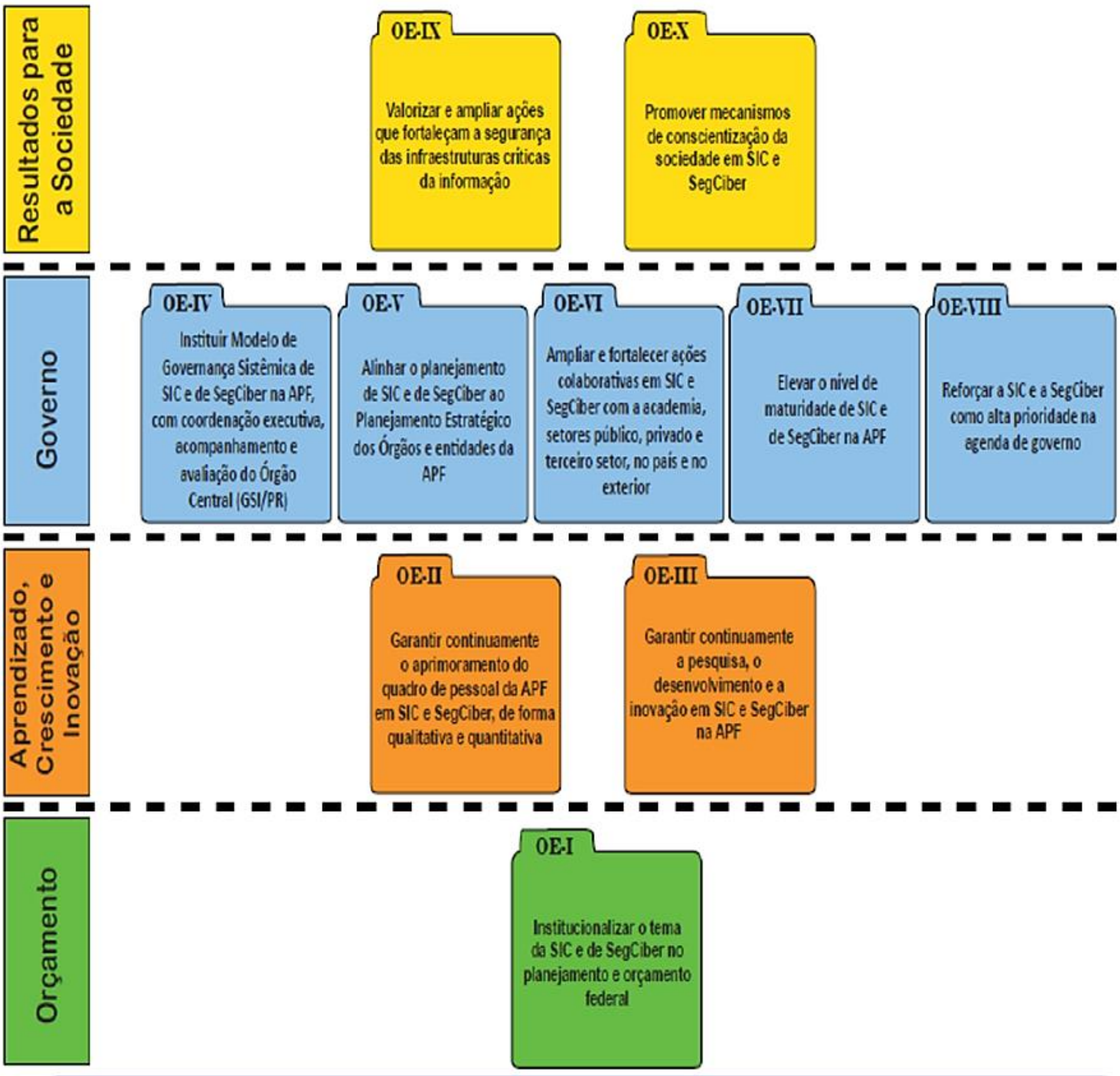
[143] Informações complementares disponíveis em: <http://www.iti.gov.br/certificado-digital/cases>. Acesso em: 18 jan. 2018.

[144] Disciplina de criptologia que trata dos princípios, dos meios e dos métodos de transformação de documentos com o objetivo de mascarar seu conteúdo, impedir modificações, uso não autorizado e dar segurança à confidência e autenticação de dados. Ciência que estuda os princípios, meios e métodos para tornar ininteligíveis as informações, através de um processo de cifragem, e para restaurar informações cifradas para sua forma original, inteligível, através de um processo de decifragem. A criptografia também se preocupa com as técnicas de criptoanálise, que dizem respeito às formas de recuperar aquela informação sem se ter os parâmetros completos para a decifragem. Disponível em: <http://www.iti.gov.br/glossario>. Acessado em: 17 jan. 2018.

### *7.1.3 Estratégia de Segurança da Informação e Comunicações*

Em 2015, o Gabinete de Segurança Institucional da Presidência da República (GSI), por intermédio do seu Departamento de Segurança da Informação e Comunicações (DSIC), publicou a *Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal 2015-2018* (ESIC). A ESIC (Brasil, 2015) possui a finalidade de apresentar as diretrizes estratégicas (nível político), para o planejamento, a articulação e a coordenação de esforços dos diversos atores envolvidos. Atuando em quatro perspectivas, estabelece dez objetivos estratégicos desdobrados na figura 16.

Figura 16 - Mapa estratégico da ESIC (2015-2018)




Fonte: Brasil (2015, p. 41)

A *Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética*, no período de 2015 a 2018, desdobra 38 metas estratégicas, das quais, em particular, a proteção dos ativos de informação implica a definição de investimentos para um melhor posicionamento das instituições governamentais em relação à produção e custódia, principalmente, das informações dos cidadãos brasileiros e do Estado (BRASIL, 2015).

## 7.2 Segurança Cibernética

A princípio, poder-se-ia supor que segurança cibernética (*cybersecurity*), também conhecida como segurança digital ou do espaço cibernético, seria uma evolução de segurança da informação. Na realidade, segurança cibernética encontra-se inserida num contexto mais amplo e multifacetado da segurança da informação, em consonância com a norma ISO/IEC 27032- *Guidelines for cybersecurity (*Diretrizes para a segurança cibernética*).*

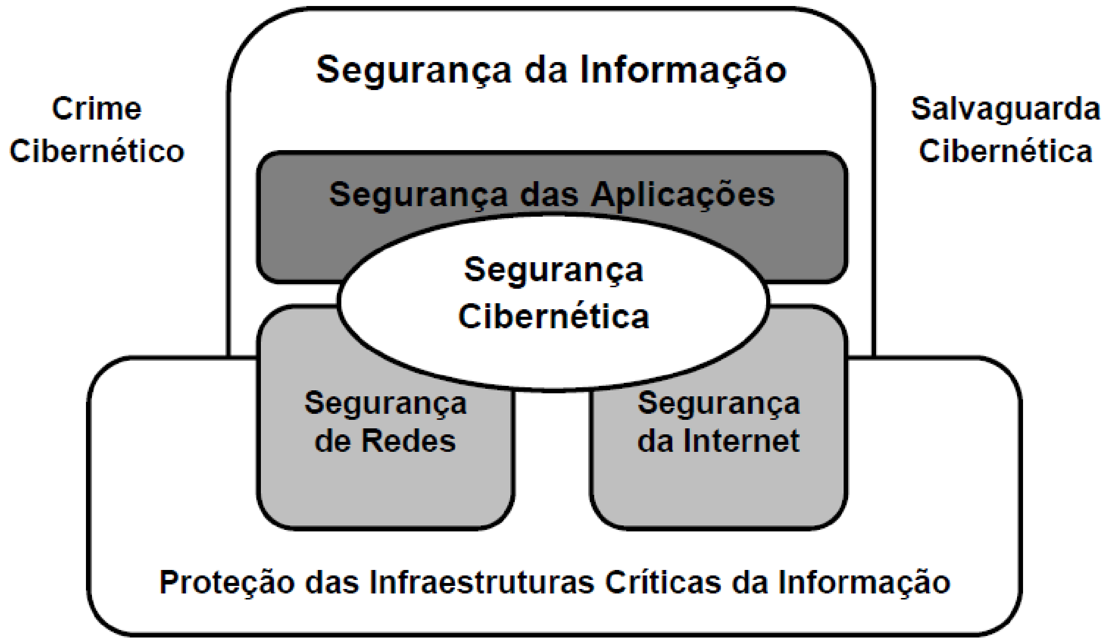
A ISO/IEC 27032, alinhada com o "espírito" de segurança da informação inerente à família das normas internacionais 27000, define segurança cibernética como preservação da confidencialidade, da integridade e da disponibilidade da informação no espaço cibernético**.** Adicionalmente, outras propriedades, tais como: autenticidade, responsabilidade, não repúdio e confiabilidade podem também estar envolvidas nesse contexto (ISO/IEC 27032, 2012, tradução nossa)[145].

A figura 17, inspirada na norma ISO/IEC 27032, exemplifica uma forma de inserção da segurança cibernética no campo da segurança da informação.

---

[145] *Cybersecurity: preservation of confidentiality, integrity and availability of information in the cyberspace. In addition, other properties. such as authenticity, accountability, non-repudiation, and reliability can also be involved.*

Figura 17 - Segurança cibernética e outras seguranças




Fonte: Vianna (2015)

Nesta linha de abordagem, emerge o entendimento da Organização dos Estados Americanos:

> o conceito de "ciber segurança" costuma ser usado como um termo amplo para se referir a diversos temas, desde a segurança da infraestrutura nacional e das redes pelas quais os serviços de Internet são prestados, até a segurança ou integridade dos usuários. No entanto, desenvolvimentos posteriores sugerem a necessidade de limitar o conceito exclusivamente à proteção dos sistemas [de informação] e dados de informática. [...] essa abordagem mais restrita permite uma melhor compreensão do problema e uma adequada identificação das soluções necessárias para proteger as redes interdependentes e a infraestrutura da informação (OEA, 2013, p. 56).

Neste sentido, o escopo de pesquisa da presente tese alinha-se, também, com a ESIC, ao considerar as áreas de atuação da segurança da informação/cibernética como:

> questões nacionais, horizontais e estratégicas, que afetam todos os níveis da sociedade, e representa importante instrumento de apoio ao planejamento dos órgãos e entidades do Governo, objetivando melhorar sobremaneira a segurança e a resiliência das infraestruturas críticas e dos serviços públicos nacionais (Brasil, 2015, p. 17).

Entretanto, no âmbito governamental, permanece, ainda, o entendimento do Grupo Técnico de Segurança Cibernética de 2009, instituído no âmbito da Câmara de Relações Exteriores e Defesa Nacional (CREDEN), onde o termo segurança cibernética foi definido como: "a arte de assegurar a existência e a continuidade da Sociedade da Informação de uma Nação, garantindo e protegendo, no Espaço Cibernético, seus

Ativos de Informação e suas Infraestruturas Críticas” (BRASIL, 2010a, p. 116). No que concerne à esfera governamental e no entendimento deste autor, o conceito de segurança cibernética carece de atualização e maior grau de especificidade, particularmente, quando se refere à “arte de” e à “sociedade da informação”. Assim, adota-se, nesta tese, o definido pela ISO/IEC 27032, entre outros motivos, por estar alinhado à própria Instrução Normativa n.1 do GSI e às suas Normas Complementares decorrentes.

Grande parcela dos principais desafios da Segurança Cibernética, no âmbito governamental, foi listada durante os trabalhos da CPI de Crimes Cibernéticos na Câmara dos Deputados em 2015, pelo Secretário de Tecnologia da Informação do Ministério do Planejamento, Orçamento e gestão (STI/MPOG), a saber:

a) crescente dependência da gestão do Estado por recursos de TIC;
b) maior demanda de informações pelos cidadãos (LAI);
c) compartilhamento de informações entre órgãos;
d) padronização e interdependência entre ativos de informação;
e) alta disponibilidade e armazenamento robusto de dados;
f) sigilo de dados e informações e tratamento de vulnerabilidades;
g) tecnologias proprietárias;
h) restrições técnicas e orçamentárias;
i) marcos legais;
j) crescimento do crime virtual (HECKERT, 2015).

Diferentemente da segurança cibernética, que possui tratamento e orientações de diversos órgãos da APF, a defesa cibernética é abordada, praticamente com exclusividade, pelo Ministério da Defesa, sendo objeto da próxima seção.

## 7.3 DEFESA CIBERNÉTICA

A defesa cibernética, de forma passiva ou ativa, torna-se atividade indispensável para a segurança nacional e o êxito das operações militares. Alinhado com as grandes nações, o Brasil vem fomentando diversas atividades de defesa cibernética, particularmente após a publicação da END/2008.

No contexto estratégico nacional, em ambiente operacional ainda em exploração, onde é maximizado o relacionamento entre pessoas, instituições públicas e privadas, bem como em que se ignoram os limites fronteiriços entre Estados-Nações, pode-se definir o termo Defesa Cibernética (*Cyber Defense*) como:

> conjunto de ações ofensivas, defensivas e exploratórias, realizadas no Espaço Cibernético, no contexto de um planejamento nacional de nível estratégico, coordenado e integrado pelo Ministério da Defesa, com as finalidades de proteger os sistemas de informação de interesse da Defesa Nacional, obter dados para a produção de conhecimento de Inteligência e comprometer os sistemas de informação do oponente (BRASIL, 2014b, p. 18).

No Brasil, a ampla interação entre Segurança Nacional e Cibernética tem início em 2008, quando a *Estratégia Nacional de Defesa* (END) identificou três setores de importância estratégica: o espacial, o **cibernético** [grifo nosso] e o nuclear (BRASIL, 2008a). Assim, o recém criado setor cibernético passou a demandar elementos intrínsecos e interorganizacionais ao Ministério da Defesa (MD). Como decorrência direta da END, em 2010, foi criado, no Comando do Exército, o "Núcleo" do Centro de Defesa Cibernética (NuCDCiber), com a atribuição de coordenação e integração das atividades de defesa cibernética, no âmbito do Ministério da Defesa. Ao Centro de Defesa Cibernética competia[146]:

a) assessorar o Comandante do Exército e o Ministro de Estado da Defesa nas atividades do setor, formular doutrina, obter e empregar tecnologias;
b) planejar, orientar e controlar as atividades operacionais, doutrinárias e de desenvolvimento das capacidades cibernéticas;
c) executar atividades de exploração cibernética, em conformidade com as políticas e diretrizes do Ministério da Defesa.

Em 2012, foi ativado o Centro de Defesa Cibernética, que recebeu seu batismo de fogo, ao planejar e coordenar a segurança e a defesa cibernéticas, na Conferência das Nações Unidas sobre Desenvolvimento Sustentável - Rio+20. Ainda em 2012, foi publicada pelo Ministério da Defesa (MD), a *Política Cibernética de Defesa* (PCD/MD), com a finalidade de orientar as atividades de Defesa Cibernética, no nível estratégico e de Guerra Cibernética, nos níveis operacional e tático (BRASIL, 2012d). Dentre seus

---

[146] Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2015/Decreto/D8491.htm>. Acesso em: 24 nov. 2016.

pressupostos básicos e objetivos relacionados diretamente à pesquisa em tela, destacam-se:

a) a eficácia das ações de Defesa Cibernética depende, fundamentalmente, da atuação colaborativa da sociedade brasileira, incluindo, não apenas o MD, mas também a **comunidade acadêmica** [grifo nosso], os setores público e privado e a base industrial de defesa;
b) a eficácia das ações de Defesa Cibernética no MD depende diretamente do grau de conscientização alcançado, junto às organizações e pessoas acerca do **valor da informação** [grifo nosso] que detêm ou processam;
c) a Segurança da Informação e Comunicações é à base da Defesa Cibernética e depende diretamente das ações individuais [...];
d) assegurar, de forma conjunta, o uso efetivo do espaço cibernético (preparo e emprego operacional) pelas Forças Armadas (FA) e impedir ou dificultar sua utilização contra interesses da Defesa Nacional;
e) levantar as infraestruturas críticas de informação associadas ao Setor Cibernético [relacionadas às ameaças internas e externas, reais ou potenciais], a fim de contribuir para a formação da consciência situacional necessária às atividades de Defesa Cibernética;
f) estabelecer critérios de risco, inerentes aos ativos de informação, e realizar o seu gerenciamento, reduzindo os riscos às infraestruturas críticas da informação de interesse da Defesa Nacional a níveis aceitáveis;
g) contribuir para a segurança dos ativos de informação da Administração Pública Federal, no que se refere à Segurança Cibernética, situados fora do âmbito do MD (BRASIL, 2012d, p. 11-13).

O Ministério da Defesa, por intermédio da Portaria n. 2.777/MD, de 28 de outubro de 2014 (BRASIL, 2014c), definiu responsabilidades para execução de medidas visando à potencialização da Defesa Cibernética Nacional. As medidas relacionadas com o presente estudo podem ser assim sintetizadas:

a) criação e implantação do Comando de Defesa Cibernética (ComDCiber);
b) criação e implantação da Escola Nacional de Defesa Cibernética (ENaDCiber);
c) implantação e consolidação do desenvolvimento conjunto de Defesa Cibernética;

d) implantação e consolidação do Sistema de Homologação e Certificação de Produtos de Defesa Cibernética (SHCDCiber);
e) apoio à pesquisa e ao desenvolvimento de produtos de Defesa Cibernética.

Assim sendo, a partir de outubro de 2014, iniciou-se o Projeto Defesa Cibernética na Defesa Nacional (Viabilidade e Concepção da Escola Nacional de Defesa Cibernética - ENaDCiber e do Sistema de Homologação e Certificação de Produtos e Serviços de Defesa Cibernética - SHCDCiber). O referido projeto foi executado sob a responsabilidade da Fundação Universidade de Brasília (FUB), por demanda do Exército Brasileiro/MD. Na sequência, em novembro, foi aprovada, no âmbito do MD, a *Doutrina Militar de Defesa Cibernética* (DMDC) e ativado o núcleo da EnaDCiber no início de 2015.

No viés acadêmico, a ENaDCiber tem por objetivo criar uma “célula nacional” capaz de fomentar e disseminar as competências necessárias à defesa cibernética, no âmbito da Defesa Nacional, nos níveis de sensibilização, conscientização, formação e especialização. A ENaDCiber tem como missão contribuir para as áreas de pesquisa, desenvolvimento, operação e gestão da ciber defesa, proporcionando melhoria da qualificação da mão-de-obra nacional para setor cibernético.

No campo das tecnologias da informação, o SHCDCiber busca a obtenção de um ambiente favorável à eliminação ou à redução de vulnerabilidades cibernéticas, baseado em uma estrutura de coordenação e integração de laboratórios especializados em certificação e homologação de produtos e serviços de TI, para emprego nas atividades de defesa cibernética, tendo como foco o desenvolvimento de capacitações nacionais.

Marco significativo, consolidando a participação acadêmica e civil na defesa cibernética, deu-se pela Portaria Interministerial n. 1421, de 31 de dezembro de 2014, assinada pelo Ministério da Defesa e o pelo Ministério da Ciência, Tecnologia e Inovação (MCTI), que instituiu o Programa de Pesquisa, Desenvolvimento e Inovação em Defesa Cibernética[147], com o objetivo de estimular ações de defesa cibernética, como mecanismo de apoio civil do MCTI, para a implementação da Estratégia Nacional de Defesa. Dentre os objetivos da Portaria multissetorial destacam-se:

---

[147] Disponível em: <http://www.editoramagister.com/legis_26349623_PORTARIA_INTERMINISTERIAL_N_1424_DE_31_DE_DEZEMBRO_DE_2014.aspx >. Acesso em: 24 nov. 2016.

a) promover e realizar Pesquisa, Desenvolvimento e Inovação, em tecnologias de defesa cibernética para a APF e para a indústria nacional;
b) contribuir para a inovação na indústria nacional nas áreas de segurança de sistemas de informação e defesa cibernética;
c) buscar aderência e alinhamento dos projetos desenvolvidos no âmbito do Programa de Pesquisa, Desenvolvimento e Inovação em defesa cibernética, com os desenvolvidos por outros órgãos e entidades, públicos ou privados;
d) promover a interação entre centros e institutos de pesquisa, universidades, setor produtivo e de serviços de infraestrutura de tecnologias da informação, órgãos de governo, e outras entidades que atuem em Defesa Cibernética;
e) contribuir para a defesa das infraestruturas críticas e para o esforço de Segurança Cibernética do País.

No contexto da Doutrina Militar de Defesa Cibernética e do cenário atual e mutante, onde se observa o aumento do risco de perpetração de ataques por Estados, organizações e até mesmo por pequenos grupos, com as mais diversas motivações, a Defesa no Ciberespaço vem-se estabelecendo como atividade fundamental ao êxito das operações militares em todos os escalões de comando, na medida em que viabiliza o exercício do Comando e Controle ($C^2$), por meio da proteção dos ativos de informação, ao mesmo tempo permitindo que esse exercício seja negado ao oponente (BRASIL, 2014b). Ao tratar do Sistema Militar de Defesa Cibernética (SMDC), a DMDC destaca a necessidade de atuar em ambiente colaborativo:

> a eficácia das ações de Defesa Cibernética depende, fundamentalmente, da atuação colaborativa da sociedade brasileira, incluindo, não apenas o MD, mas também a comunidade acadêmica, os setores público e privado e a base industrial de defesa. Nesse contexto, avulta de importância a necessidade de interação permanente entre o MD e os demais atores externos envolvidos com o Setor Cibernético, nos níveis nacional e internacional, conforme estabelece a END (BRASIL, 2014b, p. 25).

Em abril de 2016, entrou em operação o ComDCiber, com o objetivo de planejar, orientar e controlar as atividades operacionais, de inteligência, doutrinárias, de ciência e tecnologia, e de capacitação no âmbito do Sistema Militar de Defesa Cibernética.

Como atividade especializada, com métodos, procedimentos, características e vocabulário que lhe são peculiares, a defesa cibernética pode desdobrar-se em ações de guerra cibernética, assunto a ser explorado na próxima seção.

## 7.4 Guerra Cibernética

As TIC estão mudando o mundo para o bem e para o mal. Cresce um novo sentimento de insegurança e o medo de conflitos claramente não convencionais. Garantir a segurança na ordem mundial significa assegurar os chamados *global commons*, isto é, a liberdade de acesso e de circulação terrestre, bem como no espaço marítimo, no espaço aéreo, no espaço extra-atmosférico e, atualmente, no ciberespaço.

Ataques cibernéticos contra países, nações, economias com representatividade nacional, empresas e infraestruturas críticas fazem parte da realidade contemporânea, independentemente de suas motivações, autoria e formas de realização (ostensivamente ou na clandestinidade).

A guerra cibernética (*ciber war*) desenvolve-se em ambiente totalmente artificial – o ciberespaço criado pelo homem que, por vezes, abrange termos como guerra eletrônica (*eletronic warfare*)[148], guerra centrada em redes (*netwar*)[149], ciberterrorismo, cibercrime, ataques *hackers* e ciberespionagem.

De modo consolidado, no escopo desta tese, tem-se que a guerra cibernética faz parte de um contexto mais abrangente e conhecido da guerra da informação, onde a própria informação é considerada alvo e arma, podendo sua ausência ou excesso causar paralisia e derrota.

Na guerra da informação, busca-se afetar a informação disponível ao oponente, de maneira a degradar, interromper, enganar, negar ou destruir sua capacidade de perceber uma dada situação e passar a exercer, então, o comando efetivo. Para tanto, esforços são direcionados na consolidação do chamado Poder Informacional Nacional, o qual se constitui em amplo espectro de capacidades governamentais, civis e militares com a finalidade de explorar o ambiente global de informação e obter domínio estratégico.

---

[148] Conjunto de ações que visam explorar as emissões do inimigo, em toda a faixa do espectro eletromagnético, com a finalidade de conhecer a sua ordem de batalha, intenções e capacidades, e, também, utilizar medidas adequadas para negar o uso efetivo dos seus sistemas, enquanto se protege e utiliza, com eficácia, os próprios sistemas (BRASIL, 2015, p. 135).

[149] Reúne em rede os mais diversos elementos das forças armadas de um país, permitindo-lhe administrar diversas tarefas que vão desde a coleta até a distribuição de informações críticas entre esses muitos elementos. [...]. Visa obter melhor sincronismo [...], assim como o incremento na velocidade das operações bélicas e do processo decisório de comando (BRASIL, 2015, p. 133).

A *ciber war*, também é conhecida como "guerra de quarta geração", particularmente no teatro de ação europeu, onde o termo é, também, muitas vezes utilizado para se referir aos conflitos assimétricos, designando o conflito multidimensional, envolvendo ações em terra, no mar, no ar, no espaço exterior, no espectro eletromagnético e no ciberespaço. Nesse novo contexto estratégico, o Estado perde o monopólio sobre a guerra propriamente dita, onde o "inimigo" pode não ser exatamente um Estado organizado, mas um qualquer outro ator não estatal, um grupo terrorista ou uma organização criminosa.

Assim, a Internet e a nova sociedade da informação trouxeram a guerra para o direto; os campos de batalha são transpostos para as "cidades de batalha" e um simples soldado, ou o seu (mau) comportamento, pode ter implicações verdadeiramente estratégicas (CUNHA, 2010).

No contexto de possibilidade de conflito, que ameace a Segurança Nacional brasileira, a *Doutrina Militar de Defesa Cibernética* assim define guerra cibernética:

> corresponde ao uso ofensivo e defensivo de informação e sistemas de informação para negar, explorar, corromper, degradar ou destruir capacidades de C² do adversário, no contexto de um planejamento militar de nível operacional ou tático ou de uma operação militar. Compreende ações que envolvem as ferramentas de Tecnologia da Informação e Comunicações (TIC) para desestabilizar ou tirar proveito dos Sistemas de Tecnologia da Informação e Comunicações e Comando e Controle (STIC2) do oponente e defender os próprios STIC2. Abrange, essencialmente, as Ações Cibernéticas. A oportunidade para o emprego dessas ações ou a sua efetiva utilização será proporcional à dependência do oponente em relação à TIC (BRASIL, 2014b, p. 19).

De acordo com a *Política Cibernética de Defesa* (PCD), as ações de guerra no espaço cibernético são realizadas nos níveis operacional e tático, restritas ao âmbito interno das Forças Armadas/Ministério da Defesa (FA/MD). No caso, considera-se o ciberespaço também como um domínio operacional, permeando os outros quatro domínios: terrestre, marítimo, aéreo e espacial, bem como interagindo de forma interdependente.

Dentre as ações tipificadas de guerra cibernética, no âmbito das FA/MD, destaca-se o Ataque Cibernético que "compreende ações para interromper, negar, degradar, corromper ou destruir informações ou sistemas computacionais armazenados em dispositivos e redes computacionais e de comunicações do oponente" (BRASIL, 2014b, p. 23).

Uma forma prática e realística de compreender a definição e as atividades supracitadas, bem como as graves consequências que ações hostis podem infligir contra o ambiente cibernético de um país, seria tomar, a título de estudo de caso, dois acontecimentos contemporâneos internacionais: os ataques cibernéticos em grande escala sofridos pela Estônia em 2007 e a Guerra da Geórgia em 2008 (VIANNA, 2015).

Em 2007, a Estônia viria a ser alvo do primeiro ataque virtual da história perpetrado contra um Estado-Nação. Extremamente dependente de redes de computadores em serviços públicos e privados, teve suas principais infraestruturas paralisadas por cerca de duas semanas[150], em virtude de um ataque massivo de negação de serviço (*Distributed Denial of Service* - DDoS)[151], em retaliação à decisão do governo estoniano de retirar de Tallin um monumento às Forças Armadas Soviéticas.

Como consequência, uma comunidade de *hackers* russos, a princípio cooptados pelo governo da Rússia, paralisou os meios de comunicação, algumas operações bancárias e *sites* do governo durante alguns dias, sem que houvesse uma intervenção militar correspondente para tirar proveito dos efeitos da campanha cibernética. Consequência imediata, ainda em 2008, foi a criação do NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE), Centro de Excelência e Cooperação de Defesa Cibernética da Organização do Tratado do Atlântico Norte (OTAN) com sede em Tallin, naquele mesmo país. O Centro possui como objetivo apoiar as nações-membro com competências cibernéticas nas áreas de tecnologia, estratégia, operações e direito.

No caso da Geórgia, os ataques cibernéticos foram coordenados com uma operação militar russa, servindo como multiplicadores do poder de combate. De fato, a ocupação de parte da Geórgia por forças russas foi antecedida por ataques cibernéticos desencadeados com objetivos bem definidos, como o de calar a mídia georgiana, diminuindo a repercussão da ocupação e possíveis retaliações do Ocidente. Posteriormente, a operação cibernética russa foi ampliada, incluindo instituições financeiras, empresas, organizações de ensino, mídia ocidental (BBC e CNN) e um sítio internet

[150] A Estônia está classificada entre os países mais conectados e tecnologicamente avançados do mundo, com altos níveis de alfabetização em informática e conectividade, possuindo quase todos os seus serviços públicos e atividades cotidianas integrados em sistemas informatizados e na Internet (VIANNA, 2015).

[151] Técnica pela qual um atacante utiliza, de forma coordenada e distribuída, um conjunto de equipamentos para tirar de operação um serviço, um computador ou uma rede conectada à Internet. Disponível em: <http://nic.br/noticia/releases/web-br-2016-internet-das-coisas-na-web-e-debatida-por-centenas-de-participantes>. Acesso em: 25 nov. 2016.

de *hackers* da Geórgia. Outro aspecto interessante deve-se ao fato de que a guerra cibernética, também, foi empregada para maximizar um alvo puramente econômico, como os portos e instalações georgianos do setor de petróleo e gás.

Adicionalmente, cita-se, neste contexto, outro exemplo comprovado e com conotações bélicas. Trata-se do ataque do *worm*[152] Stuxnet às instalações nucleares em Natanz, no Irã, o qual gerou consequências reais em objetos físicos, no caso, o alvo do ataque foram centrífugas nucleares.

De acordo com Clarke e Knake (2015), o Stuxnet foi, primeiramente, reconhecido, no segundo semestre de 2010, pelo especialista de sistemas de controle industrial (ICS - Industrial Control System) Ralph Langer como uma grande, complexa e sofisticada arma cibernética[153], criada com o objetivo de tornar inoperantes as centrífugas de enriquecimento de urânio iranianas. As instalações nucleares estavam localizadas na cidade de Natanz e possuíam um forte aparato de segurança (inclusive com defesa antiaérea). Segundo os autores, o Stuxnet atacou o sistema SCADA[154] Siemens WinCC-7 que monitorava e enviava instruções para as centenas de centrífugas iranianas. O *worm,* ao infectar o sistema de monitoração e controle, enviou comandos alterados aos motores elétricos, criando uma oscilação que terminou por quebrar quase mil centrífugas.

Os impactos causados pelo Stuxnet no sistema SCADA, utilizado nas instalações nucleares iranianas, foram tão expressivos, que o mesmo chegou a receber a alcunha de “primeira” arma de guerra cibernética já utilizada com êxito. Dentre as peculiaridades e características do emprego do Stuxnet, destacam-se:

a) o ataque foi realizado por meio de ações remotas via *software* (*worm*) a uma infraestrutura crítica estratégica baseada em sistema SCADA;
b) não foi necessário que o sistema iraniano estivesse conectado à Internet para ser infectado;

---

[152] *Worm* é um programa capaz de se propagar automaticamente pelas redes, enviando cópias de si mesmo de computador para computador. Propaga-se pela execução direta de suas cópias ou pela exploração automática de vulnerabilidades existentes em programas instalados em computadores. *Worms* são notadamente responsáveis por consumir muitos recursos, devido à grande quantidade de cópias de si mesmo que costumam propagar e, como consequência, podem afetar o desempenho de redes e a utilização de computadores (CERT.br, 2016).
[153] Conjunto de ferramentas utilizadas para reconhecimento e exploração em contexto de guerra cibernética, comparada com armas atômicas, por exemplo, pode causar menos efeitos colaterais e duradouros, além de reduzida mortalidade.
[154] Sistemas SCADA *(Supervisory Control And Data Acquisition* - Controle Supervisório e Aquisição de Dados).

c) a técnica de penetração em redes de computares utilizado pelo *worm* Stuxnet nunca havia sido vista antes, o que caracteriza a mesma como um complexo e oneroso "*ataque zero day*";

d) a estrutura tipo "*plug and play*", empregada na fabricação do Stuxnet, permite sua customização e utilização em sistemas SCADA de outros fabricantes.

Em termos político-estratégicos, o Stuxnet evitou o início de mais um conflito armado direto entre Israel e o Irã, pois, apesar de o programa nuclear do Irã referir-se somente a enriquecimento de urânio para a geração de energia pacífica, as centrífugas possuíam potencial de uso no desenvolvimento de armas/bombas nucleares.

De fato, segundo Clarke e Knake (2015), as instalações de Natanz já estavam na iminência de ataque aéreo israelense, o que possivelmente provocaria uma nova guerra no Oriente Médio. Ainda, segundo os autores (2015, p. 233), "os Estados Unidos atravessou o Rubicão cibernético. Eles lançaram um ataque cibernético que causou a destruição de um equipamento sensível. Eles legitimaram esse comportamento".

A utilização da arma Stuxnet em uma infraestrutura crítica estratégica, de um Estado-Nação oponente (Irã), pode ser caracterizada como uma ação de sabotagem cibernética.

Neste contexto, de acordo com Vianna e Izycki (2018), a guerra cibernética já é uma realidade, pois inúmeras "campanhas" foram realizadas, entre 2010 e 2017, por intermédio de ataques avançados persistentes (*Advanced Persitent Threats* – APT), praticados por atores estatais ou por atores não estatais, como criminosos ou ativistas. As referidas campanhas destacaram-se: pela repercussão internacional, nível de sofisticação dos artefatos empregados e a gravidade das suas consequências (danos materiais diretos ou indiretos), bem como por terem extrapolado a dimensão cibernética e terem produzido, ou possuíam condição para gerar, resultados cinéticos em infraestruturas críticas/estratégicas.

Na sequência, será abordado o tema Infraestruturas Críticas (IC), com destaque para as IC de informação, levando-se em consideração aspectos da segurança e da proteção da informação no ciberespaço de interesse nacional.

## 7.5 INFRAESTRUTURAS CRÍTICAS

No campo político nacional, a segurança das Infraestruturas Críticas (também conhecidas como “Infraestruturas Estratégicas”) vem sendo tratada no âmbito do Conselho de Defesa Nacional (CDN) e da Câmara de Relações Exteriores e Defesa Nacional (CREDEN). No que se refere às ações estratégicas que devem orientar a implementação de medidas de proteção às IC, a *Estratégia Nacional de Defesa* ressalta que:

> todas as instâncias do Estado deverão contribuir para o incremento do nível de Segurança Nacional, com particular ênfase sobre: [...] as medidas para a segurança das áreas de infraestruturas críticas, incluindo serviços, em especial no que se refere à energia, transporte, água e telecomunicações, a cargo dos Ministérios da Defesa, das Minas e Energia, dos Transportes, da Integração Nacional e das Comunicações, e ao trabalho de coordenação, avaliação, monitoramento e redução de riscos, desempenhado pelo GSIPR (BRASIL, 2012c, p. 155).

Não obstante, em operações reais e de grande vulto como os Grandes Eventos, a segurança das IC envolvidas diretamente com a realização do Evento foi, na prática, coordenada e articulada pelo responsável executivo de segurança/defesa cibernética. As Infraestruturas Críticas compreendem as “instalações, serviços, bens e sistemas cuja interrupção ou destruição, total ou parcial, provoque sério impacto social, ambiental, econômico, político, internacional ou à segurança do Estado e da sociedade” (BRASIL, 2018a).

Segundo análise de Jorge Fernandes, a aceitação pelo Estado de que existe um conjunto de infraestruturas críticas nacionais representa um modo de organização do poder nacional, que reconhece a dependência da nação perante um conjunto específico de áreas prioritárias nacionais, nomeadamente Energia, Transporte, Água, Telecomunicações e Finanças; exemplificado nas imagens da figura 18.

Figura 18 - Exemplo de infraestruturas críticas no Brasil


Fonte: adaptado de GP3/CAEM (2018)

Segundo Fernandes (2012), esse modelo baseia-se na validade de, pelo menos, quatro indicadores, que diretamente se relacionam com:

a) as implicações da "guerra total" (*total war*), que produz mudança social duradoura e real, uma vez que a sociedade é impactada de forma profunda pela ocorrência de conflitos bélicos [155];

b) o fato de que danos às infraestruturas, em geral, podem ser feitos com relativa facilidade e causam grande transtorno à população civil;

c) o foco dado ao terrorismo e ao aumento do repúdio internacional contra o mesmo;

d) a suposição de que as infraestruturas críticas dependem cada vez mais de sistemas de informação e comunicação, abrindo a possibilidade de que, por meio de alta tecnologia especialmente de natureza cibernética, sejam potencializadas doutrinas de guerra total ou o terrorismo *high-tech*.

---

[155] Seja pela ruptura ou destruição de sua infraestrutura em larga escala; seja pelo esforço que é demandado das suas instituições sociais e políticas; seja pela participação de todos os segmentos da sociedade, inclusive minorias, no esforço de manutenção da máquina militar e outros instrumentos do poder nacional através de uma 'mobilização nacional'; seja pela 'colossal experiência psicológica' experimentada pelos cidadãos (FERNANDES, 2012, p. 21).

Christopher J. Furlow, em entrevista durante a realização do 20º Congresso Mundial de Tecnologia da Informação - WCTI 2016, alertou que as motivações para os ataques cibernéticos hoje são diversificadas variando de organizações bem financiadas, estruturadas e articuladas, até os chamados ‘lobos solitários’ que fazem ações por conta própria. O veterano da Casa Branca na área de segurança e presidente da Ridge Global prosseguiu, recomendando que, como uma forma de vencer esse desafio, as empresas e o governo identifiquem quais são os ativos mais importantes que precisam defender e quais são as respectivas vulnerabilidades antes de desenvolver um plano de ação (WCTI, 2016).

No contexto da Segurança Integrada[156], pesquisadores do Curso de Altos Estudos Militares (GP3/CAEM, 2018) caracterizam os setores estratégicos a serem protegidos da seguinte forma:

a) Transporte - é composta por toda estrutura existente no País nos diversos tipos de modais (aéreo, marítimo, rodoviário e ferroviário) responsáveis pelo transporte de passageiros e de cargas. Atualmente, a Empresa Brasileira de Infraestrutura Aeroportuária (Infraero) é o órgão do Estado Brasileiro por gerenciar o modal aéreo. O Departamento Nacional de Transportes Terrestres (DNIT) é o órgão responsável pelo modal rodoviário do País;

b) Energia - refere-se a todas as infraestruturas relacionadas com a geração e transmissão de energia elétrica, estruturas responsáveis pela produção de petróleo e gás natural e na produção e escoamento da produção de combustíveis renováveis. O Brasil possui uma diversificada Matriz Energética, característica essa que atribui maior importância à proteção desse patrimônio;

c) Comunicações - é integrada por todos os sistemas essenciais ao funcionamento dos equipamentos de transmissão e comutação (prédios, torres de transmissão, sistema de detecção e alarme de incêndio, sistema de aterramento e para-raios, sistema de refrigeração e sistema de energia). Destacam-se as inúmeras estações de transmissão de celulares existentes no território brasileiro;

[156] medidas preventivas e/ou repressivas, integrando diferentes agências, que visam à garantia da lei e da ordem, bem como ao combate às ameaças inerentes à segurança nacional.

d) Água - abrange todo o sistema de abastecimento de água (captação, adução, recalque, reservação, tratamento e rede de distribuição). Podem-se destacar no país a grande quantidade de barragens e a existência de Aquíferos estratégicos (Guarani e Alter do Chão);
e) Finanças - são estruturas destinadas para o gerenciamento de relações financeiras e comerciais do País, como por exemplo, o Banco Central do Brasil (Edifício- Sede), Ministério da Fazenda (Sede), Centro de Processamento de Dados do Banco do Brasil, Casa da Moeda, entre outros;
f) Setor Espacial - abrange as estruturas destinadas à pesquisa e desenvolvimento espacial do país, como por exemplo, o Centro de Lançamento de Alcântara e o Centro de Lançamento de Barreira do Inferno;
g) Setor Nuclear - é integrado por usinas nucleares para a geração de energia, a existência de reservas de materiais empregados na área nuclear e estruturas relacionadas à pesquisa e desenvolvimento nuclear (Unidade de Concentrado de Urânio de Caetité, Central Nuclear de Angra dos Reis e a Fábrica de Combustível Nuclear);
h) Setor Cibernético - abrange as estruturas, pessoas, processos e conhecimento necessários para o funcionamento do espaço virtual ou espaço cibernético. Compreende os dispositivos computacionais ou ativos da informação conectados em rede ou não, nos quais as informações transitam, são processadas e/ou armazenadas.

Sobre a salvaguarda das Infraestruturas Críticas, particularmente em relação à situação da segurança dos sistemas de controle e à automação industrial das mesmas, a Rede Nacional de Segurança da Informação e Criptografia (RENASIC), com apoio do Centro de Pesquisa e Desenvolvimento em Telecomunicações (CPqD), promoveram o 1º Painel sobre Segurança em Sistemas SCADA, realizado em julho de 2014 (RENASIC, 2014). Dentre as principais conclusões do evento que buscou traçar um panorama, uma visão geral sobre a segurança das infraestruturas do país, com ênfase nos seus aspectos técnicos e operacionais, compilam-se:

a) a importância de uma visão sistêmica de segurança no novo cenário tecnológico e na capacidade de dar pronta resposta aos incidentes;

b) a falta de fontes oficiais de informações sobre incidentes de segurança em redes industriais e SCADA, no Brasil, gerando uma lacuna importante no ciclo de proteção das infraestruturas críticas nacionais;

c) a importância das estruturas normativas para a efetividade de um trabalho integrado, no sentido da implementação da segurança global das infraestruturas críticas do país;

d) a falta de capacitação e conscientização dos usuários das redes de automação, sendo um dos fatores responsáveis pela alta taxa de erros humanos computados;

e) os ataques de baixa sofisticação e artefatos maliciosos (*malwares)* caseiros, que têm provocado danos substanciais aos sistemas SCADA desprotegidos;

f) um senso de segurança por desconhecimento do risco, em grande parte das plantas de automação nacionais;

g) as infraestruturas críticas acabam por investir bem mais na segurança das redes de TI, do que naquelas de automação que são consideradas o coração do negócio de suas empresas;

h) a tendência de que, ano a ano, a quantidade de ataques cresça de forma exponencial e global.

O painel concluiu pela pertinência e viabilidade de construção de um centro de resposta e análise de incidentes de segurança cibernética, voltado aos sistemas de controle industrial (ICS-CERT: Industrial Control Systems – Cyber Emergency Response Team) de abrangência nacional e alertou:

> a disseminação das redes de informação, a integração entre diferentes infraestruturas e a interdependência cada vez maior entre os setores resulta em consequências que não podem ser negligenciadas. Uma delas é que as vulnerabilidades em Infraestruturas Críticas tendem a crescer, o que tem tornado os problemas cada vez mais complexos. Outra consequência é que uma interrupção pode se propagar de um setor para outro, ocasionando o efeito cascata de problemas, tornando indisponíveis um ou mais serviços (RENASIC, 2014).

No final do ano de 2018, foi aprovada a *Política Nacional de Segurança de Infraestruturas Críticas* (PNSIC), através do Decreto n. 9.573, de 22 de novembro, definindo segurança de infraestruturas críticas como um “ conjunto de medidas, de caráter preventivo e reativo, destinadas a preservar ou restabelecer a prestação dos serviços relacionados às infraestruturas críticas“ (BRASIL, 2018a, p. 1). A PNSIC propõe o estabelecimento nacional de uma Estratégia, seguida de um Plano para as IC, no prazo de dois anos, bem como estabelece competência ao Gabinete de Segurança Institucional da Presidência da República para implementar e gerir o Sistema Integrado de Dados de Segurança de Infraestruturas Críticas. Dentre os objetivos e diretrizes da PNSIC destacam-se:

a) a garantia da segurança e da resiliência das infraestruturas críticas do País e a continuidade da prestação de seus serviços;
b) o estabelecimento da prevalência do interesse da defesa e da segurança nacional na proteção, na conservação e na expansão das infraestruturas críticas;
c) a cooperação entre órgãos e entidades federais, estaduais, distritais e municipais nas ações necessárias à implementação e à manutenção da segurança das infraestruturas críticas;
d) o incentivo à cooperação e à realização de parcerias entre os setores público e privado, com vistas a elevar o nível de segurança das infraestruturas críticas;
e) a integração de dados sobre ameaças, tecnologias de segurança e gestão de riscos.

De forma não exaustiva, como embasamento preliminar, buscou-se nas seções anteriores analisar temas relacionados à proteção da informação no espaço cibernético de interesse nacional.

Configuraram-se, então, a contemporaneidade, a dinâmica e a relevância da proteção no ciberespaço, bem como o seu entrelaçamento com expressões como: sistemas de informação automatizados, segurança da informação, Ativos de informação, redes de computadores, Internet, preservação digital, ameaças virtuais, ataques cibernéticos, infraestruturas críticas estratégicas, segurança, defesa e guerra cibernéticas, todos componentes do conceito de Ciber Proteção desenvolvido no próximo capítulo.

# 8 A GÊNESE DA CIBER PROTEÇÃO

A percepção do autor deste trabalho, adquirida ao longo da sua vivência profissional, de se estabelecer cientificamente o que denominamos ‘Ciber Proteção’ (proteção da informação no ciberespaço proteção cibernética) foi ratificada durante a revisão da respectiva literatura.

Assim, de forma indutiva, desenvolveu-se o conceito de Ciber Proteção alicerçado na Teoria do Conceito de Ingetraut Dalhberg. No entendimento da autora:

> se o conhecimento pode ser considerado a totalidade de proposições verdadeiras sobre o mundo, existindo, em geral, nos documentos ou nas cabeças das pessoas, pode parecer que existe, também, em todas as afirmações verdadeiras (em todos os julgamentos) e em todas as proposições científicas que obedecem a um postulado de verdade. Isto pressupõe a aceitabilidade e o reconhecimento por indivíduos de uma mesma área de interesse/profissão/especialidade, dessas proposições como verdadeiras e passíveis de serem comunicadas através de uma forma verbal (DAHLBERG, 1978a, p. 143).

Segundo Pereira e Bufrem (2007), o intento de representar o conhecimento exige a compreensão pelo analista dos princípios, fundamentos teóricos e elementos constitutivos do campo específico do saber. Em complemento, Melo (2013, p. 33) caracteriza conceito como um objeto de natureza interdisciplinar, relacionado à cognição humana e à noção de significado, e esclarece:

> a Filosofia foi a área do conhecimento que iniciou os estudos sobre a gênese e formação de conceitos. Porém, ao longo da história do pensamento científico, o conceito tornou-se objeto de estudo de diversas áreas do conhecimento: Lógica, Semântica, Linguística, Terminologia, Psicologia, Ciência da Informação, entre outras.

O novo conceito proposto tem por missão precípua consolidar, devidamente adequado à realidade brasileira, o contexto da pesquisa, buscando, também, um incremento do diálogo entre a proteção dos recursos informacionais no ciberespaço e a Ciência da Informação, em particular com a gestão da informação e a preservação digital. A análise de Marta Pinheiro exemplifica a necessidade, importância e abrangência do que se espera da Ciber Proteção a ser discutida neste capítulo:

> por desconhecimento das potencialidades e da apropriação possível dessas tecnologias, há ainda muita vulnerabilidade dos satélites, da segurança cibernética, e possíveis falhas de energia. A mesma infraestrutura que “carrega a informação para dar suporte à economia, à inovação e à atividade militar” é a encarregada de levar as comunicações usadas para organizar os grupos terroristas e suas atividades. O mesmo sistema de informação que apoia a educação “pode ser utilizado pelos cartéis de droga”. Proteger as diferentes redes de computadores é proteger privacidades, já que as guerras do mundo pós-moderno podem ser estabelecidas pura e simplesmente pelo ataque aos sistemas de informações vitais ao funcionamento do Estado e da sociedade, já altamente impregnados e dependentes das novas tecnologias de Informação.

> O equilíbrio a ser alcançado localiza-se em não permitir a intrusão e, ao mesmo tempo, não permitir a interrupção do nosso desenvolvimento incoativo (PINHEIRO, 2012, p. 75-76).

Neste segmento do presente trabalho, considera-se como fundamento teórico, a fim de subsidiar o processo analítico-sintético de conceituar Ciber Proteção, a Teoria do Conceito de Ingetraut Dalhberg que, em essência, visa dar uma versão fidedigna à representação da informação.

## 8.1 Bases do Conceito Ciber Proteção

### *8.1.1 A Teoria do Conceito*

Dalhberg, inicialmente, define conceito como a compilação de enunciados verdadeiros sobre determinado objeto, fixada por um símbolo linguístico[157] que pode ser verbal ou não verbal. Ao tratar sobre organização do conhecimento, a autora reconhece conceito como unidade do conhecimento, definindo-o como a síntese de características essenciais de um referente [objeto de interesse] que é representado por designações (termos, nomes, códigos)[158] [ou qualquer outro signo] (DALHBERG, 1978a, 1978b, 2009).

Em sintonia com o tema, o padrão ISO 1087-1 (2000) apresenta conceito como uma unidade de conhecimento criada por uma combinação única de características. Dessa forma, o conceito torna-se algo passível de ser capturado e explicitado.

Buscando sintetizar a questão, Dias e Naves (2007) definem conceito como um conjunto de características, que são elementos dos mesmos e traduzem os atributos das coisas designadas. Para os autores, os conceitos são essenciais à vida dos indivíduos, pois eles simplificam sua percepção do ambiente e o acréscimo de novos elementos aos esquemas individuais de cada um.

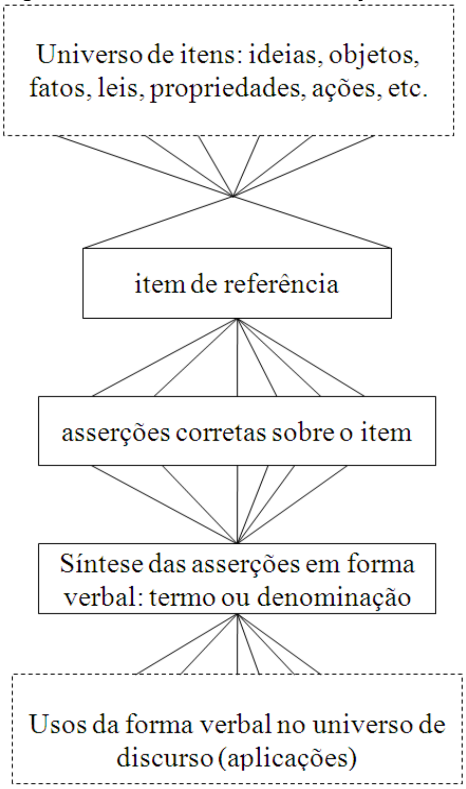
Em suma, Dalhberg considera conceito como a unidade de conhecimento que surge pela síntese dos predicados (enunciados/asserções) necessários, relacionados

[157] Por meio da linguagem, o ser humano pode expressar e relacionar os objetos (fenômenos, processos, propriedades, relações ou ideias) que compõem o seu universo, bem como elaborar enunciados (elementos do conceito) sobre os mesmos (DALHBERG, 1978b).

[158] *A knowledge unit (concept) is the synthesis of the essential characteristics of a referent to be represented by designations (terms, names, codes)* (DALHBERG, 2009).

com determinado objeto e passível de ser comunicado. Buscando relacionar os componentes básicos para a sua formação: referencial, predicacional e representacional, a autora propõe um modelo de construção de conceito conforme a figura 19.

Figura 19 - Modelo de construção de conceito




Fonte: Adaptado de Medeiros (2010, p. 48)

Como pode ser depreendido, termo e conceito estão intrinsicamente relacionados e por vezes são confundidos. Conceito contextualiza-se no campo das ideias e termo, como esclarece a própria Dahlberg, podendo ser definido como a forma verbal de um conceito, representando-o e sintetizando-o com o propósito de designação e de comunicação.

Edmeire Pereira e Leilah Brufen, neste quesito, complementam:

> os termos são tomados com um significado próprio, num dado contexto, destaca-se a indissociável relação entre linguagem, pensamento e realidade. Esta evidência se realiza via conceitos, e não entre palavras, dada a relação direta entre o conceito e o termo, isto é, um conceito é representado por um termo (símbolo) e este termo é usado para designar aquele conceito. (2005, p. 31)

Segundo a norma ISO 1087-1 (2000), termo também é a designação verbal de um conceito geral em um domínio específico, sendo definido como “uma declaração que descreve um conceito e permite sua diferenciação de outros conceitos dentro de um sistema de conceitos”.

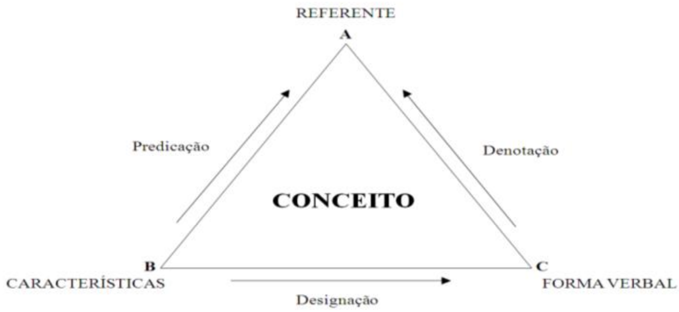
O Triângulo do Conceito proposto por Dahlberg, representado na figura 20, sintetiza a Teoria do Conceito e divide-se em três partes:

a) item de referência (*Referent*) - componente que mantém relações sobre as afirmações verdadeiras e a forma verbal, chegando ao referente por meio da predicação (asserção de alguma coisa sobre um sujeito);

b) características (*Characteristics*) - afirmações, proposição enunciada como verdadeira (asserções), que expressam atributos sobre o item de referência;

c) formal verbal (*Verbal forms*) - termo/nome que sintetiza o conceito com o propósito de representação.

Figura 20 - Triângulo do Conceito




Fonte: Adaptado Medeiros (2010, p. 48)

Partindo do Triângulo do Conceito, Eduardo Dias e Madalena Naves observam que os itens integrantes da elaboração final completa do conceito são, também, representados pelas relações entre o objeto de referência, o próprio conceito e sua expressão linguística, incluindo:

> (i) a referência de um item (da realidade); (ii) as afirmativas sobre o item de referência, produzindo os elementos ou características da unidade do conceito e a necessária verificabilidade (ou controlabilidade) por outras dessas afirmativas; e (iii) a designação por um termo, representando a síntese dos elementos do conhecimento (2007, p. 65).

### *8.1.2 Construindo o conceito de Ciber Proteção*

Campos (2001), ao analisar diversas teorias relacionadas com sistemas de conceitos, no contexto das linguagens documentárias, conclui que a Teoria do Conceito oferece o melhor suporte teórico-metodológico para a recuperação da informação, possibilitando a representação do conhecimento e, em consequência, comunicações mais precisas nas áreas relativas à ciência e à tecnologia.

Utilizando como base o Triângulo do Conceito, podem-se agrupar os componentes do conceito de Ciber Proteção, de acordo com o quadro 12.

Quadro 12 - Síntese do conceito de Ciber Proteção

| **ELEMENTOS** | **DESCRIÇÃO** |
|---|---|
| REFERENTE | Proteção dos sistemas de informação no ciberespaço de interesse nacional |
| CARACTERÍSTICAS / PROPRIEDADES DECLARADAS | - estabelece uma rede colaborativa interagências com os responsáveis pela segurança e defesa do espaço cibernético de interesse, buscando atuação integrada e essencialmente cooperativa;<br>- participa da construção de comunidades horizontais de proteção do espaço cibernético, exercendo coordenação centralizada e intervenção descentralizada, favorecendo a consciência situacional;<br>- participa do planejamento da preservação das informações digitais de interesse à soberania e ao poder nacional no espaço cibernético;<br>- acompanha as atividades de salvaguarda nos sistemas e ativos de informação nas infraestruturas críticas, cooperando na mitigação de vulnerabilidades, na análise de riscos e no fortalecimento da resiliência cibernética[159];<br>- analisa cenários e ameaças futuras, focando atenção especial à prevenção de ameaças externas (P.ex.: ciber terrorismo);<br>- relaciona-se com os serviços de inteligência nacionais e dos países amigos;<br>- favorece o intercâmbio e a interoperabilidade entre as equipes de tratamento de incidentes em redes de computadores, cooperando com a formulação de estratégias para gestão de incidentes de segurança;<br>- funciona como ferramenta de coesão social e coletiva da sociedade brasileira para a salvaguarda da ciber cultura nacional;<br>- coopera na formação e disponibilização de recursos humanos vocacionados e altamente capacitados (P.ex.: *Hacking*);<br>- abrange tanto o meio civil (P.ex.: a Internet das coisas - IoT como os equipamentos de uso militar, por meio da avaliação de sistemas de segurança físicos ou lógicos, podendo desenvolver e implantar soluções de *hardware, software*, processos e metodologias;<br>- opera alinhada com as necessidades e anseios da sociedade, organizando-se em prol dos objetivos estratégicos de um Estado-Nação;<br>- atua em diferentes realidades e ambientes (P.ex.: a atual Sociedade em Rede constituída por indivíduos, empresas e Estado); podendo operar em campo local, nacional e internacional, incluído a “nuvem” (*cloud*);<br>- pode demandar ações de guerra cibernética, objetivando a obtenção de informações, exploração e medidas de defesa ativa em sistemas de informação de interesse nacional, não respeitando fronteiras geográficas definidas. |

[159] A resiliência cibernética está diretamente relacionada com a violação da disponibilidade de um serviço. As soluções resilientes buscam identificar, prevenir, detectar e responder a ataques diversos, tolerando intrusões, mitigando danos e mantendo as atividades/serviços essenciais.

| | |
|---|---|
| FORMA VERBAL | Ciber Proteção, Proteção Cibernética e Proteção da informação no ciberespaço |

Fonte: elaboração própria

Dessa forma, entende-se que o conceito de Ciber Proteção possui características típicas da complexidade[160] e da multidisciplinaridade, onde o termo Ciber Proteção designa um conceito geral dentro de um universo de um discurso pretendido, destacando-se os seguintes relacionamentos:

a) com a Ciência da Informação, em particular, por intermédio das suas disciplinas: gestão da informação e do conhecimento, Segurança da Informação, Organização da Informação, Preservação Digital e, também, na Política de Informação;
b) com a Ciência da Computação, por meio das especialidades em segurança de equipamentos (*hardware*), das aplicações (*software*) e das redes de comunicação de dados;
c) com as infraestruturas críticas de interesse nacional, públicas ou privadas;
d) com as instituições relacionadas com a governança da rede mundial de computadores - Internet;
e) com os órgãos envolvidos diretamente com a segurança e a defesa cibernéticas.

## 8.2 CIBER PROTEÇÃO - UMA PROPOSTA CONCEITUAL

Na gestão da informação, em particular no seu tratamento e recuperação, o conceito é elemento-chave no tratamento temático, corroborando com a descrição do conteúdo temático de um recurso informacional (P.ex.: documento).

Capurro e Hjorland (2007) entendem que, no discurso científico, conceitos teóricos são construções planejadas para desempenhar um papel, da melhor maneira possível, não devendo ser rotulados como verdadeiros ou falsos. Os autores afirmam

---

[160] Complexidade: possui aspectos científicos, filosóficos e tecnológicos, tornando difícil a formulação do comportamento geral de um sistema, mesmo quando seu funcionamento e inter-relacionamentos parecem ser compreendidos. Possui como características propriedades gerais transdisciplinares como: não linearidade, não determinismo, auto-organização e emergência (LEMOS *et al*, 2007).

que há dependência do significado dos conceitos em relação com a estrutura da teoria em que ocorrem.

O estudo de Ciber Proteção, desenvolvido a partir da Teoria do Conceito e suportado pela multidisciplinaridade tão cara à Ciência da Informação, proporcionou um corpo de conhecimento consistente teoricamente, respaldado na prática de atividades de segurança e defesa cibernéticas, bem como aderente à realidade nacional.

A proposta de estudo da proteção da informação digital, no macrocontexto da CI, fortalece-se a partir das considerações da professora Marta Pinheiro:

> a ciência da informação muito tem a oferecer nesse campo [paradigmas técnico-econômicos da TI] pelos estudos das políticas de informação, em particular nos domínios cruciais de informação, em que lacunas ou entropias são percebidas nos processos de técnicas ligadas à estratégia cultural, social e de **segurança** [grifo nosso], nos conceitos de uso e de difusão da informação e na construção de conteúdos veiculados pelas redes (PINHEIRO, 2012, p. 62).

No que concerne à Teoria dos Conceitos e seus desdobramentos, não foi objeto deste trabalho o detalhamento das relações entre os conceitos do domínio em questão (informação, cibernética, defesa e segurança), embora seja fato de que a Ciber Proteção é vínculo de destaque nessa rede conceitual.

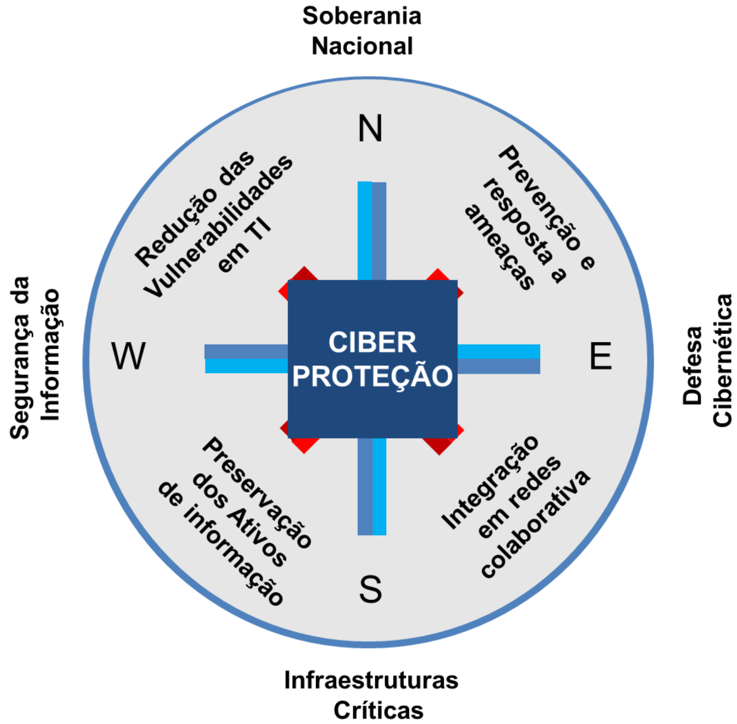
A Ciber Proteção, norteada pelas demandas da soberania nacional, relaciona-se notadamente com a segurança da informação em meio digital e com a ciber defesa, atuando, particularmente, nos ativos de informação das infraestruturas críticas.

Para fins deste estudo, considera-se que atividades inerentes à proteção cibernética estão imbricadas no contexto abrangente e multidisciplinar da Ciência da Informação (CI), vinculadas, particularmente, pelas áreas de estudo inerentes à segurança da informação, à gestão de documentos arquivísticos e à preservação da informação digital.

Dessa forma, busca-se preservar a informação (ativos de informação) nos sistemas informacionais de interesse nacional, contribuindo para a redução das fragilidades e vulnerabilidades inerentes às Tecnologias de Informação, englobando, também: a Internet, as aplicações para dispositivos móveis e os serviços via *Web.* Estrategicamente, pode a mesma colaborar com a prevenção de ameaças (regionais ou globais) e com a resposta aos ataques, não descartando medidas ativas sobre elementos hostis internos ou externos ao país.

A Ciber Proteção apresenta, também, o entendimento colaborativo, de articulação em rede e cooperação interagências, vitais ao desenvolvimento da Sociedade de um Estado-Nação. A figura 21 pretende sintetizar, graficamente, o conceito de Ciber Proteção.

Figura 21 - Bússola da Ciber Proteção




Fonte: elaboração própria

Cabe destacar que o conceito de Ciber Proteção não foi desenvolvido como um projeto universal (apesar de ser factível sua aplicação em organizações públicas ou privadas; nacionais ou estrangeiras), mas, particularmente, como um conjunto de respostas ao Estado nacional brasileiro, tipicamente um emergente informacional na sociedade global interconectada.

A percepção da relevância da informação (entendida como um recurso) nas infraestruturas críticas estratégicas demonstra importante contribuição da Ciber Proteção para a Segurança da Informação no âmbito da CI.

Dentre as contribuições que a Ciber Proteção pode adicionar ao campo de atuação da CI, em especial à segurança dos sistemas de informação de interesse nacional, destacam-se:

a) o incremento de fatores como resiliência dos ativos de informação a ataques;
b) coordenação e cooperação em rede, em favor da mitigação de vulnerabilidades relacionadas às “soluções de segurança” cibernéticas;
c) detecção e prevenção de ameaças cibernéticas, com ações ativas sobre elementos/sistemas potencialmente hostis internos ou não nacionais.

Encerra-se, com esta seção, a abordagem científica da pesquisa suportada pelos pilares da observação participante, da pesquisa bibliográfica e da análise documental que culminaram com o conceito de Ciber Proteção. No capítulo seguinte, apresentam-se os resultados e análises do estudo empírico centrado em entrevistas semi-estruturadas.

# 9 ESTUDO EMPÍRICO

Prosseguindo o percurso metodológico, foram aplicadas entrevistas semiestruturadas, com questões abertas, permitindo: (i) fluidez lógica do entrevistado, limitada, apenas, pelas instruções temáticas, nomeadamente, os requisitos para a segurança da informação em meio digital, o conceito de Ciber Proteção e a validação do modelo proposto, (ii) atitude de empatia sem formulação de juízo de valor por parte do entrevistador e (iii) possibilidades de remissões e respostas reflexos por parte de ambos: o especialista entrevistado e o entrevistador.

Buscou-se compreender, analisar, sintetizar e descrever a essência das experiências dos respondentes sobre os assuntos e atividades contemplados pela segurança da informação em meio digital. Foi enfatizado o levantamento de novos aspectos e conjunturas do tema, bem como do conhecimento adquirido pelos entrevistados no planejamento, na execução e na normatização (gestão) das atividades relacionadas ao Modelo de Ciber Proteção proposto. O planejamento e a execução das entrevistas estão detalhados no Apêndice A- Levantamento de Requisitos e no Apêndice B - Entrevista Administração Pública Federal.

Nesse contexto, a análise dos dados da pesquisa foi majoritariamente qualitativa, devido ao teor político-social das questões envolvidas, proporcionando, na opinião de Baptista e Cunha (2007), um enfoque mais holístico ao estudo.

Como ponto de partida, utilizou-se, parcialmente, a proposta investigativa de Laurence Bardin, nomeadamente ‘Análise de Conteúdo’ (AC), que, de acordo com a autora, seria:

> um conjunto de instrumentos metodológicos cada vez mais sutis em constante aperfeiçoamento, que se aplicam a <<discursos>> (conteúdos e continentes) extremamente diversificados. O fator comum destas técnicas múltiplas e multiplicadas – desde o cálculo de frequências que fornecem dados cifrados, até a extracção [sic] de estruturas traduzíveis em modelos – é uma hermenêutica controlada baseada na dedução: **inferência** (grifo nosso) (BARDIN, 2009, p. 11).

O uso da inferência[161] possibilitou informações complementares, extrapolando a simples leitura das entrevistas, a partir dos próprios entrevistados e da situação na

[161] Operação lógica, pela qual se admite uma proposição em virtude da sua ligação com outras proposições já aceitas como verdadeiras (BARDIN, 2009, p. 41).

qual eles se encontravam, particularmente no contexto da Ciber Proteção. Outra contribuição da AC foi levar, também, em consideração a técnica de análise de enunciação, de forma que cada entrevista foi estudada de *per si*, em sua completude, como uma totalidade organizada e única.

Não obstante ao todo singular e original de cada entrevista extraído de *per si*, em momento posterior, as mesmas puderam ser 'comparadas' em conjunto, na medida em que as problemáticas de partida e condições situacionais foram pré-estabelecidas e padronizadas.

Em relação ao exame do conteúdo coletado, com a finalidade de auferir maior qualidade, foi realizada uma associação de diferentes formas de análise e de comunicação dos resultados, destacando-se:

a) análise de conteúdo;

b) condensação dos significados;

c) análise comparativa por intermédio de tabelas;

d) mineração de texto por meio da ferramenta Sobek[162];

e) análise de dados (textual) por meio do *software* IRAMUTEC[163].

## 9.1 Levantamento preliminar de requisitos

Preliminarmente, foram realizadas entrevistas com integrantes de estruturas imbricadas com a segurança e gestão da informação em meio digital, de acordo com o planejado no Apêndice A e tipificadas no quadro 13. A principal finalidade das referidas entrevistas foi levantar-se, no contexto internacional da Comunidade Europeia, novos insumos, abordagens, atividades e conjunturas imbricadas com a Ciber Proteção.

---

[162] A ferramenta Sobek foi desenvolvida no Programa de Pós-Graduação em Informática na Educação, na Universidade Federal do Rio Grande do Sul (UFRGS). Disponível em: <http://sobek.ufrgs.br/>. Acesso em: 10 abr. 2018.

[163] O IRAMUTEQ é um *software* gratuito e com fonte aberta, que permite fazer análises estatísticas sobre *corpus* textuais e sobre tabelas indivíduos/palavras. Para a utilização do aplicativo, foi necessário novo tratamento dos textos das entrevistas (*corpus*) de forma a adequá-lo ao processamento, bem como ajustar configurações para análise. Não obstante o elevado esforço despendido para a utilização da ferramenta, as possibilidades de análise geradas pelo IRAMUTEC, não foram, explicitamente, inseridas no presente relatório, devido as suas características, majoritariamente, quantitativas.

Quadro 13 - Estudo empírico – levantamento de requisitos

| INSTITUIÇÃO/ESTRUTURA | REFERÊNCIA | ENTREVISTADO |
|---|---|---|
| Centro de Competências em Cyber segurança e Privacidade - C3P (Portugal) | Competence Centre for Cyber Security and Privacy <http://c3p.up.pt/?lang=pt> | Diretor |
| Instituto da Defesa Nacional -IDN (Portugal) | National Defense Institute <http://www.idn.gov.pt/index.php> | Assessor do Diretor |
| Fraud Management Group of TM Forum | Global industry association <https://www.tmforum.org/> | Member Chairman's Committee |
| Centro Nacional de Ciber Segurança - CNCS (Portugal) | https://www.cncs.gov.pt/ | Coordenador |
| Gabinete Nacional de Segurança (GNS) | https://www.gns.gov.pt/ | Autoridade Nacional de Segurança |
| Centro de Investigação em Comunicação, Informação e Cultura Digita - Porto (CIC.Digital) | Center for Research in Communication, Information and digital Culture <http://web4.letras.up.pt/cic.digital.porto/> | Membro da Direção |
| Programa Doutoral em Informação e Comunicação em Plataformas Digitais (ICPD) | http://icpd.web.ua.pt/index.php/index/ | Diretor |

Fonte: elaboração própria

As entrevistas fizeram parte do rol de atividades desenvolvidas durante a participação no Programa de Doutorado Sanduíche no Exterior (PDSE), no período de abril a julho de 2017, na Universidade de Porto, Portugal. Na oportunidade, foram consultados especialistas em atividade nos ambientes de domínio científico (acadêmico), governamental e empresarial, ou seja, em consonância com a abordagem conhecida como Hélice Tríplice[164].

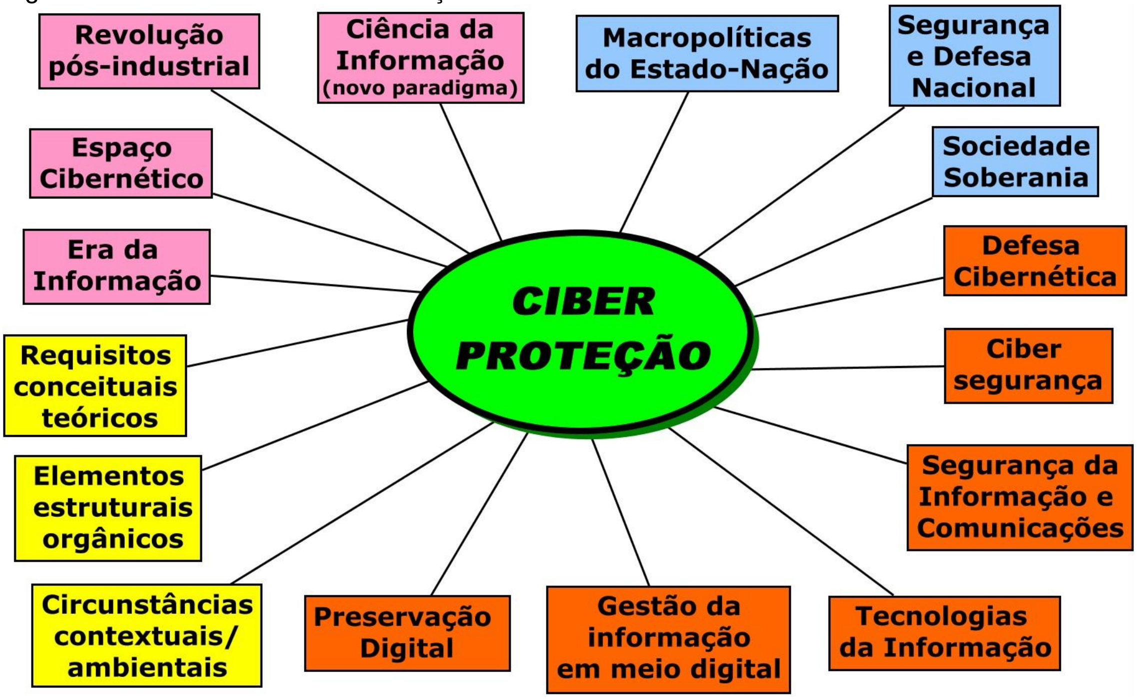
Como amostra simplificada dos frutos do levantamento supracitado, realizado durante o intercâmbio internacional, ressaltam-se alguns exemplos que foram, direta ou indiretamente, incorporados ao estudo:

[164] A abordagem da Hélice Tríplice, desenvolvida por Henry Etzkowitz e Loet Leydesdorff, é baseada na perspectiva da Universidade como indutora das relações com as Empresas (setor produtivo de bens e serviços) e o Governo (setor regulador e fomentador da atividade econômica), visando à produção de novos conhecimentos, à inovação tecnológica e ao desenvolvimento econômico. A inovação é compreendida como resultante de um processo complexo e dinâmico de experiências nas relações entre ciência, tecnologia, pesquisa e desenvolvimento nas universidades, nas empresas e nos governos, em uma espiral de 'transições sem fim'. Disponível em: <http://www.triple-helix.uff.br/sobre.html>. Acesso em: 20 jun. 2017.

a) aprimoramento da pesquisa bibliográfica, com a suplementação de fontes relacionadas à nova ordem mundial (plataformas digitais e interconectividade), ao paradigma pós-custodial, informacional e científico da CI e aos fluxos informacionais;
b) internalização de novas concepções e metodologias, particularmente o Método Quadripolar e o Modelo Sistêmico de Informação Ativa e Permanente (SIAP);
c) consolidação de abordagens, perspectivas e desafios relacionadas à investigação qualitativa na Gestão da Informação, no âmbito da CI;
d) inserção da segurança na gestão e na preservação da informação em meio digital;
e) conhecimento, *in loco*, de soluções, *modus operandi* e de estruturas relacionadas à segurança e defesa cibernéticas, inseridas no contexto globalizado, dinâmico e heterogêneo da comunidade europeia.

Parte expressiva das informações coletadas foi utilizada em várias seções desta pesquisa, subsidiando e norteando diversas fases do estudo, especialmente a estruturação metodológica e a revisão da literatura, culminando com a adequação e consolidação de entendimentos essenciais pré-estabelecidos, tais como: informação (em meio digital), segurança e Ciber Proteção. Neste último item, o levantamento realizado contribuiu para o fortalecimento do respectivo conceito, por meio do mapeamento de um conjunto de ‘entrantes’, que atuam na construção e atualização da Ciber Proteção, como demonstrado na figura 22.

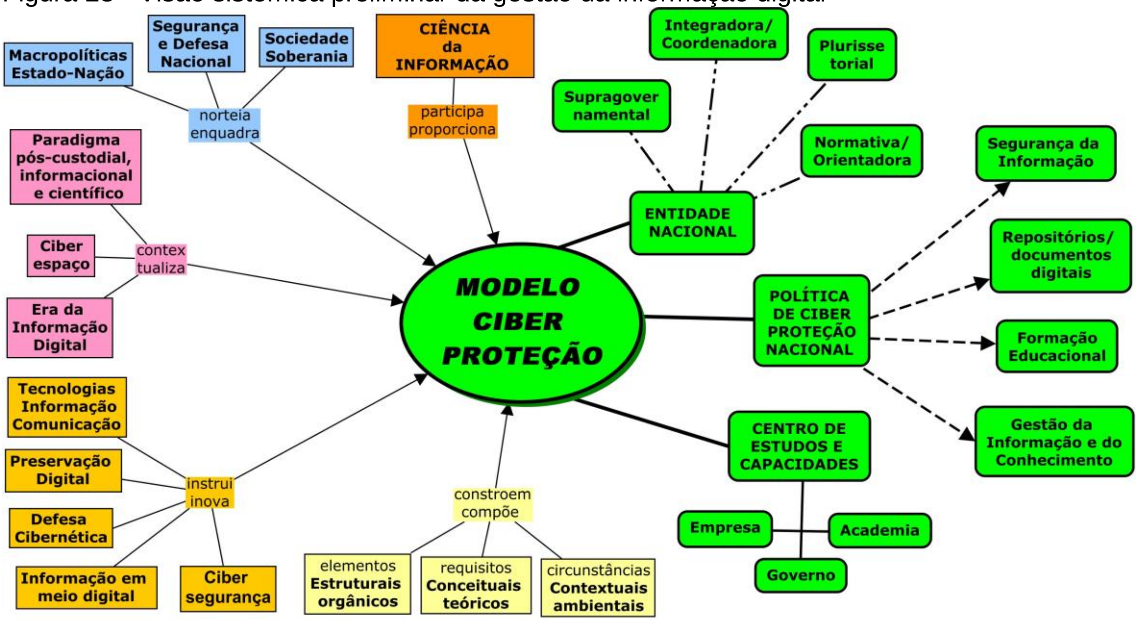
Figura 22 - Entrantes da Ciber Proteção




Fonte: elaboração própria

Tais interações possibilitaram alargar os horizontes acadêmicos da pesquisa, otimizar seu escopo técnico-científico e proporcionar a internalização de visões e soluções cosmopolitas para a segurança da informação digital. Proporcionaram as mesmas, também, a idealização de novos processos e reorganização dos requisitos para a gestão da informação em meio digital, potencializando uma primeira visão sistêmica do modelo de Ciber Proteção, graficamente representada na figura 23.

Figura 23 - Visão sistêmica preliminar da gestão da informação digital




Fonte: elaboração própria

A fim de complementar o levantamento internacional realizado durante o intercâmbio, bem como proporcionar uma visão mais abrangente e heterogênea dos entendimentos e dos *frameworks* globais, quanto à segurança e à defesa cibernéticas, foram analisadas diferentes concepções de outros países/organizações internacionais, destacando-se:

a) as atividades desenvolvidas pelo Inter-American Committee against Terrorism (CICTE) e pelo Cyber Security Program, da Organização dos Estados Americanos (OEA)[165], tais como as missões de apoio à estruturação da cibersegurança nos países-membros e os relatórios/estudos produzidos pela entidade;
b) as publicações da Asociación de Colegios de Defensa Iberoamericanos, em especial os elaborados durante seminários e conferências[166];
c) os estudos e orientações da OTAN como, por exemplo, o *National Cyber Security Framework Manual;*
d) as diretrizes sobre a proteção e o uso do ciberespaço do Reino Unido (UK), particularmente a *National Cyber Security Strategy 2016 to 2021*[167];
e) as estratégias nacionais e as estruturas de segurança dos Estados Unidos da América (USA), sobretudo a *National Cyber Strategy 2018*[168].

Na próxima seção, por meio de tabelas qualitativas, demonstra-se o resultado da segunda fase do estudo empírico, qual seja, as entrevistas com especialistas da Administração Pública Federal brasileira, imprescindível para a consolidação da proposta de Modelo para a Ciber Proteção nacional.

---

165 Disponível em: <http://www.oas.org/en/topics/cyber_security.asp>. Acesso em: 10 jun. 2018.
166 Disponível em: <http://www.asociacioncolegiosdefensaiberoamericanos.org/acdibero/LibrosReunionesDirectores/LIBRO+XVII+CONFERENCIA+-+CIBERDEFESA+E+CIBEREGURAN%C3%87A+NOVAS+AMEA%C3%87AS+%C3%80+SEGUR....pdf>. Acesso em: 10 mar. 2017.
167 Disponível em: <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf>. Acesso em: 13 dez. 2016.
168 Disponível em: <https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf>. Acesso em: 10 nov. 2018.

## 9.2 ESPECIALISTAS DA APF – DEMONSTRAÇÃO DE RESULTADOS

Procurou-se entrevistar especialistas da APF com histórico comprometimento com a Ciber Proteção brasileira, destaca-se que parte dos entrevistados participaram direta ou indiretamente nos planejamentos e/ou nas atividades operacionais, envolvendo a segurança da informação no ciberespaço de interesse nacional nos Grandes Eventos, entre 2012 e 2016. O quadro 14 resume os órgãos/instituições objeto das entrevistas, seu relacionamento com a APF, bem como tipifica os entrevistados.

Quadro 14 - Estudo empírico – consolidação e validação dos requisitos

| INSTITUIÇÃO/ESTRUTURA | VÍNCULO APF | ENTREVISTADO |
|---|---|---|
| Centro de Defesa Cibernética (CDCiber) | ComDCiber/MD | Subchefe |
| Rede Nacional em Segurança da Informação e Criptografia (RENASIC) | Comando do Exército/MD | Coordenador geral |
| Comando de Defesa Cibernética (ComDCiber) | EB/MD | Chefe de Gabinete |
| Departamento de Segurança da Informação e Comunicações (DSIC) | GSI | Diretor |
| Instituto de Tecnologia da Informação (ITI) | Casa Civil da PR | Coordenador-Geral de Operações |
| Secretaria de Política de Informática (SEPIN) | MCTIC | Assessor do Departamento de Ciência, Tecnologia e Inovação Digital (DECTI) |
| Secretaria de Tecnologia da Informação e Comunicação (SETIC) | MPOG | Coordenador geral de segurança da informação |
| Serviço de processamento de dados do governo federal (SERPRO) | MF | Analista de sistemas da Coordenação estratégica de gestão de segurança dos ativos da informação |
| Serviço de Repressão a Crimes Cibernéticos | DPF/MJ | Pesquisador e colaborador na área de crimes cibernéticos |
| Universidade de Brasília (UnB) | MEC | Professor do PPGCINF e da FCC<br>Ex-Diretor do CPD/UnB |

Fonte: elaboração própria

Inicialmente, o áudio das entrevistas foi transcrito na íntegra, com o objetivo de se manter o contexto original do momento das mesmas, resultando em um texto bruto constituído de perguntas feitas pelo entrevistador e respostas do entrevistado. Em seguida, sem a necessidade de alterar o conteúdo em si, houve uma edição dos dados para a retirada de expressões sem sentido, digressões e, em poucos casos, as falas que não possuíam relação objetiva com as perguntas, bem como tratou-se da pontuação e da correção gramatical de alguns trechos selecionados. Nessa etapa da transcrição, ressalte-se, houve especial cuidado de não permitir a mudança quanto ao sentido original da fala.

Na sequência, devido à extensão das respostas (duração média de oitenta (80) minutos por entrevista), foi utilizado o método de "condensação dos significados" sugerido por Kvale (1996, p. 192)[169], de modo que a resposta do entrevistado fosse resumida em formulações mais breves e sucintas para que, posteriormente, pudesse ser feita a identificação dos significados das mesmas.

Dessa forma, com algumas adaptações necessárias, como a anonimização do entrevistado e a descaracterização de sua instituição, as respostas foram condensadas em sentenças mais curtas, nas quais a essência e o sentido principal do que foi dito foram mantidos. Finalmente, tais condensações foram organizadas em tabelas, de forma que cada coluna armazenou as respostas individuais para cada uma das oito questões da entrevista.

Para os três blocos da entrevista (vide Apêndice B), foram elaboradas quatro tabelas a seguir representadas: a tabela 1 sobre os desafios do ciberespaço (questões 1 e 2), a tabela 2 abordando gestão segura e compartilhamento da informação (questões 3 e 4), a tabela 3 tratando das ações e políticas governamentais no âmbito da APF (questões 5 e 6) e a tabela 4 trazendo competências e entidades para a Ciber Proteção (questões 7 e 8).

---

[169] O autor descreve alguns métodos para a análise e interpretação das entrevistas, entre os quais: condensação de significados, categorização dos significados, estruturação da narrativa, interpretação dos significados e geração dos significados pela condensação das diferentes partes do material coletado nas entrevistas.

Tabela 1 - Proteção da informação no ciberespaço

| En | Questão 1- Em relação à proteção da informação no ciberespaço, quais seriam os principais desafios | Questão 2- Atuação dos governos em face da utilização do espaço cibernético no desenvolvimento nacional e da sociedade |
|---|---|---|
| E1 | A falta de percepção da insegurança latente que esse ciberespaço traz à pessoa comum e às organizações, e que as informações pessoais e institucionais transitem livremente e sejam um ativo importante. | O governo federal está patinando há bastante tempo: é a incapacidade governamental de formular políticas públicas nacionais efetivas para melhorar a questão da proteção da informação nos diversos níveis. |
| E2 | O principal desafio é com as pessoas. As administrações e as diretorias só vão olhar para segurança quando houver problema. A capacitação das pessoas e o aculturamento têm que ser sempre gradativas, constantes e crescentes, não só do pessoal de segurança. | O governo está parcialmente preocupado em utilizar o espaço cibernético, por meio de demandas de serviços. Necessita ampliar o cruzamento das informações nas bases de dados do governo. |
| E3 | Estabelecer qual informação interessa ser protegida e trabalhar as atitudes das pessoas. A fronteira daquilo que é privativo está muito fluida para as pessoas e afeta os ambientes corporativos, como, por exemplo, a publicidade de informações sensíveis, pessoais, nas redes sociais. | O governo federal está tentando seguir a corrente mundial. O os governos estaduais, municipais, federais poderiam aproveitar melhor os recursos digitais. Há carências de serviços. Poderiam ser trabalhadas muitas outras questões para inserção social, pois o atendimento em balcão é realizado em situações precárias. |
| E4 | Compreender, em termos nacionais, um conjunto básico de conceitos como: sistema de informação protegido, cibernética e a sua relação com a informação, a segurança e a defesa. Proteção das plataformas tecnológicas que o Estado utiliza para estabilizar os sistemas de informação que são usados para atender aos interesses da constituição de uma nação. | Para dar efetividade à utilização do espaço cibernético, os governos têm que lançar normas e estratégias de controle da informação e de comunicação da informação. A comunicação tem uma conotação muito política, e, ainda, há muita limitação. A comunicação do Estado com a sociedade ainda está muito frágil. No controle da informação, temos bons sistemas estruturantes dentro do governo federal, mas existe muita dificuldade nas agências individuas, cada qual com a sua política de informação própria, com o seu sistema e com seus controles particulares. |
| E5 | Uma estrutura mínima governamental de ciência e tecnologia para todo esse trabalho, que começa pela capacitação, porque não temos empresas nacionais que possam investir a fundo perdido. Não temos uma vontade nacional e isso acaba esbarrando sempre em problemas de Estado, de continuidade, no aspecto financeiro e na própria vontade das pessoas. | O governo federal brasileiro já tem uma estrutura para desenvolver políticas de TI, mas está fragmentada, com sobreposição de atividades e de mandos. Tem que se unificar o comando dessa estrutura na área operacional. |

| | | |
|---|---|---|
| E6 | O primeiro desafio de todos é a conscientização do governo, a cabeça dos dirigentes com a segurança do estado. O segundo é a nossa capacitação tecnológica, as pessoas capacitadas no nível mais 'micro', competência de base, de conhecimentos que possam gerar ferramentas próprias. Terceiro desafio seria criar uma estrutura eficiente e estratégica, uma estrutura de governança, que possa implementar, de forma mais eficiente possível, a segurança da informação no país, equilibrando o gasto com os controles e os prejuízos possíveis. A luta é praticamente permanente. | Eu não vejo, da parte do governo federal, nenhuma possibilidade, a curto prazo, disso. O governo tem atuado mal, porque ele não se preocupa com a geração do conhecimento no país. Há grande dependência de vontades individuais e políticas. O foco tem que ser no desenvolvimento nacional das ferramentas cibernéticas. |
| E7 | Baixa maturidade dos órgãos da APF nos processos e priorização de segurança da informação, aliada à descontinuidade do conhecimento produzido, bem como à falta de cultura de segurança pelos altos dirigentes. Baixa consciência individual e cultura organizacional, nas organizações públicas, de que a informação é do Estado e não do servidor. Faltam uma discussão sobre segurança no nível estratégico e uma legislação específica nacional de segurança da informação. | Os governos perderam tempo: a utilização do espaço cibernético foi precária e com poucos avanços. Houve muita descontinuidade administrativa, fragmentação da gestão e das propostas. Falta unidade nacional, há muitas soluções independentes e segmentadas. Por vezes, a infralegislação é mais forte que as políticas ou decretos. As soluções devem atingir, verticalmente, a União, estados e municípios e horizontalmente, os poderes executivo, legislativo e judiciário, além do setor produtivo e acadêmico. Falta articulação eficiente com a academia e as empresas nacionais. |
| E8 | Uma estrutura padronizada, tanto de compartilhamento de informação, quanto de ação coordenada, com canais de comunicação e os papéis de cada entidade bem definidos, além de uma mínima cadeia de comando, envolvendo não só o serviço público em si, mas, a indústria, as operadoras de telecomunicações e o próprio CGI.br. | O Brasil precisa entender que o espaço cibernético é um espaço de negócio e torná-lo um ambiente seguro para as pessoas usarem, portanto deve ter um mínimo de controle, de regulação. Os governos têm um foco muito forte nessa questão de neutralidade, de liberdade, de cada um fazer o que quiser na Internet, que é um espaço livre, mas não pode ser uma terra sem lei. |
| E9 | O Brasil não possui um instrumento normativo maior, na área da segurança da informação, que dê uma grande linha mestra nacional. Nas três esferas, nos três poderes, as diferentes iniciativas, normativos de diversos níveis: leis, decretos, resoluções, normas e instruções gerais, trazem, em seu bojo, várias informações ou recomendações sobre o tema. Entretanto, elas estão fragmentadas e completamente desalinhadas estrategicamente. O segundo desafio relaciona-se com educação e cultura. Nosso povo não tem fundamentos e maturidade cultural, em suma, não vê relevância ou preocupação com segurança. Seria fundamental inserir nos currículos acadêmicos e escolares, nos mais diferentes níveis, noções sobre a importância da segurança da informação em meio digital. | Na última década, houve um crescimento em termos de migração e de relevância de serviços públicos em plataformas *web*, porém, ainda aquém do necessário, com cerca de 60 por cento dos serviços, enquanto na União Europeia é um pouco acima de 80 por cento. Esses serviços estão sendo disponibilizados de forma crescente, o que também pode abrir uma grande janela, uma plataforma de ataques, particularmente porque os recursos de segurança necessários para a proteção são insuficientes. |

Fonte: elaboração própria

Tabela 2 - Gestão da Informação segura e organizacional

| En | Questão 3- Características/requisitos para a gestão 'segura' da informação em meio digital em uma estrutura ligada à proteção cibernética | Questão 4- Gestão da informação envolvendo atores governamentais e da sociedade civil em estruturas heterogêneas públicas e privadas |
|---|---|---|
| E1 | O fundamental é ter um documento normativo maior que alcance todos os segmentos, como as infraestruturas críticas, para que se possam uniformizar os procedimentos da proteção cibernética. | É o grande desafio do mundo: a confiança entre organizações. Um modelo de compartilhamento de informação tem que ser algo contínuo, fluindo naturalmente em situação de normalidade, com mecanismos tais como: reuniões de coordenação, manter rede de parcerias/relacionamentos e exercícios de segurança em infraestruturas críticas. |
| E2 | Proteção física do ambiente: energia, ar-condicionado, controle de acesso, combate ao incêndio. Pessoas com certificações em segurança e em gestão da informação, mais as campanhas de conscientização e treinamentos, promovendo a cultura de segurança. Monitoração e armazenamento com soluções de redundância para não se perder a informação. Todas as áreas têm que ter em suas equipes de segurança, no mínimo, pessoas de referência. | O que ajuda esse compartilhamento é ter confiança, que deve ser conquistada ao longo do tempo, mantendo o vínculo pessoal, e com reuniões de planejamento, não somente por causa de um problema. O governo peca em não manter o pessoal da segurança interligado. As infraestruturas críticas abrangem quase todo mundo, não há só órgãos de governo envolvidos. |
| E3 | Processos bem definidos, as informações valoradas, qualificadas e quantificadas e os controles estabelecidos claramente. Não adianta pôr tecnologia onde não há processo definido. Ponto mais importante, ao mesmo tempo mais frágil, é a gestão das pessoas, informadas e treinadas, bem como a avaliação permanente do que está sendo controlado. | Entendimento de que um grupo isolado não resolve quase nada, não há autossuficiência na proteção cibernética e é uma questão que se encaixa no Estado. A interação deve ser um mecanismo formal, com autorizações, com contato entre seres humanos em ambiente conhecido. Saber da necessidade e do planejamento da interação, onde, como e quando interagir, além de avaliar as lições aprendidas do que foi planejado e realizado. |
| E4 | Maior desafio é a constituição de um padrão ético de trabalho na administração pública. Em seguida, é a criação de uma estrutura de controle interno, que envolva a gestão de riscos, governança, comunicação e informação interna dentro das agências de governo. A ética considerada como uma ação reflexiva de pensar sobre o impacto de uma tomada de decisão. | Estabelecimento de processos de comunicação muito claros, a partir do desenvolvimento de percepções compartilhadas de mundo nas agências e nos seus integrantes. Construção de padrões básicos de comportamento (ética) comunicacional nas agências. Trazer a cada ente público envolvido uma percepção sistêmica da interdependência entre as partes, pois nenhuma agência é capaz de atuar isolada, devido à grande complexidade na solução dos problemas e no espaço do tempo em que é demandado. |
| E5 | Uma estrutura de dados brasileira, não só de proteção física como *data center*, mas também de salvaguarda da informação na Internet. Valorar e ampliar o entendimento da sociedade quanto ao valor da segurança da informação, não apenas individual, mas nacional, no contexto do tempo. | Algumas iniciativas foram muito boas, mas falta a noção de tempo, agilidade e uma estratégia do Estado que dê continuidade. O ser humano só se atina em trabalhar junto quando há catástrofe. Pensar a longo prazo, como unificar as grandes bases de dados estruturantes nacionais. |

| | | |
|---|---|---|
| E 6 | A segurança envolve tudo, todos esses ciclos da gestão da informação. A gestão tem que ser flexível e objetiva com ferramentas mais rápidas, não pode ser com essa burocracia fantástica que existe hoje no país, sem uma legislação específica para a cibernética. | A gestão deve ser distribuída e flexível, com o mínimo de burocracia, mas tem que haver um órgão central, no país, que cuidasse disso. |
| E 7 | Rastreabilidade para fazer auditoria nas informações, desde sua criação e classificação até o descarte, O ciclo da gestão é o grande desafio. Como definir qual é a informação que compromete a soberania nacional, essas metas têm que ser garantidas pela gestão do Estado, em 'datagovs', em ambientes controlados pelo governo. As informações que são ostensivas, com temporalidade, forma de guarda, e a integridade mantida. Legislação específica com abordagem singular para o Estado brasileiro. | É como se cada órgão/ministério fosse uma coisa isolada do outra, como se não fosse peça de um quebra-cabeça nacional. Falta comunicação e integração, além da descontinuidade e da alternância técnica, que gera muito retrabalho nas áreas mais operacionais. O modelo atual está fragmentado e gerou poder nas pontas, é preciso que haja uma agência central que favoreça uma plataforma única de gestão, um barramento, interoperabilidade das bases de dados. |
| E 8 | Proteger instalações que têm informação digital é muito mais complexo quando tudo é interconectado. Primeiro: seria classificar essa informação, o que é sensível, que necessita de elevada proteção do que é pública. Segundo: manter as regras de classificação definidas e terceiro: a questão da transparência da informação, com interesses diversos e difusos de grupos de ativistas, além de não existir proteção 100%. | Compartilhar informação é muito fácil, mas há um problema político: a gente não consegue organizar as entidades e definir um padrão de compartilhamento, de armazenamento de informação e até de relatórios entre os órgãos do governo e, menos ainda, com as operadoras de telecomunicações ou empresas de segurança, por exemplo. Falta centralizar e usar inteligência para correlacionar essas as informações. |
| E 9 | Preparo tanto no nível de técnico, como no de gerência. Confiabilidade: tem que passar um sentimento de confiança para população e objetividade pois o beneficiário último é o cidadão. Comprometimento de quem trabalha com proteção cibernética, buscando o autoaperfeiçoamento continuamente. | Os diferentes órgãos de proteção, hoje, atuam de forma episódica, dependendo do evento que venha a ocorrer. Eles deveriam atuar de forma sistêmica, perene e não de forma episódica, com a delimitação das missões de cada órgão, modelos de comunicação e reporte, relatórios de inteligência, reuniões sobre lições aprendidas, compilação de dados com amplo compartilhamento de informações, identificação de tendências e ameaças cibernéticas e o estabelecimento de protocolos de notificação de incidentes. |

Fonte: elaboração própria

Tabela 3 - Modelo de Ciber Proteção – APF

| En | Questão 5- As soluções governamentais adotadas, particularmente as políticas/regulatórias, têm apresentado resultado satisfatório | Questão 6- Pontos-chave ou requisitos imprescindíveis para otimizar a Ciber Proteção no Brasil/APF |
|---|---|---|
| E1 | Há grande carência de políticas públicas com o setor cibernético, não há nenhuma organização que esteja à frente, pensando na proteção. Cada órgão está cuidando da sua segurança, dando a sua solução. As estruturas existentes no país não se prestam a esse trabalho integrado, que alcance os envolvidos na segurança cibernética nacional. | Questão da normatização e da criação de uma equipe de resposta incidente (ETIR) nas organizações. Treinar e manter essas equipes especializadas para a proteção cibernética. Incentivo governamental para que as organizações pudessem investir parte do seu orçamento na qualificação do pessoal e na sua infraestrutura de segurança. Criar mecanismos para auditar a segurança de todos os órgãos da APF. |
| E2 | São importantes, há aquele Decreto 3505, mas ele está muito antiquado. As Normas Complementares do DSIC/GSI não estão sendo suficientes, são muito superficiais. As soluções precisam ser conversadas, ser montadas em conjunto, coordenadas e integradas, para serem confiáveis. Diferentemente da ESIC que o DSIC/GSI fez lá dentro, fechado, e depois queria a aprovação da APF. | Sinto falta de uma ação mais forte de coordenação e integração governamental, principalmente em relação à ocorrência de incidentes. Tem que se criar uma agência, fazer reuniões, assim, úteis, dar rumo, orientar, obrigar a ver dificuldades. Publicação de uma política de infraestrutura crítica do Brasil. |
| E3 | Em relação à proteção cibernética, as políticas e normas vigentes podem melhorar, mas estão favorecendo e já têm trazido resultados positivos. O que antes era meramente teórico e estava nos livros, hoje está na prática de algumas organizações governamentais. | É uma questão orçamentária geral, para permitir uma manutenção e até mesmo um acréscimo de investimentos voltados para Proteção Cibernética. O Estado possui um papel fundamental da educação para a Proteção Cibernética, na formação do conhecimento atual e futuro. |
| E4 | O Estado brasileiro tem uma percepção da estrutura que se refere ao serviço público. Na parte tecnológica, estamos muito mais vulneráveis do que antes, exatamente porque incorporou-se de forma muito rápida um conjunto muito grande de tecnologias, sobre o qual, de fato, não existe um domínio local, nacional. Quem tem o entendimento da consciência situacional do país, hoje, o que pensa a sociedade, para onde ela vai, o que está acontecendo na ponta, são as mídias sociais, o Facebook e o Google. É a chamada colonização cibernética. | A construção econômica determina muito do que a gente precisa fazer em termos de segurança e de defesa no futuro. A ausência de tecnologia informática própria, de infraestrutura e indústria de *software* ou de *hardware* nacionais causa uma dependência muito forte e vulnerável. Desenvolvimento da indústria local, o empreendedorismo, e a substituição dessas plataformas estrangeiras por plataformas que a gente possa controlar. |
| E5 | A gente caminha para uma sociedade mundial de autodisciplina, então, essa proteção, esse controle deveria vir abaixo. A regulamentação desde a TI até as comunicações andam bem, mas em termos de política, a gente tem soluços, falta trabalho conjunto, uma política de Estado. | Aglomerar órgãos, ministérios para fazer um trabalho contínuo, não se pode parar no tempo, acreditar que vai dar certo, que vai se transformar em produto, com pessoas qualificadas, com pessoas que deram certo. |

| | | |
|---|---|---|
| E 6 | Para a consciência situacional, evidentemente que não. A 3505 precisa ser atualizada e ter as suas missões claramente distribuídas e cumpridas, tanto interna, como externamente ao GSI. | Estrutura vinculada a um órgão de Estado do país. Com procedimento sistemático, interagências, com capacidade de liderança e capacidade técnica, não político. O objetivo é ter ferramentas que possam compartilhar informações entre as centrais e esses órgãos, principalmente das infraestruturas críticas, entre a TI e as TA. |
| E 7 | Está ineficiente. O arcabouço jurídico/legal é arcaico, distribuído, limita, não permite interoperabilidade, troca de informações. Falta legislação única que determine a criação de um núcleo que avaliasse a segurança, a partir de matrizes setoriais, envolvendo as bases de dados federais, a fim de proporcionar um mapa de risco cibernético da APF. Tem que insistir nessa meta, sob pena de responsabilidade. | Discussão nacional (atualização) em torno da legislação nacional que afeta a segurança cibernética. Implementar a gestão do risco e continuidade do negócio. Compartilhar as infraestruturas de TI e a constituição de um núcleo com os *data centers* nacionais. Disciplinar mais a fundo e mesmo reduzir a terceirização da TI, principalmente em áreas sensíveis e a criação de uma carreira de Estado específica para a segurança. Diretrizes de atuação de segurança centralizadas com operacionalização descentralizada. |
| E 8 | A resposta simples seria não: faltam políticas. E as que existem são muito genéricas e não são cumpridas, falta conformidade e fiscalização. As normas do GSI, por exemplo, não têm força ou poder de implementação, falta uma cobrança pela execução do que os normativos propõem. | A questão de comando, ter informação de segurança centralizada e padronizada para ser disseminada, ter a informação sensível, saber o que é crítico no país, como nas infraestruturas críticas, de uma forma organizada. Criar uma agência de segurança cibernética central, que ela coordene o processo normativo e operacional. Ter um nível mínimo nacional público e privado, não somente na APF, de segurança cibernética, pensar nisso de uma forma sinérgica e de ambiente cibernético brasileiro mais seguro. |
| E 9 | Essas soluções governamentais têm funcionado de modo setorizado para determinada parte do estado brasileiro, ou parte da população, mas não para todos. Os resultados são muito fragmentados, apesar de ser muito difícil mensurar. Acredito que ela tem representado resultado satisfatório para essas fatias representativas, mas não no âmbito nacional. | Tentar trabalhar em conjunto, por meio de um instrumento macropolítico, uma política de alcance nacional, que 'vertebralize' todas as iniciativas vigentes e futuras. Nós esperamos que o Estado faça isso, porque a segurança, em âmbito 'macro', é responsabilidade da União, embora a Constituição não mencione segurança da informação ou proteção cibernética, até porque, quando a constituição foi escrita, nós não nos preocupávamos tanto com isso, uma vez que é a segurança do cidadão que está em jogo. |

Fonte: elaboração própria

Tabela 4 - Modelo de Ciber Proteção – Competências

| En | Questão 7- Criação de uma entidade articuladora e normativa, em âmbito nacional, voltada para a salvaguarda do ciberespaço brasileiro | Questão 8- Competências cibernéticas representativas no contexto nacional/internacional? Proposta de um centro aglutinador baseado no padrão triplo hélice |
|---|---|---|
| E1 | Para nossa cultura, para o Brasil, tem que haver uma agência que possa começar a normatizar todos esses assuntos, e ter o poder também de órgão de fiscalização, para fazer cumprir, senão fica mais um documento que vai ser letra-morta e sem nenhuma implementação. Utilizar de premiações para motivar, trabalhar a mentalidade, conscientizar as pessoas com relação à segurança e atingir padrões de desempenho mais elevados. | Em termos de capacidades, não há dúvida de que nós temos de sobra, falta é algo que possa amalgamar essas pessoas nessas três grandes áreas. Seria estratégia para atrair esse pessoal, dentro do país, a fim de construir uma equipe que possa conduzir e melhorar a proteção cibernética no âmbito nacional. Não adianta fazer uma agência que seja só governo, ela não vai alcançar os outros setores. Sob perspectiva geopolítica, a base de tudo é a formulação de políticas públicas e a construção de organizações, como a de segurança cibernética dentro do próprio país, para que a gente possa vir a exportar modelos e ser referência no nosso entorno estratégico. |
| E2 | Eu imagino alguma coisa mais ampla, como essas outras agências, como a Anatel, sem subordinação a um Ministério, com um plano de resposta cibernética e uma continuidade planejada e mínima dos seus integrantes. | É importante criar, ter um centro de referência, de excelência em termos de segurança junto às Universidades, como nos Estados Unidos, tipo o NIST que pudesse disponibilizar boas especializações para quem sai da Universidade. As competências no Brasil estão espalhadas. |
| E3 | Eu acho que é viável uma entidade articuladora e que a gente vai chegar lá, em breve. Eu só espero que as atitudes de um ente dessa natureza não sejam exageradas, como em alguns outros estados nacionais que acabam tropeçando nisso, e vão muito além do que deveriam ir. | Se o assunto é conhecimento, tem se que dar liberdade, com diversos locais, segmentos e grupos trabalhando e pensando por conta própria. Deve-se buscar a interação entre eles com a sociedade e com as atividades empresariais. Um ciclo da ciência pura para ciência aplicada bem fluente, dentro do dinamismo da sociedade. Ter um órgão da Administração Pública para compreender e favorecer alguns temas e trazê-los para o Estado. |
| E4 | A construção de uma agência de Estado que venha fazer um trabalho efetivo de Ciber Proteção, respondendo a problemas complexos emergentes, depende da consolidação do pacto federativo que envolva os entes federais, a União, com estados e municípios. As contaminações cibernéticas se espalham como doenças contagiosas e elas têm ciclos complexos sistêmicos. Seria como um sistema único cibernético, à imagem de um SUS da saúde. | Nós temos muitas competências, mas a estrutura é muito caótica, imatura, deveria ser uma estrutura de um sistema integrado nacional.<br>Sem dúvida, uma estrutura de tríplice hélice pode ajudar nesse caso. O grande problema é a necessidade de possuir uma dimensão econômica muito forte para poder sustentar o investimento, além da existência de um isolamento grande entre o setor, vamos dizer, produtivo, e as instituições de pesquisa, as universidades. É preciso haver uma grande desregulamentação / flexibilização em níveis altos, na área de pesquisa nacional. As amarras para o investimento, por meio de uma empresa privada, são muito grandes. |

| | | |
|---|---|---|
| E5 | A estrutura deve ter visão global e ser autônoma, em que a gente possa se apropriar de todas essas informações governamentais. Interligando tudo, em âmbito geral, somando esforços, mandatário e que cubra resultados dos gestores, utilizando as instituições já existente na APF. | Não há dúvida de que possuímos competências. Órgão, estrutura governamental para isso, a gente também tem, o que falta é gestão com qualidade, trabalhar em conjunto para o bem comum, faltam modelos e maturidade para errar até acertar. |
| E6 | A agência é uma entidade articuladora, normativa, operacional, científico-tecnológica, prospectiva. Ela tinha que pensar em tudo, é o perigo da centralização, mas, se continuar distribuída, não vai avançar, precisa de uma articulação governamental, uma consciência do governo e da alta camada da administração sobre o problema. | Eu não tenho dúvida de que já possuímos ou demonstramos competências na área pessoal. Na área de *software* nós temos vocação, na área de pesquisa e inovação também. Quanto ao *hardware* é mais complicado. Temos uma classe de *hackers* do bem no Brasil, e inclusive no exterior, trabalhando em cargos de destaque em grandes empresas internacionais. |
| E7 | Nós temos que criar a agência nacional nucleadora de segurança da informação independente, onde as pessoas que compõem essa agência, tenham a menor ligação política possível, pois Informação é um ativo muito valioso. Ela tem que ter rotatividade: quem estiver no comando, não pode ficar ali mais de dois anos, tem que ser dinâmico, com servidores de Estado e colaboradores setoriais. | O desafio cibernético passa por uma atuação desse órgão tripartite, e essencial: setor produtivo, governo e academia, nós deveríamos criar, pensar, sempre ligados a um nucleador, tendo o Estado como o gestor e comprador de soluções. |
| E8 | É viável e imprescindível, mas tem que haver quebra de muitas barreiras políticas e pessoais. O CGI é um elemento-chave nessa questão. Nós temos um ambiente muito de desconfiança do setor privado com o governo, e vice-versa, às vezes, até entre setores dentro do próprio governo. talvez precise de uma lei para se criar essa agência, neutra, e com poder de coordenar todo resto. | A gente tem essa competência, mas ela não é global. Você tem centros de excelência em locais específicos. Mas há uma de fuga de cérebros absurda, que tende a se intensificar. Os elementos existem, mas falta direcionamento, uma visão mais ampla do negócio, apoiar o mercado e, às vezes, proteger um pouco essas empresas, valorizar conteúdo nacional, essas iniciativas de tecnologia de ponta privadas e públicas, pois existe um conflito entre a parte comercial global e a soberania nacional. |

| | | |
|---|---|---|
| E9 | O fundamento de tudo é a educação, que vai levar à mudança de cultura. Nós não temos como fazer diferente e, sem progredir na educação na área de proteção cibernética, nós não vamos conseguir diminuir o *gap* que nós temos para outros países. Nós acreditamos que seja viável, realmente, a criação de uma entidade articuladora e normativa. Um conselho e uma Agência nacional, estabelecendo requisitos mínimos de proteção a nível nacional para organizações públicas e privadas, inseridos em um sistema nacional de segurança da informação. Não seria uma agência reguladora, como é a Anatel, Anac, ou ANTT, mas uma agência de agentes, como é a Abin. | Sobre a competência pessoal, nossa massa crítica é muito boa: nós temos grandes conhecimentos A diferença é o nível de organização das pesquisas e competências. Na parte de *software,* são poucas as instituições nacionais que possuem independência no nosso país, ainda estamos embrionários, nós teríamos que fomentar o desenvolvimento dessas empresas. Na parte de *hardware*, a situação é um pouco pior, porque nós dependemos de algumas tecnologias de proteção de *chips* e circuitos integrados, cuja grande maioria vem de fora. O isolamento é a fórmula do fracasso, mas a criação de estrutura no país é muito difícil, porque, do ponto de vista político, nós estamos vivendo um momento em que os recursos estão sendo muito parcos, mas é uma iniciativa excepcional tentar construir um pensamento comum, inclusive com organizações não governamentais e outras entidades civis sem fins lucrativos, que pesquisem a segurança e bem-estar da população. |

Fonte: elaboração própria

De acordo com Gibbs (2009, p. 103), “as tabelas qualitativas são uma forma conveniente de mostrar o texto proveniente de todo um conjunto de dados, de uma forma que facilita uma comparação sistemática”.

Assim, além de demonstrar os resultados do levantamento empírico, as tabelas viabilizaram a realização de análises comparativas, desenvolvidas na próxima seção, demonstrando diferenças e associações entre os posicionamentos e percepções dos entrevistados.

## 9.3 Especialistas da APF - Análise dos Resultados

Como ficou apresentado na seção anterior, os dados e evidências coletados foram tratados do ponto de vista comparativo (busca de pontos em comum, divergências e interações), no caso, entre o conhecimento técnico e gerencial de especialistas nacionais acerca da questão central da pesquisa, nomeadamente a segurança da informação digital em âmbito nacional. Assim, a utilização das informações coletadas, nas entrevistas, requereu ações transformadoras tais como:

a) tratamento do elevado volume de dados coletados (aproximadamente 17 horas de áudio);
b) conversão dos áudios em texto escrito;
c) interpretação das posturas e posicionamentos dos entrevistados durante as entrevistas;
d) estruturação e apresentação dos resultados alcançados por meio da condensação de significados (tabelas);
e) adequação na estrutura dos textos-base (áudios convertidos), a fim de proporcionar conformidade com os aplicativos (*softwares* de mineração de texto) utilizados para tratamento das respostas.

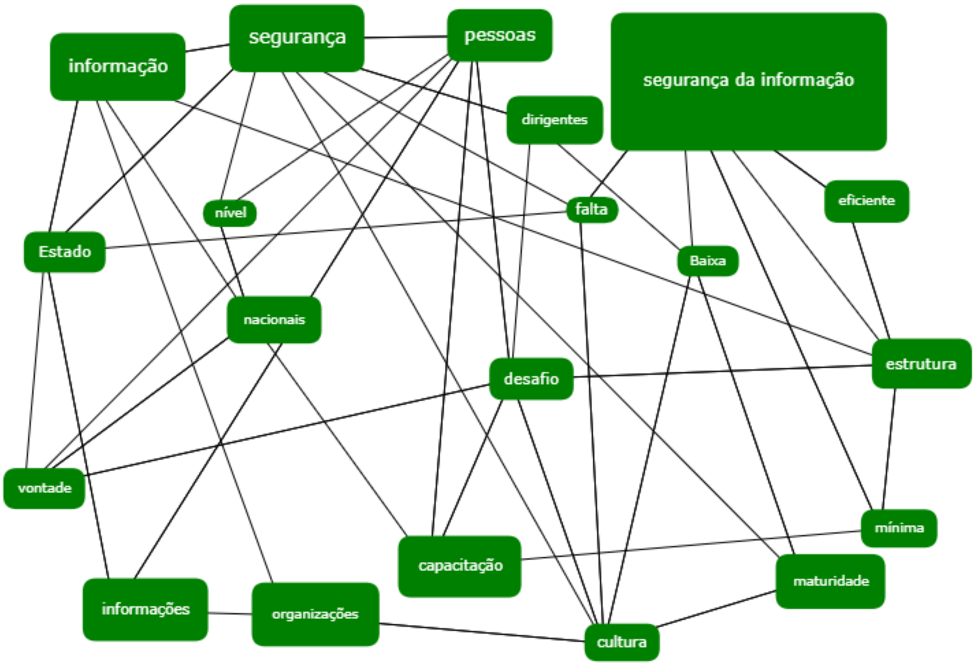
Nesta fase, foi utilizada, como suporte de análise, a técnica de mineração de texto, a qual permite a extração, a análise e a identificação de informações relevantes (P.ex.: os termos mais frequentes e as conexões/relações entre eles), a partir de dados não estruturados ou semiestruturados como entrevistas.

Foi utilizada a ferramenta Sobek, que possibilitou visualizar um diagrama conciso com os principais termos e as relações de um texto, no caso específico deste trabalho, o conjunto das respostas dos nove entrevistados para cada uma das oito questões formuladas. Foram considerados não só o número máximo de vinte conceitos como também a frequência mínima superior a dois, para relacionamento dos termos, bem como descartadas algumas palavras frequentes tais como artigos, preposições, advérbios entre outras.

### *9.3.1. Q1 – Ciberespaço e seus desafios*

No que se refere aos desafios do ciberespaço, na primeira pergunta da entrevista, representada graficamente pela figura 24, destaca-se a importância da Segurança (em seu sentido *lato*) e da informação para o Estado, paradoxalmente a precariedade e falta da maturidade, no que tange à segurança da informação, encontradas, principalmente, nas pessoas, dirigentes e organizações. Os desafios para alavancar uma cultura de segurança da informação digital apontam para a necessidade de vontade política (P.ex.: conscientização da alta administração e continuidade na distribuição de recursos financeiros), de capacitação tecnológica e de estruturas de proteção cibernética eficientes.

Figura 24 - Questão 1 - Desafios da informação no ciberespaço

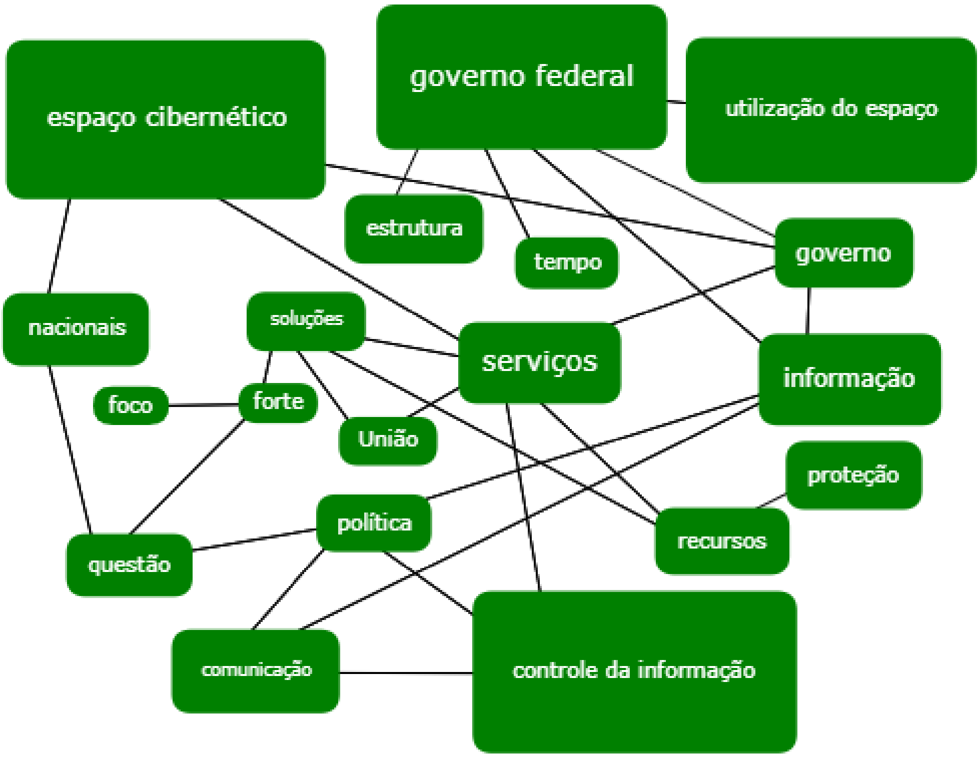



Fonte: elaboração própria

### *9.3.2 Q2 – Ciberespaço e a atuação governamental*

A figura 25 aborda a atuação dos governos, em face da utilização do espaço cibernético, no desenvolvimento nacional e da sociedade, ressaltando-se a necessidade premente de políticas, estratégias e normas mais efetivas. Neste contexto, avulta de importância uma melhor adequação das soluções e das estruturas de TIC nacionais nos diversos níveis de governo e poderes constituídos, de forma que a prestação de serviços, a comunicação com o cidadão e o uso da Internet, como espaço globalizado de negócios, atinjam um padrão competitivo internacionalmente. Percebe-se, também, a necessidade de uma 'centralização' de propostas de Estado, aliada a iniciativas de controle, essenciais à boa execução da gestão e da segurança da informação em meio digital.

Figura 25 - Questão 2 - Atuação governamental no ciberespaço

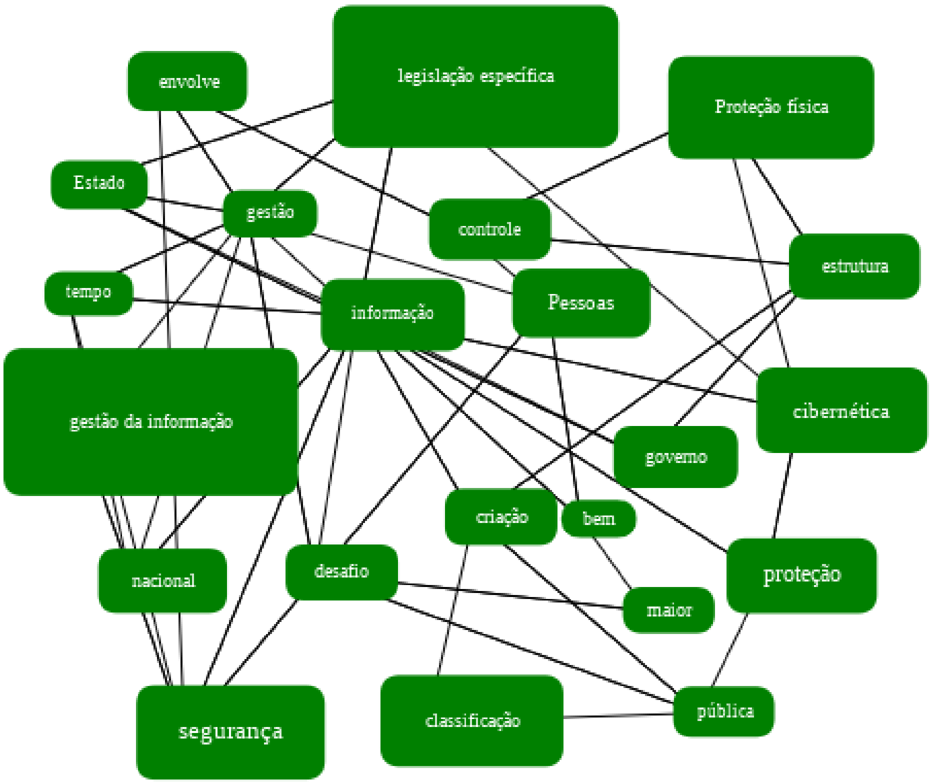



Fonte: elaboração própria

### *9.3.3 Q3 – Requisitos para a gestão segura da informação digital*

Evidenciaram-se três macrotemas acerca das características ou requisitos para a gestão ‘segura’ da informação em meio digital: recursos humanos, arcabouço normativo e gerenciamento informacional, conforme ilustrado na figura 26. Destacou-se a gestão de pessoas, englobando desde equipes de segurança capacitadas com elevados padrões éticos e caracterizadas pelo autoaperfeiçoamento, até a conscientização do valor da segurança da informação no seio da Sociedade/Nação. A legislação específica, particularmente normativa de Estado, deve contemplar processos, controles e ferramentas de auditoria, incluindo a proteção da informação nas instalações estratégicas, como as infraestruturas críticas. Apontou-se a necessidade de promover a gestão 'segura' do ciclo da informação, ressaltando-se a criação, classificação (caráter sensível/comprometimento *versus* transparência), armazenamento, rastreabilidade e descarte da informação, tanto ostensiva como sigilosa, pública ou privada, desde que seja de interesse do Estado.

Figura 26 - Questão 3 - Requisitos para a gestão segura da informação

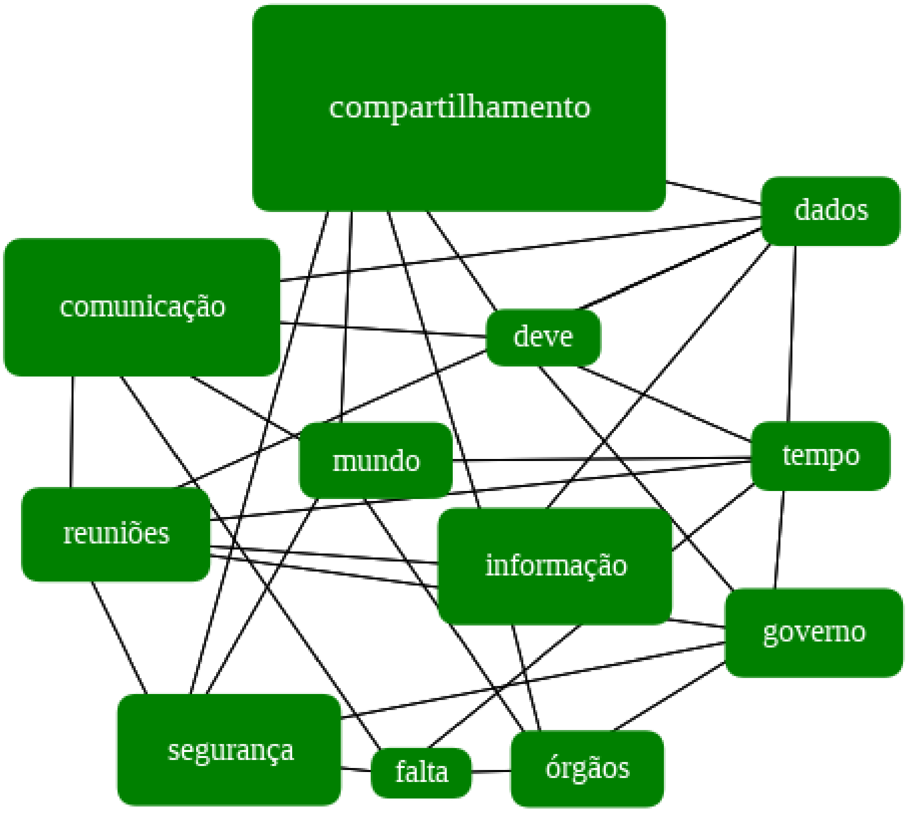



Fonte: elaboração própria

### *9.3.4 Q4 – Gestão da informação em estruturas heterogêneas*

A necessidade de compartilhamento de dados, em tempo oportuno, entre órgãos governamentais e a falta de comunicação contínua e padronizada sobre segurança afloram de importância nas respostas sobre a quarta questão: gestão da informação, envolvendo atores governamentais e da sociedade civil em estruturas heterogêneas públicas e privadas, como ressalta a figura 27. Entende-se que a complexidade e a capilaridade das soluções demandam uma visão sistêmica e de interdependência na proteção cibernética. Nesse sentido, a disseminação de novas vulnerabilidades, ameaças e tendências globais, bem como das formas de mitigação favoreceriam uma maior interação e cooperação, estabelecendo laços indispensáveis de confiança entre as equipes de segurança/órgãos de proteção.

Figura 27 - Questão 4 - Gestão da informação em estruturas heterogêneas

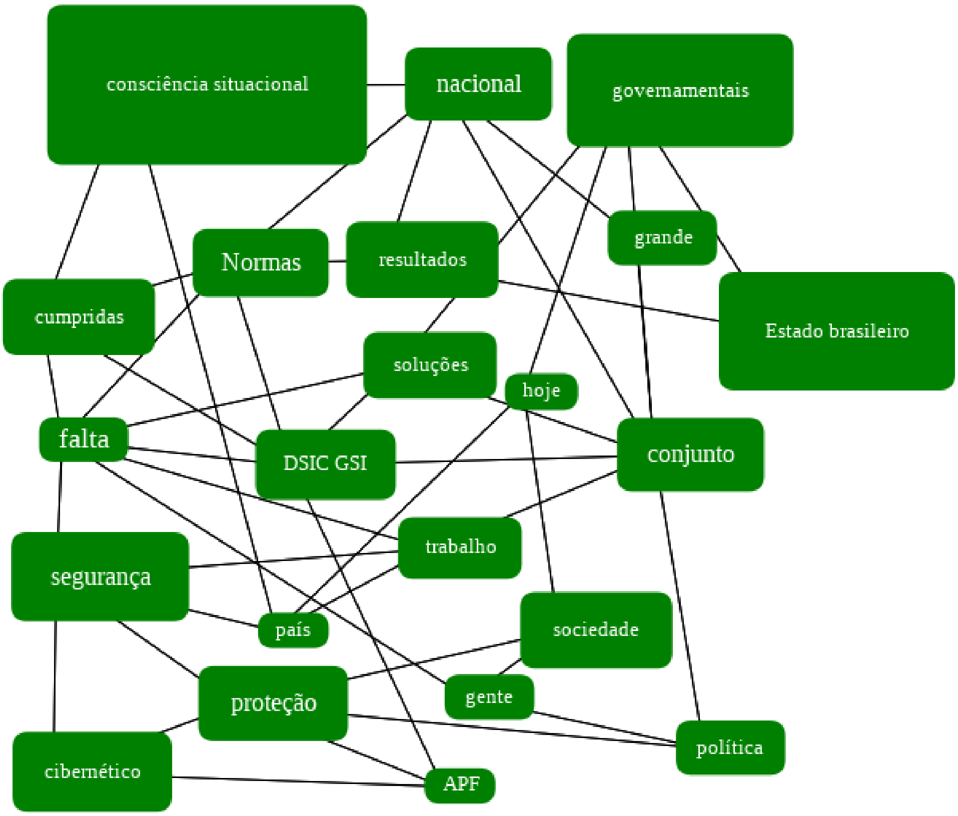



Fonte: elaboração própria

### *9.3.5 Q5 – Soluções políticas/regulatórias governamentais*

Os entrevistados foram unânimes ao apontar diferentes deficiências no que tange à regulamentação da segurança do espaço cibernético nacional, amalgamadas na figura 28. Registra-se que os normativos de base, como leis e decretos, estão defasados temporalmente e/ou tecnologicamente, ressentindo-se de ferramentas de responsabilização, cobrança de execução, conformidade e fiscalização. As regulamentações deveriam ser estratégias e não setoriais, favorecendo a integração e a interoperabilidade entre público e privado, assim como a construção da consciência situacional nacional (uma visão conjuntural) da proteção cibernética.

Figura 28 - Questão 5 - Soluções políticas/regulatórias governamentais




Fonte: elaboração própria

*9.3.6 Q6 – Pontos-chave para otimização*

Como requisitos imprescindíveis para otimizar a Ciber Proteção no Brasil, foram apresentadas propostas centradas na segurança das infraestruturas críticas, na necessidade de compartilhamento de informações de segurança cibernética e no trabalho em conjunto das equipes de tratamento de incidentes. A figura 29 destaca, também, o papel do Estado como catalizador das atividades de proteção por meio de políticas e ações integradoras, bem como no desenvolvimento de tecnologias (*hardware/software*) nacionais. Nesse aspecto, enfatizaram-se não só a questão orçamentária governamental, como também a redução da burocracia estatal como elementos cruciais no desenvolvimento da indústria local e do empreendedorismo.

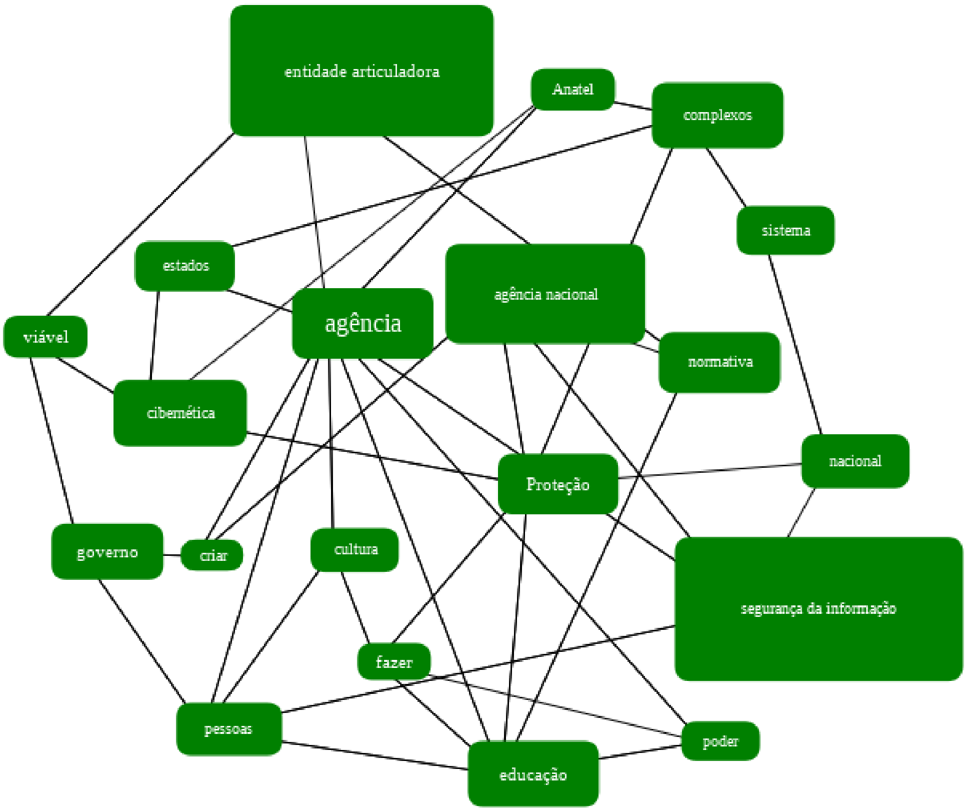
Figura 29 - Questão 6 - Pontos-chave para otimização


Fonte: elaboração própria

### *9.3.7 Q7 – Entidade articuladora e normativa*

A seguir, a figura 30 reflete a crença dos pesquisados na necessidade de uma entidade autônoma, articuladora e prospectiva, com capacidade de trabalhar as ações inerentes à proteção cibernética nacional, sob o mínimo de interferência política. Independentemente da sua estrutura, que pode ser, por exemplo, um conselho ou uma agência, seus integrantes devem possuir formação técnico-científica, que contribua para a proteção cibernética, e serem originários de diferentes setores nacionais, com servidores do Estado e colaboradores do setor privado. É necessário, ainda, haver uma ação normativa e fiscalizadora, atingindo todos os níveis da administração pública, todos os poderes do Estado, bem como o setor privado.

Figura 30 - Questão 7 - Entidade articuladora e normativa

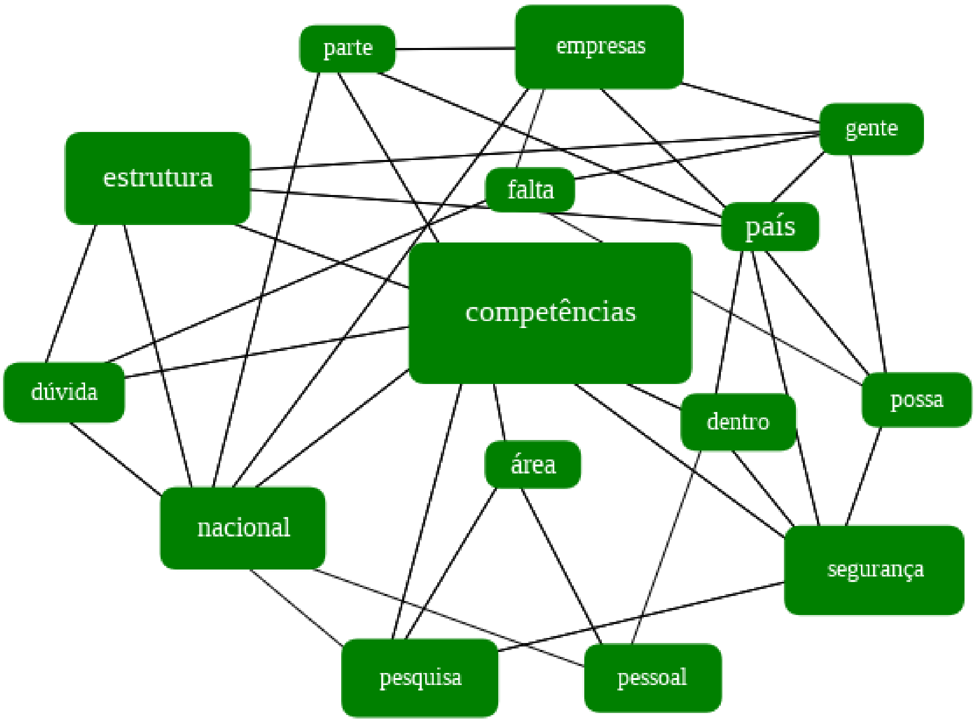



Fonte: elaboração própria

*9.3.8 Q8 – Competências e centro aglutinador*

Os entrevistados concordaram quanto à necessidade de se instituir uma estrutura aglutinadora de referência nacional, vocacionada para a salvaguarda das competências do país tanto em termos de recursos pessoais como em soluções desenvolvidas (processos, *hardware* e *software*). De fato, na figura 31 aponta-se que não há falta de competências, mais sim de direcionamento. Assim, a referida entidade se encarregaria da gestão efetiva dos incentivos públicos, orientando e integrando a pesquisa acadêmica, quanto às demandas empresariais e governamentais.

Figura 31 - Questão 8 - Competências e centro aglutinador




Fonte: elaboração própria

De acordo com os pontos centrais das perguntas, as respostas foram compiladas por meio das quatro tabelas de cunho qualitativo, enriquecendo o *corpus* investigativo da tese, assim como, de modo particular, as análises comparativas (instrumentadas por meio do aplicativo Sobek) corroboraram para a validação do modelo proposto de Ciber Proteção nacional.

A próxima seção consolida e estrutura os requisitos para um modelo de gestão da informação nos órgãos e entidades públicos, relacionados diretamente com a Ciber Proteção.

# 10 MODELO PARA A CIBER PROTEÇÃO NACIONAL - MCPN

Neste capítulo, apresenta-se uma proposta de “Modelo para Ciber Proteção Nacional" (MCPN). As considerações que se seguem tiveram como ponto de partida as evidências e as experiências obtidas na observação participante, bem como nos trabalhos acadêmicos realizados pelo autor. Como elementos construtores e delimitadores, a revisão da literatura e o estudo empírico foram fundamentais na estruturação, otimização e validação do modelo proposto.

Neste estudo, alinha-se o entendimento do termo 'modelo', no contexto da análise de dados qualitativos, com o de Graham Gibbs (2009, p. 112): "Estrutura que tenta explicar o que foi identificado como aspectos fundamentais de um fenômeno em estudo, em termos do número de outros aspectos ou elementos da situação".

Os elementos angulares do MCPN, que se tipifica como um modelo conceitual, são baseados nas sugestões de Strauss e Corbin (Gibbs, 2009, p. 113), onde “as condições causais produzem o fenômeno, que, por sua vez, gera as estratégias nos contextos. Estas são mediadas por condições que intervêm, produzindo ações e interações que resultam em consequências”. Essa codificação axial, quer dizer códigos que representam e destacam as questões ou temas centrais nos dados, encontra-se exemplificada no quadro 15.

Quadro 15 - Elementos do modelo de Ciber Proteção

| CÓDIGOS | ELEMENTOS/ARGUMENTOS DO ESTUDO | OBSERVAÇÕES |
|---|---|---|
| CONDIÇÕES CAUSAIS | Era da Informação; Sociedade em rede; Espaço Cibernético; Paradigma pós-custodial, Informacional e científico; Macropolíticas do Estado-Nação; Segurança e Defesa Nacional; Sociedade e Soberania; Defesa Cibernética; Segurança da Informação e Comunicações; Tecnologias da Informação; Gestão da informação em meio digital; Preservação Digital | Influencia a proteção da informação em meio digital, embasa a construção do conceito de Ciber Proteção e seus desdobramentos no modelo |
| FENÔMENO | Propostas para reduzir as vulnerabilidades e mitigar as ameaças aos recursos informacionais do Estado brasileiro – Proteção da informação em meio digital - Ciber Proteção | Ideia central, conceito angular construído pelo autor |
| OBJETIVOS ESPECÍFICOS/ESTRATÉGICOS | - Contextualizar a proteção da informação no ciberespaço<br>- Analisar conceitos e perspectivas de gestão da informação sob a ótica de segurança em meio digital e defesa do ciberespaço<br>- Identificar os padrões e a situação da gestão da informação nas estruturas institucionais relacionadas com a Ciber Proteção<br>- Definir os requisitos para um modelo de gestão da informação nas estruturas institucionais relacionadas diretamente com a Ciber Proteção | Ações tomadas ao longo do estudo para alcançar a melhor proposta de Ciber Proteção nacional |

| | | |
|---|---|---|
| CON-TEXTO | - Administração Pública Federal – APF<br>- Gestão e *modus operandi* das "Estruturas" voltadas para a gestão de segurança e defesa cibernética | Contexto da pesquisa, escopo de aplicação (inicial) da Ciber Proteção |
| CONDI-ÇÕES IN-FLUENCI-ADORAS | - Acesso a registros e relatórios operacionais acerca de atividades sensíveis de segurança e defesa<br>- Elevada influência política (em detrimento da técnica) nos órgãos responsáveis pela SIC<br>- Falta de consciência cibernética em particular entre políticos e dirigentes<br>- Extinção/enfraquecimento/criação de instituições imbricadas com a Ciber Proteção<br>- Ausência de atualização e de integração do arcabouço normativo inerente à proteção da informação digital<br>- Descontinuidade de atividades e projetos em SIC | Condições que moldaram, facilitaram ou dificultaram a consecução dos objetivos/estratégias |
| AÇÃO/IN-TERAÇÃO | - Participação operacional na gestão de incidentes em redes de computadores<br>- Coordenação e assessoramento nas atividades de segurança e defesa cibernéticas nos GE<br>- Avaliação do arcabouço legal<br>- Análise da literatura e das melhores práticas<br>- Entrevistas com especialistas nacionais e estrangeiros | Ações realizadas na construção e validação das propostas para reduzir as vulnerabilidades e mitigar as ameaças aos recursos informacionais em meio digital |
| CONSE-QUÊN-CIAS | - Diagnóstico e conceituação do fenômeno Ciber Proteção<br>- Macrossistema de proteção cibernética<br>- Política nacional de Ciber Proteção<br>- Estrutura integradora e supragovernamental<br>- Centro de inovação e competências | Desdobramento e ações do Modelo de Ciber Proteção Nacional |

Fonte: elaboração própria

Não obstante, devido às características *sui generis* do fenômeno da proteção da informação em meio digital, convém que a referida proposta: organize normas e procedimentos, formalize (novas) estruturas, estabeleça responsabilidades e áreas de atuação; não se limitando, apenas, a 'modelos pré-existentes' ou já estabelecidos.

Na realização da modelização foi, também, utilizado o faseamento sugerido no Modelo Sistêmico de Informação Ativa e Permanente (SIAP) [170]. Segundo Armando Malheiro da Silva, o SIAP, que vem sendo aplicado na área da gestão de informação, é inspirado na teoria dos sistemas e composto por vários módulos, que correspondem a duas fases distintas:

> a do diagnóstico/análise e a da explicação [intervenção]. Aquela é essencialmente descritiva e "radiográfica", na medida em que põe em relevo características e problemas vários, associados a um caso concreto em estudo; e esta é interventiva ao apresentar soluções de curto, médio e longo prazo com um

[170] O Sistema Integral de Informação Ativa e Permanente (SIAP), produzido por meio da aplicação da teoria sistêmica ao estudo da informação, apresenta-se como "alternativa às abordagens sincréticas e demasiado empíricas que incidem sobre gestão da informação e comportamento informacional" (SILVA; RIBEIRO, 2009, p. 38).

> plano de optimização [sic] de resultados positivos bem definidos (SILVA, 2010, p. 3).

A partir de uma visão gerencial da informação, envolvendo de forma ‘macro’ e holística a proteção da informação no meio digital, a primeira fase do 'SIAP-Ciber Proteção', dividida em duas partes, analisa a situação atual da Ciber Proteção nacional, consolidando o diagnóstico de forma sistêmica. A segunda fase aborda os agentes intervenientes do Modelo proposto, tipificando as estruturas envolvidas. As referidas fases são desdobradas nas três seções seguintes.

## *10.1 Ciber Proteção – Análise contemporânea*

Inicia-se, nesta seção, a primeira parte da fase 1 do SIAP-Ciber Proteção a partir da análise atualizada de um conjunto de constructos angulares, requisitos específicos e componentes essenciais baseados nas revisões, vivências, análises e resultados obtidos nas etapas anteriores.

Assim sendo, caracterizando o diagnóstico necessário para a construção do Modelo de Ciber Proteção Nacional, entende-se que o ciberespaço de um país soberano deva ser protegido contra ações hostis de qualquer motivação (política, econômica, religiosa etc.) ou origem (Estados, organizações, grupos etc.), de modo a propiciar o adequado funcionamento dos sistemas de informação, das redes de comunicação de dados, bem como das infraestruturas estratégicas nacionais.

Devido ao seu potencial inédito no trato das informações, o ciberespaço caracteriza-se como ferramenta especial e singular de transformação para um Estado-Nação e deve ser protegido com ações típicas de segurança e medidas de defesa cibernética, criando-se, de certa forma, um macroambiente ou Ecossistema de Ciber Proteção.

Portanto, no âmbito da área de conhecimento da Ciência da Informação, tornou-se primordial avançar em estudos amplos e diversificados, como promover o debate e o desenvolvimento de procedimentos de segurança da informação no ciberespaço, no contexto em que se planejam e se realizam, atualmente, as estratégias e ações inerentes à Segurança e à Defesa Nacional. É importante ressaltar que a informação tem sido estudada em diferentes contextos da realidade humana, especialmente o científico e o organizacional. Na visão de Olga Pombo (2006, p. 211), a Ciência da

Informação pode ser classificada como uma interdisciplina: “as novas disciplinas que aparecem com autonomia acadêmica a partir de 1940/50 e que surgem do cruzamento de várias disciplinas científicas com o campo industrial e organizacional”. Mais recentemente, e de acordo com Zins (2007), a CI preocupa-se com a criação, disseminação e utilização do conhecimento e possui duas subáreas, a saber: uma relacionada aos aspectos humanos e sociais e outra ligada aos aspectos técnicos que são os sistemas de informações.

Na contramão de um possível reducionismo no entendimento do que seria informação nesta Tese (considerada como recurso tangível materializado por *bits*), invoca-se a revisão de Capurro e Hjorland (2007, p. 185): “na medida em que a informação é tratada como produto de atividades específicas de construção do mundo, isto convida ao questionamento discursivo quanto ao seu significado e relevância".

Em relação ao papel da informação nos tempos atuais, de forma mais abrangente e filosófica, James Gleick reforça nosso estudo, na medida em que:

> a informação é aquilo que alimenta o nosso mundo: o sangue e o combustível, o princípio vital. Ela permeia a ciência de cima a baixo, transformando todos os ramos do conhecimento. [...] A economia está se reorganizando nos moldes de uma ciência da informação, agora que o próprio dinheiro está concluindo um arco de desenvolvimento de matéria para os *bits*, armazenado na memória dos computadores [...], e que as finanças correm pelo sistema nervoso global [Internet] (GLEICK, 2013, p. 16-17).

Infere-se que as implementações massivas e ininterruptas de Tecnologia da Informação nas organizações geraram novas necessidades na administração dos recursos, alavancadas pelas inúmeras possibilidades de inovação no trato da informação institucional. É fato que as (r)evoluções da TI, os tempos e movimentos da era da Informação, acontecem mais rapidamente do que outras áreas do conhecimento conseguem acompanhar, particularmente no contexto da necessidade de proteção da informação no meio digital.

Em escala global, no bojo de uma visão comportamental e social, em relação ao mundo digital, percebe-se que há um profundo e grave desequilíbrio mundial, especialmente referente à:

a) intensidade de uso e de acesso às TI;

b) produção e propriedade dos meios de TI;

c) regionalização do fluxo mundial de informação;

d) concentração e controle das comunicações;

e) capacidade de salvaguarda (segurança e privacidade) da informação.

Tal desequilíbrio traz o surgimento de novas centralidades e periferias mundiais, novas categorizações dos países quanto à estrutura em TI, bem como impactos consideráveis na soberania e no contexto social, econômico e cultural dos Estados-Nação, particularmente os ditos emergentes, como é o caso do Brasil.

No cotidiano da sociedade atual, apesar de ser comumente considerado como sinônimo da rede mundial de computadores – Internet, bem como, nesta pesquisa, o ciberespaço desenvolve-se e amplia-se baseado nas tecnologias de informação e comunicação, sendo suporte para as atividades (sociais, econômicas, políticas etc.; públicas ou privadas) desenvolvidas na era da Informação.

Não obstante o pioneirismo do *Marco Civil da Internet* no estabelecimento de diversas garantias, direitos e deveres, disciplinando o acesso e o uso da Internet no Brasil, o referido marco legal não aborda diretamente questões ligadas à proteção integrada da informação no ciberespaço de interesse nacional.

Importante é notar-se que, dentre as propostas de alteração do Marco Civil da Internet, estão presentes, direta ou indiretamente, temas relacionados à presente pesquisa como preservação, segurança e sigilo. Neste contexto, destaca-se a inserção de mais atribuições ao CGI.br, particularmente, a de se verificar o cumprimento da legislação brasileira, por parte dos provedores de conexão e de aplicações de internet, referentes: (i) à coleta, guarda, armazenamento e tratamento de dados; (ii) ao respeito à privacidade e ao sigilo de comunicações e (iii) à tarefa de armazenar, manter o sigilo e a segurança dos registros de conexão e aplicações.

Sancionada primordialmente para beneficiar o cidadão, a *Lei de Acesso à Informação* está, na realidade, alterando o processo informacional dentro das organizações públicas. Sem embargo, mesmo com o amplo e pleno acesso aos documentos arquivísticos, as informações institucionais produzidas devem ser preservadas, controladas e protegidas. Neste sentido, percebe-se que o 'pleno acesso' definido pela referida Lei contradiz, de certa forma, a base tradicional da segurança, qual seja, 'inicialmente protege-se tudo, para, em seguida, liberar-se paulatinamente a informação, à medida que for comprovada a necessidade'.

Ao se discutir a segurança da informação digital como complementar da Ciência da Informação nas atividades da gestão da informação, entende-se que há compatibilidade com a clássica, e ainda atual, definição de Ciência da Informação por Borko (1968, p. 3):

> é a disciplina que investiga as propriedades e o comportamento da informação, as forças que governam seu fluxo e os meios de processamento para otimizar sua acessibilidade e utilização. Relaciona-se com o corpo de conhecimento relativo à produção, coleta, organização, armazenagem, recuperação, interpretação, transmissão, transformação e utilização da informação.

Passadas quase duas décadas da definição de Borko, Saracevic (1996) define Ciência da Informação como campo que se dedica à investigação e à prática profissional de tornar mais efetiva a comunicação do conhecimento registrado entre os homens, no contexto de uso social, institucional e/ou individual da informação.

No escopo desta pesquisa, considera-se que a gestão segura da informação no ciberespaço compõe e atualiza o entendimento da almejada 'efetividade', proposta por Saracevic vinte anos atrás.

Considerando-se a gestão da informação contemporânea, entende-se que, particularmente no ambiente da era digital, os termos informação, documento e documento arquivístico aproximam-se, podendo receber tratamento semelhante em termos de Ciber Proteção.

Dentre os mais diversos entendimentos e perspectivas sobre o tema da gestão ou gerenciamento da informação, adotam-se alguns consensos:

a) depende intrinsicamente do conceito de informação utilizado e do tipo de organização em que é aplicada;
b) não se limita a gerir ou processar um recurso, abrangendo estratégia e operacionalização;
c) suas atividades tendem a compor um ciclo virtuoso;
d) caminha, lado a lado, com a Gestão do Conhecimento (GC)[171];
e) deve ser flexível, ajustando-se às características e à complexidade do ambiente;
f) é fator imprescindível na sustentabilidade e no desenvolvimento das organizações (sejam elas públicas ou privadas);
g) quando inserida no contexto de pesquisa acadêmica, a GI possui caráter tão ‘aplicável’, que dificilmente o pesquisador conseguirá se afastar do objeto

[171] Em relação à Gestão do Conhecimento (GC), este autor reconhece que a mesma ‘corre em paralelo’ com a GI, não havendo necessariamente uma subordinação hierárquica entre elas, pois são complementares, não obstante, a opinião de Kira Tarapanoff, “não se chega à inteligência pelo acesso passivo à informação. A inteligência deve ser criada, e é, ao longo desse processo de criação, o processo da gestão da informação e do conhecimento, que se vai elaborando um sistema útil às organizações, integrado em sua cultura e em seus cenários voltados ao futuro” (TARAPANOFF, 2006, p. 31).

investigado, pois, envolvido na ação, terá percepção mais precisa do problema.

Neste contexto, destaca-se que a Ciber Proteção possui, por premissa, contemplar a gestão da informação em toda sua extensão, independentemente da teoria ou da metodologia utilizada.

Interagindo com áreas afins da CI, a segurança deve andar lado a lado com a preservação, que, embora distintas e com características peculiares, são complementares no que tange ao escopo das ações de proteção cibernética.

Na PD, por exemplo, devem ser considerados os elementos necessários para a produção, a manutenção e o acesso aos documentos digitais, implicando não apenas transferências periódicas dos suportes de armazenamento e a conversão para outros formatos digitais, mas também a atualização do ambiente tecnológico, o *hardware* e o *software*[172].

De fato, a introdução da preservação digital, como fator fundamental no conceito de Ciber Proteção, amplia, de forma significativa e inovadora, o escopo atual da segurança da informação, fazendo, por exemplo, mais uma integração entre a Ciência da Informação e a Arquivologia. Nesta "ponte", buscam-se a garantia do acesso e a autenticidade, que podem ser ameaçadas quando a informação digital é transmitida através do espaço (por pessoas ou máquinas) ou armazenada e comunicada ao longo do tempo. É possível, também, incluírem-se, no escopo da proteção da informação no ciberespaço, aspectos como:

a) manutenção dos suportes, P.ex.: *sites*, páginas *web*, interfaces de sistemas, banco de dados entre outros;
b) obsolescência do *hardware,* P.ex.: vida curta das mídias e dependência dos fabricantes;
c) perenidade dos *softwares* e dos formatos de arquivos (padrões utilizados na interpretação dos *bits,* tais como: .doc, .pdf., .xml, .odt, .png, .gif, .jpeg etc.), independentemente de serem públicos ou proprietários;
d) segurança da informação armazenada na "nuvem".

[172] Disponível em: <http://www.conarq.arquivonacional.gov.br/documentos-eletronicos-ctde/perguntas-mais-frequentes.html>. Acesso em: 23 jan. 2017.

Percebe-se um “sombreamento” entre preservação e segurança da informação digital, por intermédio da essência (conceitos e definições específicas de cada área) de cada atributo e/ou característica comum desejável, tais como: autenticidade, disponibilidade de acesso e integridade, entre outros. Exemplo estratégico seria aproximarem-se do escopo das infraestruturas críticas os Centros de Informação Especiais, tais como a Biblioteca Nacional e a sua “Rede da Memória Virtual Brasileira”, que preservam a memória, a história e a cultura da Nação brasileira. Dessa forma, o gerenciamento da preservação da informação digital remete, ainda, a estratégias diversificadas que se estendem a processos, redes de dados, ambientes heterogêneos de armazenamento e produção, entre outros, envolvendo atividades complexas de segurança.

Na visão de Castells (Castells; Cardoso, 2005), quando se trata da esfera governamental, as ações de segurança dos sistemas de informação são diferentes das encontradas em outros setores; muitos dados da memória institucional e conhecimento das redes governamentais devem permanecer dentro dos serviços permanentes, em vez de espalhados por um leque extenso de contatos.

Não obstante a necessidade de controle dos sistemas de informação de interesse nacional no ciberespaço, percebe-se forte dependência de um amplo leque de atores, principalmente privados, que atuam como intermediários na prestação de serviços, tais como:

a) o acesso e interconexão;
b) a transmissão, processamento e (re) encaminhamento de tráfego;
c) a hospedagem de materiais publicados por terceiros e o acesso aos mesmos;
d) a referência a conteúdos ou a busca de materiais na rede;
e) a realização de transações financeiras;
f) a conexão entre usuários por meio de plataformas de redes sociais[173].

Em âmbito nacional, a ciber segurança orienta-se para a redução das vulnerabilidades encontradas nos sistemas de informação e no uso das tecnologias digitais, enquanto a defesa cibernética, atuando em rede, busca mitigar as ameaças internas

---

[173] Adaptado da publicação 'Liberdade de expressão e internet', OEA (2013).

ou externas aos interesses do ciberespaço de um Estado-Nação. Via de regra, as ameaças (internas ou externas), caracterizadas pela complexidade na identificação de possíveis origens e atores das ameaças e de suas reais intenções, concretizam-se por meio da exploração das vulnerabilidades existentes, que podem existir por: desconhecimento dos gestores dos ativos de informação, falha não intencional durante o desenvolvimento do *software* ou do *hardware*, ou ainda criadas/inseridas deliberadamente.

Apresentando característica multidisciplinar, o ambiente cibernético vem possibilitando a geração de produtos e serviços tecnológicos diversos, além de métodos e processos gerenciais em todos os níveis. No que tange à evolução do setor cibernético nacional, no caso específico da defesa cibernética, o tema é conduzido prioritariamente pelo Comando de Defesa Cibernética. A constituição de um Comando Conjunto, com integrantes das três forças armadas e capitaneado pelo Exército Brasileiro, vem proporcionando maior velocidade e efetividade ao desenvolvimento das atividades e projetos de alcance nacional.

Atualmente, o ComDCiber, além de um Estado Maior Conjunto e de um Departamento de Gestão Estratégica, possui como braço operacional o Centro de Defesa Cibernética, tendo, ainda, no Núcleo da Escola de Defesa Cibernética, seu vetor de capacitação, pesquisa e inovação.

Cabe ressaltar que, entre 2012 e 2016, o CDCiber em muito extrapolou sua área de atuação, prevista quando da sua ativação em 2010, tornando-se protagonista na coordenação e integração das atividades de defesa e de segurança cibernéticas nos grandes eventos internacionais ocorridos no país.

A ameaça cibernética cresceu em importância, principalmente por colocar em risco os sistemas de informação das infraestruturas críticas estratégicas, sensíveis e essenciais à operação e ao controle de diversos sistemas e órgãos diretamente relacionados à segurança nacional.

Destaca-se que a Ciber Proteção almeja detectar e prevenir a ocorrência de ações indesejáveis, sem, necessariamente, apreender o objeto a ser protegido, promovendo, também, a busca de resiliência institucional baseada em ações cooperativas interagências. Não obstante, no atendimento aos interesses nacionais, diante de ameaças externas, cabem à Ciber Proteção (no segmento da defesa cibernética) medidas de defesa ativa, bem como a exploração de sistemas de informação exógenos aos nacionais.

Em consequência, faz-se imperioso responder às ameaças cibernéticas com medidas de defesa ativa, ou mesmo ofensivas, como o ataque ou a exploração cibernética em sítios/forças adversas que tendem a comprometer a estabilidade nacional. Nesse contexto, é possível, então, inferir que a ciber defesa pode ser considerada como um vetor militar, ou seja, tem-se uma quinta e nova dimensão - a cibernética, ao lado das dimensões bélicas tradicionais: terrestre, marítima, aérea e espacial.

Em casos extremos, mas factíveis, a guerra cibernética situa-se em um ambiente de conflito deliberado, onde se percebe ameaça frontal à soberania nacional, normalmente pela possibilidade ou intenção de degenerar/interromper o funcionamento das infraestruturas críticas estratégicas essenciais à sobrevivência da sociedade e do Estado-Nação.

Os sistemas e os ativos de informação intrínsecos e necessários ao funcionamento e controle dos serviços essenciais à sociedade, públicos ou privados, tornam-se cada vez mais automatizados e dependentes tecnologicamente. À medida em que esses sistemas se tornam interligados a uma rede de comunicação de dados e podem ser acessados remotamente, aumenta a insegurança e amplia-se o rol de ameaças e de vulnerabilidades, particularmente quando conectados à Internet.

Assim sendo, reforça-se a inserção indissociável e transversal da proteção nos sistemas de informação das Infraestruturas Críticas, bem como caracteriza-se a informação como mais uma área prioritária para o país. Destaca-se, ainda, que a manutenção e a proteção das IC inserem-se no contexto da Defesa Nacional, por afetar diretamente a soberania do Estado brasileiro e o Poder Nacional.

A Ciber Proteção, vocacionada para a coordenação e integração de uma massa de sistemas heterogêneos e multissetoriais, pode contribuir para a ampliação das seguintes atividades inerentes à proteção dos sistemas de informação críticos: segurança sistêmica, consciência situacional do ciberespaço nacional, atuação em rede, ações colaborativas e trabalho cooperativo. Nesse sentido, considera-se que o ato de proteger não implica, necessariamente, interferir ou se apropriar quanto às medidas de segurança aplicadas pelas organizações, ou seja, as possíveis correções são encargo dos responsáveis pela segurança orgânica computacional dos sistemas de informação institucionais. Da mesma forma, não há obrigatoriedade em neutralizar o objeto atacante, bastando prevenir ou mitigar suas ações maliciosas. Neste caso, em especial, encontra-se consonância em Capurro e Hjorland (2007, p. 187), quando afirmam que:

> os aspectos **computacionais** [grifo nosso] da ‘geração, coleta, organização, interpretação, armazenamento, recuperação, disseminação, transformação e uso da informação’ não são específicos da CI, mas são, em grande medida, partes da ciência da computação, embora, certamente, estes dois campos estejam superpostos.

Em síntese, a Ciber Proteção pode proporcionar:

a) ações mais efetivas contra ameaças de grande complexidade e envergadura[174];

b) gestão de incidentes de forma coordenada e cooperativa;

c) fortalecimento das atividades de preservação digital;

d) salvaguarda do uso econômico, governamental, social etc. do ciberespaço de interesse nacional;

e) projeção da soberania e do poder nacional.

Almeja-se, com esta proposta de modelo, ampliar a capacidade de assegurar o funcionamento adequado dos sistemas de informação nas instituições governamentais de áreas diversificadas e níveis político-administrativos distintos, bem como nas infraestruturas críticas nacionais a cargo da iniciativa privada, por meio da articulação de diversas atividades inerentes à segurança e à defesa cibernéticas, agilizando e coordenando a redução de vulnerabilidades, além de ampliar a resiliência diante dos ataques.

Na próxima seção, detalham-se os sistemas e estruturas imbricados na proposta do modelo de Ciber Proteção, compilados e caracterizados, a partir dos resultados obtidos ao longo da dinâmica investigativa deste estudo.

## 10.2 Macrossistema da Ciber Proteção - MSCP

Nesta seção, conclui-se a fase 1 do SIAP-Ciber Proteção com a sistematização das análises/diagnóstico realizados.

---

[174] Por exemplo: ataques de negação de serviços distribuídos reflexivos – DRDoS *(Distributed Reflected Denial-of-Service),* que em parte se assemelham ao DDoS (negação de serviços aos usuários/clientes), onde o atacante pode enviar pacotes forjados para outra rede/máquina e permitir que esta rede/máquina realize o ataque, sem que a máquina/rede zumbi esteja, necessariamente, sob sua posse.

A concepção do Macrossistema de Ciber Proteção (MSCP) tem por pretensão agrupar, de forma simplificada e esquemática, os mais representativos ambientes e atores nacionais relacionados com o entendimento de 'Ciber Proteção' estabelecido nesta pesquisa. Dentre as mais relevantes características do MSCP destacam-se:

a) elevada complexidade por envolver e impactar a totalidade da sociedade brasileira;
b) necessidade de sustentabilidade político-estratégica;
c) busca incansável na autorrenovação (entropia negativa) por meio da flexibilização de processos e procedimentos;
d) foco permanente na ampliação da interoperabilidade, cooperação interagências nacionais e estrangeiras.

Interessante destacar-se, que o MSCP apresenta algumas características típicas de um sistema biológico, tais como: (i) grande número de participantes, (ii) fraca interconexão, (iii) elevada dependência uns dos outros e (iv) reação multifacetada a perturbações internas e externas.

A fim de atender às necessidades conjunturais, o Macrossistema de Ciber Proteção foi organizado em cinco conjuntos ou sistemas dinâmicos. Para cada sistema, buscou-se, sempre que possível, caracterizar aspectos basilares e evolutivos:

a) órgão central, catalizadores ou coordenadores em âmbito nacional;
b) nível de maturidade e escopo atual;
c) principais peculiaridades estruturais e normativas;
d) necessidades de ligação e interação com outros sistemas;
e) processos relevantes em curso ou necessários para implementação satisfatória do sistema;
f) pontos fortes e oportunidades de melhoria.

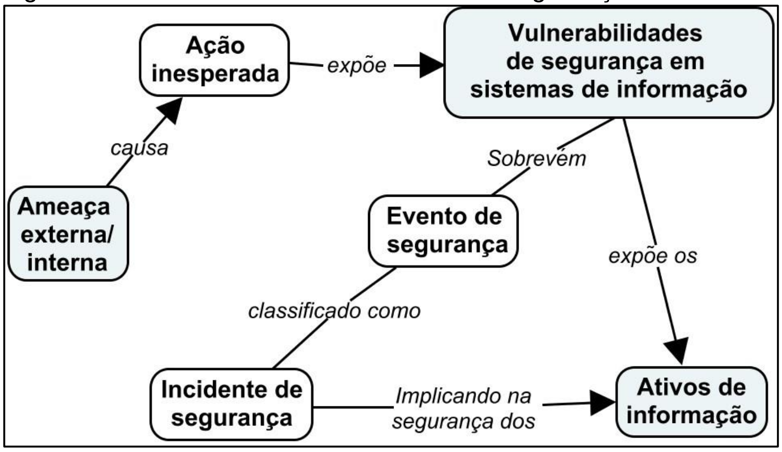
Na sequência, foram estruturados mapas mentais, que pretendem oferecer uma fotografia dos mesmos, apresentados na próxima seção.

### *10.2.1 Sistema de Gerenciamento de Incidentes de Redes (SGIR)*

A meta principal do Sistema de Gerenciamento de Incidentes de Segurança (SGIR) é coordenar a gestão de incidentes de segurança da informação em redes de computadores de interesse nacional.

De acordo com a ISO/IEC 27035 (2016), elementos pré-existentes em ambientes informacionais digitais (sombreados) são afetados por objetos resultantes de uma ação não esperada (não sombreados), resultando em um incidente de segurança, conforme ilustrado na figura 32.

Figura 32 - Elementos de um incidente de segurança




Fonte: adaptado da ISO/IEC 27035 (2016, p. 9)

O SGIR, basicamente, é composto por equipes de tratamento e resposta a incidentes (ETIR)[175], que operam em proveito de um ambiente, comunidade ou instituição pré-definidos, provendo segurança por meio da prevenção, detecção e resposta de incidentes. De forma genérica, a gestão de incidentes compõe-se das seguintes fases:

a) Planejamento e preparação pré-incidente;
b) Detecção e relatório inicial;
c) Formulação de uma estratégia de resposta;
d) Investigação do incidente, envolvendo coleta de dados e análise forense;
e) Resolução do incidente, incluindo restauração dos sistemas envolvidos e implementação de contramedidas;

---

[175] Conhecidas, também, como Centro, Times ou Grupos de resposta a incidentes de segurança da informação em redes de computadores, por exemplo: CSIRT (Cyber Security Incident response Team) e CERT (Computer Emergency Response Team).

f) Produção de relatórios, inserindo as lições aprendidas.

Como fator embrionário do SGIR, destaca-se a criação do Comitê Gestor da Internet no Brasil (CGI.br), que estabeleceu, em 1997, o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança. O CERT.br possui a missão de promover estudos e recomendações de procedimentos, normas e padrões técnicos e operacionais para a segurança das redes e serviços de Internet, assim como para a sua crescente e adequada utilização pela sociedade. O CERT.br atua no tratamento e resposta a incidentes de segurança em computadores envolvendo redes conectadas à Internet no Brasil, sendo inclusive reconhecido na comunidade internacional, como ponto de contato brasileiro no trato de incidentes dessa natureza.

Na mesma época, foi criado, pela Rede Nacional de Ensino e Pesquisa (RNP), o Centro de Atendimento a Incidentes de Segurança (CAIS), que passou a atuar na detecção, resolução e prevenção de incidentes de segurança na rede acadêmica brasileira, além de elaborar, promover e disseminar práticas de segurança em redes de computadores.

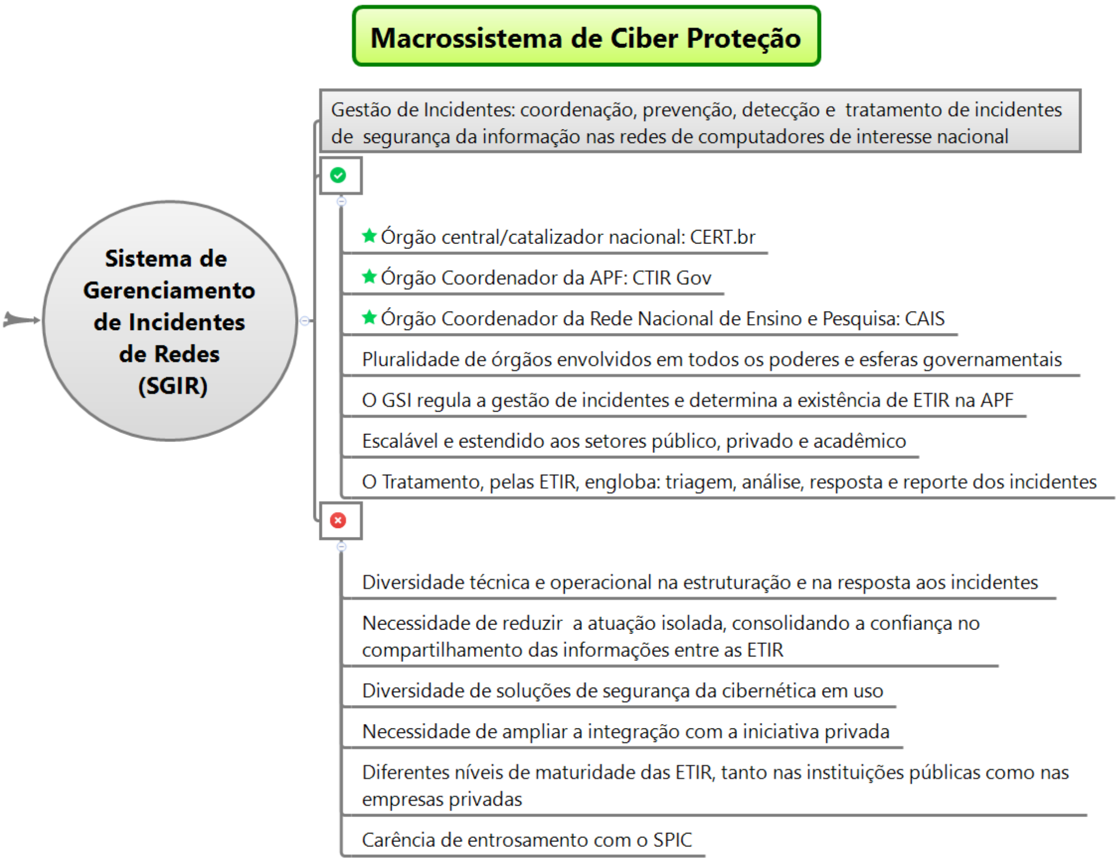
No âmbito da Administração Pública Federal, a gestão de incidentes é regulada por normas complementares da IN 01/GSIPR, que determinam, aos órgãos e entidades da APF, a implementação de equipe de tratamento e resposta a incidentes em redes computacionais (ETIR). Especificamente, a NC 05 Disciplina a criação das ETIR, enquanto a NC 08 estabelece as Diretrizes para Gerenciamento de Incidentes[176].

Pela ocorrência generalizada de incidentes de segurança nas redes de computadores, tanto das organizações públicas como das empresas privadas, o SGIR tende a relacionar-se com os demais sistemas de Ciber Proteção, de modo coletar as tentativas, exitosas ou não, e o grau de sofisticação dos ataques, de modo a fornecer a situação, real e tempestiva, da segurança cibernética no país (também conhecida como 'consciência situacional'). A figura 33 ilustra os principais aspectos que caracterizam o SGIR.

---

[176] Informações detalhadas sobre ETIR e a gestão de incidentes de segurança nas redes de computadores da APF, consultar monografia do autor sobre a temática em Vianna (2011).

Figura 33 - Sistema de Gerenciamento de Incidentes de Redes (SGIR)




Fonte: elaboração própria

### *10.2.2 Sistema Militar de Defesa Cibernética (SMDC)*

A *Estratégia Nacional de Defesa*, em 2008, ao considerar a importância do setor cibernético, protagonizou a necessidade do estabelecimento de um sistema de defesa típico, no âmbito do Ministério da Defesa. Também de acordo com a END, deverão ser criados e normatizados processos de segurança cibernética, bem como estabelecidos programas e projetos para assegurar a capacidade de atuar em rede com segurança.

A *Política Cibernética de Defesa*, em 2012, preconizou a necessidade de criação de um Sistema Militar de Defesa Cibernética (SMDC), considerando a participação de civis e militares da Marinha, do Exército e da Aeronáutica.

Em 2014, a *Doutrina Militar de Defesa Cibernética*, tipifica o SMDC como

> um conjunto de instalações, equipamentos, doutrina, procedimentos, tecnologias, serviços e pessoal essenciais para realizar as atividades de defesa no Espaço Cibernético, assegurando, de forma conjunta, o seu uso efetivo pelas

> FA, bem como impedindo ou dificultando sua utilização contra interesses da Defesa Nacional. (BRASIL, 2014b, p. 25).

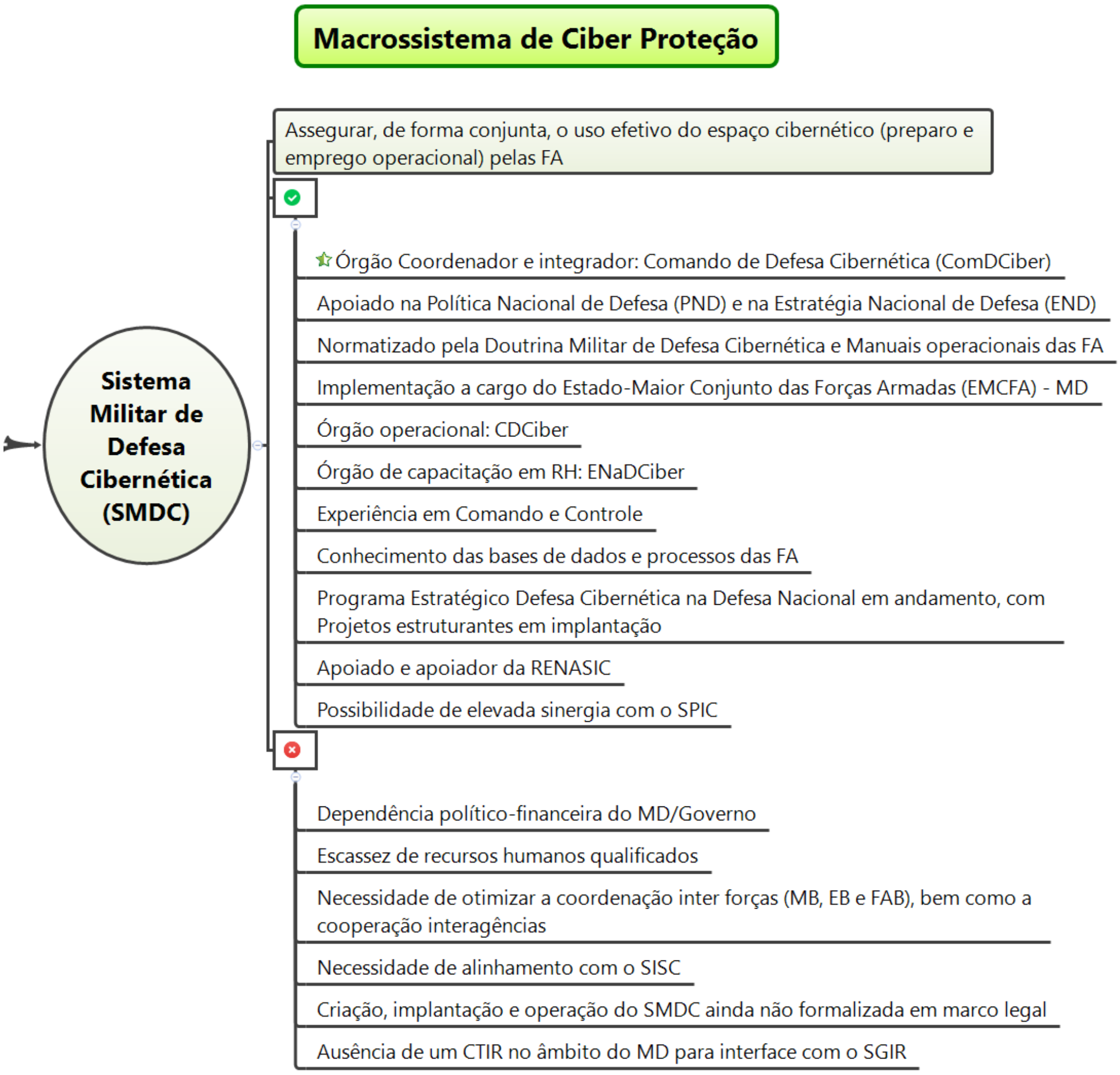
Ainda de acordo com a Doutrina, cabe ao SMDC assegurar a proteção cibernética do Sistema Militar de Comando e Controle, de sorte que as ações cibernéticas de defesa são desdobradas em três tipos:

a) Ataque Cibernético - compreende ações para interromper, negar, degradar, corromper ou destruir informações ou sistemas computacionais armazenados em dispositivos e redes computacionais e de comunicações do oponente;
b) Proteção Cibernética - abrange as ações para neutralizar ataques e exploração cibernética contra os nossos dispositivos computacionais e redes de computadores e de comunicações, incrementando as ações de Segurança, Defesa e Guerra Cibernética em face de uma situação de crise ou conflito. É uma atividade de caráter permanente;
c) Exploração Cibernética - consiste em ações de busca ou coleta, nos Sistemas de Tecnologia da Informação de interesse, a fim de obter a consciência situacional do ambiente cibernético. Essas ações devem, preferencialmente, evitar o rastreamento e servir para a produção de conhecimento ou identificar as vulnerabilidades desses sistemas(BRASIL, 2014b, p. 23).

A figura 34 ilustra as características mais relevantes do SMDC, que possui, atualmente, como órgão central do sistema o Comando de Defesa Cibernética[177].

[177] Informações complementares no artigo: "O SMDC e seus reflexos ´para a Defesa Nacional", disponível em: <https://pt.calameo.com/read/0034858642c1f26edda24>. Acesso em: 15 out. 2018

Figura 34 - Sistema Militar de Defesa Cibernética (SMDC)




Fonte: elaboração própria

### *10.2.3 Sistema de Proteção das Infraestruturas Críticas (SPIC)*

As infraestruturas Críticas, independentemente de serem físicas ou virtuais, públicas ou privadas, sistemas ou redes são vitais para o bem-estar, desenvolvimento e segurança dos cidadãos de uma nação. No Brasil, a segurança das IC foi previamente estabelecida pela END, de forma que, amparado pela CREDEN, cabe ao GSI coordenar, avaliar e monitorar as infraestruturas críticas/estratégicas nacionais.

Dessa forma, desde 2010, o GSI organiza Grupos Técnicos de Segurança de Infraestruturas Críticas (GTSIC) para as áreas prioritárias, nomeadamente Comunicações (Telecom, serviços postais, radiodifusão), Transporte (aquaviário, aéreo e terrestre), Energia (elétrica, petróleo, gás natural e combustível renovável), Água (abastecimento urbano e barragem) e Finanças (Bancário e Financeiro). Além das citadas, outras áreas podem compor o cenário das IC, por exemplo: Serviços de Governo, TIC, Serviços de Emergência e Alimentos e Informações (*software, hardware* e Internet).

Abordagem muito peculiar e aderente a pesquisa foi desenvolvida, em 2010, pelo Grupo de Trabalho de Segurança das Infraestruturas Críticas da Informação (GT-SICI). O GT-SICI publicou o *Guia de Referência para a Segurança das Infraestruturas Críticas da Informação*, o qual consolidou Infraestruturas Críticas da Informação (ICI) como:

> o subconjunto de Ativos de Informação - meios de armazenamento, transmissão e processamento, sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso - que afetam diretamente a consecução e a continuidade da missão do Estado e a segurança da sociedade (BRASIL, 2010a, p. 115).

Conforme consta no "Guia", as instituições responsáveis pelas infraestruturas críticas nacionais são orientadas a realizar, no mínimo: (i) mapeamento de seus ativos de informação para a identificação daqueles que são críticos; (ii) gestão de risco, com identificação de potenciais ameaças e vulnerabilidades; e (iii) estabelecimento de método de geração de alerta de segurança das infraestruturas críticas da informação.

Devido a oscilações políticas, como a própria extinção do GSI e da SAE, em 2015, bem como carência de visão estratégica de Estado, pouco se avançou, de forma sistêmica, integrada e coordenada rumo à consolidação de um plano 'nacional' de segurança das IC.

No ano de 2017[178], foi atribuída ao Gabinete de Segurança Institucional (GSI) da Presidência da República (como uma de suas competências), a responsabilidade de acompanhar os assuntos relacionados às infraestruturas críticas, com prioridade ao que se refere à avaliação de riscos.

A publicação da *Política Nacional de Segurança de Infraestruturas Críticas*, em novembro de 2018, aponta como uma significativa oportunidade de impulsionamento e otimização do SPIC. Entretanto, a concreta efetividade do proposto, na referida Política, só será possível com o desenvolvimento e a implementação de três instrumentos essenciais previstos na PNSIC, especificamente: (i) a Estratégia Nacional, (ii) o

---

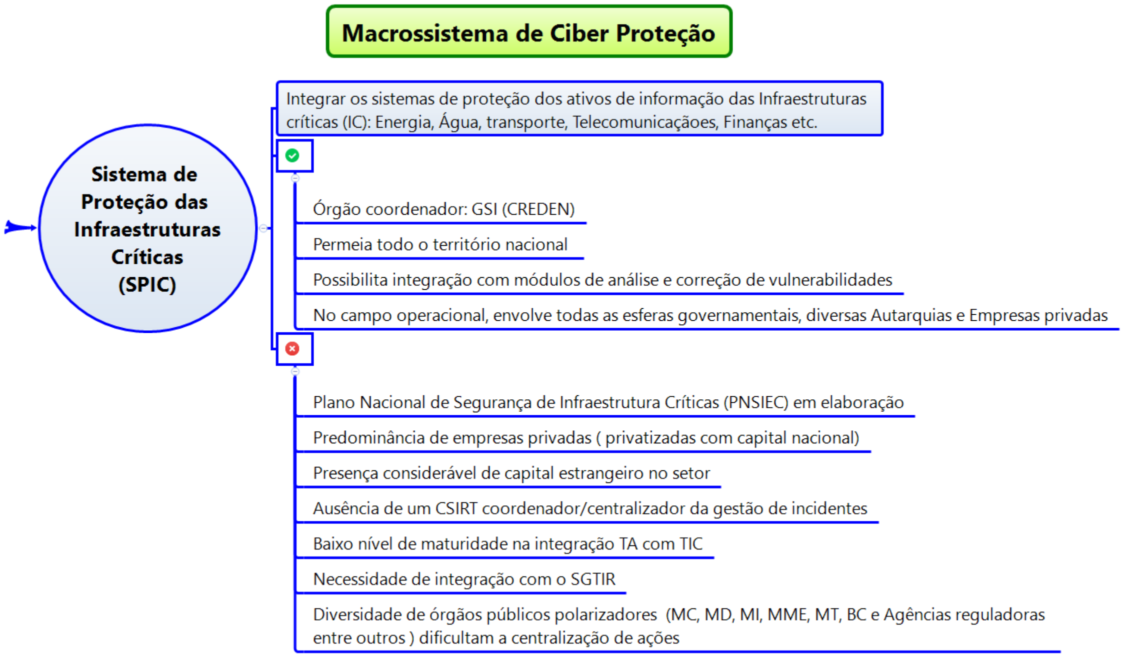
[178] Disponível em: <http://www.asbin.org.br/noticia/medida-provisoria-amplia-competencias-do-gsi>. Acesso em: 30 abr. 2018.

Plano Nacional e (iii) o Sistema Integrado de Dados de Segurança de Infraestruturas Críticas.

Um fator complicador para a ciber segurança nas infraestruturas críticas, trata-se da elevada diversidade de sistemas de controle industrial, assim como da alta especificidade no que se refere as tecnologias de automação (TA), que requerem um elevado nível de especialização. Além disso, a grande brecha/vulnerabilidade dos sistemas autônomos surge quando se conecta à rede de TA com a rede de TI, em busca das facilidades do ciberespaço, particularmente no caso da monitoração remota (P.ex.: controle de um sistema SCADA via Internet).

A figura 35 intenta representar as principais particularidades intrínsecas a uma concepção preliminar de um sistema de proteção para as infraestruturas críticas e/ou estratégicas.

Figura 35 - Sistema de Proteção das Infraestruturas Críticas (SPIC)




Fonte: elaboração própria

### *10.2.4 Sistema de Preservação da Informação Digital (SPID)*

Considera-se a Preservação Digital como um conjunto de estratégias e metodologias destinadas a preservar os documentos em formato digital, que deve alcançar, entre outros aspectos, características essenciais tais como: físicas (suporte e registro físico), lógicas (aplicativos e formato digital) e conceituais (estrutura e conteúdo exibido), bem como englobar a proteção via guarda de 'cópia' em outro local físico, espelhamento de dados, gestão e treinamento específicos para pessoal.

Nesta linha de pensamento, ao considerar a preservação digital não como um processo isolado, mas como um componente de um conjunto de serviços, políticas e especialistas que constituem o contexto do ciclo de vida da informação digital, Sonia Boeres (2017) reforça nossa proposta de modelagem para a Ciber Proteção nacional, de modo que, a preservação digital seja, efetivamente, um 'sistema' estruturante e imprescindível na segurança da informação no ciberespaço.

Dentre os atores principais do SPID, destacam-se o CONARQ e a Rede Brasileira de Serviços de Preservação Digital (Rede Cariniana), coordenada pelo IBICT.

O CONARQ possui como uma das suas finalidades exercer orientação normativa visando à proteção especial aos documentos de arquivo, atuando no SPID por intermédio da implementação dos requisitos para um repositório digital confiável. O RDC-Arq está organizado em três conjuntos: (i) infraestrutura organizacional, (ii) gerenciamento do documento digital e (iii) tecnologia, infraestrutura técnica e segurança. Especificamente no quesito segurança, o RDC-Arq descreve que a mesma não se limita aos aspectos de tecnologia, mas abrange, também, instalações físicas e ações de pessoas, incluindo (CONARQ, 2015, p. 18):

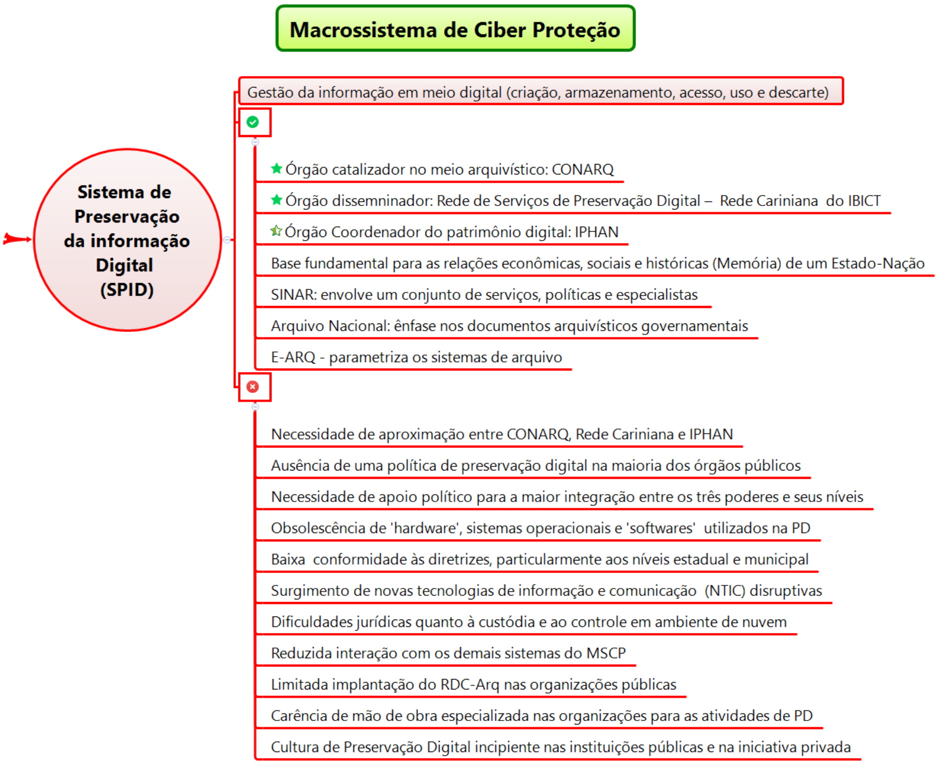
a) análise sistemática de dados, sistemas, pessoas e instalação física;
b) adoção de procedimentos de controle para tratar adequadamente das necessidades de segurança;
c) delineamento de papéis, responsabilidades e autorizações relativas à implementação de mudanças no sistema;
d) plano de prevenção de desastres e de reparação, que inclua, ao menos, um *backup, offsite*, de tudo o que é mantido no repositório (documentos, metadados, trilhas de auditoria etc.), inclusive do próprio plano de reparação.

O Sistema Nacional de Arquivos (SINAR), tendo o CONARQ como órgão central, assegura ao SPID sua integração e acessibilidade nacional, particularmente pela diversidade dos seus integrantes, a saber: Arquivo Nacional; arquivos dos três poderes, arquivos estaduais e do Distrito Federal, arquivos municipais bem como pessoas físicas e jurídicas de direito privado detentoras de arquivos, mediante convênio com um órgão central.

A Rede Cariniana (detalhada na seção 6.3.2 - A PD governamental – uma abordagem) promove a disseminação, em âmbito nacional, das práticas de preservação digital, por meio da utilização de sistemas de armazenamento de PD (P.ex.: *DSpace* e *LOCKSS*). De acordo com Silva Junior (2017), todos os repositórios institucionais das universidades federais brasileiras utilizam o *DSpace* como plataforma de armazenamento e preservação, sendo que algumas universidades utilizam o *LOCKSS* para preservação e compartilhamento, com outros parceiros da Rede Cariniana, de periódicos científicos de acesso aberto.

O Instituto do Patrimônio Histórico e Artístico Nacional (IPHAN) também participa do SPID como órgão que responde pela preservação (digital, em particular) do Patrimônio Cultural Brasileiro, assegurando sua permanência e usufruto para a sociedade. Segundo a Carta da Unesco (2003, p. 2-4 *apud* Costa; Cunha; Boeres, 2017), o desaparecimento do patrimônio, não importa em que forma esteja, é um empobrecimento das nações. Para a entidade, o patrimônio digital são recursos de informação e expressão criativa produzidos, distribuídos, acessados e mantidos em forma digital, e sua preservação é um benefício para a presente e para as futuras gerações. A figura 36 pretende representar algumas perspectivas que tipificam o SPID.

Figura 36 - Sistema de Preservação da Informação Digital (SPID)




Fonte: elaboração própria

### *10.2.5 Sistema de Segurança da Informação e Cibernética (SSIC)*

Infere-se que o SSIC teve início a partir da publicação do Decreto n. 3505, de 13 de junho de 2000, que instituiu a política de segurança da informação (PSI) nos órgãos e entidades da APF. Na sequência, destaca-se que, em 2008, a IN 01/GSIPR estruturou a gestão da SIC nos órgãos e entidades da Administração Pública Federal, direta e indireta.

Observa-se que o SSIC detém um viés fortemente político e regulador, inicialmente restrito à APF, embora, tecnicamente e na prática, esteja estendido aos demais poderes e níveis governamentais. A diversidade de temas contemplados pelas normas complementares a IN 01, compiladas no quadro 16, favorecem a organização e padronização de procedimentos do sistema de segurança da informação no ciberespaço.

Quadro 16 - Normas complementares à IN 01/GSI

| NC | DESCRIÇÃO/OBJETIVO |
|---|---|
| 01/IN01 2008 | Atividade de Normatização. |
| 02/IN01 2008 | Metodologia de gestão de Segurança da Informação e Comunicações. |
| 03/IN01 2009 | Diretrizes para a Elaboração de Política de Segurança da Informação e Comunicações. |
| 04/IN01 2009 | Diretrizes para o processo de gestão de Riscos de Segurança da Informação e Comunicações - GRSIC. (Revisão 01 - 2013) |
| 05/IN01 2009 | Disciplina a criação de Equipes de Tratamento e Respostas a Incidentes em Redes Computacionais - ETIR. |
| 06/IN01 2009 | Estabelece Diretrizes para gestão de Continuidade de Negócios, nos aspectos relacionados à Segurança da Informação e Comunicações. |
| 07/IN01 2010 | Estabelece as Diretrizes para Implementação de Controles de Acesso Relativos à Segurança da Informação e Comunicações. (Revisão 01-2014) |
| 08/IN01 2010 | Estabelece as Diretrizes para Gerenciamento de Incidentes em Redes Computacionais. |
| 09/IN01 2013 | Estabelece orientações específicas para o uso de recursos criptográficos em Segurança da Informação e Comunicações. (Revisão 02-2014) |
| 10/IN01 2012 | Estabelece diretrizes para o processo de Inventário e Mapeamento de Ativos de Informação, para apoiar a SIC. |
| 11/IN01 2012 | Estabelece diretrizes para avaliação de conformidade nos aspectos relativos à Segurança da Informação e Comunicações. |
| 12/IN01 2012 | Estabelece diretrizes e orientações básicas para o uso de dispositivos móveis nos aspectos referentes à SIC. |

| | |
|---|---|
| 13/IN01 2012 | Estabelece diretrizes para a gestão de Mudanças nos aspectos relativos à Segurança da Informação e Comunicações. |
| 14/IN01 2012 | Estabelece diretrizes para a utilização de tecnologias de Computação em Nuvem, nos aspectos relacionados à SIC. (Revisão 01 - 2018) |
| 15/IN01 2012 | Estabelece diretrizes de Segurança da Informação e Comunicações para o uso de redes sociais. |
| 16/IN01 2012 | Estabelece as Diretrizes para o Desenvolvimento e Obtenção de *Software* Seguro. |
| 17/IN01 2013 | Estabelece Diretrizes nos contextos de atuação e adequações para Profissionais da Área de Segurança da Informação e Comunicações. |
| 18/IN01 2013 | Estabelece as Diretrizes para as Atividades de Ensino em Segurança da Informação e Comunicações. |
| 19/IN01 2014 | Estabelece Padrões Mínimos de Segurança da Informação e Comunicações para os Sistemas Estruturantes da APF. |
| 20/IN01 2014 | Estabelece as Diretrizes de Segurança da Informação e Comunicações para Instituição do Processo de Tratamento da Informação. (Revisão 01-2014) |
| 21/IN01 2014 | Estabelece as Diretrizes para o Registro de Eventos, Coleta e Preservação de Evidências de Incidentes de Segurança em Redes nos órgãos e entidades da Administração Pública Federal, direta e indireta. |

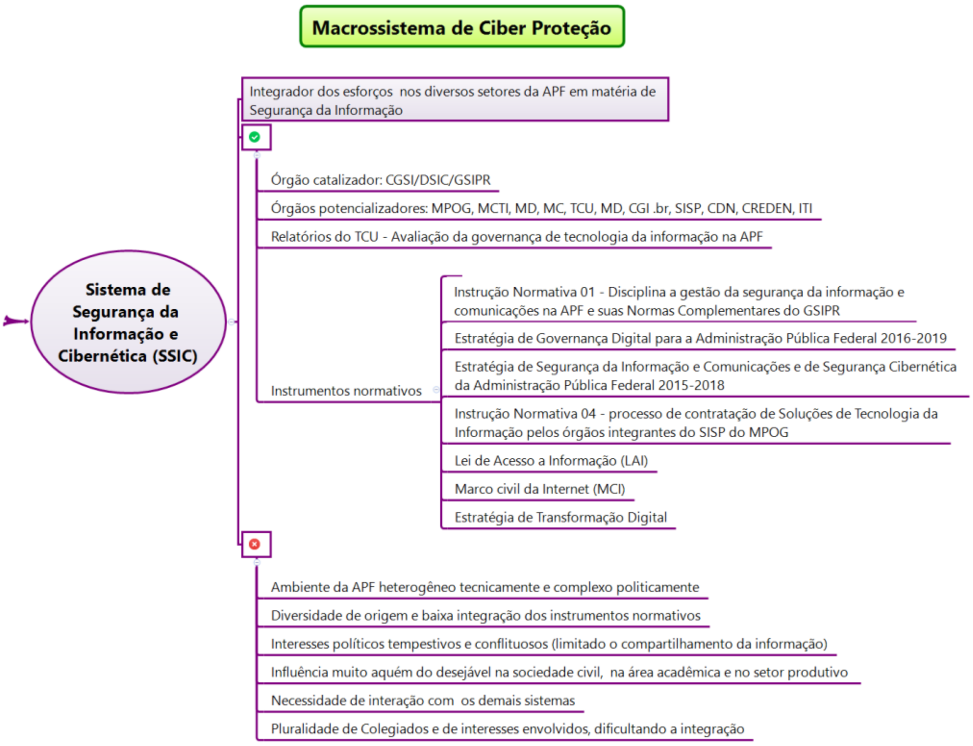
Fonte: elaboração própria

A *Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética (2015-2018)*, em fase de revisão pelo DSIC, constitui-se em documento norteador do SSIC, pois visa atingir o aprimoramento da área no Governo e a mitigação dos riscos aos quais se encontram expostas as organizações e a sociedade. Dentre seus dez objetivos estratégicos, destacam-se seis que se relacionam umbilicalmente com a Ciber Proteção:

a) promover mecanismos de conscientização da sociedade sobre SIC/SegCiber;
b) elevar o nível de maturidade de SIC/SegCiber na APF;
c) garantir continuamente a pesquisa, o desenvolvimento e a inovação;
d) instituir modelo de governança sistêmica, com coordenação executiva, acompanhamento e avaliação de um órgão central;
e) valorizar e ampliar ações que fortaleçam a segurança das infraestruturas críticas da informação;
f) ampliar e fortalecer ações colaborativas com a **academia** [grifo nosso], setores público, privado e terceiro setor, no país e no exterior (BRASIL, 2015, p. 42).

A figura 37 organiza os fatores e circunstâncias mais impactantes à consolidação do SSIC.

Figura 37 - Sistema de Segurança da Informação e Cibernética (SSIC)




Fonte: elaboração própria

Complementando a fase de diagnóstico, análise e síntese da situação atual, a presente proposta de um Modelo de Ciber Proteção Nacional contempla três alternativas intervencionistas, complementares e integradas, que são abordadas nas próximas seções.

## 10.3 Agentes Intervenientes

Esta seção aborda a segunda fase do SIAP-Ciber Proteção, apresentando três ‘soluções’ tipicamente intervencionistas: uma política nacional, uma entidade de Estado e um centro de competências.

### 10.3.1 *Centro de Inovação e Competências Cibernéticas (CICC)*

Infere-se que a efetividade do Modelo para a Ciber Proteção Nacional sustenta-se, em muito, nas capacidades e competências cibernéticas nacionais, oriundas da interação entre o governo, as instituições de ensino e a iniciativa privada.

O primeiro pilar intervencionista do MCPN trata-se do denominado - Centro de Inovação e Competências Cibernéticas (CICC). O CICC, de forma holística, nacional e aglutinadora visa atender às expectativas da Sociedade em face das oportunidades e dos desafios do ciberespaço e das plataformas digitais. Neste sentido, Passarelli (2014) apresenta a sociedade preocupada com o acesso às tecnologias digitais de duas formas: a primeira busca uma inclusão digital como modo de democratização; a segunda, de cunho mais educacional, preocupa-se com a apropriação e produção do conhecimento desses novos atores em rede (também inseridos, de forma particular, os especialistas dos sistemas inerentes à Ciber Proteção).

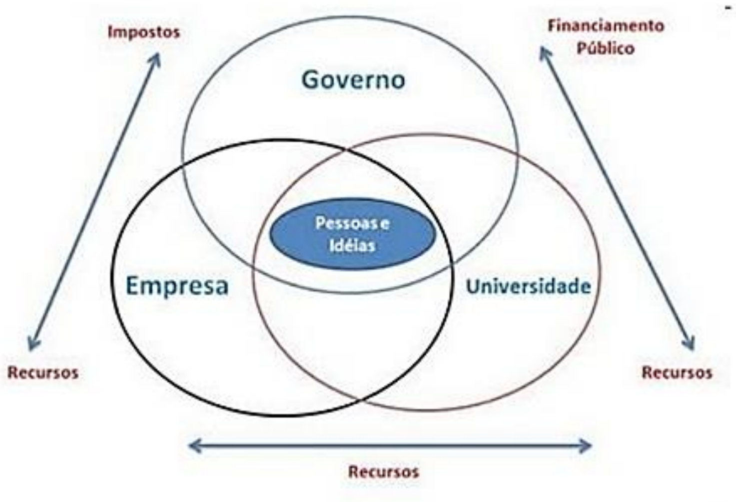
O CICC possui, como foco, a inovação e o incremento das potencialidades cibernéticas nacionais, desenvolvendo estudos, pesquisas, competências e capacidades. Neste contexto, a metáfora da Hélice Tríplice (*Triple Helix*)[179] é utilizada como uma moldura para o CICC, pois foi desenvolvida como um conceito *ex post*, refletindo a realidade dos países desenvolvidos, onde a inovação tem sido associada aos setores baseados em atividades de pesquisa e desenvolvimento (P&D). A abordagem considera a interação entre as organizações que compõem essas três hélices, representadas na figura 38, em diversos níveis e que acarretam:

a) transformações internas em cada esfera;
b) influências das organizações de uma esfera sobre outra em decorrência dos relacionamentos existentes;
c) criação de novas estruturas devido à sobreposição ocasionada pela interação das três hélices;
d) um efeito recursivo desses três níveis.

---

[179] A abordagem/modelo da Hélice Tríplice foi proposta em 1996 por Henry Etzkowitz e Loet Leydesdorff. No país, o Triple Helix Research Group – THERG-Brasil foi formalizado em agosto de 2008, entretanto, o núcleo de pesquisadores integrantes do grupo vem, desde 1997, trabalhando em conjunto temas relacionados à gestão da inovação. Disponível em: <http://www.triple-helix.uff.br/sobre.html>. Acesso em: 15 jun. 2017.

Figura 38 - CICC e a abordagem Hélice Tríplice




Fonte: InovaBrasil (2010)[180]

O modelo tridimensional (academia, governo e empresa) busca a interação e a sinergia entre as partes, de modo que, geralmente:

a) o meio acadêmico é o indutor da pesquisa e do conhecimento por meio das universidades, centros e institutos de pesquisa, desenvolvimento e inovação;

b) o setor produtivo, contemplando indústria, bens e serviços, fornece produtos e soluções com escalabilidade;

c) a vertente governamental atua como elemento financiador, regulador e fomentador, demandando produtos e processos.

Espera-se que, ao adotar o modelo da Hélice Tríplice, as redes de relacionamento do CICC criem interfaces, subdinâmicas de intenções, estratégias e projetos, gerando valor agregado adicional aos seus integrantes. Por exemplo, no viés acadêmico, não obstante a manutenção de considerável autonomia, a ‘Universidade’ incorpora, além do ensino e da pesquisa, a missão de ser um ator ativo do desenvolvimento econômico, via geração de conhecimento científico e tecnológico e, consequente, inovação. No caso, os grupos de pesquisa atuam como 'quase-firmas' e interagem com os atores das demais esferas ou hélices, dando origem a estruturas como:

---

[180] Disponível em: <https://www.researchgate.net/figure/Figura-2-Helice-Triplice-Fonte-InovaBrasil-2010-adaptado-de-Leydesdorff-e-Etzkowitz_fig2_319130888>. Acesso em: 20 out. 2018.

a) firmas *spin-off*, incubadoras e parques tecnológicos;
b) escritórios de propriedade intelectual e comercialização de tecnologia;
c) redes de conhecimento;
d) arranjos e sistemas produtivos e inovadores locais;
e) universidades corporativas entre outros[181].

Dessa forma, cabe ao CICC promover a cooperação, via ação governamental, entre universidades e centros de pesquisa com o ambiente empresarial, a fim de facilitar a troca de conhecimentos e de tecnologias relevantes para o setor cibernético. Deve o mesmo atuar como estrutura facilitadora na construção, no emprego e na propagação das TIC genuinamente brasileiras, bem como favorecer a retenção dos recursos humanos especializados em Ciber Proteção no país. Como elementos norteadores, podem-se destacar, entre outros:

a) Lei n. 12.598 que estabelece normas especiais para as compras, as contratações e o desenvolvimento de produtos e de sistemas da área estratégica de defesa;
b) END, LBDN e PND;
c) Portaria Interministerial n. 1421 que instituiu o Programa de Pesquisa, Desenvolvimento e Inovação em Defesa Cibernética;
d) *Plano Nacional de Internet das Coisas*;
e) Decreto n. 9283 que dá incentivo à inovação e à pesquisa científica e tecnológica no ambiente produtivo;
f) Decreto n. 9319 que institui o Sistema Nacional para a Transformação Digital/E-Digital.

Deve-se, ainda, utilizar como referência positiva (*benchmarking)* as atividades e projetos desenvolvidos pela RENASIC, não obstante suas limitações políticas-governamentais-operacionais, comentadas anteriormente nesta pesquisa; bem como os trabalhos desenvolvidos pela Associação Brasileira das Indústrias de Materiais de Defesa e Segurança (ABIMDE), fortemente relacionados com as empresas nacionais que atingiram o *status* de Empresa Estratégica de Defesa (EED).

---

[181] THERG-Brasil. Disponível em: <http://www.triple-helix.uff.br/sobre.html>. Acesso em: 15 jun. 2017.

### *10.3.2 Entidade Nacional de Ciber Proteção (ENCP)*

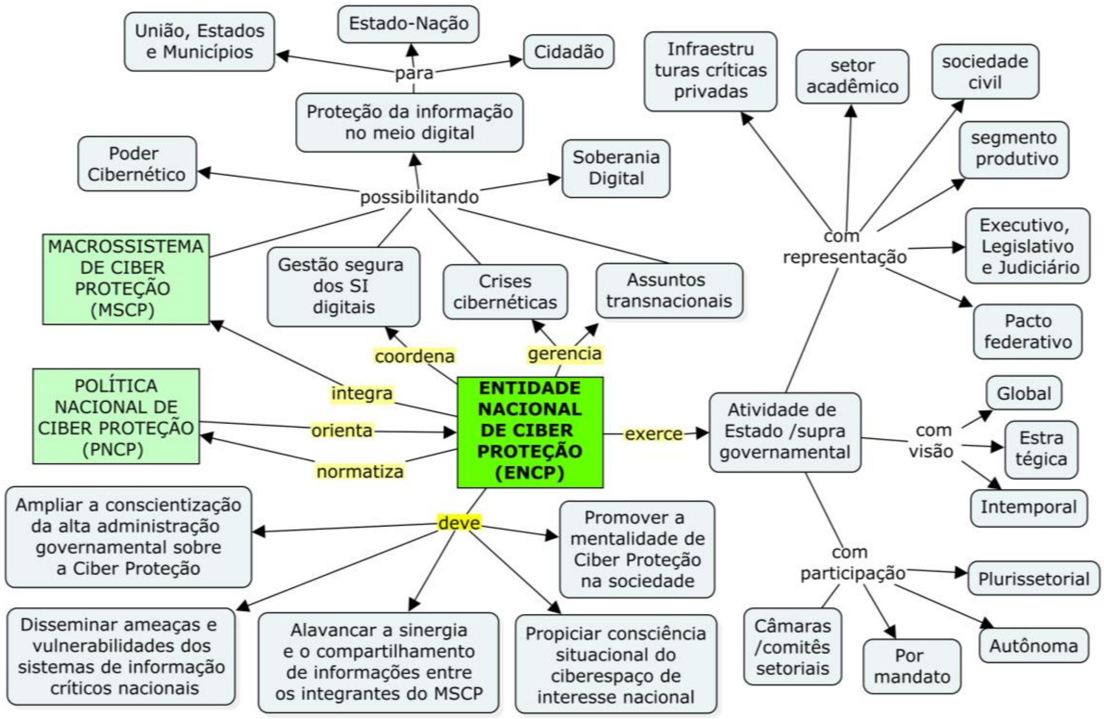
Durante o aprofundamento analítico para a concepção inicial do Modelo de Ciber Proteção Nacional, foi percebida a necessidade de se implementar uma 'estrutura' dedicada à proteção da informação no ciberespaço de interesse nacional. Posteriormente, à necessidade desse órgão articulador e normativo nacional foi ratificada por todos os especialistas entrevistados por ocasião do estudo empírico.

Denominada, abstratamente, de Entidade Nacional de Ciber Proteção (ENCP), a mesma deve possuir perfil que proporcione regras e enquadramento para as ações humanas. Sugere-se assim, que seja tipificada como Instituição, particularmente por aproximar-se do enquadramento dado ao termo por Peter Scott: "estruturas cognitivas, normativas e reguladoras e atividades que fornecem estabilidade e significado ao comportamento social" (SCOTT, 1995 *apud* PINTO, 2015). Dentre as características de cunho institucional da ENCP, destacam-se:

a) apresentam uma natureza formal (leis, regulamentos etc.);
b) são identificadas com sistemas normativos que operam nas áreas básicas: família [sociedade], governo, economia, educação etc.
c) constituem sistemas multifacetados que conduzem e dão forma ao comportamento social, incorporando processos reguladores e normativos;
d) sendo construídas e mantidas pelos indivíduos, assumem, no entanto, a aparência de realidade impessoal e objetiva;
e) estão embutidas, ou são transportadas, em vários meios/suportes que operam em múltiplos níveis de jurisdição;
f) evoluem de forma incremental, ligando o passado, presente e futuro (PINTO, 2015, p. 111).

O mapa apresentado na figura 39 representa, de forma conceitual, características, premissas e relacionamentos entendidos como fundamentais e imprescindíveis na composição e implementação da ENCP, como instituição centralizadora das ações de Ciber Proteção, em âmbito nacional.

Figura 39 - Visão conceitual da Entidade Nacional de Ciber Proteção




Fonte: elaboração própria

A Entidade Nacional de Ciber Proteção deve ser conduzida de forma autônoma e centralizada, composta por representantes dos variados setores da sociedade (múltiplas partes interessadas - *multistakeholders*), sendo, naturalmente, descolada das feições e das instabilidades político-governamentais, bem como evitando a criação de novos níveis hierárquicos e de nichos de especialização endógenos. Dentre as principais missões da ENCP, particularmente, como uma estrutura perene do Estado brasileiro, destacam-se:

a) acolher as demandas da sociedade e as macroestratégias do Estado brasileiro;
b) desenvolver a governança do espaço cibernético nacional, cooperando com os países aliados para a Ciber Proteção Global, bem como resolvendo *ciber* questões transfronteiriças;
c) articular-se com os três poderes da União nos níveis estratégico e operacional;
d) consolidar-se como ponto focal das políticas setoriais governamentais (ministérios) em relaçao ao setor cibernético;
e) editar decretos regulamentadores da PNCP, assim como resoluções que tratam de temas comuns inerentes aos sistemas de Ciber Proteção;

f) conduzir atividades sistemáticas de revisão do arcabouço regulatório inerentes à Ciber Proteção;

g) promover ações técnico-científicas no âmbito do MSCP;

h) estruturar a consciência situacional do ciberespaço de interesse nacional.

Em um primeiro momento, na busca de ações efetivas e oportunas, propõe-se a organização, baseada nos aspectos levantados no mapa conceitual (figura 39), de um "grupo de especialistas", independente[182], responsável pela formulação de uma Política Nacional de Ciber Proteção, proporcionando, de imediato, articulação entre as áreas de segurança e preservação da informação digital, gestão de incidentes em redes de computadores, defesa cibernética e infraestruturas críticas.

### *10.3.3 Política Nacional de Ciber Proteção (PNCP)*

A Organização para a Cooperação e Desenvolvimento Econômico, com a finalidade de contribuir para a definição de políticas dos Governos e promover uma maior inclusão social (digital) dos países-membro, busca identificar tendências para o futuro. Sobre o tema 'regulação', a OCDE esclarece que[183]:

a) é um dos três principais instrumentos de poder formal do Estado (juntamente com tributação e gastos);

b) é frequentemente desenvolvida como uma medida de resposta a um risco percebido;

c) é de vital importância na formação do bem-estar das economias e da sociedade;

d) é necessário que haja coerência de regulamentação nos diferentes Níveis de Governo de forma simultânea e em rede: verticalmente - entre os diferentes níveis de governo e horizontalmente - dentro do mesmo nível de governo.

---

[182] A princípio, não haveria uma vinculação formal a um Ministério ou órgão da APF. Sendo imprescindível um vínculo governamental, poderia ser avaliada a ligação com o Conselho de Defesa Nacional (CDN), ou mesmo com a Câmara de Relações Exteriores e Defesa Nacional (CREDEN).

[183] Informações disponíveis em: <http://www.oecd.org/gov/regulatory-policy/Recommendation%20PR%20with%20cover.pdf>. Acesso em: 31 out. 2018.

No cenário político-estratégico nacional e, por vezes, no operacional, o arcabouço regulatório (Leis, Decretos, Resoluções, Portarias, Instruções Normativas e Normas Complementares ), bem como outros dispositivos legais (políticas, estratégias, doutrinas etc.), devem ser revistos sistematicamente e de forma periódica a fim de atualizar, eliminar ou substituir aqueles que são obsoletos, insuficientes, ineficientes, fragmentados e desalinhados com os níveis superiores. Neste contexto, cabe aos orquestradores da PNCP avaliar as regulamentações nacionais que, em alguma circunstância, impactam a proteção da informação no ciberespaço de interesse nacional, com sugestões de ações nas mesmas.

No entendimento de Pinheiro (2012), o campo das pesquisas das políticas, em especial sobre informação e inteligência, ainda é imaturo pois:

> a Sociedade da Informação desvia o foco para as técnicas e o aparato de infraestrutura de redes. Proporcionalmente à importância da informação como ativo, estratégia e segurança das nações e empresas, percebe-se a ausência de coerência e interpretação do seu real valor. A política, como processo de longo prazo, “explicitada em leis”, tem sido substituída pela “política como ação” em forma de programas e planos (PINHEIRO, 2012, p. 76).

A política[184], acerca da proteção da informação no ciberespaço, deve ser fruto de intenso trabalho colaborativo e consensual, dos mais diversos seguimentos do país, visando, acima de tudo, ao bem comum a aos interesses da Sociedade e do Estado brasileiro. A Política, deve, portanto, incidir sobre os três poderes da União, Estados, Distrito Federal e Municípios, Tribunais de Conta e Ministério Público, além de todos os órgãos da administração pública, bem como sobre empresas enquadradas como infraestruturas críticas e entidades sem fins lucrativos que receberam recursos governamentais para realização de ações de interesse público.

As evidências e tendências apresentadas nesta pesquisa corroboram para a necessidade de se avançar no implemento de uma política tipicamente 'pública'[185], de âmbito nacional, voltada para o enfrentamento dos desafios da Ciber Proteção, com independência e autonomia dos planos de governos ou de grupos nos diversos

---

[184] Entende-se que política (*policy*) está relacionada com orientações subjetivas, baseadas em entendimentos conceituais, que buscam o consenso, a decisão e a ação (e/ou não ação), particularmente as relativas à organização e ao desenvolvimento de uma demanda de um grupo/sociedade.

[185] Políticas públicas – concebidas para enfrentar um problema público (nacional), na qual se observa o 'governo' como núcleo promotor de ações intervencionistas e reorganizadoras (possíveis soluções), que impactam a vida do cidadão e do Estado-Nação.

poderes, devendo ser formulada por representantes dos diversos setores da sociedade e alinhada com as Macropolíticas nacionais.

Silva (2008, p. 52) identifica as seguintes características comuns às políticas públicas, ainda que ocorram em diferentes graus e níveis:

a) relações de poder e legitimidade;
b) espaço de trocas, elementos de valor e de conhecimento;
c) normas, regulamentos e procedimentos;
d) necessidades de escolhas, sentidos e valores culturais, bem como ideologia que a gere ou sustente;
e) planejamento orçamentário;
f) organograma e estrutura organizacional hierárquica setorial;
g) integração e inter-relacionamento entre seus vários aspectos e níveis (federal, estadual e municipal);
h) programas e projetos específicos;
i) dinamismo para as necessárias atualizações;
j) participação dos setores interessados;
l) representação democrática da sociedade na sua formulação e implementação;
m) atendimento de diferentes demandas;
n) critérios de aferição e avaliação de resultados;
o) atenção para as correções necessárias ao longo de sua trajetória.

Na concepção da Política Nacional de Ciber Proteção, torna-se, portanto, imperioso que as iniciativas voltadas à gestão segura da informação possuam a participação de equipes transdisciplinares e multissetoriais (governo, academia e empresa – setor público e privado), alicerçadas por visões multilaterais e holísticas, particularmente na proteção cibernética de sistemas de informação estratégicos para o país. Isto posto, fruto dos diagnósticos e da modelização, realizados anteriormente nesta seção, sobressaem-se os seguintes requisitos e desafios:

a) prover alinhamento normativo, estratégico e operacional no setor cibernético;
b) equilibrar segurança nacional e privacidade pessoal;
c) instituir fontes de custeio e investimento próprios para a Ciber Proteção;
d) estruturar o CICC e a ENCP;
e) alinhar-se com as macroestratégias do Estado brasileiro;

f) alavancar o desenvolvimento do setor cibernético nacional;

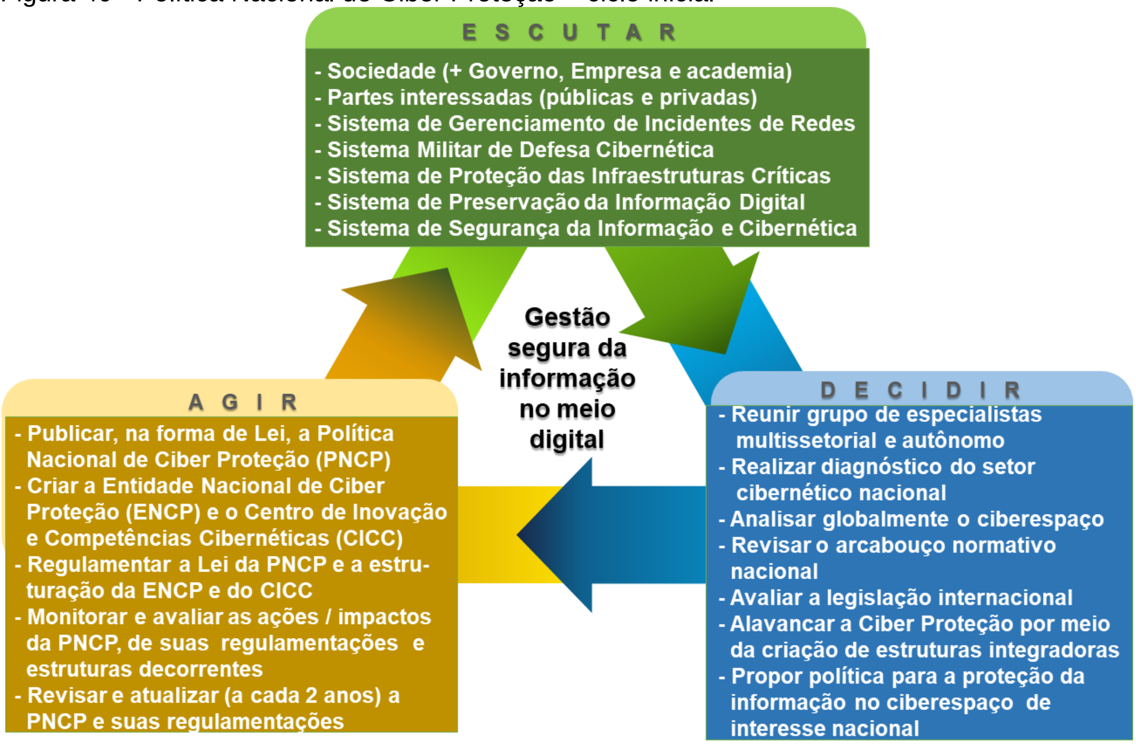
g) considerar os acordos e tratados internacionais signatários na área da proteção da informação no ciberespaço e PD, a fim de promover a coerência regulatória global;

h) contemplar a proteção em todo o ciclo informacional;

i) realizar Análise de Impacto - através de uma avaliação *ex ante* (prospectiva), incorporando a avaliação dos impactos econômicos, sociais, tecnológicos, políticos etc.

A PNCP deve ser dinâmica e simples de se executar, tendo um movimento cíclico e permanente em torno dos polos 'Escutar – Decidir – Agir', como sintetizado na figura 40.

Figura 40 - Política Nacional de Ciber Proteção – ciclo inicial




Fonte: elaboração própria

A figura acima representa a primeira volta do ciclo que busca gestão segura da informação no meio digital. Na publicação da PNCP, deve ser contemplada, necessariamente, a criação dos outros dois agentes intervenientes do Modelo de Ciber Proteção: a ENCP e o CICC. Após dois anos de monitoramento e embasada nos ensinamentos e repercussões da publicação da Política, a fase 2 teria início com a atualização da própria PNCP e/ou de sua regulamentação decorrente, pela Entidade Nacional já estabelecida, devidamente assessorada pelo Centro de Inovação e Competências Cibernéticas.

Para tanto, a revisão proposta no fechamento do ciclo inicial deve ser global, ou seja, atuar em todos os processos da gestão 'segura' da informação, tais como: criação, armazenamento, recuperação, preservação, partilha (comunicação), uso, entre outros; envolvendo atividades humanas, processos, fluxos informacionais, *hardware* e *Software.*

O CICC, a ENCP e a PNCP são os três pilares 'operacionais' que impulsionam e atualizam o Modelo de Ciber Proteção Nacional. O capítulo seguinte encerra o relatório desta pesquisa.

# 11 CONSIDERAÇÕES FINAIS

## 11.1 Pretérito - Primícias do estudo

A necessidade de comunicar, de colocar no papel meus entendimentos, obtidos a partir das vivências operacionais no ambiente do ciberespaço, sobre as bases, atividades e vicissitudes da proteção da informação no meio digital, possibilitou excelente teste sobre a indispensável coerência e a minha compreensão dos mesmos. Considera-se, pois, esta pesquisa qualitativa, particularmente, pelos seguintes motivos:

a) foi um processo de entendimento de um problema técnico-social - a Segurança (digital) da sociedade brasileira;
b) buscou construir um quadro holístico da proteção cibernética no ambiente complexo da APF;
c) mesclou diversas abordagens metodológicas, nomeadamente: Teoria Fundamentada, Investigação Empírica/'positivista', Investigação-ação, Método Quadripolar e SIAP;
c) trabalhou, em especial, com materiais elaborados a partir da observação e de entrevistas, buscando a união tempestiva entre a coleta e a análise de dados;
d) foram valorizadas, em âmbito nacional e internacional, as experiências e interações (do autor e de especialistas), bem como os documentos em seus contextos originais;
e) conceitos foram desenvolvidos e refinados no processo da pesquisa (P.ex.: Ciber Proteção).

No desenvolvimento da pesquisa, a revisão da literatura mostrou-se fundamental na construção do conceito de Ciber Proteção, *core* deste estudo. As atividades e inquéritos internacionais foram imprescindíveis à consolidação e à ampliação dos requisitos necessários à estruturação e à orquestração do modelo em tela. O estudo empírico, baseado em entrevistas com especialistas de destaque no cenário cibernético brasileiro, proporcionou maior aderência ao contexto singular e dinâmico da APF, bem como possibilitou a validação da proposta de um Modelo (nacional) para a proteção da informação no meio digital.

Por seu aspecto inovador, que carece de interação dinâmica e crescente entre diversas Ciências, a presente proposta de modelo de proteção da informação no ciberespaço encontrou terreno favorável de desenvolvimento na jovialidade e interdisciplinaridade da CI.

Assim, avultou de importância e urgência desenvolver o fenômeno proteção da informação no ciberespaço, alicerçado nas contribuições teóricas e metodológicas, bem como nos saberes e atividades da Ciência da Informação, dentro da realidade nacional e orientada pelos anseios e objetivos de um Estado-Nação soberano como o Brasil.

A primeira hipótese desta pesquisa, que trata do impacto político nas atividades de proteção cibernética, foi ratificada ao longo do relatório pela análise das entrevistas realizadas no âmbito da APF, pelo exame evolutivo dos tempos e movimentos das estruturas nacionais envolvidas com a proteção do ciberespaço, bem como por meio do mapeamento e da avaliação dos diversos atores que compõem o Macrossistema de Ciber Proteção.

Em relação à apresentação inadequada do arcabouço regulatório, relacionada à segurança e à defesa dos ambientes digitais, objeto da segunda hipótese, duas constatações confirmam sua pertinência: (i) a necessidade urgente de atualização ou adequação de documentos basilares para a Ciber Proteção, tais como: o Decreto n. 3505/2000, a IN 01/GSI com suas normas complementares decorrentes, a Política Cibernética de Defesa, dentre outros, e (ii) a diversidade na infralegislação (portarias, normas ministeriais, estratégias etc.), por vezes desconectadas entre si, excedendo as respectivas áreas de competência, bem como apresentando realidades e objetivos conflitantes com as Diretrizes superiores.

O problema fulcral desta pesquisa: "quais seriam as maneiras mais efetivas de reduzir as vulnerabilidades e mitigar as ameaças aos recursos informacionais em ambiente digital e globalmente interconectado?", por certo, inicia sua lenização, a partir da primeira rodada de implementação do Modelo, por intermédio da consolidação da versão inicial da Política Nacional de Ciber Proteção. De fato, chega-se à convicção de que a PNCP é vetor precursor da operacionalização do Modelo para a Ciber Proteção nacional proposto.

Dessa forma, pode-se ratificar, parcialmente, a Tese desta pesquisa, pois a sua validação só poderia ser aferida no início do segundo ciclo da PNCP. Sem embargo à validação da Tese, e no escopo das variáveis levantadas, elencam-se alguns dos principais óbices, desafios e limitações desta pesquisa, a saber:

a) ingerência política, por parte da Presidência da República, substancialmente prejudicial e descolada das tendências mundiais, nas estruturas encarregadas da segurança da informação governamental. Como exemplo, pode-se citar, entre outros: a saída da RENASIC da Presidência da República/GSI em 2011 para o Exército Brasileiro, reduzindo a autonomia, a visibilidade e a influência da Rede que deveria estar sempre em expansão, promovendo e caminhando, *pari passu*, com as atividades e iniciativas institucionais;

b) extinção, em 2015, da Secretaria de Assuntos Estratégicos da Presidência da República (SAE) fomentadora da END, de eventos governamentais sobre o setor cibernético, tais como: a Reunião Técnica sobre Segurança e Defesa Cibernéticas em 2010, o XIII Encontro Nacional de Estudos Estratégicos em 2013 e o Grupo de Trabalho Interministerial (GTI) sobre segurança e defesa do espaço cibernético nacional em 2014;

c) retirada do *status* de ministério, em 2015, do Gabinete de Segurança Institucional (incluindo a perda de cargos e integrantes), o que se refletiu, negativamente, no ambiente cibernético nacional e internacional, acarretando declínio das atividades de SIC na APF e de monitoramento de IC, além de modificações substanciais danosas (enfraquecimento/prostração/extinção) em diversas estruturas envolvidas no MSCP;

d) instabilidade política governamental, experimentada no país, no período de produção da Tese (2015 a 2018);

e) alterações no arcabouço jurídico normativo, relacionado ao ciberespaço de interesse nacional, no último trimestre da Tese (P.ex.: PNSIC e PNSI);

f) incorporação de novas tendências, tecnologias e ameaças aos sistemas de informação estruturantes, alterando especialidades e procedimentos de proteção cibernética (P.ex.: Plano Nacional de IoT e ataques de *ransomware*).

Em relação ao arcabouço científico investigado, o entendimento contextualizado da Ciber Proteção traz aspectos relevantes ao estudo da gestão da Informação e do Conhecimento, tendo em vista que podem ser considerados aspectos individuais, institucionais e da sociedade durante sua construção. A Ciber Proteção pode ser o vetor que amálgama as diferentes estruturas e redes de informação, por meio da coordenação de atividades de segurança e de defesa no espaço cibernético de interesse nacional.

De forma não exaustiva, pode-se afirmar que a proteção do ciberespaço se apresenta complexa politicamente, heterogênea na sua operacionalização, envolvendo diversos segmentos governamentais, acadêmicos, empresariais e da sociedade em geral. Nesse sentido, argumenta-se, também, que a proteção da informação no ciberespaço tem impactos relevantes na sustentação da nação, na construção da cidadania e no desenvolvimento econômico, ratificando-se, assim, o entendimento de que a Ciber Proteção não é questão apenas da organização (pública/privada) ou de ações estabelecidas durante um governo, com seus fisiologismos e limitado poder político temporal. É, sem dúvida, assunto de Estado, pois sustenta a sobrevivência da sociedade civil e política, merecendo, pois, considerar a Ciber Proteção, também, como vetor de projeção do poder nacional por meio do setor cibernético. Em consequência, acredita-se que, por meio de abordagens envolvendo experiências concretas, suposições filosóficas e procedimentos distintos, o estudo em questão aproximou-se do pragmatismo, na busca de uma ampla governança digital (viés proteção) para o Estado brasileiro.

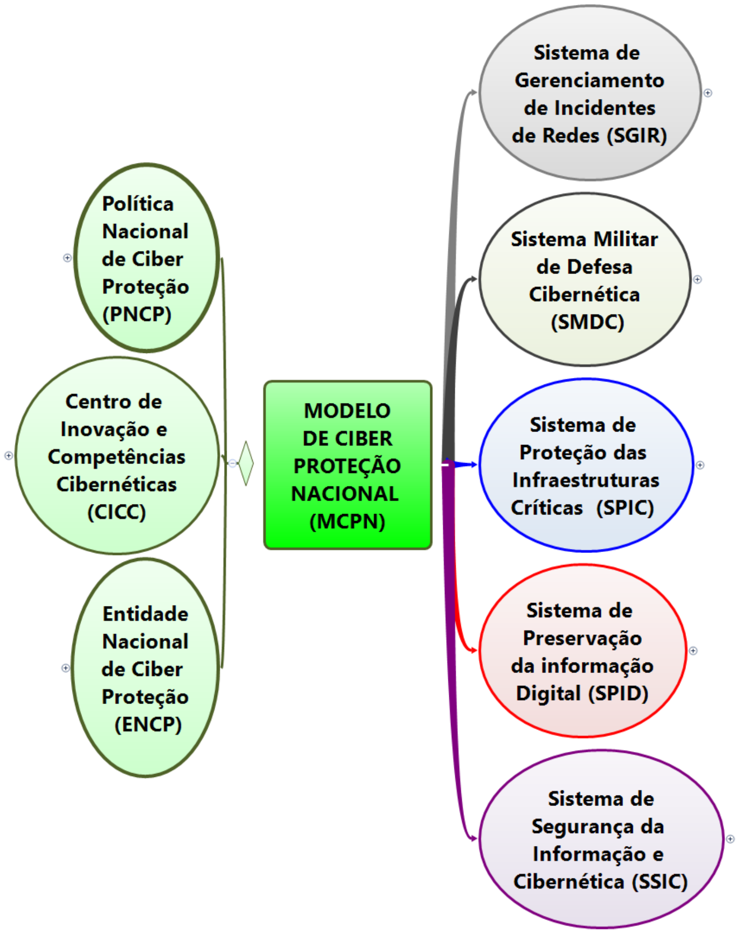
## 11.2 Presente - Visão consolidada do MCPN

Na concepção do Modelo de Ciber Proteção Nacional, fez-se uso de abordagens operacionais (práticas no terreno), bases empíricas e científicas tanto nacionais como estrangeiras. Tornou-se, pois, imprescindível, compilar uma série de requisitos conceituais e teóricos, diagnosticar circunstâncias contextuais e ambientais, assim como analisar elementos estruturais e orgânicos relacionados com o fenômeno da proteção da informação em meio digital.

O uso do MCPN pressupõe superar divisões ou separações convencionais ainda vigentes entre as estruturas imbricadas com a segurança da informação, a defesa cibernética e a preservação digital. A simplicidade e interatividade proporcionadas pela sistematização da informação de forma ativa e permanente (SIAP), particularmente quando usado na Gestão [segura] da Informação, facilitou a visualização do Modelo.

O Modelo proposto apresenta-se em dois grupos distintos, não obstante seu elevado e necessário nível de interação/atualização, a saber: o primeiro abrange o diagnóstico, a análise e a visão sistêmica/contemporânea da proteção da informação digital nacional, representados pelos cinco sistemas que integram o Macrossistema de Ciber Proteção (SGIR, SMDC, SPIC, SPID e SSIC); o segundo grupo, tipicamente intervencionista, estrutura-se em três pilares: uma política nacional, uma entidade de Estado e um centro de inovação e competências em Ciber Proteção, como apresentado na figura 41.

Figura 41 - Modelo de Ciber Proteção Nacional




Fonte: elaboração própria

No contexto do Macrossistema, não há, necessariamente, uma hierarquia entre os sistemas, porquanto os mesmos foram dispostos por ordem alfabética dos respectivos acrônimos. Não obstante, percebe-se que dois sistemas, nomeadamente o SGIR e o SSIC, possuem, na atualidade, capilaridade e pontos de contato mais significativos com a sociedade, enquanto outros, como o SMDC, SPID e o SPIC atuam em ambientes singulares, com tecnologias e controles peculiares.

Percebe-se, pois, que os sistemas componentes do MSCP possuem diferenças significativas, particularmente, devido às suas características técnicas, operacionais, cadeias de valores e níveis de maturidade. Entretanto, apesar de heterogêneos, pode-se observar, paradoxalmente, que os cinco sistemas possuem expressivas áreas de sombreamento e intersecção, devido ao macro-objetivo norteador de suas atividades-fim: a busca da proteção da informação no meio digital. Em termos nacionais e holísticos, os mesmos visam ao uso seguro e soberano do ciberespaço pela sociedade brasileira. Episódio recente, que exemplifica a possibilidade real de interação sistêmica no âmbito do MSCP, em contraponto ao pendor dos sistemas de se isolarem em ilhas funcionais e especializadas, foi a realização do "Exercício Guardião Cibernético", em julho de 2018. Tal iniciativa teve por objetivo treinar especialistas na proteção de ataques virtuais, sendo conduzida pelo ComDCiber (órgão central do SMDC). Cabe destacar-se a participação de vários atores importantes de outros sistemas: CERT.br e CTIR Gov do SGIR, GSIPR e MRE do SSIC, FEBRABAN, SERPRO e Eletrobrás do SPIC, dentre outras 23 organizações participantes[186].

Na intenção de se prover uma visão efetiva do Macrossistema de Ciber Proteção, o quadro 17 relaciona os atores e as características principais de cada sistema com diferentes 'níveis de decisão', a saber:

a) político – com instituições de elevado poder decisório e autonomia, envolvendo fóruns e diretrizes governamentais;
b) estratégico – com organizações realizando atividades de coordenação e normatização;
c) tático - abrangendo planejamento e atuação colaborativa interagências;
d) operacional - execução das ações planejadas no ciberespaço de interesse (P.ex.: guerra cibernética).

Quadro 17 - Níveis de Decisão no MSCP

[186] Informações disponíveis em: <https://www.defesa.gov.br/noticias/44716-exerc%C3%ADcio-guardi%C3%A3o-cibern%C3%A9tico-treina-especialistas-na-prote%C3%A7%C3%A3o-de-ataques-virtuais>. Acesso em: 12 out. 2018.

| NÍVEL/ SISTEMA | SGIR | SMDC | SPID | SPIC | SSIC |
|---|---|---|---|---|---|
| POLÍTICO | CGI.br | MD | MJ | CREDEN | GSI |
| ESTRATÉGICO | CERT.br | ComDCiber | CONARQ IPHAN | GTSIC do GSI | DSIC |
| TÁTICO | CERT.br - CTIR Gov-CAIS/RNP | CDCiber ETIR FA | ARQUIVO NACIONAL | Áreas de TI/TA das IC | Gestores de SIC |
| OPERACIONAL | ETIR (públicas/privadas) | Forças Componentes | RDC-Arq Equipes de campo | Equipes de segurança das IC | Equipes de segurança institucional |

Fonte: elaboração própria

O trabalho colaborativo e interagências é imprescindível para o êxito e efetividade do MSCP. Outro fator desafiador para os sistemas envolvidos com a Ciber Proteção é a busca permanente e efetiva da capacidade de continuar operando, mesmo sob presença de ataques ou incidentes, assumindo eventuais degradações nos serviços prestados (resiliência cibernética), seja em condições de normalidade institucional, durante crises regionais e nacionais, seja em situação de conflitos transnacionais.

Elemento tipicamente articulador, a Entidade Nacional de Ciber Proteção canaliza as demandas do MSCP, proporcionando um fluxo informacional com os outros intervenientes do Modelo: o CICC e a PNCP. Neste sentido, sob o viés operacional, destaca-se a proposta de criação de uma plataforma nacional colaborativa, com capacidade de funcionar não apenas como um repositório de dados, mas que organize a informação e promova o seu intercâmbio. Tal plataforma, capitaneada pela ENCP, possibilitaria estimular o compartilhamento de dados e informações entre os atores componentes do MCPN, incluindo-se aí: a disseminação de vulnerabilidades com suas respectivas correções, o estabelecimento das melhores práticas e o gerenciamento de ações conjuntas, dentre outros.

No cenário político-econômico nacional contemporâneo, avulta de importância o papel do governo como líder e principal fomentador do Centro de Inovação e Competências Cibernéticas, atuando, ao menos inicialmente, como precursor e mentor, na estruturação das características-chave das interações universidade-governo-indústria, sob a forma de um sistema de inovação, especialmente por meio de:

a) formação da célula-tronco por meio da interação entre os integrantes da Hélice Tríplice;

b) coordenação do funcionamento dos espaços e das relações entre os componentes, incluindo suas amplas cadeias de atores;
c) análise de tendências, normalização e boas práticas de inovação;
d) liderança colaborativa e moderação de conflitos;
e) promoção da 'qualidade cibernética' (P.ex.: detectar vulnerabilidades e mitigar as inserções de códigos e artefatos maliciosos nos produtos), por meio de homologação e de certificação de 'produtos', voltados para a segurança e a defesa cibernéticas, desenvolvidos no Brasil ou no exterior.

Dentre as missões do CICC, destaca-se o desafio em proporcionar a redução da dependência externa, acerca de *hardwares* e a *softwares* avaliados como essenciais para a proteção da informação em meio digital, fornecendo, aos segmentos do Macrossistema de Ciber Proteção, soluções tecnológicas nacionais, apropriadas e atuais, com elevado nível de efetividade no cumprimento das missões de cada Sistema. No bojo dessas tecnologias, incluem-se, dentre outros, equipamentos eletrônicos e de telecomunicações, assim como soluções criptográficas e de segurança de redes de computadores.

Pensada como orientadora e reguladora, nunca limitadora, a Política Nacional de Ciber Proteção, a partir de um diagnóstico atual e observando as tendências para o futuro, deve contribuir, em muito, para a definição de políticas setoriais da APF, tendo em vista que cabe ao poder público nortear suas normas e ações governamentais pelos anseios da Sociedade e do Estado. Não se trata, entretanto, de somente integrar as ações dos ministérios, autarquias e entidades/organizações envolvidas com a ciber segurança, mas alavancar a ciberdefesa, a Preservação Digital e a salvaguarda das Infraestruturas Críticas.

Buscou-se, assim, elaborar um modelo conceitual orientado de forma a contemplar visões sistêmica, holística e estratégica. Em síntese, o modelo proposto é um macrossistema lógico que representa estruturas essenciais da Ciber Proteção nacional, buscando reproduzir a interação e características (pontos positivos e negativos) dos sistemas-alvo, com as especificações e os requisitos de uma política de Estado, alicerçada por uma estrutura integradora supragovernamental e um núcleo nacional de inovação, estudos e competências.

Do ponto de vista de aplicação prática, acredita-se que este trabalho poderá gerar novas e exequíveis possibilidades para os processos de tomada de decisão e de gerenciamento da informação/conhecimento organizacional, no contexto das estruturas envolvidas com a proteção do ciberespaço nacional.

Pelo aspecto epistemológico da interdisciplinaridade, almeja-se que, além das contribuições objetivas centradas na gestão da informação em um espaço informacional típico, como o cibernético, a pesquisa colabore com as discussões sobre:

a) os meios computacionais e a realidade digital no âmbito da Ciência da Informação;
b) o papel da Gestão da Informação como área transversal e aplicada da Ciência da Informação;
c) a clarificação conceptual e disciplinar da preservação e da segurança da informação no domínio intercientífico da Ciência da Informação;
d) a formulação de políticas ou planos de ação envolvendo a Gestão e a Preservação Digital, reforçadas com a inserção da segurança da informação;
e) a diminuição das fronteiras entre Ciências da Informação, da Computação e da Comunicação, a partir do esforço para vencer os desafios da segurança informacional em meio digital.

No macroambiente político-social e do ciberespaço brasileiro, espera-se que os resultados obtidos com a presente pesquisa contribuam para:

a) a consolidação do valor da informação como vetor de sustentabilidade de um Estado-Nação e da sociedade[187];
b) a proteção da informação no contexto da Política e da Estratégia Nacional de Defesa (PND/END)[188];

---

[187] Alinhado com a Iniciativa Estratégica 03.12 da EGD/MP: ‘Melhorar a taxonomia da área de Segurança da Informação e Comunicação, inclusive com definições de limites relacionados ao uso de dados da sociedade por parte do Estado, à privacidade e ao sigilo das informações do cidadão. (BRASIL, 2016b).

[188] Alinhado com a Meta de Estado do “Plano Brasil 2022”: garantir pleno exercício do direito de acesso a informações públicas e consolidar a Internet como um terreno de liberdade de expressão (BRASIL, 2010b).

c) o aperfeiçoamento das atividades das instituições públicas ou privadas encarregadas de, periodicamente, formular e fomentar estudos, bem como fixar metas, estratégias, planos e cronogramas, referentes ao uso e desenvolvimento da Internet no País[189];

d) a compilação, na forma de Lei Nacional, de uma "Política de Ciber Proteção"[190];

e) a modernização do funcionamento da administração pública[191];

f) a busca de convergência entre as políticas macroestratégicas (P.ex.: LAI e MCI) e os planos de atuação setoriais (P.ex.: e-ARQ e EGD) por meio da GI, sob o viés da Ciber Proteção;

g) a ampliação do envolvimento do envolvimento da sociedade brasileira com os assuntos de Defesa e de Segurança[192];

h) a melhoria dos níveis de proteção dos recursos informacionais nas organizações, independentes de serem públicas ou privadas.

## 11.3 Futuro – Desdobramentos e Conclusões

O Modelo estabelecido, com multiplicidades de sistemas, controles e interações, assemelha-se a um organismo vivo e dinâmico. A figura 42, a seguir, apresenta uma visão em círculos concêntricos distintos, mas de elevada permeabilidade e interação.

---

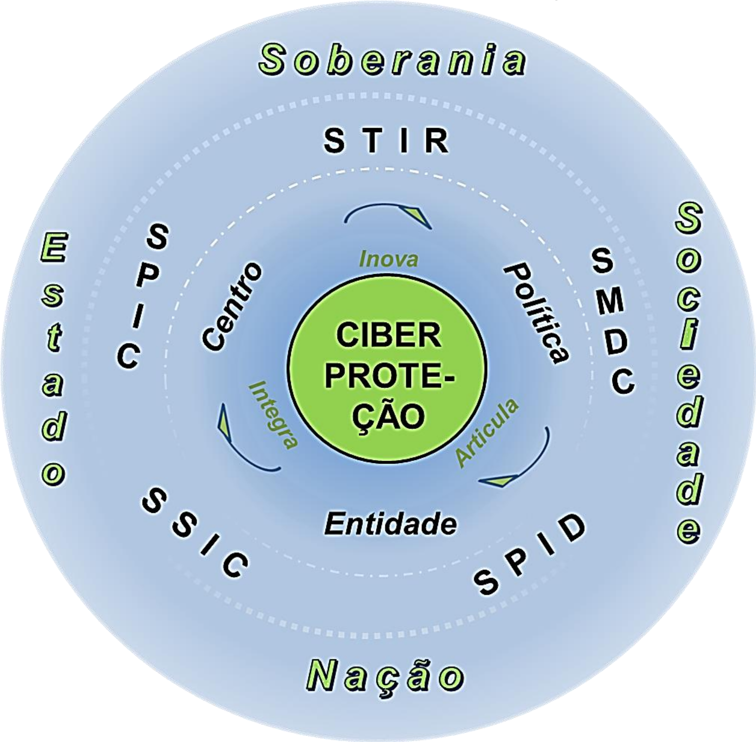
[189] Alinhado com o Art. 28 do Marco Civil da Internet (BRASIL, 2014a) e com o “Plano Brasil 2022”, publicado pela Secretaria de Estudos Estratégicos da Presidência da República (BRASIL, 2010b).

[190] Em consonância com o Relatório Final da CPI da Espionagem, elaborado em 2014, pela Comissão Parlamentar de Inquérito (CPI) destinada a investigar a denúncia de existência de um sistema de espionagem, estruturado pelo governo dos Estados Unidos, com o objetivo de monitorar *e-mails*, ligações telefônicas, dados digitais, além de outras formas de captar informações privilegiadas ou protegidas pela Constituição Federal (BRASIL, 2014d).

[191] Alinhado com uma das Metas Econômicas do “Plano Brasil 2022” (BRASIL, 2010b).

[192] Alinhado com a END (BRASIL, 2012c)

Figura 42 - Mandala do Modelo de Ciber Proteção Nacional




Fonte: elaboração própria

O conceito de Ciber Proteção é o núcleo do Modelo que, para manter sua efetividade e vitalidade, necessita de periódicas revisões, atualizações e adaptações às novas tendências e às inovações advindas do ciberespaço. Os integrantes do Macrossistema influenciam (novas demandas) e são influenciados pela PNCP, CICC e a ENCP, de forma que o MSCP estrutura e colabora com a proteção dos ativos de informação, que suportam as primícias, os interesses e os atores pétreos do País, bem como justificam a finalidade, necessidade e relevância do Modelo:

a) Estado – apesar de não ser estático, o modelo deve ser perene, pensado estrategicamente e a longo prazo. Não pode servir a propostas tempestivas, partidárias, passionais, fisiológicas e políticas de governos;
b) Nação - voltado às expectativas e às prioridades do cidadão, relacionada aos sentimentos de pertença à pátria brasileira;
c) Sociedade - busca o interesse coletivo, a sobrevivência e o desenvolvimento no ciberespaço de interesse;
d) Soberania - prioriza, frente a outras nações, a autoridade e autonomia do país no ciberespaço, almejando a projeção do poder cibernético nacional.

O estado da arte para entendimento dos fenômenos imbricados com a proteção da informação no ciberespaço envolve o ecossistema Brasil, representado pelo Estado-Nação-Sociedade-Soberania (no sentido lato). Os diversos sistemas detalhados no Macrossistema de Ciber Proteção, se interpenetram, ou seja, é característica de que os (super) sistemas de informação de interesse nacional transcendem e se fundem ao ambiente externo.

A proposta organizacional do modelo almeja consolidar entendimentos sobre a situação contemporânea à Ciber Proteção, sistematizando os principais atores e responsabilidades. Busca-se, ainda, sugerir atividades, operações e elementos de intervenção, a fim de proporcionar oportunidades de melhoria na gestão político-administrativa, factíveis e aderentes ao contexto de uma realidade nacional emergente, bem como evidenciando a necessidade de monitoração intensa, seguida de correções e aperfeiçoamentos.

O modelo Ciber Proteção é vocacionado para o atendimento de complexos ambientes (ecossistema digital nacional) desde cada organização *de per si*, mesmo que de forma mínima, com seus sistemas de informação locais (SegCiber), os repositórios informacionais das instituições (PD), transcendendo as fronteiras das redes de computadores e a salvaguarda os ativos de informação de interesse nacional (IC), em face das ameaças e dos ciberataques (DefCiber).

A conquista da proteção cibernética é factível se for abordada em etapas crescentes, como uma espiral ascendente, ou seja, o modelo proposto deve ser dinâmico, buscando continuadamente a sua renovação e ampliação.

Outro fator de suma importância é o entendimento de que a Ciber Proteção não depende, exclusivamente, de leis, estruturas ou tecnologias, mas da educação da sociedade. Neste contexto, deve-se incluir a conscientização de governantes e a de empresários, bem como a ampliação das competências no campo da literacia digital[193] dos cidadãos, tanto no acesso seguro e na aquisição de novas habilidades sobre novas ferramentas, quanto na maneira (segura) com que elas são utilizadas e incorporadas no cotidiano dos indivíduos e da sociedade.

---

[193] Habilidade de entender e utilizar a informação de múltiplos formatos e proveniente de diversas fontes quando apresentada por meio de computadores (GILSTER, *apud* PASSARELLI, 2014, p. 99).

O êxito das ações e atividades de Ciber Proteção passa, necessariamente, pelo engrossamento da cultura de segurança cibernética nacional, abarcando a compreensão dos problemas e suas consequentes vulnerabilidades, bem como mudando a forma de como as pessoas usam e desenvolvem a tecnologia. Nesse sentido, como exemplos, destacam-se: o entendimento dos riscos das redes sociais pelos cidadãos, o uso do governo digital, a preservação das informações digitais nas organizações e o desenvolvimento de *software* 'seguro' nas instituições de ensino, empresas, *startups* etc.

O modelo proposto opera, diretamente, no pacto federativo brasileiro, por intermédio de três vetores de intervenção:

a) a Política Nacional atua de forma consensual no *modus operandi* das instituições e organizações públicas e privadas, fornecendo subsídios para o uso seguro do ciberespaço de interesse nacional, bem como favorecendo a padronização e normatização de procedimentos necessários à Ciber Proteção;
b) o Centro de Cibernética potencializa as instituições, empresas e pesquisas nacionais, fornecendo suporte humano, tecnológico e científico às atividades de Ciber Proteção;
c) a Entidade Nacional articula a cooperação interagências, por meio de diretrizes e estratégias, favorecendo o crescimento da sinergia operacional das estruturas do pacto federativo relacionadas à Ciber proteção.

Com os devidos ajustes e adaptações, o Modelo em questão pode ser adotado em macrorregiões (P.ex.: América Latina), por países com similaridades político-governamentais, ou ainda pela iniciativa privada, mais precisamente empresas transnacionais e de grande porte.

Como desafio complementar operacional, o mundo quântico sugere um mergulho investigativo que transcende os limites desta pesquisa. Pode-se, então, aprofundar estudos sobre: (i) a influência da física quântica na codificação da informação, onde *bits* são substituídos por *qubits,* e (ii) os ataques a partir de computadores quânticos contra sistemas criptográficos convencionais, particularmente os assimétricos (criptografia de chaves públicas).

De igual forma, diante da crescente interação entre Tecnologias Autônomas e as de Informação e Comunicação (TA/TIC), que ampliou e diversificou a superfície de ataque, torna-se instigante estudar formas de otimizar a 'resiliência' do Sistema de Proteção das infraestruturas críticas. Nesta linha, podem-se acrescentar a análise de 'novos' entrantes no contexto da Ciber Proteção, como as soluções baseadas em Blockchain para a segurança do Modelo de Ciber Proteção Nacional ou mesmo, pontualmente, na preservação digital, bem como o impacto da IoT no Macrossistema, particularmente no SGIR, SPIC e SSIC.

Na seara da Ciência da Informação, sugere-se que se aprofundem estudos sobre a inteligência organizacional nas estruturas institucionais do MCPN. A CI caberia, também, nas áreas de gestão e de segurança da informação em meio digital, avaliar os impactos dos instrumentos instituídos (Estratégia e planos) pela *Política Nacional de Segurança da Informação*[194], a serem consolidados em 2019; bem como a entrada em vigor, no início de 2020, da *Lei de Proteção de Dados Pessoais*. Além disso, no viés acadêmico, a sinergia entre segurança e preservação favoreceriam a otimização de esforços intelectuais orientados ao aperfeiçoamento das áreas e o consequente aperfeiçoamento das grades curriculares, assim como das linhas de pesquisa no âmbito da CI.

O Modelo de Ciber Proteção Nacional apresenta atuações transversais, de forma que seus componentes persigam ininterrupta articulação, cooperação e integração. O Modelo, assim, pretende criar pontes cibernéticas e desconstruir barreiras técnicas e políticas, alinhando o arcabouço jurídico-normativo, bem como objetivos de Defesa e de Segurança nacionais.

Concluindo, no contexto contemporâneo da proteção da informação no meio digital, nada mais atual e verdadeiro do que a assertiva do filósofo grego Heráclito (535 - 475 a.C.): “Nada é permanente, exceto a mudança”.

Tenho convicção de que o Modelo proposto, a partir de metáforas tais como a 'Ciber Proteção', seja um símbolo, uma síntese, fruto de diversas análises e de pesquisas científicas, mas, de forma alguma um arquétipo findo. De fato, a implementação do Modelo de Ciber Proteção faz parte de um macroprocesso nacional, de uma jornada desafiadora em constante construção e desconstrução, em que não se pode

---

[194] No final do ano de 2018, em 26 de dezembro, o Decreto n. 9.637 instituiu a Política Nacional de Segurança da Informação no âmbito da APF, dispondo, também, sobre a governança da segurança da informação e a dispensa de licitação nos casos que possam comprometer a segurança nacional. (BRASIL, 2018b).

ter receio de quebrar paradigmas e de se reinventar. Não é uma linha de chegada, mas um esforço laborioso e perene, permanentemente renovado com as expectativas e mudanças do cotidiano nacional, bem como arejado pelas tendências globais.

## REFERÊNCIAS


ALBERCH Fugueras, Ramón. Los archivos, entre la memoria histórica y la sociedad del conocimiento. Barcelona: UOC, 2003.

ALVARENGA, L. A Teoria do Conceito Revisitada em Conexão com Ontologias e Metadados no Contexto das Bibliotecas Tradicionais e Digitais. **Datagrama Zero**: Revista de Ciência da Informação, v. 2, n. 6, dez. 2001.

ALVES, Alda Judith. A "revisão da bibliografia" em teses e dissertações: meus tipos inesquecíveis. **Cadernos de Pesquisa**, São Paulo, n. 81, p. 53-60, maio 1992. Disponível em: <http://www.fcc.org.br/pesquisa/publicacoes/cp/arquivos/916.pdf>. Acesso em: 08 jan. 2018.

ANGROSINO, Michael V. **Etnografia e observação participante.** Porto Alegre: Artmed, 2009.

AUSTRÁLIA. NATIONAL ARCHIVES OF AUSTRALIA (NAA). **Glossary.** Camberra, 2016. Disponível em: <http://www.naa.gov.au/records-management/publications/glossary.aspx#i>. Acesso em: 02 nov. 2016.

BANCO NACIONAL DO DESENVOLVIMENTO (BNDES). **Cartilha de Cidades.** Brasília, 2018.

BAPTISTA, S. G., CUNHA, M. B. Estudos de Usuários: Visão Global dos Métodos de Coleta de Dados. **Perspectiva em Ciência da Informação**, Belo Horizonte, v. 12, n. 2, p. 168-184, maio/ago. 2007.

BARDIN, Laurence. **Análise de Conteúdo**. Lisboa: Edições 70, 2009.

BARROS, Dirlene Santos; RODRIGUES, Georgete Medleg. A Lei brasileira de Acesso à Informação: análise das ações de atores sociais e do Arquivo Nacional na construção da LAI. In: Encontro Nacional de Pesquisa em Ciência da Informação, 17., 2016, Salvador. **Anais**... Salvador: ANCIB, 2016.Disponível em: Acesso em: 06 dez. 2018.

BESSER, H. Longevidade digital. **Acervo**, v. 23, n. 2, p. 57–70. Rio de Janeiro, 2010. Disponível em: <http://revista.arquivonacional.gov.br/index.php/revistaacervo/article/view/26/26>. Acesso em: 01 ago. 2016.

BODÊ, Ernesto C. Documento digital e a preservação digital: algumas considerações conceituais. **Revista Ibero-Americana de Ciência da Informação - RICI**, v. 9, n. 2, p. 503-516, jul./dez. 2016. ISSN 1983-5213. Disponível em: <http://periodicos.unb.br/index.php/RICI/article/view/18631>. Acesso em: 02 nov. 2016.

BOERES, Sonia Araújo de Assis. **Competências necessárias para equipes de profissionais de preservação digital**. 2017. 293 f. : il. Tese (Doutorado em Ciência da Informação) – Universidade de Brasília, 2017. Disponível em: <http://repositorio.unb.br/handle/10482/24354>. Acesso em: 08 set. 2018.

BORKO, H. Information science: what is it? **American Documentation**, v. 19, n. 1, p. 3-5, 1968.

BRAMAN, Sandra. **Change of State**: information, policy and power. Cambridge: MIT Press, 2006.

BRAMAN, Sandra. **Defining information**: An approach for policy-makers. Telecommunications Policy, v. 13, n. 3, p. 233-242. 1989.

______. Poder, privacidade e segurança: discussões sobre acesso, controle e uso da informação. **O Debatedouro**, v. 12, n. 01, 84. ed. p. 26-32, Belo Horizonte, 2014. Disponível em: <https://odebatedouro.files.wordpress.com/2014/05/debat84_v1.pdf>. Acesso em: 29 ago. 2016.

BRASIL. Decreto n. 3.505, de 13 de junho de 2000. **Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal**. Diário Oficial [da] República Federativa do Brasil. Brasília, DF, 2000. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto/d3505.htm>. Acesso em: 22 mar. 2018.

BRASIL. Decreto n. 4.829, de 3 de setembro de 2003. **Dispõe sobre a criação do Comitê Gestor da Internet no Brasil - CGI.Br, sobre o modelo de governança da Internet no Brasil, e dá outras providências**. Disponível em <http://www.planalto.gov.br/ccivil_03/decreto/2003/d4829.htm>. Acesso em: 4 mar. 2016.

BRASIL. Decreto n. 6.703, de 18 de dezembro de 2008. **Aprova a Estratégia Nacional de Defesa, e dá outras providências**. Diário Oficial [da] República Federativa do Brasil. Brasília, DF, 19 de dezembro de 2008a. Disponível em: <http://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?data=19/12/2008&jornal=1&pagina=4&totalArquivos=160 >. Acesso em: 29 abr. 2015.

BRASIL. Decreto n. 8.638, de 15 de janeiro de 2016. **Institui a Política de Governança Digital no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional**. Diário Oficial [da] República Federativa do Brasil. Brasília, DF, 18 de janeiro de 2016a. Disponível em: <http://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?data=18/01/2016&jornal=1&pagina=2&totalArquivos=680>. Acesso em: 11 mar. 2016.

BRASIL. Decreto n. 9.573, de 22 de novembro de 2018. **Aprova a Política Nacional de Segurança de Infraestruturas Críticas.** Brasília, DF, 2018a. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/D9573.htm>. Acesso em: 07 dez. 2018.

BRASIL. Decreto n. 9.637, de 26 de dezembro de 2018. **Institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação, e altera o Decreto nº 2.295, de 4 de agosto de 1997, que regulamenta o disposto no art. 24, caput , inciso IX, da Lei nº 8.666, de 21 de junho de 1993, e dispõe sobre a dispensa de licitação nos casos que possam comprometer a segurança nacional**. Brasília, DF, 2018b. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/D9637.htm>. Acesso em: 27 dez. 2018.

BRASIL. Gabinete de Segurança Institucional da Presidência da República. **Diretrizes relacionadas à segurança da informação e comunicações para o uso de computação em nuvem nos órgãos e entidades da administração pública federal.** Brasília, 2012a. Disponível em <http://dsic.planalto.gov.br/documentos/nc_14_nuvem.pdf>. Acesso em: 02 nov. 2016.

BRASIL. Gabinete de Segurança Institucional da Presidência da República. **Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal 2015-2018.** Brasília: Presidência da República, 2015.

BRASIL. Gabinete de Segurança Institucional da Presidência da República. **Guia de referência para a segurança das infraestruturas críticas da informação.** Brasília, 2010a. Disponível em <http://dsic.planalto.gov.br/documentos/publicacoes/2_Guia_SICI.pdf>. Acesso em: 10 ago. 2015.

BRASIL. Gabinete de Segurança Institucional da Presidência da República. Portaria n. 45, de 8 de setembro de 2009. **Institui, no âmbito da Câmara de Relações Exteriores e Defesa Nacional (CREDEN), o Grupo Técnico de Segurança Cibernética e dá outras providências.** Disponível em <http://www.in.gov.br/visualiza/index.jsp?data=09/09/2009&jornal=1&pagina=2&totalArquivos=80>. Acesso em: 10 maio 2013.

BRASIL. Gabinete de Segurança Institucional da Presidência da República. Instrução Normativa GSI n. 1, de 13 de junho de 2008. **Disciplina a gestão da segurança da informação e comunicações na administração pública federal, direta e indireta e dá outras providências.** Diário Oficial [da] República Federativa do Brasil. Brasília, DF, 13 de junho de 2008b, n. 115 - Seção 1.

BRASIL. Lei n. 12.527 de 18 de novembro 2011. **Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei n. 8.112, de 11 de dezembro de 1990; revoga a Lei n. 11.111, de 5 de maio de 2005, e dispositivos da Lei n. 8.159, de 8 de janeiro de 1991; e dá outras providências.** Diário Oficial [da] República Federativa do Brasil, Brasília, DF, 18 nov. 2011a. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm>. Acesso em: 22 nov. 2016.

BRASIL. Lei n. 12.965, de 25 de abril de 2014. **Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil e determina as diretrizes para atuação da União, dos Estados, do Distrito Federal e dos Municípios em relação à matéria**. Diário Oficial [da] República Federativa do Brasil. Brasília, DF, 2014a. Disponível em: <http://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?jornal=1&pagina=1&data=24/04/2014>. Acesso em: 21 fev. 2016.

BRASIL. Lei n. 13.709, de 15 de agosto de 2018. **Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet)**. Diário Oficial [da] República Federativa do Brasil. Brasília, DF, 2018c. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Lei/L13709.htm>. Acesso em: 21 set. 2018.

BRASIL. Ministério da Ciência, Tecnologia, Inovações e Comunicações. **Estratégia Brasileira para a Transformação Digital.** Brasília : Presidência da República, 2018d**.**

BRASIL. Ministério da Defesa. **Doutrina de Operações Conjuntas** – MD30-M-01. 1. 1º Volume Brasília, 2011b. Disponível em: <https://www.defesa.gov.br/arquivos/File/legislacao/emcfa/publicacoes/md_30_m_01_1volume.pdf> Acesso em: 09 jun. 2013.

BRASIL. Ministério da Defesa. **Doutrina Militar de Defesa Cibernética - MD31-M-07**. Brasília, DF, 2014b.

BRASIL. Ministério da Defesa. **Glossário das Forças Armadas** – MD35-G-01. Brasília, 2015.

BRASIL. Ministério da Defesa. **Livro Branco da Defesa Nacional**. Brasília, DF, 2012b. Disponível em: <http://www.defesa.gov.br/arquivos/2012/mes07/lbdn.pdf>. Acesso em: 04 mar. 2016.

BRASIL. Ministério da Defesa. **Política Nacional de Defesa (PND) e a Estratégia**

**Nacional de Defesa (END)**. Brasília, DF, 2012c. Disponível em: <http://www.defesa.gov.br/arquivos/estado_e_defesa/END-PND_Optimized.pdf. Acesso em: 15 jul. 2015.

BRASIL. Ministério da Defesa. Portaria Normativa n. 2.777, de 27 de outubro de 2014. **Dispõe sobre a diretriz de implantação de medidas visando à potencialização da Defesa Cibernética Nacional e dá outras providências. Diário Oficial [da] República Federativa do Brasil.** Brasília, DF, 2014c. Disponível em: <http://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?jornal=1&pagina=7&data=28/10/2014>. Acesso em: 29 out. 2014.

BRASIL. Ministério da Defesa. Portaria Normativa n. 3.389, de 21 de dezembro de 2012. **Dispõe sobre a Política Cibernética de Defesa**. Diário Oficial [da] República Federativa do Brasil. Brasília, DF, 2012d. Disponível em: <http://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?jornal=1&pagina=11&data=27/12/2012>. Acesso em: 29 abr. 2015.

BRASIL. Ministério do Planejamento. **Estratégia de Governança Digital para a Administração Pública Federal 2016-2019**. Brasília, 2016b. Disponível em: <https://www.governoeletronico.gov.br/biblioteca/arquivos/egd-estrategia-de-governanca-digital-da-administracao-federal-2016-2019/download>. Acesso em: 10 mar. 2016.

BRASIL. Presidência da República. Secretaria de Assuntos Estratégicos. **Brasil 2022**. Brasília: SAE, 2010b.

BRASIL. Presidência da República. Secretaria de Assuntos Estratégicos. **O setor cibernético brasileiro**: Contexto atual e perspectivas. Relatório do XIII Encontro Nacional de Estudos Estratégicos. Rio de Janeiro, RJ, setembro de 2013. Disponível em: <https:// http://www.sae.gov.br/site/wp-content/uploads/relatorio_XIIIENEE_ebook.pdf>. Acesso em: 09 jun. 2014.

BRASIL. Senado Federal. **Em Discussão!** Brasília, n.21, jul. 2014d. Disponível em: <http://www.senado.gov.br/noticias/jornal/emdiscussao/espionagem/>. Acesso em: 29 nov. 2014.

BRASIL. Tribunal de Contas da União. Acórdão n. 2308/2010 – TCU – Plenário. **Relatório de Levantamento**. Avaliação da governança de tecnologia da Informação na administração pública federal. Brasília: TCU, 2010c. Disponível em: <http://portal2.tcu.gov.br/portal/page/portal/TCU/comunidades/tecnologia_informacao/pesquisas_governanca/D500E3BC0A19993DE040010A8900136B>. Acesso em: 29 nov. 2014.

BRASIL. Tribunal de Contas da União. Acórdão n. 2585/2012 – TCU – Plenário. **Relatório de Levantamento.** Avaliação da governança de tecnologia da Informação na administração pública federal. Brasília: TCU, 2012e. Disponível em: <http://portal2.tcu.gov.br/portal/page/portal/TCU/comunidades/tecnologia_informacao/pesquisas_governanca/D500BE942EEF7793E040010A89001367>. Acesso em: 29 nov. 2014.

BRASIL. Tribunal de Contas da União. Acórdão n. 3117/2014 – TCU – Plenário. **Relatório de Levantamento**. Avaliação da governança de tecnologia da Informação na administração pública federal. Brasília: TCU, 2014e. Disponível em: <http://www.tcu.gov.br/Consultas/Juris/Docs/judoc/Acord/20141114/AC_3117_45_14_P.doc>. Acesso em: 01 dez. 2014.

BRASIL. Tribunal de Contas da União. Acórdão n. 882/2017 – TCU – Plenário. **Relatório de Levantamento**. Avaliação da governança de tecnologia da Informação na administração pública federal. Brasília: TCU, 2017. Disponível em: <http://portal.tcu.gov.br/imprensa/noticias/nivel-de-governanca-e-gestao-de-tecnologias-da-informacao-e-muito-baixo-1.htm. Acesso em: 27 set 2017.

BRASIL. Tribunal de Contas da União. **Boas práticas em segurança da informação**. 2. ed. Brasília: TCU, Secretaria de Fiscalização de Tecnologia da Informação, 2007.

BRASIL. Tribunal de Contas da União. Levantamento Integrado de Governança Organizacional Pública - ciclo 2018**. Sumário Executivo**. Brasília: TCU, 2018. Disponível em: < https://portal.tcu.gov.br/governanca/governancapublica/organizacional/levantamento-2018/resultados.htm>. Acesso em: 08 dez. 2018.

BUCKLAND, M. K. Information as thing. **Journal of the American Society for Information Science** (JASIS), v. 45, n .5, p. 351-360, 1991.

CAMPOS, M. L. de Almeida. **Linguagem documentária**: teorias que fundamentam sua elaboração. Niterói: EdUFF, 2001.

CAPURRO, Rafael. Epistemologia e ciência da informação. In: Encontro nacional de pesquisa em ciência da informação, 5., 2003. **[Anais].** Belo Horizonte: Associação Nacional de Pesquisa e Pós-Graduação em Ciência da Informação e Biblioteconomia, 2003. Disponível em: <http://www.capurro.de/enancib_p.htm>. Acesso em: 02 mar. 2015.

CAPURRO, R.; HJORLAND, B. O conceito de informação. **Perspectivas em Ciência da Informação,** Belo Horizonte, v.12, n.1, p. 148-207, abr. 2007. Disponível em: < http://portaldeperiodicos.eci.ufmg.br/index.php/pci/article/view/54>. Acesso em: 28 jul.2016

CASTELLS, Manuel. **A era da Informação:** Economia, Sociedade e Cultura. A sociedade em rede. v.1., 4.ed. Lisboa: Fundação Caloute Gulbenkian, 2010.

CASTELLS, Manuel. **A galáxia Internet:** Reflexões sobre Internet, Negócios e Sociedade. 2.ed. Lisboa: Fundação Caloute Gulbenkian, 2007.

CASTELLS, Manuel. **A sociedade em rede**. v. 1., 8. ed. atualizada. São Paulo: Paz e Terra, 1999.

CASTELLS, Manuel; CARDOSO, Gustavo (Orgs.). **A Sociedade em Rede: do conhecimento à ação política**; Conferência. Belém (Portugal): Imprensa Nacional, 2005.

CAVALCANTE, Leonardo de Oliveira; SILVA, Armando Malheiro da, FREIRE, Gustavo Henrique de Araújo. Gestão informacional em meio digital: caso Rede Paraíba de Comunicação afiliada da Rede Globo de Televisão. **Prisma.com**, Porto, n.21, 2014. Disponível em: <http://revistas.ua.pt/index.php/prismacom/article/view/2649>. Acesso em: 27 abr. 2017.

CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL (CERT.br). **Cartilha de segurança para a Internet.** São Paulo: Comitê Gestor da Internet no Brasil, 2016. Disponível em:<http://cartilha.cert.br/>. Acesso em: 29 out. 2016.

CENTRO REGIONAL DE ESTUDOS PARA O DESENVOLVIMENTO DA SOCIEDADE DA INFORMAÇÃO (CETIC.br). **Pesquisa sobre o uso das tecnologias de informação e comunicação no setor público brasileiro**: TIC governo eletrônico

2015. São Paulo: CGI.br, 2016. Disponível em: <http://cetic.br/media/docs/publicacoes/2/TIC_eGOV_2015_LIVRO_ELETRONICO.pdf>. Acesso em: 19 nov. 2016.

CENTRO REGIONAL DE ESTUDOS PARA O DESENVOLVIMENTO DA SOCIEDADE DA INFORMAÇÃO (CETIC.br). **Pesquisa sobre o uso das tecnologias de informação e comunicação no setor público brasileiro**: TIC governo eletrônico 2017. São Paulo: CGI.br, 2018. Disponível em: <http://cetic.br/media/docs/publicacoes/2/TIC_eGOV_2017_LIVRO_ELETRONICO.pdf>. Acesso em: 10 dez. 2018.

CERVO, Amado Luiz; BERVIAN, Pedro Alcino; SILVA Roberto da. **Metodologia Científica.** 6. ed. São Paulo: Pearson Prentice Hall, 2007.

CHOO, Chun Wei. **A organização do conhecimento**: como as organizações usam a informação para criar significado, construir conhecimento e tomar decisões. 2. ed. São Paulo: SENAC, 2006.

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

COMITÊ GESTOR DA INTERNET NO BRASIL (CGI.br). **[Revista] .br**. São Paulo, n.09, fev. 2016a. Disponível em: <http://www.cgi.br/media/docs/publicacoes/3/revista-br-ano-07-2016-edicao-09.pdf >. Acesso em: 15 nov. 2016.

COMITÊ GESTOR DA INTERNET NO BRASIL (CGI.br). **[Revista] .br**. São Paulo, n.10, fev. 2016b. Disponível em: <http://www.cgi.br/media/docs/publicacoes/3/revista-br-ano-07-2016-edicao-10.pdf>. Acesso em: 15 nov. 2016.

CONSELHO NACIONAL DE ARQUIVOS (CONARQ). **Carta para preservação do patrimônio arquivístico digital.** Rio de Janeiro: Arquivo Nacional, 2004.

CONSELHO NACIONAL DE ARQUIVOS (CONARQ). **Diretrizes para a implementação de repositórios arquivísticos digitais confiáveis***:* RDC-Arq 2015. Rio de Janeiro, 2015. Disponível em: < http://www.conarq.gov.br/images/publicacoes_textos/diretrizes_rdc_arq.pdf>. Acesso em: Acesso em: 23 jan. 2018.

CONSELHO NACIONAL DE ARQUIVOS (CONARQ). Diretrizes para a Presunção de Autenticidade de Documentos Arquivísticos Digitais. Rio de Janeiro: Arquivo Nacional, 2012.

CONSELHO NACIONAL DE ARQUIVOS (CONARQ). **e-ARQ Brasil**: Modelo de Requisitos para Sistemas Informatizados de gestão Arquivística de Documentos. Rio de Janeiro: Arquivo Nacional, 2011.

CONSELHO NACIONAL DE ARQUIVOS (CONARQ). **Glossário Documentos arquivísticos digitais**. 2014. Disponível em: <http://www.conarq.gov.br/images/ctde/Glossario/2014ctdeglossario_v6_public.pdf>. Acesso em: 25 set. 2016.

CÔRTE, Kelson. **Segurança da informação baseada no valor da informação e nos pilares tecnologia, pessoas e processos**. 2014. 212 f., il. Tese (Doutorado em Ciência da Informação) - Universidade de Brasília, Brasília, 2014.

COSTA, Maíra M.; CUNHA, Murilo B. da; BOERES, Sonia de A. Dados de pesquisa: o que são, impactos do grande volume produzido, como organizá-los e quais preservar. In: MÁRDERO ARELLANO, M. Á., ARAÚJO, L. M. de S. (Org.). **Tendências para a gestão e preservação da informação digital**. Brasília: Ibict, 2017. p. 98-142. Disponível em: <http:/livroaberto.ibict.br/handle/123456789/1069>. Acesso em: 23 jan. 2018.

CUNHA, Agostinho Paiva da. Acerca do Conceito Estratégico da NATO. **Nação e Defesa**: revista do Instituto da Defesa Nacional, Lisboa, n.125, p. 121-128, 2010. Disponível em: <http://www.idn.gov.pt/publicacoes/nacaodefesa/textointegral/NeD125.pdf>. Acesso em: 16 jan. 2017.

CUNHA, M. B. da; CAVALCANTI, C. R. de O. **Dicionário de biblioteconomia e arquivologia.** Brasília: Briquet de Lemos, 2008.

DAHLBERG, I. A referent-oriented, analytical concept theory for interconcept. **International Classification,** v. 5, n. 3, p. 142-151, 1978a.

DAHLBERG, I. Concepts and terms: ISKO's major challenge. **Knowledge Organization**, v. 36, n. 2/3, p. 169-177, 2009.

DAHLBERG, I. Teoria do conceito. Tradução Astério Tavares Campos. **Ci. Inf.**, Rio de Janeiro, v. 7, n. 2, p. 101-107, 1978b.

DIAS, Eduardo José Wense; NAVES, Madalena Martins Lopes. **Análise de assunto: teoria e prática.** Brasília: Thesaurus, 2007.

DURANTI, Luciana. InterPARES Trust. **Acervo**: revista do Arquivo Nacional, Rio de Janeiro, v. 28, n. 2, p. 11-18, jul./set. 2015. Disponível em: < http://revista.arquivonacional.gov.br/index.php/revistaacervo/article/view/607>. Acesso em: 25 set. 2016.

ESTADOS UNIDOS. Department of Defense. **Dictionary of Military and Associated Terms**. Washington D.C.: DoD Press, Feb. 2016. (Joint Publication 1-02). Disponível em: <http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf>. Acesso em: 20 maio 2016.

FERNANDES, Jorge. H. C. A perniciosa armadilha cibernética e uma proposta de mobilização nacional. In: Gheller *et al*. (Orgs.). **Amazônia e Atlântico Sul**: desafios e perspectivas para a defesa no Brasil. Brasília: IPEA: NEP, 2015.

FERNANDES, Jorge. H. C. **Segurança e Defesa Cibernéticas para Reduzir Vulnerabilidades nas Infraestruturas Críticas Nacionais** (Relatório Técnico). Núcleo de Estudos Prospectivos do Exército Brasileiro. Brasil: Exército Brasileiro, 2012.

FERNANDES, Jorge H. C.; RODRIGUES, Roberto W. **Auditoria de Segurança Da Informação**. Notas de Aula (Especialização) - Curso de Especialização em Gestão da Segurança da Informação e Comunicações - CEGSIC / Departamento de Ciência da Computação, Instituto de Ciências Exatas, Universidade de Brasília, Brasília. 2013.

FLICK, Uwe. **Desenho da pesquisa qualitativa.** Porto Alegre: Bookman, 2009a.

FLICK, Uwe. **Introdução à pesquisa qualitativa.** 3. ed. Porto Alegre, RS: Bookman, 2009b.

FLORIDI, L. (Ed.) **The Onlife Manifesto**: Being Human in a Hyperconnected Era. London: Springer, 2015.

GASQUE, Kelley Cristine G. D. Teoria fundamentada: nova perspectiva à pesquisa exploratória. In: MUELLER, Suzana Pinheiro Machado (Org.). **Métodos para a pesquisa em Ciência da Informação**. Brasília: Thesaurus, 2007. p. 83-118.

GETSCHKO, Demi. Internet, Mudança ou Transformação? In: CGI.br (Comitê Gestor da Internet no Brasil). **Pesquisa sobre o uso das tecnologias da informação e da comunicação 2008**. São Paulo, 2009, pp. 49-52.

GIBBS, Graham. **Análise de dados qualitativos.** Porto Alegre: Bookman; 2009.

GIL, Antônio Carlos. **Métodos e técnicas de pesquisa social**. 6. ed. São Paulo: Atlas, 2008.

GLEICK, James. **A informação:** uma estória, uma teoria, uma enxurrada. 1. ed. São Paulo: Companhia das Letras, 2013.

GP3/CAEM. A proteção das estruturas estratégicas no contexto da segurança integrada. PADECEME, Rio de Janeiro, v. 12, n. 21, p. 92-107. 2018.

HECKERT, Cristiano R. **Segurança da informação e comunicação (SIC):** ações e desafios da SLTI. Brasília: Câmara dos Deputados, 2015. Disponível em: <http://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-temporarias/parlamentar-de-inquerito/55a-legislatura/cpi-crimes-ciberneticos/documentos/apresentacao-cristiano-hechert>. Acesso em: 09 nov. 2016

INNARELLI, Humberto Celeste. **Gestão da preservação de documentos arquivísticos:** proposta de um modelo conceitual**.** 2015. 348 f., il. Tese (Doutorado em Ciência da Informação) -Universidade de São Paulo, São Paulo, 2015.

INTERPARES. The international research on permanent authentic records in electronic systems. **InterPARES 2 Project.** 2007. Disponível em: <http://www.interpares.org/ip2/display_file.cfm?doc=ip2_preserver_guidelines_booklet--portuguese.pdf>. Acesso em: 28 out. 2016.

ISO. **ISO 1087-1** - Terminology work – vocabulary- Part 1: Theory and application. 2000.

ISO/IEC. **ISO/IEC 27000** - Information technology - Security Techniques - Information security management systems - Overview and vocabulary. 2014.

ISO/IEC. **ISO/IEC 27032** - Information technology - Security Techniques - Guidelines for cybersecurity. 2012.

ISO/IEC. **ISO/IEC 27035** - Information technology - Security Techniques - Information security incident management. 2016.

JARDIM, Jose Maria. Caminhos e perspectivas da gestão de documentos em cenários de transformações. **Acervo**: revista do Arquivo Nacional, Rio de Janeiro, v. 28, n. 2, p. 19-50, jul./set. 2015. Disponível em: < http://revista.arquivonacional.gov.br/index.php/revistaacervo/article/view/607>. Acesso em: 25 set.2016.

KLIMBURG, Alexander (Ed.), **National Cyber Security Framework manual**, NATO CCD COE Publication, Tallinn, 2012

KVALE, S. **Interviews:** an introduction to qualitative research interviewing, Thousand Oaks; London: Sage, 1996,

LAKATOS, Eva Maria; MARCONI, Marina de Andrade. **Fundamentos de metodologia científica**. 5. ed. São Paulo: Atlas, 2003.

LEMOS, André; LÉVY, Pierre. **O futuro da internet:** em direção a uma ciberdemocracia planetária. São Paulo: Paulus, 2010.

LEMOS, Renata T. S. et al. Tecnontologia & complexidade. **Ciências & Cognição**, v. 11, jul. 2007. ISSN 1806-5821. Disponível em: <http://www.cienciasecognicao.org/revista/index.php/cec/article/view/664>. Acesso em: 30 jan. 2017.

LÉVY, Pierre. **Cibercultura.** São Paulo: Ed. 34, 2002.

LINS, Greyciane Souza. **Colaborações dos estudos de cibercultura para a ciência**

**da informação.** 2013. 170 f., il. Tese (Doutorado em Ciência da Informação) -Universidade de Brasília, Brasília, 2013.

LLANSO SANJUAN, Joaquin. Sistemas archivísticos y modelos de gestión de documentos en el ámbito internacional (Parte II)1. **Códices**, [S.l.], v. 2, n. 2, 2006. Disponível em: <http://revistas.lasalle.edu.co/index.php/co/article/view/614/531>. Acesso em: 18 nov. 2016.

LUNA, S. V. **Planejamento de Pesquisa**: uma introdução. São Paulo: Educ. 1997

LUZ, Charlley. Ontologia Digital Arquivística. In: MÁRDERO ARELLANO, M. Á., ARAÚJO, L. M. de S. (Org.). **Tendências para a gestão e preservação da informação digital**. Brasília: Ibict, 2017. p. 77-97. Disponível em: <http:/livroaberto.ibict.br/handle/123456789/1069>. Acesso em: 23 jan. 2018.

MÁRDERO ARELLANO, Miguel Ángel. **Critérios para a preservação digital da informação científica.** 354 p. Tese (Doutorado em Ciência da Informação). Universidade Federal de Brasília, Departamento de Ciência da Informação, 2008. Disponível em: < http://repositorio.unb.br/bitstream/10482/1518/1/2008_MiguelAngelMarderoArellano.pdf>. Acesso em: 15 nov. 2016.

MÁRDERO ARELLANO, Miguel Ángel. La preservación digital y la Red Cariniana. In: MÁRDERO ARELLANO, M. Á., ARAÚJO, L. M. de S. (Org.). **Tendências para a gestão e preservação da informação digital**. Brasília: Ibict, 2017. p. 200-220. Disponível em: <http:/livroaberto.ibict.br/handle/123456789/1069>. Acesso em: 23 jan. 2018.

MARQUES, Anna. Maria de O.; VIANNA, Eduardo Wallier. Identificação das necessidades de informação dos profissionais de segurança da informação. **Revista Tecnologias em Projeção**, v. 4, n. 2, dez., 2013. Disponível em: <http://revista.faculdadeprojecao.edu.br/index.php/Projecao4/article/view/321/240>. Acesso em: 02 mar. 2014.

MARQUES, Camila *et al.* Marco Civil da Internet: seis meses depois, em que pé estamos? **Artigo 19,** 2015. Disponível em: < http://artigo19.org/wp-content/uploads/2015/01/an%C3%A1lise-marco-civil-final.pdf>. Acesso em: 20 fev. 2016.

MARTINS, Moisés de Lemos. A sociedade da informação, as ciências da comunicação e da informação e a comunidade científica. In: PASSARELLI, B.; SILVA, A. M. da; RAMOS, F. (Org.). **e-Infocomunicação**: estratégias e aplicações. São Paulo: Editora Senac, 2014. p. 9-14.

MCLUHAN, Marshall. Os Meios de Comunicação como Extensões do Homem. São Paulo: Cultrix, 1969.

MEDEIROS, Jackson da Silva. A construção do conceito: aproximações complementares entre a análise de Michel Foucault e Ingetraut Dahlberg. **Revista ACB**: Biblioteconomia em Santa Catarina, Florianópolis, v.15, n.2, p. 41-53, jul./dez., 2010. Disponível em: <http://www.brapci.inf.br/index.php/article/view/0000009682/17e09fd8ea0f858312fc1731746e5814>. Acesso em: 21 abr. 2018.

MELO, Maria Antônia Fonseca. **Contribuições das abordagens positivista e pragmática do estudo do conceito para o modelo conceitual FRSAD**. 2013. 133 f., il. Dissertação (Mestrado em Ciência da Informação) - Universidade de Brasília, Brasília, 2015. Disponível em: < http://repositorio.unb.br/handle/10482/16160 > Acesso em: 08 set. 2015.

MINAYO, Maria C. de S. (Org.). **Pesquisa social**: teoria, método e criatividade. 26.

ed. Petrópolis: Vozes, 2007.

MITNICK, Kevin D.; SIMON, William L. **A arte de enganar:** controlando o fator humano na segurança da informação. São Paulo: Pearson Education, 2003.

MITNICK, Kevin D.; SIMON, William L. **A arte de invadir**: as verdadeiras histórias por trás das ações de hackers, intrusos e criminosos eletrônicos São Paulo: Pearson Education, 2006.

OLIVEIRA, Marcos Aurélio Guedes de *et al*. **Guia de defesa cibernética na América do Sul.** Recife: Editora UFPE, 2017. Disponível em: <http://pandia.defesa.gov.br/images/acervodigital/GuiaDefesaCiberneticaAmericaSul.pdf>. Acesso em: 05 out. 2017

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD). **Recommendation of the Council on Digital Government Strategies.** Organisation for Economic Co-operation and Development, 2014. Disponível em: <http://www.oecd.org/gov/digital-government/Recommendation-digital-government-strategies.pdf>. Acesso em: 30 out. 2018.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS PARA A EDUCAÇÃO, A CIÊNCIA E A CULTURA (UNESCO). **Communication-and-information.** 2016. Disponível em: <http://www.unesco.org/new/pt/brasilia/communication-and-information/>. Acesso em: 05 nov. 2016.

ORGANIZAÇÃO DOS ESTADOS AMERICANOS (OEA). **Liberdade de expressão e internet**. Comissão Interamericana de Direitos Humanos. 2013. Disponível em: <http://www.oas.org/pt/cidh/expressao/docs/publicaciones/2014%2008%2004%20Liberdade%20de%20Express%C3%A3o%20e%20Internet%20Rev%20%20HR_Rev%20LAR.pdf>. Acesso em: 25 set. 2016.

PASSARELLI, Brasilina *et al*. Identidade conceitual e cruzamento disciplinares. In: PASSARELLI, B.; SILVA, A. M. da; RAMOS, F. (Org.). **e-Infocomunicação**: estratégias e aplicações. São Paulo: Editora Senac, 2014. p. 25-47.

PENNOCK, Maureen. **Digital Curation and the management of digital library cultural heritage resources**. Local Studies Librarian, [S.l], v. 25, n. 2, 2006. Disponível em: <http://www.ukoln.ac.uk/ukoln/staff/m.pennock/publications/docs/lslcuration_mep.pdf>. Acesso em: 25 jan. 2016.

PEREIRA, Edmeire Cristina; BUFREM, Leilah Santiago. Princípios de organização e representação de conceitos em linguagens documentárias. **Encontros Bibli**: revista eletrônica de biblioteconomia e ciência da informação, Florianópolis, v. 10, n. 20, p. 21-37, nov. 2007. Disponível em: <https://periodicos.ufsc.br/index.php/eb/article/view/1518-2924.2005v10n20p21/302>. Acesso em: 20 nov. 2015.

PINHEIRO, Lena V. R.; FERREZ, Helena D. **Tesauro Brasileiro de Ciência da Informação.** Brasília: Instituto Brasileiro de Informação em Ciência e Tecnologia (Ibict), 2014.

PINHEIRO, Marta Macedo Kerr. Estado Informacional implicações para as políticas de informação e de inteligência no limiar do século XXI. 2012. **Varia História**, Belo Horizonte, v. 28, n. 47, p. 61-77, jan./jun. 2012.

PINTO, Maria Manuela de Gomes de Azevedo. **A Gestão da Informação nas Universidades Públicas Portuguesas:** Reequacionamento e proposta de modelo**.** 2015. Tese. (Doutoramento em plataformas Digitais). Universidade do Porto, Faculdade de

Letras, Porto, Portugal. Universidade de Aveiro, Departamento de Comunicação e Artes, Aveiro, Portugal.

PINTO, Maria Manuela de Gomes de Azevedo. Gestão da Informação e preservação digital: uma perspectiva portuguesa de uma mudança de paradigma. CONGRESO ISKO-SPAÑA, 9, Valencia. **Nuevas perspectivas para la difusión y organización del conocimiento: actas**. Valencia: Universidad Politecnica de Valencia. 2009a. p. 323-355. Disponível em: <http://hdl.handle.net/10216/25380>. Acesso em: 10 maio 2017.

PINTO, Maria Manuela de Gomes de Azevedo. **Os Arquivos e a Gestão da Informação: uma reflexão em Ciência de Informação**. Jornadas Ibero-Americanas de Arquivos Municipais: reinventando os Arquivos no século XXI. Lisboa, 2016. https://repositorio-aberto.up.pt/bitstream/10216/86549/2/164465.pdf>. Acesso em: 06 dez. 2018.

PINTO, Maria Manuela de Gomes de Azevedo. **Preservmap:** Um roteiro de preservação na era digital. Porto: Edições Afrontamento, 2009b. ISBN: 978-972-36-1070-3.

POMBO, Olga. Práticas Interdisciplinares. **Sociologias**, Universidade Federal do Rio Grande do Sul, n.15, jan./jun. 2006, p. 208-249. Disponível em: <http://www.scielo.br/pdf/soc/n15/a08v8n15.pdf>. Acesso em: 05 maio 2017.

PORTO, Luís Carlos de Oliveira. **Diretrizes para melhoria da política de segurança da informação da infraestrutura de chaves públicas**. Monografia (Especialização em gestão de Segurança da Informação e Comunicações) - Universidade de Brasília, Brasília, 2014.

RAMOS, Anderson *et al*. (Orgs.). **Security Officer – 1:** Guia Oficial para Formação de Gestores em Segurança da Informação**.** 2. ed., Porto Alegre, RS: Zouk, 2006.

REDE NACIONAL EM SEGURANÇA DA INFORMAÇÃO E CRIPTOGRAFIA (RENASIC). **Painel Segurança em Sistemas SCADA**. Relatório, Brasília, 2014. Disponível em: < http://www.renasic.org.br/eventos/detalhe/3>. Acesso em: 02 dez. 2016.

RONDINELLI, Rosely Curi. **O Conceito de documento arquivístico frente à realidade digital: uma revisitação necessária**. 2011. 270 f.: il. Tese (Doutorado em Ciência da Informação) – Universidade Federal Fluminense, Niterói, 2011. Disponível em: <https://www.siarq.unicamp.br/siarq/images/siarq/publicacoes/preservacao_digital/tese_rondinelli.pdf>. Acesso em: 08 set. 2015.

RONDINELLI, Rosely Curi. **O documento arquivístico ante a realidade digital**: uma revisitação conceitual necessária. Rio de Janeiro: Editora FGV, 2013.

SANTOS, Helena. Complexidade e informacionalismo: as contribuições de Edgar Morin e Manuel Castells. In: PASSARELLI, B.; SILVA, A. M. da; RAMOS, F. (Org.). **e-infocomunicação: estratégias e aplicações**. São Paulo: Editora Senac São Paulo, 2014. p. 25-47.

SANTOS, V. B. dos. Preservação de documentos arquivísticos digitais. **Ciência da Informação**, Brasília, DF, v. 41, n. 1, p. 114-126, jan./abr., 2012. Disponível em: <http://revista.ibict.br/ciinf/article/viewFile/1357/1536>. Acesso em: 02 nov. 2016.

SARACEVIC, T. Ciência da Informação: origem, evolução e relações. **Perspectivas em Ciência da Informação**, v. 1, n. 1, p. 41-62, jan./jun., 1996. Disponível em: <http:// http://portaldeperiodicos.eci.ufmg.br/index.php/pci/article/view/235>. Acesso em: 02 mar. 2014.

SILVA, Armando Malheiro da. A gestão da Informação na perspectiva da pesquisa em ciência da informação: retorno a um tema estratégico. In: ALMEIDA F. A. S. et al. (Org.). **Governança, estratégia, redes de negócios e meio ambiente, Coleção Luso brasileira**. Anápolis: Universidade estadual de Goiás, 2009. cap. 15. p. 232-252.

SILVA, Armando Malheiro da. **A Informação**: da compreensão do fenómeno e construção do objeto científico. Porto: Cetac.media/Edições Afrontamento, 2006.

SILVA, Armando Malheiro da. **Informação e comunicação como projecto epistemológico em Portugal e no Brasil**. In DUARTE, Zeny; FARIAS, Lúcio (org.). A Medicina na Era da Informação. Bahia: EUFBA, 2009. p. 27-56.

SILVA, Armando Malheiro da. Modelos e modelizações em Ciência da Informação: o modelo eLit.pt e a investigação em literacia informacional. **Prisma.com**, Porto, n.13, p. 01-56, 2010. Disponível em: <http://revistas.ua.pt/index.php/prismacom/article/view/785/710>. Acesso em: 11 nov. 2017.

SILVA, Armando Malheiro da. O Método Quadripolar e a Pesquisa em Ciência da Informação. **Prisma.com**, Porto, n. 26, p. 27-44, 2014. Disponível em: <http://revistas.ua.pt/index.php/prismacom/article/view/3097>. Acesso em: 23 abr. 2017.

SILVA, A. M. da; RAMOS, F. As ciências da comunicação e da informação: casos e desafios de uma interdisciplina. In: PASSARELLI, B.; SILVA, A. M. da; RAMOS, F. (Org.). **e-Infocomunicação**: estratégias e aplicações. São Paulo: Editora Senac, 2014. p. 49-79.

SILVA, A. M. da; RIBEIRO, F. **A gestão da informação na administração pública**. Interface, Lisboa, v. 50, n. 161, p. 32-39, nov. 2009.

SILVA, A. M. da; RIBEIRO, F. **Das “ciências” documentais à ciência da informação**: ensaio epistemológico para um novo modelo curricular. Porto: Edições Afrontamento, 2002.

SILVA, Gleiciane Rosa da. **Gestão da informação para a tomada de decisão em uma instituição de ensino superior privada**: a experiência da Faculdades Integradas da União Educacional do Planalto Central (FACIPLAC/DF). 2016. 201 f., il. Dissertação (Mestrado em Ciência da Informação)—Universidade de Brasília, Brasília, 2016.

SILVA, Sérgio C. da Albite. A preservação da informação arquivística governamental nas políticas públicas do Brasil. Rio de Janeiro: AAB/FAPERJ, 2008.

SILVA JÚNIOR, Laerte Pereira da. **Os Repositórios Institucionais das Universidades Federais do Brasil:** Um Modelo de Política de Preservação Digital. 2017. 190 f. : il. Tese (Doutoramento em Informação e Comunicação em Plataformas Digitais) – Universidade do Porto, 2017. Disponível em: <https://repositorio-aberto.up.pt/bitstream/10216/105842/2/202343.pdf>. Acesso em: 21 out. 2018.

SOCIETY OF AMERICAN ARCHIVISTS (SAA). **A Glossary of Archival and Records Terminology**. 2005. Disponível em: <http://files.archivists.org/pubs/free/SAA-Glossary-2005.pdf>. Acesso em: 29 ago. 2016.

SPOLIDORO, R. The Paradigm Transition Theory: A Tool for Guiding Technopolitan Transformations, *in* **Delivering Innovation: Key lessons from the World-Wide Network of Science Parks**. FORMICA, P.; TAYLOR, D. (Eds.), Malaga: International Association of Science Parks - IASP, 1998.

SPOLIDORO, R. The Paradigm Transition Theory. **Proceedings of the 5th World Conference on Science Parks**, International Association of Science Parks - IASP; Association of University Related Research Parks – AURP; Brazilian Association of Science Parks and Business Incubators – ANPROTEC, Rio de Janeiro, Brazil, 1996.

TARAPANOFF, Kira. Inteligência, informação e conhecimento em corporações: Relações e Complementariedade. In: TARAPANOFF, Kira (Org.). **Inteligência, informação e conhecimento em corporações**. Brasília: IBICT, UNESCO, 2006. p. 19-36.

TARAPANOFF, Kira. O contexto da mudança. In: TARAPANOFF, Kira (Org.). **Inteligência Organizacional e competitiva.** Brasília: UnB, 2001. p. 51-58.

TAVARES, Maria de Fátima D. Preservação digital: entre a memória e a história. **Ciência da Informação,** Brasília, 2012. v. 41, n. 1, p. 9-21.

TOFFLER, Alvin. **A terceira onda**. 8.ed. Rio de Janeiro: Record, 1980.

UHLIR, Paul F. **Diretrizes políticas para o desenvolvimento e promoção da informação governamental de domínio público**. Brasília: UNESCO, 2006. Disponível em: <http://unesdoc.unesco.org/images/0013/001373/137363por.pdf>. Acesso em: 05 nov. 2016.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS PARA A EDUCAÇÃO, A CIÊNCIA E A CULTURA (UNESCO). **Missões UNESCO.** 2010. Disponível em: <http://unesdoc.unesco.org/images/0018/001887/188700por.pdf>. Acesso em: 05 nov. 2016.

VERGARA, Sylvia C. **Projetos e relatórios de pesquisa em administração**. 2. ed., São Paulo: Atlas, 1998.

VIANNA, Eduardo Wallier. **Análise do comportamento informacional na gestão da segurança cibernética da Administração Pública Federal**. 2015. 115 f., il. Dissertação (Mestrado em Ciência da Informação) - Universidade de Brasília, Brasília, 2015. Disponível em: <http://repositorio.unb.br/handle/10482/17832>. Acesso em: 08 set. 2015.

VIANNA, Eduardo Wallier. A Segurança Cibernética na Conferência das Nações Unidas para o Desenvolvimento Sustentável. In: NAKAIAMA M. K. et al. (Org.). **Ciência, tecnologia e inovação**: pontes para a segurança pública. Florianópolis: FUNJAB, 2013. cap. 5. p. 127-156.

VIANNA, Eduardo Wallier. Governo eletrônico e a segurança da Informação. **Boletim Eletrônico da Organização dos Estados Americanos - OEA** [ Entrevista]. Washington, 2010. Disponível em: <http://www.ctir.gov.br/arquivos/entrevistas/entrevista-OEA-2010.pdf>. Acesso em: 05 nov. 2016.

VIANNA, Eduardo Wallier. **Procedimentos para a gestão de incidentes de segurança nas redes de computadores da Administração Pública Federal**. Monografia (Especialização em gestão de Segurança da Informação e Comunicações) - Universidade de Brasília, Brasília, 2011. Disponível em: <http://dsic.planalto.gov.br/documentos/cegsic/monografias_2009_2011/16_Eduardo_Wallier.pdf>. Acesso em: 29 jan. 2017

VIANNA, Eduardo Wallier; DE SOUSA, Renato Tarciso Barbosa. A Proteção da informação em ambientes digitais: tendências e perspectivas. In: Encontro nacional de pesquisa em ciência da informação, 19 (XIX ENANCIB) – Sujeito informacional e as perspectivas atuais em Ciência da Informação **[Anais].** Londrina: Associação Nacional de Pesquisa e Pós-Graduação em Ciência da Informação e Biblioteconomia, 2018.

Disponível em: <enancib.marilia.unesp.br/index.php/XIXENANCIB/xixenancib/paper/view/947>. Acesso em: 02 nov. 2018.

VIANNA, Eduardo Wallier; DE SOUSA, Renato Tarciso Barbosa. Ciber Proteção: a segurança dos sistemas de informação no espaço cibernético. **Revista Ibero-Americana de Ciência da Informação,** [S.l.], v. 10, n. 1, p. 110-131, abr. 2017. ISSN 1983-5213. Disponível em: <http://periodicos.unb.br/index.php/RICI/article/view/19019/18072>. Acesso em: 11 maio 2017.

VIANNA, Eduardo Wallier; IZYCKI, Eduardo Arthur. **Guerra Cibernética:** ameaça real à soberania nacional. Revista da Escola Superior de Guerra. v. 33, n. 64. Rio de Janeiro: ESG, 2018 (em fase de publicação).

VIANNA, Eduardo Wallier; FERNANDES, Jorge Henrique Cabral. O gestor da segurança da informação no espaço cibernético governamental: grandes desafios, novos perfis e procedimentos. **Brazilian Journal of Information Science: research trends,** v. 9, n. 1, p. 01-28, 2015. Disponível em: <http://www2.marilia.unesp.br/revistas/index.php/bjis/article/view/5216/3668. Acesso em: 08 set. 2015.

WIENER, Norbert. **Cibernética e a sociedade**: o uso humano dos seres humanos. 2.ed., São Paulo: Cultrix, 1968.

WIENER, Norbert. **Cybernetics. – 2nd Edition**: or the control and Communication in the animal and the machine. USA: MIT Press. 1995.

WORLD CONGRESS ON INFORMATION TECHNOLOGY (WCIT 2016). **[Anais]**. Brasília, 2016. Disponível em: <http://www.wcit2016.com/home/>. Acesso em: 18 out. 2016.

WORLD ECONOMIC FORUM (WEF). **Report of WEF/2015**, 2015. Disponível em: <http://reports.weforum.org/global-risks-2015/>. Acesso em: 18 out. 2016.

WORLD ECONOMIC FORUM (WEF). **Report of WEF/2016**, 2016. Disponível em: <http://reports.weforum.org/global-risks-2016/>. Acesso em: 18 out. 2016.

WORLD ECONOMIC FORUM (WEF). **Report of WEF/2017**, 2017. Disponível em: <http://www3.weforum.org/docs/GRR17_Report_web.pdf>. Acesso em: 14 nov. 2017.

WORLD ECONOMIC FORUM (WEF). **Report of WEF/2018**, 2018. Disponível em: <http://www3.weforum.org/docs/GRR18_Report.pdf>. Acesso em: 26 set. 2018.

ZINS, Chaim. Knowledge map of information science: Research Articles**. Journal of the American Society for Information Science and Technology**, n. 58, v.4, p. 526-535, 2007.

# APÊNDICE A - Levantamento de Requisitos

| ITEM | DESCRIÇÃO |
|---|---|
| **Contexto da Pesquisa** | **TEMA** - A proteção da informação no ciberespaço de interesse nacional<br>**PROBLEMA** - Quais seriam as maneiras mais efetivas de reduzir as vulnerabilidades e mitigar as ameaças aos recursos informacionais em ambiente digital e globalmente interconectado, indissociáveis ao desenvolvimento da sociedade e à sobrevivência de um Estado-Nação? |
| **Finalidade** | Levantar novos aspectos e conjunturas sobre os assuntos e atividades contemplados pela segurança da informação em meio digital no contexto internacional (Comunidade Europeia), de forma a aprofundar as percepções do investigador sobre a situação atual da segurança da informação no ciberespaço (OE1), bem como sobre o gerenciamento da informação no desenvolvimento das atividades relativas à proteção da informação abrangendo a segurança e a defesa cibernéticas (OE2). |
| **Entrevistados** | Sete especialistas em atividade nos ambientes de domínio científico (acadêmico), governamental e empresarial, ou seja, em consonância com a abordagem conhecida como Hélice Tríplice, bem como integrantes de órgãos e entidades relacionados diretamente com a Ciber Proteção. |
| **Tipo da entrevista** | Semiestruturada, por pautas, por meio de perguntas com resposta aberta |
| **Prazo** | Realização junho/julho de 2017 |
| **Condições de execução** | Presencial, via *Web*, gravação de áudio ou textual |
| **Aspectos de compilação de dados** | Análise de Conteúdo de forma que uso da inferência possibilitasse informações complementares, extrapolando a simples leitura das entrevistas, a partir dos próprios entrevistados e da situação na qual eles se encontravam, particularmente no contexto da Ciber Proteção.<br>Enunciação - onde cada entrevista (semiestruturada) é estudada em si mesma como uma totalidade organizada, centrada na singularidade da elaboração individual. |
| **Ambientação e execução** | - Após saudação inicial, solicitar autorização para utilização na Tese, a fim de melhor proceder à coleta e à análise das informações prestadas.<br>- Apresentação pessoal e agradecimento pela participação<br>- A pesquisa em desenvolvimento, sob o título: Segurança da Informação Digital: proposta de Modelo para a Ciber Proteção governamental, trata da proteção da informação no ciberespaço. |
| **Perguntas** | **01** - Como percebe a segurança da informação em meio digital? Quais as principais ameaças e vulnerabilidades?<br>**02** – Considera o ciberespaço como instrumento (seguro) de desenvolvimento nacional e da sociedade?<br>**03** – Há (ou deveria haver) diferenças/peculiaridades em relação à gestão da informação (produção, armazenamento e compartilhamento/comunicação da informação) nas organizações/estruturas relacionadas à segurança e à defesa cibernética, considerando-se, também e por ocasião do tratamento/resposta aos incidentes?<br>**04** – Como deveria ser a capacitação técnico–operacional dos colaboradores e atores envolvidos?<br>**05** – Em face dos futuros cenários e tendências, quais seriam as oportunidades de melhoria e/ou projetos a desenvolver? |

# APÊNDICE B - Entrevista Administração Pública Federal

| ITEM | DESCRIÇÃO |
|---|---|
| **Contexto da Pesquisa** | **TEMA** - A proteção da informação no ciberespaço de interesse nacional<br>**PROBLEMA** - Quais seriam as maneiras mais efetivas de reduzir as vulnerabilidades e mitigar as ameaças aos recursos informacionais em ambiente digital e globalmente interconectado, indissociáveis ao desenvolvimento da sociedade e à sobrevivência de um Estado-Nação<br>**QUESTÃO CENTRAL** - Como estão gerenciadas as informações nas estruturas institucionais envolvidas diretamente com a proteção do espaço cibernético de interesse nacional? |
| **Finalidade** | Coletar e analisar qualitativamente o conhecimento adquirido pelos entrevistados no planejamento, na execução e na normatização (gestão) das atividades relacionadas à proteção da informação em meio digital (particularmente, preservação digital, segurança e defesa cibernéticas), bem como levantar requisitos/validar o Modelo de Ciber Proteção proposto |
| **Entrevistados** | Dez Integrantes de órgãos e entidades relacionados diretamente com a Ciber Proteção nacional |
| **Tipo** | Semiestruturada, por pautas, por meio de perguntas com resposta aberta |
| **Prazo** | Realização de outubro 2017 até março de 2018 |
| **Condições de execução** | Presencial ou por videoconferência, com gravação de áudio (após consentimento) e duração de 50 a 60 minutos |
| **Aspectos de compilação de dados** | - Análise da Conteúdo/Enunciação, onde cada entrevista (semiestruturada) é estudada em si mesma como uma totalidade organizada, centrada na singularidade da elaboração individual<br>- As informações obtidas com as entrevistas foram transcritas pelo pesquisador e analisadas conforme método de 'condensação dos significados', sugerido por Kvale (1996), onde aquilo que é dito pelo entrevistado é resumido em formulações mais breves e sucintas para que, posteriormente, possa ser feita a identificação dos significados das respostas<br>- Mineração de texto por meio da ferramenta Sobek, que possibilita visualizar um diagrama conciso, com os principais termos e as relações de um texto<br>- Análise comparativa por intermédio de tabelas, que possibilitaram buscar diferenças e encontrar associações entre as respostas dos entrevistados, inseridas de forma resumida nas células |
| **Ambientação e execução** | - Após saudação inicial, solicitar autorização para gravar (áudio), a fim de melhor proceder à coleta e à análise das informações prestadas. Vamos começar<br>- Apresentação pessoal e agradecimento pela participação<br>- A pesquisa em desenvolvimento, sob o título: Segurança da Informação Digital: proposta de Modelo para a Ciber Proteção governamental, trata da proteção da informação no ciberespaço. Apresentar (sfc) o conceito de Ciber Proteção (bússola) e a versão preliminar do mapa mental do Modelo<br>- A entrevista está dividida em dois blocos:<br>1º Bloco: ciberespaço<br>2º Bloco: Gestão da informação<br>3º Bloco: Ciber Proteção<br>- Iniciar com o Roteiro |

| ROTEIRO | |
|---|---|
| **Objetivo Específicos (OE)** | **Bloco - 1 Ciberespaço (Questões)** |
| OE1<br><br>OE 1 e OE 3 | **Q1**- Em relação à proteção da informação no ciberespaço, quais seriam os principais desafios?<br>**Q2**- Como interpreta a percepção/atuação dos governos brasileiros (última década), em face da utilização do espaço cibernético no desenvolvimento nacional e da sociedade? |
| | **Bloco 2 - Gestão da informação** (produção, armazenamento, uso) |
| OE 3<br><br>OE 3 | **Q3**- Na sua opinião quais seriam as características/requisitos para a gestão 'segura' da informação em meio digital em uma estrutura ligada à proteção cibernética?<br>**Q4**- No contexto da proteção cibernética, como considera a gestão da informação, quando há participação de diversos atores governamentais e da sociedade civil, envolvendo uma gama de estruturas heterogêneas públicas e privadas? Considere três fases: pré-evento/planejamento, durante/ em operação e posterior/lições aprendidas. (P.ex.: Grandes Eventos) |
| | **Bloco 3: Ciber Proteção – modelo** |
| OE 3 e OE 4<br><br>OE 4<br><br>OE 4<br><br>OE 4 | **Q5**- As soluções governamentais adotadas, particularmente as políticas/regulatórias, para a consciência situacional inerentes à Ciber Proteção têm apresentado resultado satisfatório?<br>**Q6**- Quais seriam os pontos-chave ou requisitos imprescindíveis para otimizar a Ciber Proteção no Brasil/APF?<br>**Q7**- Acredita ser viável a criação de uma entidade articuladora e normativa, em âmbito nacional, voltada para a salvaguarda do ciberespaço nacional (proteção/defesa/segurança cibernéticas)?<br>**Q8**- Já possuímos/demonstramos competências (em pessoal, SW/HW e pesquisa /inovação) cibernéticas representativas no contexto nacional/internacional? O que falta? Como otimizar? Um centro aglutinador baseado o padrão triplo hélice contribuiria? |

Estrutura do correio eletrônico de apresentação, ratificando o convite para participar da entrevista:

Prezado senhor, bom dia!

Conforme nosso último contato, gostaria de confirmar sua participação como entrevistado na minha Tese sobre **a proteção da informação no ciberespaço de interesse nacional.**

Como comentado, curso doutorado em Ciência da Informação na UnB, orientado pelo Prof. Doutor Renato Tarciso Barbosa de Sousa, tendo como objetivo coletar e analisar qualitativamente o conhecimento adquirido pelos entrevistados no planejamento, na execução e na normatização (gestão) das atividades relacionadas à proteção da informação em meio digital (particularmente, preservação digital, segurança e defesa cibernéticas), bem como validar (ampliar requisitos) o Modelo de Ciber Proteção proposto.

Como ponto de partida para o referido Modelo (e pedra angular da Tese), destaco o desenvolvimento, em 2016, do conceito de **Ciber Proteção**, disponível em <http://periodicos.unb.br/index.php/RICI/article/view/19019/18072>.

A entrevista está dividida em três blocos, com duração estimada de 60 minutos:

a) proteção da informação no ciberespaço;

b) situação da gestão da informação nos órgãos e entidades relacionados diretamente com a Ciber Proteção nacional;

c) requisitos para um modelo de gestão segura da informação nos órgãos e entidades da APF.

O resultado e a qualidade do trabalho dependem diretamente das respostas obtidas, dessa forma agradeço antecipadamente sua colaboração.

Poderíamos agendar para esta semana?

Atenciosamente,
Eduardo Wallier Vianna
Celular: 5561991583361
e-mail alternativo: eduardowallier@gmail.com